SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Jure Marinov

OKVIR ZA PHISHING KAMPANJE: INTEGRACIJA OSINT-A I AUTOMATIZIRANE SIMULACIJE NAPADA ZA POTREBE RED TEAMINGA I EDUKACIJE

DIPLOMSKI RAD

Varaždin, 2025.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Jure Marinov

Matični broj: 35918/07–R

Studij: Organizacija poslovnih sustava

OKVIR ZA PHISHING KAMPANJE: INTEGRACIJA OSINT-A I AUTOMATIZIRANE SIMULACIJE NAPADA ZA POTREBE RED TEAMINGA I EDUKACIJE

DIPLOMSKI RAD

Mentor/Mentorica:

Izv. prof. dr. sc. Igor Tomičić

Varaždin, prosinac 2025.

Jure Marinov

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Ovaj diplomski rad bavi se razvojem i analizom okvira za provođenje phishing kampanja koji integrira OSINT (Open Source Intelligence) metode s automatiziranom simulacijom napada u svrhu red teaminga i edukacije. Cilj rada je prikazati kako se javno dostupni podaci mogu sustavno prikupljati, analizirati i koristiti za izradu realističnih, ali kontroliranih phishing scenarija koji služe za procjenu sigurnosne svijesti i otpornosti organizacija.

Teorijsko-metodološko polazište rada temelji se na konceptima informacijske sigurnosti, društvenog inženjeringa, OSINT analitike te red team pristupa sigurnosnom testiranju. U praktičnom dijelu rada razvijena je modularna JESHKA koja omogućuje automatizirano prikupljanje podataka iz različitih izvora, obradu i pohranu prikupljenih informacija, generiranje phishing infrastrukture te simulaciju napada u kontroliranom okruženju. Sustav je implementiran kao lokalna web aplikacija s naglaskom na fleksibilnost, automatizaciju i sigurnost.

Rezultati rada pokazuju da integracija OSINT-a i automatizirane infrastrukture značajno povećava realističnost phishing simulacija te omogućuje učinkovitije testiranje ljudskog faktora u informacijskim sustavima. Zaključno, predloženi okvir može se koristiti kao alat za edukaciju, sigurnosne provjere i podizanje razine svijesti o prijetnjama društvenog inženjeringa.

Ključne riječi: OSINT; phishing; društveni inženjering; informacijska sigurnost; red teaming; automatizacija; simulacija napada

Sadržaj

1. Uvod

1.1. Kontekst cyber sigurnosti danas

Digitalna transformacija snažno je promijenila način na koji organizacije u Hrvatskoj posluju, komuniciraju i upravljaju podacima. Povećana ovisnost o digitalnim servisima, računalnim mrežama i online transakcijama istovremeno je dovela do dramatičnog rasta izloženosti kibernetičkim prijetnjama. Trendove potvrđuje više domaćih i međunarodnih izvora, a posebno ističu rast phishinga, socijalnog inženjeringa te kompromitacije korisničkih računa.

Prema analizi Poslovnog dnevnika, kibernetički kriminal u Republici Hrvatskoj udvostručio se u posljednjih pet godina, što ukazuje na ubrzani rast aktivnosti napadača i sve veću učestalost napada na tvrtke, institucije i građane [1]. U članku se navodi da su najčešće prijetnje upravo one usmjerene na krađu podataka i financijskih sredstava, pri čemu phishing i socijalni inženjering igraju ključnu ulogu.

Sigurnosno-obavještajna agencija (SOA) dodatno potvrđuje ove trendove. U svom izvješću o kibernetičkoj sigurnosti u 2025. godini, SOA ističe da je Republika Hrvatska ostvarila napredak u području digitalne otpornosti, ali unatoč tome, phishing i ciljane socijalno-inženjerske kampanje ostaju među najdominantnijim prijetnjama poslovnom i javnom sektoru [2]. SOA naglašava da se napadači sve više oslanjaju na iskorištavanje javno dostupnih podataka, kao i na emocionalnu manipulaciju korisnika, čime postižu visoku stopu uspješnosti napada.

Stručna analiza tvrtke Wahl također upozorava na složenost provedbe mjera kibernetičke sigurnosti u Hrvatskoj. Prema njihovom istraživanju, unatoč sve većoj svijesti i implementaciji sigurnosnih standarda, phishing ostaje jedna od najraširenijih prijetnji, a veliki dio napada uključuje krađu vjerodajnica putem e-maila i kompromitaciju poslovnih sustava [3]. U izvješću se ističe da organizacije često zanemaruju važnost redovitog praćenja sigurnosnih prijetnji te educiranja zaposlenika, što dodatno povećava ranjivost.

Medijski izvori također bilježe iste obrasce. Tportal u analizi stanja kibernetičke sigurnosti u Hrvatskoj navodi kako svijest o sigurnosnim rizicima raste, ali da stručnjaka i ulaganja još uvijek nedostaje. Posebno se ističe da su najčešći napadi oni koji ciljaju korisničke račune, najčešće putem phishinga i krađe lozinki [4]. To potvrđuje da je ljudski faktor i dalje ključna slabost organizacija, unatoč sve boljoj tehničkoj opremi i alatima za nadzor.

Najopsežniji pregled sigurnosnih incidenata dolazi od Nacionalnog CERT-a. U svojim mjesečnim i godišnjim izvješćima redovito evidentiraju ogromnu količinu phishing kampanja,

lažnih e-mail poruka, lažnih SMS-ova, kloniranih web stranica i drugih oblika pokušaja kompromitacije korisnika. Primjerice, u nizu publikacija CERT-a - uključujući ožujak 2025., svibanj 2025., listopad 2025. i druge - zabilježeni su deseci upozorenja o phishing kampanjama koje ciljaju hrvatske korisnike [5], [6], [7], [8], [9]. CERT posebno naglašava da se kampanje često predstavljaju kao:

- banke (OTP, PBZ, ZABA)
- dostavne službe (HP, GLS, DHL)
- telekom operatori (A1, HT, Telemach)
- državne institucije (Porezna uprava, e-Građani)

Osim toga, CERT upozorava da kriminalci sve češće iskorištavaju javno dostupne podatke korisnika, kao i njihove emocije - strah, hitnost, autoritet - kako bi povećali vjerojatnost klika, što je jasno opisano i u kampanji ECSM 2025 [10].

O ozbiljnosti situacije govori i podatak s portala Bug.hr, gdje se izvještava da Nacionalni CERT navodi kako je phishing i dalje najraširenij oblik kibernetičkog napada u Hrvatskoj, često zastupljeniji od svih ostalih incidenata zajedno [13]. Time se potvrđuje da phishing ostaje temeljna prijetnja za hrvatski digitalni prostor, unatoč svim mjerama prevencije.

Nadalje, međunarodni izvor INSECM pruža dodatni kontekst. U članku iz 2024. godine opisuje se kako su phishing, smishing i vishing globalno u porastu te da napadači koriste kombinaciju psihologije, tehničke manipulacije i lažnog predstavljanja kako bi prevarili korisnike [12]. Ovo se savršeno uklapa u obrasce koji su primijećeni i na hrvatskom području.

Šira akademska analiza iz regije također potvrđuje ozbiljnost problema kibernetičkog kriminala. Prema istraživanju Miletića, nezakonite aktivnosti u cyber prostoru rastu paralelno s razvojem interneta, a socijalni inženjering smatra se jednom od ključnih metoda napada jer ne cilja sustav već čovjeka [11]. Zbog toga napadi koji koriste OSINT i socijalnu manipulaciju imaju veliku stopu uspješnosti.

Sve ove činjenice jasno ukazuju da je kombinacija tehničkih napada i socijalnog inženjeringa dominantna prijetnja za organizacije u Hrvatskoj. Phishing ostaje najčešća metoda početnog kompromitiranja, a napadači sve češće koriste javno dostupne informacije (OSINT) kako bi personalizirali napade, povećali uvjerljivost poruka i prevarili korisnike. Stoga su preventivne mjere, edukacija i simulacije napada ključne za povećanje otpornosti digitalnog ekosustava.

1.2. Zašto su OSINT + phishing danas glavni napadi

OSINT i phishing danas predstavljaju najraširenију kombinaciju alata i tehnika koje napadači koriste za početnu kompromitaciju korisnika i organizacija. Razlog tome leži u spoju jednostavne izvedbe, niskog troška te izrazito visoke učinkovitosti. Prema Nacionalnom CERT-u, phishing je i dalje jedan od najčešćih oblika kibernetičkih napada u Hrvatskoj, a napadači ga koriste kako bi žrtve navele na otkrivanje osobnih podataka, vjerodajnica ili financijskih informacija [14]. CERT-HR naglašava da su e-mail poruke koje oponašaju banke, dostavne službe, teleoperatere ili državne institucije najčešći oblik prijevare, te da se napadi kontinuirano prilagođavaju kako bi izgledali uvjerljivije.

Upravo ovdje dolazi do izražaja OSINT - tehnike prikupljanja javno dostupnih informacija. Prema Sigurnosno-obavještajnoj agenciji Republike Hrvatske (SOA), napadači sve češće koriste podatke s društvenih mreža, poslovnih registara, internetskih stranica organizacija i drugih javnih izvora kako bi kreirali visokoprecizne i ciljane phishing kampanje [2]. S obzirom na to da većina korisnika ostavlja veliki digitalni trag, napadači mogu relativno jednostavno otkriti poslovnu hijerarhiju, kontakte, radne pozicije i navike pojedinaca. Time se phishing poruke mogu personalizirati do razine koja uvjerljivo imitira legitimnu poslovnu komunikaciju.

Međunarodni izvori potvrđuju iste trendove. Prema INSECM analizi, kombinacija phishinga, smishinga i vishinga i dalje je među najuspješnijim metodama socijalnog inženjeringa, upravo zato što napadi ciljaju ljudsku psihologiju, a ne tehničke ranjivosti sustava [12]. Napadači iskorištavaju emocije poput straha, hitnosti ili autoriteta i oblikuju poruke tako da žrtva što brže reagira, često bez razmišljanja. Kada se takve tehnike kombiniraju s OSINT-om, stopa uspješnosti napada značajno raste jer korisnici prepoznaju elemente koji im djeluju poznato ili legitimno.

Dodatni problem je nedostatak stručnjaka i sigurnosnih kapaciteta. Prema Tportalu, iako svijest o kibernetičkim prijetnjama u Hrvatskoj raste, organizacijama i dalje nedostaje dovoljno educiranih ljudi i sustava koji mogu pravovremeno prepoznati pokušaje prijevara [4]. Upravo zbog toga phishing kampanje često prolaze nezapaženo, dok OSINT informacijama obogaćeni napadi uspješno zaobilaze tehničke zaštite i ciljaju krajnjeg korisnika kao najslabiju kariku.

Kombinacija OSINT metoda i phishing napada stoga postaje dominantan oblik cyber prijetnje, jer omogućuje napadačima da uz minimalne resurse kreiraju uvjerljive, personalizirane i učinkovite napade. Organizacije su stoga primorane ulagati u edukaciju korisnika, sustave detekcije i simulacije phishing napada koje integriraju OSINT, kako bi povećale otpornost na socijalno-inženjerske prijetnje.

2. Metode i tehnike rada

Metode i tehnike primijenjene u ovom radu temelje se na izgradnji simulacijskog sustava koji povezuje OSINT pristup i automatizirane phishing kampanje u kontroliranom okruženju. Sustav je dizajniran s jasnim ograničenjima kako bi se spriječila bilo kakva stvarna šteta ili zlouporaba, pri čemu ni u jednom trenutku nije provedeno slanje phishing poruka stvarnim osobama ili organizacijama.

Proces započinje OSINT prikupljanjem informacija, pri čemu se koriste javno dostupni podaci, prvenstveno nazivi organizacija i opće informacije prikupljene tijekom web scrapinga. Prikupljeni podaci koriste se isključivo za demonstraciju tehničkih mogućnosti sustava, analizu strukture informacija i izgradnju modela personalizacije. Sustav ne prikuplja osjetljive osobne podatke niti se takvi podaci koriste u daljnjim fazama rada. Prikupljene informacije pohranjuju se u lokalnu bazu podataka, gdje se obrađuju radi prepoznavanja obrazaca i simulacije organizacijskih struktura.

Generiranje phishing predložaka i personaliziranih poruka provodi se pomoću modela za generiranje teksta. Aplikacijski backend izvodi se lokalno i služi za integraciju OSINT modula, obradu prikupljenih podataka i generiranje phishing poruka. Iako sustav tehnički omogućuje izradu i personalizaciju e-mail sadržaja, poruke se ne šalju stvarnim primateljima, već se koriste isključivo u svrhu testiranja i evaluacije generiranog sadržaja.

Za simulaciju e-mail infrastrukture korišten je vanjski servis s podrškom za testne adrese i sandbox način rada. Mehanizmi praćenja korišteni su za bilježenje simuliranih događaja, poput otvaranja poruka i klikova na linkove, bez uključivanja stvarnih korisnika. Svi URL-ovi u porukama zamjenjuju se tracking poveznicama kako bi se omogućila analiza ponašanja unutar simulacijskog okruženja.

Jedini dio sustava koji se ne izvršava lokalno jest hostanje phishing landing stranica i endpointa za praćenje, koji su postavljeni na izdvojenoj serverskoj infrastrukturi. Ta infrastruktura koristi se isključivo za prikaz simuliranih phishing stranica i prihvat testnih interakcija. Na njoj se ne provodi scraping, ne obrađuju se osjetljivi podaci i ne prikupljaju se stvarne informacije o korisnicima ili organizacijama.

Testiranje sustava provedeno je analizom funkcionalnosti OSINT modula, generiranja phishing poruka i sustava za praćenje. Evaluirane metrike uključivale su tehničku ispravnost generiranih poruka, funkcioniranje mehanizama praćenja te mogućnost povezivanja prikupljenih OSINT podataka s personalizacijom sadržaja. Budući da sustav nije korišten za stvarno ciljanje korisnika niti za slanje poruka stvarnim primateljima, rad ne predstavlja

sigurnosni, pravni niti etički rizik, već služi isključivo kao istraživački i edukativni prikaz suvremenih napadačkih tehnika.

3. Teorijska osnova OSINT-a

3.1. Definicija OSINT-a

Open-Source Intelligence (OSINT) definira se kao proces sustavnog prikupljanja, analize i interpretacije informacija koje su javno dostupne te ne zahtijevaju poseban ili ograničen pristup. OSINT obuhvaća informacije iz različitih izvora, uključujući medijske objave, javne registre, akademske dokumente, internetske portale, društvene mreže, forume, metapodatke digitalnih datoteka i druge otvorene platforme. Ključna posebnost OSINT-a jest da se oslanja isključivo na podatke koji su legalno dostupni i namijenjeni javnosti, zbog čega se značajno razlikuje od tradicionalnih obavještajnih metoda koje koriste povjerljive ili tajne izvore.

Prema Miletiću, digitalno okruženje omogućilo je nagli rast količine javno dostupnih podataka, što je rezultiralo time da OSINT postane jedan od temeljnih alata u analizi cyber kriminalnih aktivnosti i sigurnosnih trendova [11]. Kako ističe Sigurnosno-obavještajna agencija Republike Hrvatske (SOA), sve veći broj informacija postaje dostupno putem digitalnih servisa, društvenih mreža i komunikacijskih platformi, a upravo taj digitalni trag pojedinaca i organizacija omogućuje izgradnju detaljnih profila i identifikaciju potencijalnih ranjivosti [2].

U području kibernetičke sigurnosti, OSINT predstavlja ključan element u razumijevanju sigurnosne izloženosti korisnika. Napadači često koriste javno dostupne podatke kako bi identificirali osobe, njihove položaje, navike, kontakte i ponašanje na mreži, što im omogućuje stvaranje personaliziranih socijalno-inženjerskih napada. INSECM posebno naglašava kako kombinacija javno dostupnih informacija i psihološki usmjerenih manipulativnih tehnika značajno povećava učinkovitost phishinga, smishinga i drugih oblika prijevara [12]. Time OSINT postaje polazišna točka za napade temeljene na socijalnom inženjeringu.

OSINT se ne sastoji samo od tehničkih informacija. Velik dio obavještajnih podataka odnosi se na socijalni, komunikacijski i profesionalni kontekst korisnika. Tportal u analizi stanja kibernetičke sigurnosti u Hrvatskoj navodi da su upravo osobni podaci, profesionalni profili i informacije objavljene na mreži često iskorišteni za kreiranje uvjerljivih phishing napada [4]. S obzirom na to da korisnici često nesvjesno dijele podatke na internetu, OSINT omogućuje napadačima relativno jednostavno prikupljanje informacija potrebnih za izgradnju ciljanih napada.

Kombinirajući sve navedeno, OSINT se može definirati kao strukturirani proces prikupljanja i analize javno dostupnih informacija s ciljem izgradnje korisnog obavještajnog

znanja. U kontekstu kibernetičke sigurnosti i simuliranih phishing kampanja, njegova uloga je dvostruka: obrambeni timovi koriste OSINT kako bi identificirali izloženost i ranjivosti, dok napadači koriste iste podatke za precizno ciljanje i personalizaciju napada. CERT-HR u svojim publikacijama naglašava da napadači sve češće koriste upravo te javno dostupne informacije kako bi povećali vjerodostojnost svojih phishing poruka i privukli korisnike na interakciju [14].

Zbog toga OSINT danas predstavlja temeljnu komponentu u analizi sigurnosnih rizika, pripremi edukacijskih simulacija i razumijevanju načina na koji digitalni tragovi mogu postati vektor napada. U eri sve veće digitalne izloženosti, sposobnost upravljanja i razumijevanja OSINT-a postaje ključna za sigurnost svih organizacija i pojedinaca.

3.2. Povijest OSINT-a

Povijest OSINT-a seže mnogo dalje od današnjeg digitalnog okruženja i obuhvaća razvoj kroz nekoliko faza koje su oblikovale njegovu današnju ulogu u kibernetičkoj sigurnosti. Prema dokumentaciji Fakulteta organizacije i informatike (FOI), OSINT kao disciplina počinje se razvijati tijekom 20. stoljeća, kada su sigurnosne i vojne strukture počele sustavno koristiti javno dostupne informacije iz medija, novinskih članaka, emitiranih radijskih programa i drugih otvorenih komunikacijskih izvora [15]. U prvim desetljećima OSINT nije bio izdvojena disciplina, već dopunski mehanizam unutar šireg obavještajnog ciklusa.

Tijekom Drugog svjetskog rata započinje formalnije korištenje otvorenih izvora. Velike sile sustavno su analizirale objave u tisku, propagandne materijale, radio-poruke i druge javno dostupne informacije kako bi procijenile aktivnosti protivnika i pratile njihove političke, vojne i gospodarske namjere. FOI navodi kako su upravo te prakse položile temelj za kasniju standardizaciju OSINT metodologija [15].

Nakon rata, tijekom Hladnog rata, OSINT dobiva još veću ulogu zahvaljujući širenju masovnih medija i dostupnosti informacija iz različitih dijelova svijeta. Obavještajne službe počele su koristiti OSINT za praćenje javne komunikacije, političkih odnosa i međunarodnih kretanja. Prema FOI-jevim materijalima o sigurnosnim procesima, u tom se razdoblju OSINT integrirao u formalne obavještajne cikluse, iako je i dalje bio sporedan u odnosu na HUMINT i SIGINT [15].

Pravi procvat OSINT-a počinje krajem 20. stoljeća pojavom interneta, a posebno s masovnom digitalizacijom društva. Petr ističe da je internet omogućio pristup ogromnoj količini informacija u realnom vremenu, čime je OSINT transformiran iz sporog, ručnog procesa u brzu, automatiziranu obavještajnu disciplinu [16]. Razvojem web stranica, tražilica i prvih javnih baza

podataka nastao je suvremeni OSINT, a digitalni podaci postali su ključni izvor za sigurnosne analize.

Uslijed eksplozije društvenih mreža početkom 2000-ih godina OSINT prelazi u novu fazu. Prema Lupinom leksikonu, korisnici počinju svakodnevno ostavljati goleme količine osobnih, profesionalnih i vizualnih podataka, stvarajući digitalne tragove koji omogućuju izgradnju detaljnih profila pojedinaca i organizacija [17]. Ova transformacija otvorila je mogućnost prikupljanja informacija koje ranije nisu bile dostupne: stavova, navika, aktivnosti, radnih mjesta i osobnih veza.

U najnovijoj fazi OSINT postaje široko dostupna i komercijalna vještina. Eduza naglašava da OSINT više nije rezerviran samo za obavještajne službe, nego se smatra modernom digitalnom kompetencijom potrebnom stručnjacima iz poslovne analitike, sigurnosnih timova, menadžmenta, novinarstva i akademskog sektora [18]. Razvojem specijaliziranih alata, automatiziranih scraper sustava, API pretraga i analiza metapodataka, OSINT je postao temeljni element u procjeni sigurnosnih prijetnji, digitalnoj forenzici i detekciji ranjivosti.

Danas OSINT predstavlja spoj višedesetljetnog razvoja - od ručnog prikupljanja vijesti i radio-emitiranja do suvremenih sustava za automatizirano prikupljanje i analitiku velikih količina digitalnih podataka. Njegov razvoj jasno odražava evoluciju globalne komunikacije: što je više informacija javno dostupno, to OSINT postaje važniji u području kibernetičke sigurnosti, posebice kao temelj za razumijevanje digitalne izloženosti i pripremu simuliranih phishing kampanja.

3.3. OSINT ciklus

OSINT ciklus predstavlja strukturirani obavještajni proces koji omogućuje sustavno prikupljanje, obradu i pretvaranje javno dostupnih podataka u korisne informacije. Prema FOI-jevom sigurnosnom leksikonu, OSINT se temelji na standardiziranim fazama unutar obavještajnog ciklusa, pri čemu je važno jasno definirati potrebe, prikupljati relevantne informacije te ih analitički obraditi u svrhu donošenja informiranih odluka [15]. U stručnoj literaturi i praksi koristi se model s četiri osnovne faze: planiranje, prikupljanje, analiza i izvještavanje.

1) Planiranje

Planiranje predstavlja početnu fazu OSINT ciklusa i najvažniji je korak za uspješnost cijelog procesa. Cilj planiranja je definirati informacijske potrebe, opseg istraživanja te metode koje će se koristiti. Portal Interno ističe da je pravilno određivanje cilja nužno kako bi se izbjeglo prikupljanje prevelike količine nerelevantnih podataka i kako bi se proces usmjerio prema konkretnom sigurnosnom ili analitičkom problemu [19].

U ovoj fazi definira se:

- što se istražuje
- koji su izvori prioritet
- koje tehnike će se koristiti
- vremenska ograničenja
- potrebni resursi i alati

Planiranje uključuje i procjenu rizika, osobito u slučajevima kada se informacije prikupljaju o osjetljivim temama, kako navodi FPZG u materijalima o obavještajnoj analizi [24].

2) Prikupljanje podataka

Prikupljanje predstavlja najdinamičniju fazu OSINT ciklusa. U ovoj se fazi prikupljaju svi relevantni javno dostupni podaci iz različitih izvora - od web stranica i društvenih mreža do baza podataka, registara, foruma i medija.

Prema članku s Hrčka, koji analizira ulogu otvorenih izvora u poslovnoj inteligenciji, upravo prikupljanje podataka iz raznolikih izvora osigurava širinu i dubinu OSINT analize [20].

Prikupljanje uključuje:

- korištenje tražilica i naprednih operatora
- scraping javnih stranica
- praćenje društvenih mreža
- dohvat javnih registara
- analizu objavljenih dokumenata i metapodataka
- pasivno prikupljanje digitalnih tragova

OSINTCOE ističe da je moderna OSINT metodologija zasnovana na kombinaciji automatiziranih alata i analitičkih tehnika koje omogućuju efikasnu obradu velikih količina podataka [22].

3) Analiza

Analiza je faza u kojoj se prikupljeni podaci pretvaraju u korisnu informaciju. Ovdje se provodi selekcija, filtriranje, valjanost izvora, usporedba podataka i identifikacija obrazaca. Prema FOI-jevom OSINT vodiču, analiza je ključna za prepoznavanje relevantnih veza, rizika i anomalija koje nisu vidljive iz sirovih podataka [15].

Proces analize uključuje:

- validaciju izvora
- identifikaciju poveznica između subjekata
- procjenu vjerodostojnosti podataka
- prepoznavanje obrazaca ponašanja
- procjenu prijetnji i ranjivosti

FPZG navodi da je analiza intelektualno najzahtjevniji dio obavještajnog procesa jer traži multidisciplinarne pristupe i sposobnost kritičkog zaključivanja [24].

4) Izvještavanje

Izvještavanje predstavlja završnu fazu OSINT ciklusa i rezultat je svih prethodnih koraka. Cilj izvještavanja je prenijeti obavještajne zaključke u jasno strukturiranom i razumljivom obliku. Prema Eduzi, kvalitetan izvještaj mora omogućiti korisniku da brzo razumije prijetnje i donese odluke koje smanjuju rizik prije nego što se problemi pojave [21].

OSINT izvještaji mogu uključivati:

- tekstualne analize
- vizualizacije podataka
- grafove i dijagrame povezanosti
- procjene rizika
- preporuke i prijedloge za djelovanje

OSINTCOE naglašava da izvještavanje mora biti operativno uporabljivo i prilagođeno krajnjem korisniku, što je ključno za obrambene i sigurnosne procese [23].

3.4. Vrste OSINT izvora i tehnike prikupljanja informacija

Open Source Intelligence (OSINT) obuhvaća sustavno prikupljanje, obradu i analizu podataka koji su javno dostupni te se mogu koristiti u sigurnosne, operativne, istraživačke ili poslovno-obavještajne svrhe. Prema FOI-jevom OSINT leksikonu, OSINT se temelji na korištenju širokog spektra otvorenih izvora, uključujući javne internetske stranice, službene

registre, medijske objave, digitalne platforme i mrežne komunikacijske kanale [15]. Upravo zbog te dostupnosti i niske barijere pristupa, OSINT predstavlja jedan od najbrže rastućih metoda prikupljanja informacija u suvremenom digitalnom okruženju.

Hrčak navodi da se otvoreni izvori dijele u nekoliko ključnih skupina: medije (novinski članci, portali, televizijski sadržaji), akademske i znanstvene publikacije, javne baze podataka, poslovne registre, društvene mreže, blogove i forume [20]. Ti izvori omogućuju uvid u ponašanje korisnika, strukturu organizacija, tržišne trendove i kretanje informacija u stvarnom vremenu. Njihova informacijska vrijednost posebno je velika jer sadrže podatke koje korisnici nesvjesno ostavljaju - komentare, profile, fotografije, kontakte i digitalne tragove.

Prema NSK-ovoj analizi, društvene mreže i blogovi imaju posebno važnu ulogu u OSINT-u jer predstavljaju bogate izvore podataka o socijalnim vezama, profesionalnim interesima, radnim pozicijama i osobnim navikama korisnika [26]. Platforme poput Facebooka, LinkedIna i Instagrama omogućuju naprednu analizu ponašanja korisnika te identifikaciju ključnih osoba u organizacijama, što OSINT čini jednim od temeljnih alata za mapiranje struktura, identiteta i komunikacijskih obrazaca.

Osim sadržajnih, OSINT uključuje i niz tehničkih izvora informacija. FOI navodi da tehnički OSINT izvori obuhvaćaju WHOIS zapise, DNS informacije, SSL certifikate, metapodatke dokumenata, digitalne otiske IP adresa i druge infrastrukturne podatke koji se mogu koristiti za identifikaciju digitalne imovine organizacije [15]. Takvi podaci često otkrivaju ranjivosti, zastarjele sustave ili pogrešno konfigurirane servise te su korisni u kibernetičkim istragama, penetration testingu i procjeni sigurnosnog stanja.

Uz izvore, OSINT obuhvaća i tehnike prikupljanja informacija. NaVKiS navodi da su najčešće metode OSINT-a: ručno pretraživanje interneta, napredni upiti u tražilicama (dorking), korištenje specijaliziranih alata za automatsko prikupljanje informacija, scraping HTML sadržaja, analiza metapodataka, pregled javnih registara, crawling web-stranica i pasivno izviđanje digitalnih servisa [25]. Naglašava se da ove tehnike ne uključuju aktivne napade ili neovlašten pristup sustavima, već isključivo korištenje informacija koje su javno dostupne.

OSINTCOE ističe važnost metodološkog pristupa OSINT-u, posebice kod prikupljanja i validacije podataka. Prema njihovim smjernicama, svaka OSINT analiza mora slijediti definirani obavještajni ciklus - prikupljanje, vrednovanje, analiza i izvještavanje - te strogo poštivati etičke smjernice i zakonodavni okvir [22]. Profesionalni OSINT razlikuje se od običnog pretraživanja interneta upravo po strukturiranosti procesa, kategorizaciji izvora, provjeri vjerodostojnosti i dokumentiranju nalaza.

U kontekstu alata, Unite.ai navodi najpopularnije moderne OSINT alate, među kojima su Maltego, Shodan, SpiderFoot, theHarvester i drugi specijalizirani sustavi za indeksiranje i vizualizaciju informacija [27]. Ti alati omogućuju automatizirano prikupljanje podataka s velikog broja izvora, izradu grafova povezanosti, analizu infrastrukture i detekciju potencijalnih ranjivosti u digitalnim sustavima.

Edukativni izvori ističu da OSINT sve više postaje ključna digitalna kompetencija. Prema Eduzi, OSINT omogućuje donošenje informiranih odluka u poslovnom, sigurnosnom i obrazovnom kontekstu, a pravilno korištenje OSINT tehnika postaje važan element u obrani od socijalnog inženjeringa, kibernetičkih prijetnji i reputacijskih rizika [18].

Kombinacijom različitih izvora i tehnika, OSINT omogućuje dobivanje sveobuhvatnog uvida u digitalnu prisutnost pojedinaca, organizacija i infrastruktura. U sigurnosnom kontekstu, to znači identifikaciju ranjivosti, otkrivanje prijetnji i razumijevanje načina na koje napadači koriste javno dostupne informacije. OSINT stoga predstavlja temelj suvremenih sigurnosnih praksi i nezaobilaznu komponentu digitalne obrane.

3.5. Alati za OSINT

Open Source Intelligence (OSINT) alati predstavljaju ključne komponente modernih analitičkih i sigurnosnih procesa, omogućujući automatizirano prikupljanje, obradu i korelaciju javno dostupnih informacija. Kako se količina digitalnih podataka eksponencijalno povećava, učinkovitost OSINT-a uvelike ovisi o korištenju specijaliziranih alata koji mogu brzo pretraživati različite izvore, otkrivati obrasce, mapirati odnose između entiteta i pružati analitičarima cjelovit uvid u digitalnu sliku organizacije ili pojedinca. U nastavku se opisuju najrelevantniji i najkorišteniji alati u OSINT zajednici, uz naglasak na njihove mogućnosti, praktične primjene i ulogu u kibernetičkoj sigurnosti.

Maltego predstavlja jedan od najnaprednijih alata za vizualizaciju podataka u OSINT praksi. Njegova glavna vrijednost leži u mogućnosti automatskog otkrivanja i prikazivanja veza između različitih tipova informacija - poput domena, e-mail adresa, IP adresa, DNS zapisa, organizacija, društvenih profila i metapodataka. Maltego koristi tzv. transformacije, unaprijed definirane module koji povezuju ulazne podatke s vanjskim izvorima i bazama, stvarajući graf koji jasno prikazuje strukture i odnose u digitalnom ekosustavu [28]. Zbog sposobnosti vizualnog prikaza složenih mreža, široko se koristi u digitalnoj forenzici, kriminalističkim istragama, praćenju cyber prijetnji, mapiranju infrastrukture, ali i u novinarstvu i akademskim istraživanjima.

SpiderFoot je automatizirani OSINT sustav koji omogućuje izvlačenje podataka iz stotina javnih izvora putem samo jedne pretrage. Ovaj alat može analizirati domene, IP adrese, e-mailove, metapodatke, korisnička imena i niz drugih entiteta, pritom spajajući prikupljene informacije u jedinstven analitički model [29]. SpiderFoot je posebno učinkovit u otkrivanju ranjivosti, detektiranju izloženih servisa, identifikaciji starog ili zaboravljenog digitalnog sadržaja te izradi kompletnih OSINT profila meta. Jedna od njegovih prednosti je i mogućnost integracije s vlastitim API-jima i ranjivostima, što ga čini fleksibilnim u različitim analitičkim scenarijima.

theHarvester je specijalizirani alat za prikupljanje informacija o e-mail adresama, domenama, IP adresama i zaposlenicima organizacija. Koristi različite tražilice (Google, Bing, DuckDuckGo), PGP baze i društvene mreže kako bi identificirao potencijalne kontakte povezane s ciljem [30]. Budući da mnogi phishing i social-engineering napadi počinju identifikacijom točnih e-mail adresa zaposlenika, theHarvester je jedan od najčešće korištenih alata u inicijalnim fazama sigurnosnih testiranja i OSINT analiza. Također omogućuje izvođenje pasivnih analiza, što znači da meta nema direktnu interakciju s alatima, čime se izbjegava detekcija.

Shodan je jedinstvena tražilica internetski izloženih uređaja i servisa, često nazivana „Google za IoT“. Za razliku od klasičnih tražilica koje indeksiraju web sadržaj, Shodan pretražuje portove, bannere usluga, mrežne protokole i uređaje poput kamera, servera, routera, industrijskih kontrolnih sustava (ICS/SCADA) i medicinske opreme [31]. Ovaj alat omogućuje identificiranje ranjivosti, starog softvera, pogrešno konfiguriranih servisa i kritične infrastrukture izložene internetu. Shodan se široko koristi u analizi napadne površine organizacija, cyber threat intelligence operacijama i red-teaming vježbama.

Censys je vrlo sličan Shodanu, ali ide korak dalje u indeksiranju infrastrukture i SSL certifikata. Censys kontinuirano skenira cijeli javni internet, pohranjujući rezultate u napredne baze podataka koje omogućuju dubinsku analitiku sigurnosnih konfiguracija, otkrivanje novih servisa te praćenje promjena u realnom vremenu [32]. Posebno je koristan za identifikaciju poddomena, certifikata, TLS konfiguracija i slabih kriptografskih postavki, što ga čini jednim od ključnih tehničkih OSINT izvora za sigurnosne stručnjake.

FOCA (Fingerprinting Organizations with Collected Archives) fokusira se na analizu metapodataka dokumenata kao što su PDF, Word, Excel, slike i arhive. FOCA automatski izvlači skrivene informacije poput korisničkih imena, verzija softvera, internih putanja direktorija, naziva servera i mrežnih struktura [33]. Budući da organizacije često nenamjerno objave dokumente s ugrađenim metapodacima, FOCA je iznimno važna u naprednim OSINT analizama te može otkriti informacije korisne za kasniju fazu napada, poput lateralnog kretanja.

Recon-ng je modularni OSINT framework koji omogućuje dubinsko prikupljanje podataka kroz strukturirano CLI sučelje, vrlo slično penetration-testing alatima kao što je Metasploit. Recon-ng omogućuje integraciju API-ja, izgradnju vlastitih modula, izvođenje prilagođenih upita i pohranu rezultata u bazu [34]. Zbog fleksibilnosti i visoke automatizacije jedan je od najpopularnijih alata za profesionalne OSINT operacije, naročito u cyber sigurnosti, lovu na prijetnje i istraživačkom radu.

OWASP Amass specijaliziran je za mapiranje domena, otkrivanje poddomena i analizu DNS infrastrukture. Amass kombinira pasivne i aktivne metode prikupljanja podataka, uključuje brute-force tehnike, certifikate, povijesne zapise i partnerske baze [35]. Koristi se najčešće za procjenu napadne površine organizacija, identifikaciju starih ili zaboravljenih servisa koji predstavljaju sigurnosni rizik, te za napredne sigurnosne audite.

Ovi alati zajedno čine srž modernog OSINT-a, jer omogućuju prikupljanje podataka iz različitih perspektiva - od tehničkih informacija, preko digitalnog identiteta, do analize društvenih veza i povijesnih zapisa.

Osim glavnih alata, u praksi se često koriste i dodatni alati koji popunjavaju specifične potrebe: ZoomEye (pretraživanje izloženih uređaja), Datasploit (automatska OSINT enumeracija), Intelligence X (pretraživanje darknet i leak baza), HaveIBeenPwned (provjera curenja podataka), Sherlock i WhatsMyName (pretraživanje korisničkih imena), Wappalyzer i BuiltWith (identifikacija tehnologija web stranica), Archive.org (povijesne kopije web sadržaja) te DNSDumpster (DNS i poddomene). Širi pregled svih kategorija OSINT alata dostupan je na službenom OSINT Frameworku: https://osintframework.com.

3.6. Rizici i etika OSINT-a

Open Source Intelligence (OSINT) donosi snažne mogućnosti za prikupljanje i analizu javno dostupnih podataka, no istodobno otvara prostor za ozbiljne etičke, sigurnosne i pravne izazove. Kako ističe Stepić, OSINT u korporativnom kontekstu postaje „skriveni alat" koji otkriva obrasce, slabosti i prijetnje koje organizacije često ni same nisu svjesne, ali upravo zato zahtijeva viši stupanj odgovornosti i transparentnosti [36]. Snaga OSINT-a leži u jednostavnosti, pristupačnosti i brzini analize, što omogućuje i legitimnim stručnjacima i zlonamjernim akterima da dođu do podataka koji mogu imati osjetljive implikacije.

Jedan od najvećih rizika jest činjenica da kriminalci koriste OSINT na isti način kao i sigurnosni timovi. CERT-HR naglašava da veliki broj phishing kampanja i drugih socijalno-inženjerskih napada započinje analizom otvorenih izvora, uključujući društvene mreže, poslovne registre, neosigurane baze podataka i javne forume [14]. Pomoću tih informacija

napadači kreiraju personalizirane poruke koje djeluju uvjerljivo, što značajno povećava vjerojatnost manipulacije korisnikom. INSECM dodatno potvrđuje kako kombinacija OSINT-a, socijalnog inženjeringa i psiholoških tehnika poput hitnosti, straha i lažnog autoriteta dramatično povećava stopu uspješnosti napada [12].

Drugi ključni rizik odnosi se na točnost podataka. FOI Security Wiki upozorava da OSINT može dovesti do pogrešnih zaključaka ako se informacije uzimaju iz neprovjerenih ili manipuliranih izvora [15]. Nedostatak konteksta, zastarjeli podaci ili svjesno plasirane dezinformacije mogu rezultirati pogrešnim procjenama u sigurnosnim, novinarskim ili poslovnim analizama. Zbog toga je verifikacija i metodološka dosljednost nužna.

Kaspersky dodatno upozorava da OSINT, iako pasivan, može biti duboko invazivan, osobito kada se analize provode nad pojedincima, njihovim navikama, privatnim objavama ili društvenim vezama [37]. Iako su informacije javno dostupne, njihova masovna agregacija i profiliranje može predstavljati kršenje privatnosti i dovesti do zlouporabe podataka. Korisnici često nisu svjesni koliko podataka javno dijele te ne razumiju kako čak i bez hakiranja netko može izgraditi detaljan osobni profil.

Eithos naglašava još jedan problem: legalnost OSINT aktivnosti razlikuje se od države do države, a mnogi podatkovni skupovi mogu biti javni, ali ne i zakoniti za masovnu obradu [38]. Pravni izazovi obuhvaćaju GDPR, autorska prava, ograničenja korištenja API-ja, pravila web stranica (Terms of Service) i regulative o privatnosti. OSINT analitičar mora razumjeti gdje je granica između legitimne i neovlaštene obrade podataka.

Cambridge dodaje globalnu dimenziju etičkog problema. U kontekstu međunarodnih istraga i analiza digitalnih dokaza, OSINT se suočava s pitanjima verifikacije, lanaca čuvanja dokaza, zaštite izvora, sigurnosti analitičara i odgovornosti za objavljene informacije [39]. Neetično korištenje OSINT-a u osjetljivim istragama može dovesti do nanošenja štete žrtvama, pogrešnog teretnog zaključka ili narušavanja sudskog procesa.

Dodatni izazov u Hrvatskoj je nedostatak adekvatne edukacije. Tportal navodi da, iako svijest o kibernetičkim prijetnjama raste, organizacijama i dalje nedostaje dovoljno obučenih stručnjaka koji razumiju kako OSINT koristiti odgovorno, etično i zakonito [4]. To otvara prostor za pogrešne postupke, prekomjerno prikupljanje informacija ili neusklađenost s regulatornim zahtjevima.

U etičkom smislu, odgovorna primjena OSINT-a temelji se na nekoliko osnovnih principa:

1. Minimalno prikupljanje - prikupljati samo ono što je potrebno za definirani cilj.
2. Poštivanje privatnosti - iako su podaci javni, njihovo strukturiranje može biti osjetljivo.

3. Metodološka transparentnost - svaki korak mora biti dokumentiran, posebno u forenzičkom i istraživačkom kontekstu.
4. Verifikacija izvora - ključna je kako bi se izbjegle dezinformacije i pogrešne procjene.
5. Pasivnost - OSINT ne smije uključivati hakiranje, pristup zatvorenim sustavima ili manipulaciju korisnicima.
6. Zakonitost obrade - nužno je razumijevanje GDPR-a, autorskih prava i pravnih ograničenja platformi.

U konačnici, OSINT je izuzetno moćan alat - kako za obranu tako i za napad. Upravo zato etički okvir, transparentnost i profesionalna odgovornost moraju biti temelj njegove uporabe. Etika nije dodatak, nego preduvjet za legitimnu i sigurnu OSINT praksu.

4. Phishing

Phishing predstavlja oblik kibernetičkog napada u kojem napadači koriste lažne e-mail poruke, web stranice ili druge komunikacijske kanale kako bi žrtvu naveli na otkrivanje povjerljivih podataka, poput korisničkih vjerodajnica, osobnih informacija ili financijskih podataka. Napadi se najčešće predstavljaju kao legitimne poruke banaka, dostavnih službi, državnih institucija ili popularnih internetskih servisa. Nacionalni CERT upozorava da se phishing kontinuirano prilagođava trendovima, često uključuje imitaciju službenih vizualnih identiteta te predstavlja najraširenij oblik prijevare usmjeren na korisnike u Hrvatskoj [14].

4.1. Vrste phishinga

Phishing se tijekom godina razvio u iznimno širok spektar tehnika, koje kombiniraju psihološku manipulaciju, imitaciju legitimnih servisa i iskorištavanje digitalnih navika korisnika. Prema analitičkom istraživanju objavljenom u SAGE časopisu, moderni phishing temelji se na tri temeljna elementa: uvjerljivoj lažnoj poruci, psihološkom okidaču te mehanizmu krađe podataka ili kompromitacije sustava [40]. Razvojem digitalnih servisa i društvenih mreža ove metode postaju sve sofisticiranije i teže prepoznatljive.

Masovni phishing ostaje najčešći oblik. Napadač šalje velik broj generičkih poruka kako bi barem mali postotak žrtava kliknuo na zlonamjerni link. Poruke najčešće oponašaju banke, državne institucije ili velike tehnološke kompanije. Prema analizi SAGE Journal-a, učinkovitost ovih napada i dalje je visoka jer se temelje na univerzalnim emocionalnim okidačima poput straha, hitnosti ili obećanja nagrade, uz minimalne tehničke preduvjete za napadača [40]. Upravo zbog te jednostavnosti masovni phishing ostaje globalno najraširenij oblik digitalne prijevare.

Spear phishing predstavlja napredniju i ciljanu varijantu. Napadač prikuplja javno dostupne informacije o konkretnoj osobi - npr. položaj u organizaciji, kontakte, navike, poslovne projekte - te kreira personaliziranu poruku koja je prilagođena žrtvinoj ulozi i kontekstu. Prema SAGE istraživanju, personalizacija značajno podiže stopu uspješnosti, jer žrtva prepoznaje elemente koji joj djeluju poznato i smatra poruku legitimnom [40]. Ovaj pristup posebno se koristi u napadima na tvrtke, jer već mala razina OSINT-a može stvoriti vrlo uvjerljiv napad.

Whaling je specijalizirani oblik spear phishinga usmjeren na visokopozicionirane rukovoditelje, poput direktora, CFO-a ili upravnog osoblja. U napadima ove vrste poruke često imitiraju pravne zahtjeve, financijske transakcije ili hitne interne upute. Fortinet naglašava da

whaling napadi često iskorištavaju autoritet unutar organizacije, čineći korisnika sklonim promptnom djelovanju bez dodatne provjere autentičnosti [41]. Zbog visokih ovlasti meta, posljedice whaling napada mogu biti iznimno ozbiljne i financijski razorne.

Business Email Compromise (BEC) danas je jedan od najštetnijih oblika phishinga. Napadač kompromitira stvarni poslovni račun ili ga vjerno imitira te šalje upute za prijenos sredstava ili dostavu povjerljivih informacija. Istraživanje objavljeno u SAGE publikaciji naglašava da BEC spaja tehničke i psihološke elemente - kompromitirani račun daje legitimitet, dok hitne upute stvaraju pritisak i pogoduju brzom donošenju odluka [40]. Upravo zbog te kombinacije BEC spada u najskuplje oblike cyber kriminala.

Clone phishing predstavlja tehniku u kojoj napadač uzima stvarnu poruku koju je žrtva ranije primila, ali zamjenjuje legitimni link kompromitiranim. Budući da izgled poruke odgovara originalu, korisnik gotovo uvijek vjeruje njezinoj autentičnosti. Fortinet navodi da se ovaj oblik često koristi u poslovnim okruženjima gdje se redovito šalju interne datoteke ili sustavi generiraju automatizirane poruke, što napadačima daje idealnu priliku da se uklope u komunikacijski tok [41].

Smishing i vishing predstavljaju adaptacije phishinga na mobilne komunikacijske kanale. Smishing se provodi putem SMS poruka, dok vishing koristi telefonske pozive, često uz lažne call-centre i unaprijed pripremljene skripte. Prema Fortinetu, popularnost smishinga raste zbog velikog povjerenja korisnika u mobilne uređaje, dok vishing postaje sve sofisticiraniji zahvaljujući tehnologijama poput spoofinga brojeva i automatiziranih glasova [41]. U oba slučaja naglasak je na emocionalnoj manipulaciji, a ne tehničkim trikovima.

Pharming predstavlja tehniku koja ne ovisi o porukama, već o preusmjeravanju korisnika na lažne web stranice čak i kada ručno upišu ispravnu adresu. Manipulacijom DNS postavki ili kompromitacijom uređaja napadač može preusmjeriti korisnika na lažnu stranicu bez da žrtva primijeti. SAGE opisuje pharming kao jednu od najopasnijih tehnika upravo zato što žrtva nema mogućnost vizualnog prepoznavanja prijevare s obzirom na to da sve izgleda legitimno [40].

Na društvenim mrežama sve popularniji je tzv. angler phishing, gdje napadači glume službu korisničke podrške i javljaju se korisnicima koji javno objave problem. Fortinet navodi da napadači koriste lažne profile brandova, nude pomoć i zatim šalju poveznice koje vode na lažne stranice ili aplikacije [41]. Ovaj pristup iskorištava prirodno povjerenje korisnika prema službama podrške i predstavlja modernu adaptaciju socijalnog inženjeringa.

Ukupno, prikaz navedenih tehnika u obje publikacije potvrđuje da phishing više nije jedinstvena metoda, nego cijeli skup psihološki i tehnički raznolikih napada. Napadači svoje

pristupe prilagođavaju kanalima, kontekstu i ciljevima, što zahtijeva stalnu edukaciju, oprez i razumijevanje širokog spektra mogućih napadnih vektora.

4.2. Psihologija socijalnog inženjeringa

Socijalni inženjering predstavlja jednu od najopasnijih i najraširenijih metoda cyber napada jer ne cilja tehničke ranjivosti sustava, već psihološke ranjivosti ljudi. Istraživanja jasno pokazuju da ljudski mozak, bez obzira na iskustvo ili tehničko znanje, ima duboko ukorijenjene kognitivne pristranosti i emocionalne reakcije koje se mogu predvidjeti, manipulirati i iskoristiti [42]. Upravo zato socijalni inženjering ostaje ključni element gotovo svih uspješnih phishing kampanja, BEC (Business Email Compromise) napada, prijevara identiteta i digitalnih manipulacija.

Prema radu objavljenom u *Applied Sciences*, socijalni inženjering funkcionira zato što napadači uspijevaju "parazitirati" na tipičnim obrascima ljudskog ponašanja - automatizmu odlučivanja, povjerenju u autoritet, želji za pripadanjem, empatiji i strahu [42]. Ljudi rijetko donose odluke racionalno. Veliki dio odluka temelji se na emocionalnim heuristikama - mentalnim prečacima koji ubrzavaju donošenje odluka, ali ih istovremeno čine ranjivima na manipulaciju. Ove kognitivne slabosti čine ljude idealnim ciljem napadača, a digitalno okruženje dodatno povećava njihovu izloženost.

Jedno od ključnih otkrića istraživanja u području socijalnog inženjeringa jest da napadači ciljaju emocionalna stanja u kojima su korisnici najskloniji pogreškama. *ScienceDirect* ističe da čim korisnik osjeti stres, hitnost, pritisak ili paniku, njegova sposobnost kritičkog razmišljanja drastično pada [43]. U takvim situacijama korisnici brže reagiraju, manje analiziraju, a napadači upravo to iskorištavaju porukama koje simuliraju hitne zahtjeve, prijetnje ili poslovne naredbe.

Jedan od najvažnijih psiholoških faktora je autoritet. Prema istraživanju o psihologiji socijalnog inženjeringa, ljudi imaju duboko ukorijenjenu tendenciju da vjeruju porukama koje djeluju kao da dolaze od nadređenih osoba, institucija ili autoritativnih izvora [44]. Napadači zato vrlo često oponašaju banke, državne institucije, direktore ili IT službe. Kada korisnik prepozna autoritet u komunikaciji, automatski smanjuje razinu sumnjičavosti i povećava spremnost na suradnju.

Drugi ključni psihološki pokretač je povjerenje u društvene i emocionalne signale. Prema studiji iz 2024. godine, interakcije koje djeluju toplo, prijateljski ili personalizirano stvaraju osjećaj da je poruka legitimna, posebno ako uključuju osobne podatke preuzete OSINT metodama [44]. Ljudi imaju tendenciju "popuniti praznine" u informacijama i

pretpostaviti dobre namjere, što napadači koriste kako bi stvorili privid autentičnosti čak i kad tehnički elementi poruke sadrže nedostatke.

Treći psihološki element koji napadači često koriste jest reciprocitet. Socijalna psihologija pokazuje da ljudi imaju snažnu potrebu uzvratiti uslugu ili se ponašati u skladu s prethodnom interakcijom. Napadači zato često koriste strategije poput:

- slanja poklona,
- ekskluzivnih ponuda,
- "zahvalnih" poruka,
- privida prethodne komunikacije.

Korisnik često upada u zamku automatskog odgovora ili klika, ne shvaćajući da je emocionalno induciran na akciju.

Četvrti važan element je osjećaj hitnosti. Prema istraživanjima *ScienceDirecta*, korisnici pod pritiskom vremena značajno češće otvaraju zlonamjerne linkove i preuzimaju datoteke [43]. Phishing poruke poput "Vaš račun će biti ukinut u roku 24 sata" ili "Potrebna je hitna potvrda uplate" upravo aktiviraju ovaj psihološki mehanizam.

Peti element, prema *ResearchGate* studiji, je igranje na ljudsku znatiželju i emocije. Ljudi su prirodno skloni otvarati neočekivane poruke, provjeravati "tajne informacije" ili kliknuti na nešto što izgleda iznenađujuće ili šokantno [44]. Zbog toga se u socijalnom inženjeringu često pojavljuju teme poput:

- senzacionalističkih vijesti,
- lažnih obavijesti o nagradama,
- upozorenja "pogledajte tko vas je spomenuo",
- navodnih curenja podataka.

Napadači koriste i princip dosljednosti. Ljudska želja da "završe započeto" često dovodi do toga da korisnik, nakon što je kliknuo na link, nastavi ispunjavati formu ili potvrditi radnju zbog osjećaja obveze, čak i kada počinje sumnjati u autentičnost poruke [45].

Istraživanja također naglašavaju ulogu kognitivnih pristranosti. Najvažnije među njima su:

- *confirmation bias* – korisnici vjeruju informacijama koje potvrđuju njihova očekivanja
- *optimism bias* – uvjerenje da "meni se to neće dogoditi"
- *anchoring bias* – oslanjanje na prvi dojam u komunikaciji
- *loss aversion* – ljudi poduzimaju impulzivne akcije kako bi izbjegli gubitak

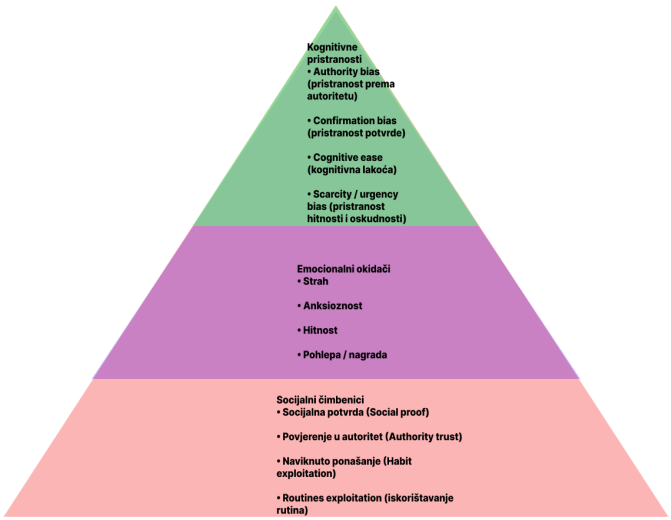
Napadači svoje kampanje strukturiraju upravo tako da aktiviraju jednu ili više od ovih pristranosti [42].

Digitalno okruženje dodatno otežava obranu. Prema *ScienceDirect* studiji, korisnici se u online komunikaciji puno više oslanjaju na površne signale (logo, ime pošiljatelja, poznatu temu) nego u fizičkoj komunikaciji [43]. Nedostatak neverbalnih signala vodi do toga da se poruke procjenjuju brzo, intuitivno i bez duboke analize - što ih čini lakom metom manipulacije.

Nadalje, *International Journal of Advanced and Applied Sciences* ističe da socijalni inženjering nije samo tehnička metoda, već psihološki proces u kojem napadač korak po korak gradi povjerenje, autoritet i emocionalni utjecaj na žrtvu [45]. U složenijim napadima, poput spear-phishinga, napadač može tjednima proučavati meta osobe, njihove navike, objave, interese i poslovne odnose, nakon čega kreira iznimno uvjerljivu, personaliziranu poruku.

Zanimljivo, *RRIOJ* analiza pokazuje da socijalni inženjering nije uvijek destruktivan - može biti i inovativan alat u cyber sigurnosti, primjerice u edukaciji, simulacijama napada ili testiranju sigurnosne kulture organizacije [46]. Međutim, njegova zlonamjerna primjena predstavlja sve veću prijetnju jer čak i najnapredniji tehnički sustavi ne mogu u potpunosti zaštititi krajnjeg korisnika od psihološke manipulacije.

U konačnici, razumijevanje psihologije socijalnog inženjeringa ključan je korak u obrani od modernih cyber prijetnji. Tehnologija napreduje, ali ljudska psihologija ostaje ista - predvidiva, emocionalna i ranjiva. Zbog toga su educiranje korisnika, jačanje sigurnosne kulture i integracija psiholoških modela u sigurnosne procese jednako važni kao i tehničke mjere zaštite.



Slika 1: Model ljudskih slabosti (Izvor: vlastita izrada)

Prikazana piramida ilustrira tri ključna sloja psiholoških ranjivosti koje napadači u phishing kampanjama najčešće iskorištavaju. Donji sloj, „Socijalni čimbenici“, predstavlja temelj jer obuhvaća obrasce ponašanja koji se ponavljaju svakodnevno i oblikuju način na koji korisnici doživljavaju digitalnu komunikaciju. Tu spadaju navike poput rutinskog otvaranja poslovnih poruka, povjerenja u autoritete te oslanjanja na socijalne norme i poznate obrasce komunikacije. Budući da su ovi čimbenici duboko ukorijenjeni u društvenom i organizacijskom kontekstu korisnika, napadači ih lako imitiraju kako bi njihova poruka izgledala legitimno i očekivano.

Srednji sloj čine „Emocionalni okidači“, psihološki mehanizmi koji aktiviraju brze, impulzivne reakcije. Napadači najčešće koriste strah (npr. gubitak računa), anksioznost (hitne poruke o sigurnosti), ili pohlepu (obećanja nagrada). Ovi okidači potiskuju racionalno prosuđivanje i prebacuju korisnika u emocionalni način odlučivanja, što značajno povećava vjerojatnost pogrešnih odluka. Emocionalni sloj funkcionira kao most između osnovnih socijalnih navika i vršnih kognitivnih pristranosti.

Na vrhu piramide nalaze se „Kognitivne pristranosti“, mentalni prečaci koji pojednostavljuju odlučivanje, ali ga čine podložnim manipulaciji. Phishing najčešće iskorištava authority bias (vjerovanje autoritetu), confirmation bias (prihvaćanje informacija koje potvrđuju očekivanja), cognitive ease (veće povjerenje u jednostavne i poznate poruke) te urgency bias (impulzivnost u situacijama hitnosti). Iako se nalaze na vrhu piramide, ove pristranosti često su presudne u trenutku kada korisnik odlučuje hoće li kliknuti na link ili otvoriti privitak.

Piramida prikazuje da uspješni phishing napadi ne djeluju samo na jednoj razini, nego ciljaju sve tri kategorije ranjivosti istodobno. Napadači najprije repliciraju socijalni kontekst (donji sloj), zatim aktiviraju emocije (srednji sloj), a na kraju iskorištavaju kognitivne pristranosti kako bi žrtva donijela brzu, automatiziranu odluku. Upravo sinergija ova tri sloja objašnjava zašto phishing ostaje jedan od najučinkovitijih oblika kibernetičkog napada čak i u organizacijama s visokim stupnjem tehničke zaštite.

4.3. Anatomija phishing kampanja

Phishing kampanje danas predstavljaju najraširenij, najprilagodljiviji i najopasniji oblik kibernetičkih prijetnji, a njihova učinkovitost proizlazi iz kombinacije tehničke sofisticiranosti i duboko ukorijenjenih psiholoških mehanizama ljudskog ponašanja. Razumijevanje anatomije phishing napada zahtijeva holistički pristup: napad ne počinje onog trenutka kada korisnik primi zlonamjernu poruku, nego mnogo ranije - u fazi izviđanja, psihološkog oblikovanja

manipulativne priče i tehničke pripreme infrastrukture. Najdetaljniji i najstručniji prikaz strukture phishing kampanja donosi Varonis u svom whitepaperu „Anatomy of a Phish“, gdje se prikazuje kako napadači kombiniraju inženjering infrastrukture s manipulacijom ljudskom psihologijom kako bi ostvarili maksimalnu učinkovitost [49]. Dodatne tehničke i proceduralne komponente objašnjene su u publikacijama zvelo i Tegodata, koje prikazuju praktične faze napada, često kroz realne scenarije [47], [48].

Phishing kampanja uvijek započinje opsežnim prikupljanjem informacija iz otvorenih izvora (OSINT). Napadači analiziraju sve što je meta ostavila na internetu: društvene mreže, poslovne web stranice, registre, forume, vijesti, objave o projektima i poslovnim uspjesima, ali i sitne detalje iz privatnog života. Ta faza, premda tehnički jednostavna, stvara psihološki temelj napada. Prema znanstvenim radovima o socijalnom inženjeringu, personalizacija poruke je ključni faktor uspješnosti manipulacije jer se ljudska kognicija oslanja na heuristiku prepoznavanja - kada korisnik vidi informacije koje su mu poznate, mentalno snižava razinu obrambene pažnje [42], [44]. Varonis navodi da napadači vrlo precizno profiliraju ciljane žrtve, stvarajući psihološki portret koji uključuje radno mjesto, hijerarhiju, emocionalne okidače i vrstu komunikacije na koju će meta najvjerojatnije reagirati [49]. Time OSINT postaje temelj manipulativne arhitekture phishing napada.

Nakon faze izviđanja slijedi oblikovanje narativa. Prema Varonisu, uspješna phishing poruka nikada nije generička: ona je proizvod ciljane psihološke konstrukcije koja se uklapa u mentalni model žrtve [49]. Napadači koriste tehnike slične profesionalnim marketinškim kampanjama - pažljivo biraju ton komunikacije, vizualne elemente, strukturu poruke i emocionalni tempo. Znanstveni radovi o socijalnom inženjeringu ističu da phishing najuspješnije djeluje kada aktivira emocionalne sustave donošenja odluka (System 1), zaobilazeći sporiji, racionalni i analitički sustav (System 2) [43], [45]. Emocije poput straha, hitnosti, autoriteta, nagrade ili gubitka utječu na kognitivne distorzije kao što su „urgency bias“, „authority bias“ i „confirmation bias“, čime se drastično smanjuje sposobnost racionalne procjene. Zbog toga phishing kampanje često koriste fraze poput „Vaš račun je zaključan“, „Naručena pošiljka čeka potvrdu“, „Nadređeni zahtijeva hitnu akciju“ ili „Vaš pristup će biti deaktiviran u roku od 24 sata“. Istraživanja navode da takve poruke stvaraju psihološki pritisak koji potiče brzu i impulzivnu reakciju [42], [43].

Tehnička priprema phishing kampanje jednako je sofisticirana kao i psihološka. Napadači registriraju domene koje su vizualno gotovo identične legitimnima, koriste typosquatting, IDN homografe i domene koje izgledaju autentično na prvi pogled. Tegodata i zvelo navode da moderni phishing napadi uključuju i profesionalno dizajnirane landing stranice koje repliciraju legitimne servise do najsitnijeg detalja [47], [48]. Varonis pojašnjava da napadači sve češće koriste TLS certifikate kako bi korisnik vidio „HTTPS“ indikator, što

dodatno povećava dojam legitimnosti [49]. Napadi često uključuju i „cloaked redirects“ - preusmjeravanja kroz međukorake koji su skriveni od korisnika, ali napadaču omogućuju precizno praćenje ponašanja. U nekim slučajevima koristi se i geo-targeting kako bi se prikaz sadržaja prilagodio lokaciji žrtve, čime se povećava uvjerljivost.

Kada je infrastruktura spremna, slijedi faza dostave. Iako je e-mail najčešći komunikacijski kanal, suvremeni phishing koristi cijeli spektar digitalnih platformi: SMS (smishing), pozive (vishing), WhatsApp i Viber poruke, LinkedIn zahtjeve, Instagram obavijesti, QR kodove (quishing), čak i Wi-Fi pristupne točke. Zvelo naglašava da raznolikost kanala ne proizlazi iz kreativnosti napadača, nego iz evolucije obrambenih sustava - kada se e-mail obrana ojača, napadači se prebacuju na kanale koji su slabije kontrolirani [47]. Međutim, e-mail i dalje ostaje najmoćniji alat jer omogućuje najveći stupanj personalizacije, automatizacije i integracije s OSINT-om.

Nakon otvaranja phishing poruke aktivira se najvažniji element napada: psihološka dinamika korisnika. Prema znanstvenim radovima iz područja socijalnog inženjeringa, ljudski mozak je arhitektonski sklon donošenju brzih odluka temeljenih na emocionalnim signalima, posebno ako se radi o porukama koje izgledaju autoritativno ili hitno [43], [44]. U praksi to znači da se korisnik često fokusira na emocionalni sadržaj, a ne na tehničke znakove upozorenja. Varonis daje primjere napada gdje poruke oponašaju interne korporativne sustave, HR odjele, IT administratore, banke ili popularne servise poput Microsofta i Googlea, koristeći minimalne vizualne razlike kako bi se žrtvi smanjila sposobnost razlikovanja pravog od lažnog [49]. Psihološka istraživanja potvrđuju da su korisnici posebno ranjivi kada se nalaze pod kognitivnim opterećenjem, emocionalnim stresom ili multitasking okruženjem, što napadači vrlo dobro iskorištavaju [45], [46].

Sljedeća faza uključuje interakciju korisnika s malicioznom stranicom. Napadači dizajniraju stranice koje gotovo u potpunosti repliciraju legitimne obrasce - logotipe, strukturu navigacije, tipografiju, mobilni prikaz, boje i čak mikroanimacije. Tegodata i zvelo navode da je cilj stvoriti iskustvo koje izgleda dovoljno poznato da žrtva ne primijeti razliku ni nakon više sekundi interakcije [47], [48]. Varonis ističe da moderni phishing obrasci često uključuju skripte za „real-time credential harvesting“ - čim žrtva unese vjerodajnice, napadač ih automatski preusmjerava na legitimnu stranicu, čime se stvara iluzija pravilnog logiranja [49]. U tom trenutku žrtva ne sumnja u kompromitaciju jer se ništa neuobičajeno nije dogodilo, a napadač može odmah iskoristiti pristup.

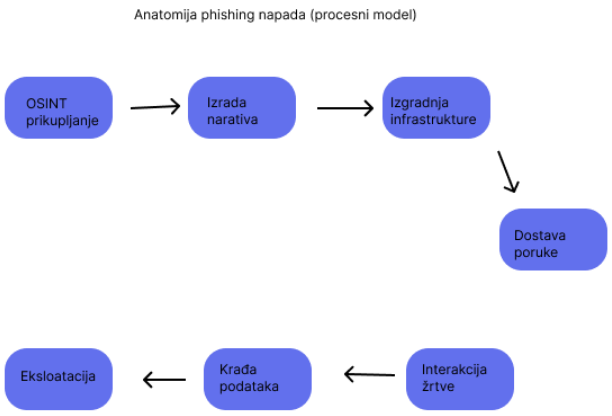
Kada napadač dobije vjerodajnice, napad prelazi u fazu iskorištavanja. Prema Varonisu, najopasniji scenarij je kompromitacija poslovnih računa u sustavima poput Microsoft

365, jer takav račun sadrži pristup e-mailovima, dokumentima, internim komunikacijama, OneDriveu, SharePointu i Teamsima, što predstavlja idealnu platformu za lateralno kretanje kroz organizaciju [49]. Napadač može postaviti pravila preusmjeravanja e-mailova, eskalirati ovlasti, krasti financijske podatke, izvoditi BEC (Business Email Compromise) prijevare ili postavljati ransomware.

Znanstveni radovi ističu da socijalni inženjering nije samo tehničko, nego primarno psihološko oružje. Napadi ciljaju podsvjesne mentalne procese kako bi natjerali korisnika da donese odluku koja mu se u tom trenutku čini racionalnom, iako je vođena emocionalnim impulsima [42], [43], [44], [46]. Socijalni inženjering kombinira elemente psihologije, komunikologije, antropologije i kognitivnih znanosti, što ga čini najopasnijim oblikom napada jer se brani protiv ljudskog uma, a ne samo protiv tehnologije. Obrambeni sustavi mogu filtrirati poruke, ali ne mogu filtrirati ljudske emocije, intuiciju, percepciju i stres - a upravo su to elementi koje napadači ciljaju.

U završnoj fazi phishinga napadač ostvaruje svoje krajnje ciljeve. To mogu biti financijske prijevare, krađa podataka, špijunaža, sabotaža, eksfiltracija podataka, kompromitacija čitave infrastrukture ili priprema terena za buduće napade. Varonis naglašava da phishing sve češće služi kao početni vektor u višefaznim napadima, gdje jedna ukradena lozinka otvara pristup cijeloj mreži i resursima organizacije [49]. Napad koji je počeo kao kratka e-mail poruka može rezultirati potpunim kolapsom poslovanja, gubitkom povjerljivih podataka, regulatornim kaznama i dugoročnom reputacijskom štetom.

Sveobuhvatna analiza anatomije phishing kampanja pokazuje da se radi o visoko strukturiranom, višeslojnom procesu koji spaja tehničku izvedbu, psihološke manipulacije, infrastrukturnu pripremu i dubinsko razumijevanje ljudskog ponašanja. Napadači ne osvajaju sustave samo tehnikom, već i sposobnošću da „pročitaju“ žrtvu, oblikuju uvjerljivu priču i potaknu emocionalnu reakciju. Zbog toga obrana od phishinga zahtijeva interdisciplinarni pristup koji uključuje tehnološke mjere, stalno praćenje prijetnji, edukaciju zaposlenika i razumijevanje psihološke dinamike napada. Tek kombinacijom svih tih elemenata moguće je značajno smanjiti rizik i povećati otpornost organizacija na ovu najrašireniju digitalnu prijetnju.



Slika 2: Procesni model anatomije phishing napada (Izvor: vlastita izrada)

4.4. Tehnike phishing napada

Iza svake uspješne phishing kampanje ne stoji samo dobra priča i psihološka manipulacija, nego i čitav skup tehničkih tehnika koje napadač koristi kako bi sakrio pravu prirodu napada, zaobišao sigurnosne sustave i žrtvi prikazao što uvjerljivije lažno sučelje. U nastavku su opisane najčešće tehničke tehnike koje se koriste u phishing napadima, uz oslanjanje na stručne izvore sigurnosne industrije i praktične primjere.

Jedna od temeljnih tehnika jest URL spoofing, odnosno manipuliranje načinom na koji se poveznica prikazuje žrtvi. Napadači iskorištavaju činjenicu da korisnici često prate samo vidljivi tekst linka (anchor tekst) ili display name, a ne stvarnu odredišnu adresu. U praksi to znači da poruka može prikazivati „https://banka.hr/račun“, dok stvarni URL vodi na potpuno drugu domenu, često maskiranu pomoću skraćenih linkova ili složenih parametara [50]. Dodatno, koriste se tehnike poput homograf napada (zamjena slova vizualno sličnim znakovima iz drugih abeceda) i vrlo dugačkih URL-ova u kojima je prava domena „skrivena“ u nizu podmapa i parametara. Cilj je stvoriti iluziju legitimnosti i iskoristiti naviku korisnika da „samo brzinski klikne“ bez detaljnog provjeravanja adresne trake.

Tijesno povezana s tim je tehnika typosquattinga, u kojoj napadač registrira domene koje su vrlo slične legitimnim, ali sadrže tipične korisničke tipfelere ili sitne izmjene [51]. Primjeri uključuju zamjenu slova („paypai.com“ umjesto „paypal.com“), dodavanje ili izostavljanje jednog znaka („micorsoft.com“), korištenje različitih TLD-ova („firma.hr“ → „firma.com“) ili iskorištavanje tipičnih pogrešaka pri pisanju na mobilnim uređajima. McAfee naglašava da napadači zatim na te domene postavljaju lažne login stranice, obrazce ili čak legitimno izgledajuće sadržaje, kako bi korisnik imao utisak da je jednostavno „krivo upisao adresu“, a

zapravo je na malicioznoj domeni [51]. Typosquatting se kombinira s phishing e-mailovima, oglasima ili SEO manipulacijom kako bi se povećala vjerojatnost da korisnik nesvjesno završi na krivoj stranici.

Napadači dodatno koriste URL masking, cloaking i redirect lance kako bi sakrili krajnje odredište linka. Servisi za skraćivanje URL-ova i DNS forwarding često se zlorabe tako da korisnik vidi neutralnu ili poznatu domenu, dok se iza nje skriva preusmjeravanje na malicioznu stranicu [56]. Urllo ističe da „maskirani" URL-ovi otežavaju korisniku provjeru autentičnosti, a višestruki redirekti (npr. legitimna domena → tracking servis → kompromitirana domena) otežavaju i filtriranje na razini sigurnosnih gatewaya [56]. U takvim lancima često se koristi tzv. „cloaking", gdje se sadržaj stranice razlikuje ovisno o tome dolazi li posjet iz automatiziranog sigurnosnog skenera ili iz stvarnog korisničkog preglednika, čime se dodatno otežava detekcija.

Kako bi dodatno prikrili namjeru, napadači primjenjuju obfuscation nad HTML i JavaScript kodom phishing stranica i skripti. Cilj je otežati analiziranje koda, zaobilaženje filtarskih pravila i statičku detekciju zlonamjernih elemenata. Digital.ai navodi da se JavaScript obfuscation tipično provodi kroz preimenovanje varijabli nerazumljivim nizovima, umetanje beznačajnog koda, enkodiranje stringova (npr. base64) i korištenje dinamičkog generiranja funkcija [52]. Slično, HTML se može „zamaskirati" kroz entitete, inline stilove i neuobičajenu strukturu, čime se otežava jednostavno pretraživanje po uzorcima [53]. Na taj način phishing skripte koje kradu podatke, keyloggeri ili skripte za dinamičko slanje vjerodajnica postaju znatno teže uočljive automatiziranim alatima, iako u pregledniku korisnika rade potpuno „normalno".

Posebno sofisticirana tehnika je browser-in-the-browser (BITB), gdje napadač unutar postojeće web stranice simulira prozor preglednika ili OAuth „pop-up" za prijavu (npr. „Prijavi se s Googleom"), koji zapravo nije sustavski prozor nego pažljivo dizajniran HTML/CSS element [54]. NordLayer opisuje kako se u BITB napadima oponaša vizualni izgled preglednika: naslovna traka, gumbi za zatvaranje, URL traka i čak ikona lokota [54]. Korisnik tako dobiva dojam da se otvara zaseban, siguran prozor, a zapravo cijeli sadržaj kontrolira napadač. Ovo je izrazito opasno u kombinaciji s SSO (Single Sign-On) servisima, jer kompromitacija jednog takvog „prozorčića" često znači i pristup nizu povezanih poslovnih aplikacija.

Još jedan ključan element je manipulacija SSL/TLS certifikatima i „https" indikatorom. Korisnici su često naučeni da prisutnost lokota znači sigurnost, no to je samo indikator enkripcije veze, a ne pouzdanosti same stranice. Heroku u dokumentaciji o self-signed certifikatima objašnjava kako je moguće generirati vlastite certifikate koji nisu izdani od

pouzdanih CA entiteta, ali i dalje mogu stvoriti dojam „zaštićene“ veze u određenim scenarijima [55]. Istovremeno, servisi poput Let’s Encrypt omogućuju automatizirano i besplatno izdavanje valjanih certifikata, što je iznimno korisno za legitimne administratore, ali i napadači mogu vrlo brzo dobiti „pravi“ certifikat za lažnu domenu registriranu isključivo za phishing [57]. Kombinacijom typosquattinga i valjanog TLS certifikata, napadači postižu da phishing stranica izgleda vizualno gotovo identično originalu, uključujući i „https“ oznaku, čime se ruši jedna od osnovnih korisničkih obrambenih heuristika.

Tehnika malicious email attachments i dalje je jedna od klasičnih, ali je u kombinaciji s modernim phishingom postala sofisticiranija. Proofpoint opisuje kako napadači koriste privitke u obliku dokumenata (Word, Excel, PDF), ZIP arhiva ili izvršnih datoteka koji sadrže makro-skripte, ugrađene linkove ili exploit kod [58]. Umjesto izravnog slanja .exe datoteka, danas se češće šalju dokumenti s „Enable Content“ ili „Enable Macros“ upozorenjem, gdje korisnik vlastitim klikom omogućuje pokretanje skripte. Takve skripte zatim preuzimaju malver, otvaraju „tihi“ komunikacijski kanal prema C2 poslužitelju ili pokreću dodatne faze napada. U mnogim kampanjama privitak ne sadrži sam malver, nego služi samo kao prvi korak koji korisnika vodi na malicioznu web stranicu, kombinirajući tako tehniku privitka i URL phishinga [58].

Sve izraženiji problem su i tehnike zaobilaženja višefaktorske autentikacije (MFA bypass). SecureWorld navodi nekoliko glavnih pristupa kojima se napadači služe: phishing proxy poslužitelji koji „u stvarnom vremenu“ prosljeđuju korisnikove vjerodajnice i MFA kod legitimnom servisu, napadi „MFA fatigue“ (ponavljana slanja push zahtjeva dok korisnik iz nervoze ne prihvati), preusmjeravanje SMS kodova kroz SIM-swap ili zlonamjerne aplikacije, te iskorištavanje rezervnih kodova ili fallback mehanizama [59]. U tzv. real-time proxy napadima, žrtva se preko phishing stranice zapravo spaja na legitimni servis, a napadač „stoji u sredini“, promatra login proces i presreće vjerodajnice i MFA tokene [59]. Time se razbija uvjerenje da je MFA „srebrni metak“ - napad ostaje phishing, ali je tehnički znatno napredniji i zahtijeva temeljitu obranu na razini preglednika, e-mail gatewaya i korisničke edukacije.

Sve ove tehnike često se ne koriste izolirano, nego kao dio lančanog napada. Tipičan scenarij može izgledati ovako: napadač registrira typosquatting domenu s valjanim Let’s Encrypt certifikatom [51], [57], obfuscira JavaScript kod koji prikuplja vjerodajnice [52], [53], maskira URL kroz servis za skraćivanje i redirect lanac [56], a zatim žrtvi pošalje e-mail s malicioznim privitkom koji kroz „sigurnosnu obavijest“ navodi na klik [58]. Kada žrtva otvori link, dočekuje je BITB prozor s lažnim SSO loginom koji zatim kroz phishing proxy presreće i lozinku i MFA token [54], [59]. Tehnički slojevi i psihološke poruke pritom djeluju zajedno, ali upravo ove opisane tehnike čine kostur tehničke strane phishing kampanje.

Razumijevanje najčešćih tehničkih tehnika phishing napada ključno je za dizajn obrambenih mjera. Sigurnosni timovi moraju računati na to da napadači više ne šalju „grube“ e-mailove s očitim greškama, nego kombiniraju URL spoofing, typosquatting, obfuscation, zlouporabu TLS certifikata, maliciozne privitke i MFA bypass u jedinstven, dobro isplaniran lanac. Obrana zato treba uključivati stroge kontrole domena i certifikata, napredne sustave za analizu URL-ova i skripti, sandboxing privitaka, detekciju real-time proxy obrazaca te kontinuiranu nadogradnju sigurnosnih politika i alata koji prate evoluciju ovih tehnika.

4.5. Obrana od phishing napada

Učinkovita obrana od phishing napada zahtijeva kombinaciju tehničkih mehanizama, organizacijskih politika i kontinuirane edukacije korisnika. Suvremeni radovi o phishingu naglašavaju da niti jedna pojedinačna mjera nije dovoljna: zaštita mora biti višeslojna i obuhvaćati sve razine – od mrežne i aplikacijske infrastrukture do konfiguracije mail servera i ponašanja samih korisnika [60], [61], [62]. Ključnu ulogu imaju pravilno konfigurirani e-mail sustavi (SMTP, SPF, DKIM, DMARC), arhitektura mail servera, abuse mehanizmi (RBL liste, anti-spam sustavi), odabir pouzdanih transakcijskih e-mail servisa te ispravno upravljanje domenama i DNS zapisima [63], [64], [65].

Simple Mail Transfer Protocol (SMTP) temeljni je protokol za razmjenu e-mail poruka na internetu. Dizajniran je u vrijeme kad sigurnost nije bila primarni fokus, pa mu je izvorno nedostajala autentikacija pošiljatelja i provjera integriteta sadržaja. Upravo ta povijesna naslijeđena „otvorenost“ čini ga idealnim vektorom za phishing – napadač relativno jednostavno može lažirati adresu pošiljatelja (spoofing) i poslati poruku koja naizgled dolazi od banke, poslodavca ili druge pouzdane institucije [60], [61]. U osnovi, SMTP funkcionira kao razgovor između klijenta (pošiljateljev mail server) i poslužitelja (primateljev mail server), gdje se kroz niz naredbi (HELO/EHLO, MAIL FROM, RCPT TO, DATA) prenosi poruka od izvorišnog do odredišnog servera. Problem nastaje jer polje „MAIL FROM“ i zaglavlje „From:“ nisu inherentno kriptografski zaštićeni – bez dodatnih mehanizama, primatelj nema jamstvo da je pošiljatelj doista onaj za koga se predstavlja [60]. Znanstveni radovi o phishingu naglašavaju da se većina napada oslanja upravo na ovu slabost – napadači registriraju relativno slične domene, šalju poruke putem legitimno izgledajućih SMTP relaya i koriste stvarne SPF/DKIM propuste organizacija kako bi povećali vjerojatnost isporuke u inbox [61], [62]. Zato se zaštita ne može svesti samo na sadržaj poruke (filtere), nego mora početi od razine protokola i identiteta domene pošiljatelja.

Kako bi se nadoknadile sigurnosne slabosti SMTP-a, uvedena su tri ključna standarda: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) i DMARC (Domain-

based Message Authentication, Reporting and Conformance). Zajedno čine temeljnu tehničku liniju obrane od spoofinganih phishing poruka [60], [63], [64]. SPF je mehanizam kojim vlasnik domene u DNS zapis (TXT) upisuje popis IP adresa i/ili servera koji smiju slati e-mail „u ime“ te domene. Kada primateljev server zaprimi poruku, provjerava poklapa li se IP pošiljatelja s ovim zapisom. Ako se IP ne nalazi u SPF politici, server može označiti poruku kao sumnjivu ili je odbaciti [63], [64]. SPF sam po sebi ne štiti sadržaj poruke, ali otežava korištenje tuđe domene za slanje phishing e-mailova. DKIM uvodi kriptografsku autentikaciju: pošiljateljev mail server digitalno potpisuje određene dijelove poruke (zaglavlja i/ili tijelo) privatnim ključem, dok se javni ključ objavljuje u DNS-u kao TXT zapis. Primatelj može verificirati potpis – ako je poruka izmijenjena ili je poslana od neovlaštenog servera, potpis neće biti ispravan [63]. DKIM tako osigurava integritet i djelomičnu autentičnost poruke, smanjujući mogućnost manipulacije sadržajem u tranzitu.

DMARC je „nadogradnja“ na SPF i DKIM. Omogućuje vlasniku domene da definira politiku: što napraviti s porukama koje ne prolaze SPF/DKIM provjere (npr. prihvatiti, označiti kao sumnjive ili odbaciti), te gdje slati izvještaje o neuspjelim provjerama [64]. Ključan koncept DMARC-a je „alignment“ – poruka prolazi DMARC samo ako je domena u From: zaglavlju usklađena s domenom korištenom za SPF i/ili DKIM. Time se smanjuje mogućnost da napadač koristi neku drugu, tehnički ispravnu domenu, a vizualno imitira legitimnu organizaciju. Pravilno implementirani SPF, DKIM i DMARC značajno smanjuju uspješnost klasičnog e-mail spoofinga. Međutim, studije pokazuju da mnoge organizacije ili nemaju ispravno konfigurirane zapise, ili koriste previše „meke“ politike (npr. DMARC = none), čime efektivno ne iskorištavaju puni potencijal ovih standarda [60], [61], [64]. Stoga je ispravna konfiguracija i redovito praćenje DMARC izvještaja ključan dio obrane od phishing kampanja.

Arhitektura mail servera važan je element u obrani od phishing napada jer određuje kako se poruke primaju, filtriraju, analiziraju i pohranjuju. Tipična arhitektura obuhvaća više komponenti: MTA (Mail Transfer Agent), MDA (Mail Delivery Agent), filtre za spam i zlonamjerni sadržaj, antivirusne motore, te sustave za logiranje i nadzor [60], [61]. Istraživanja pokazuju da su najotporniji sustavi oni koji uvode slojevitu obranu: na ulazu greylisting, provjera reverznih DNS zapisa, SPF/DKIM/DMARC validacija, provjera protiv RBL (Real-time Blackhole List) lista, te osnovna reputacijska analiza IP adrese i domene pošiljatelja [60], [61]; na sadržajnoj razini analiziranje URL-ova u poruci, heuristička i signaturna detekcija malicioznih privitaka, sandbox analiza sumnjivih datoteka i mašinsko učenje za detekciju phishing obrazaca [62], [63]; te na izlazu kontrola volumena slanja, zaštita od kompromitiranih računa (npr. nagli skok broja poslanih poruka), DMARC usklađenost i monitoring reputacije vlastitih IP-eva. Moderni radovi naglašavaju i važnost segmentacije mail infrastrukture: odvajanje servera za interne poruke od onih za vanjsku komunikaciju, odvajanje transakcijskih

e-mailova (npr. reset lozinke, potvrde plaćanja) od marketinških kampanja, kao i uvođenje zasebnih domena ili poddomena za različite tipove komunikacije [61], [63]. Takva arhitektura smanjuje rizik da kompromitacija jednog dijela sustava dovede do potpune reputacijske štete domene ili do širenja phishing kampanje iznutra.

Abuse mehanizmi predstavljaju prvu liniju obrane mrežne zajednice od masovnih phishing kampanja. Riječ je o sustavima koji prate, kategoriziraju i blokiraju izvore zlonamjernog prometa, najčešće kroz RBL liste, reputacijske sustave i napredne anti-spam filtere [60], [61], [62]. RBL (Real-time Blackhole List) su liste IP adresa i domena za koje je utvrđeno da šalju spam ili sudjeluju u zlonamjernim aktivnostima. Mail serveri mogu u realnom vremenu provjeriti nalazi li se IP pošiljatelja na jednoj ili više takvih lista, te na temelju toga donijeti odluku o odbijanju poruke ili njenom označavanju kao sumnjive [60]. Anti-spam sustavi kombiniraju bayesovske filtre, signaturne baze, URL reputation baze, analizu strukture poruke i algoritme strojnog učenja, što omogućuje detekciju i složenih phishing poruka koje izbjegavaju tradicionalne filtere [61], [62]. Međutim, napadači kontinuirano prilagođavaju svoje taktike – mijenjaju IP adrese, koriste kompromitirane legitimne račune, rotiraju domene i kodiraju URL-ove – pa je korelacija više izvora podataka nužna za održavanje učinkovitosti.

Organizacije mogu birati između izgradnje vlastitog mail servera i korištenja komercijalnih transakcijskih e-mail servisa poput AWS Simple Email Service (SES), Mailgun ili SendGrid. Custom mail server pruža potpunu kontrolu nad konfiguracijom, integracijom, logovima i sigurnosnim pravilima, ali zahtijeva stalno održavanje i praćenje reputacije [60], [61]. AWS SES i slični servisi nude upravljanu infrastrukturu, ugrađenu reputacijsku zaštitu, automatiziranu konfiguraciju SPF/DKIM zapisa i napredne abuse mehanizme, što smanjuje rizik pogrešne konfiguracije i povećava isporučivost [63], [64]. Preporučuje se hibridni pristup – interne komunikacije preko vlastite infrastrukture, a masovni e-mail promet preko odvojenih poddomena i komercijalnih servisa, čime se smanjuje ukupna izloženost napadima i reputacijski rizik [61], [63].

Upravljanje domenama i DNS zapisima predstavlja temelj svih tehnoloških mjera protiv phishinga. Bez precizne DNS konfiguracije, SPF, DKIM i DMARC ne mogu pravilno funkcionirati, što otvara mogućnost zloupotrebe domene i smanjuje učinkovitost cjelokupnog sustava zaštite [63], [65]. DNS Made Easy i slični servisi naglašavaju važnost pravilnog postavljanja A, MX, TXT, CNAME i NS zapisa, uz posebnu pažnju na SPF, DKIM i DMARC TXT zapise koji definiraju autentikacijske politike [65]. Preporučuje se korištenje odvojenih poddomena za transakcijske, marketinške i automatizirane poruke, redovito praćenje isteka domene, zaštita registrarskog računa dvofaktorskom autentikacijom i monitoring registracije sličnih (homoglyph, typosquatting) domena koje napadači mogu koristiti u phishing kampanjama [60], [63]. Sve ove prakse – od SMTP konfiguracije, SPF/DKIM/DMARC

mehanizama, arhitekture mail servera, abuse sustava, odabira e-mail servisa do upravljanja domenama i DNS-om – zajedno čine tehnički temelj obrane od phishing napada. Bez njih, čak i najbolja korisnička edukacija ostaje nedovoljna, jer napadači i dalje mogu isporučivati uvjerljivo izgledajuće poruke iz lažiranih ili kompromitiranih izvora.

4.6. Najistaknutiji cyber napadi temeljeni na socijalnom inženjeringu

Socijalni inženjering i phishing napadi predstavljaju jedan od najučinkovitijih i najrasprostranjenijih oblika kompromitacije organizacija. Za razliku od tehničkih napada koji zahtijevaju iskorištavanje specifičnih ranjivosti sustava, socijalno-inženjerski napadi ciljaju na ljudsku psihologiju, rutinu i povjerenje. Upravo zato u praksi postižu iznimno visoke stope uspješnosti i sve češće su inicijalna faza većih sigurnosnih incidenata. Kao što ističe literatura [42], većina globalno najpoznatijih provala započela je jednostavnom manipulacijom zaposlenika, lažnim e-mailom ili vještim impersonacijskim tehnikama.

Napadi prikazani u Tablici 1 odražavaju spektar mogućih posljedica – od financijskih gubitaka i krađe podataka do kompromitacije kritične infrastrukture. Posebno zabrinjava činjenica da pogođene organizacije uključuju najveće globalne korporacije s visokorazvijenim sigurnosnim sustavima. To potvrđuje ključnu tezu da najslabija karika sigurnosti ostaje čovjek, bez obzira na količinu tehnologije ili ulaganja u obranu.

Organizacija / godina	Vrsta napada	Opis napada	Posljedice
Saudi Aramco (2021.)	Phishing + ransomware	Zaposlenici kompromitirani phishing e-mailom koji je omogućio inicijalni pristup mreži	Krađa TB podataka, zahtjev za otkupninom od 50 mil. USD
Microsoft (2021.)	Phishing	Masovno slanje lažnih e-mailova korisnicima s ciljem krađe vjerodajnica	Financijski gubici, reputacijska šteta
Marriott (2018.–2020.)	Phishing + malware	Phishing poruke korištene kao ulazna točka za dugotrajan pristup sustavima	Krađa osobnih podataka milijuna gostiju
Twitter (2020.)	Spear-phishing + impersonacija	Napadači kompromitirali interne alate i verificirane račune	Prijevare, reputacijska šteta, gubitak povjerenja
Toyota Boshoku Corporation (2019.)	BEC napad	Lažna e-mail komunikacija s financijskim odjelom	Gubitak ~37 mil. USD

Privatna žrtva (UK)	Deepfake voice phishing	Imitacija glasa CEO-a korištenjem AI tehnologije	Neovlašteni prijenos sredstava
Google i Facebook (2013.–2015.)	BEC prijevara	Lažno predstavljanje dobavljača putem e-maila	Ukupni gubici >100 mil. USD

Tablica 1: Prikaz nekih phishing napada

Primjer Saudi Aramca (2021.) pokazuje kako jednostavni phishing može dovesti do kompromitacije terabajta podataka i zahtjeva za otkupninom od 50 milijuna USD. Slučaj Microsoftovih korisnika iste godine ilustrira kako čak i relativno mali financijski iznosi, kad se multipliciraju na velik broj žrtava, stvaraju ozbiljne posljedice i reputacijsku štetu. Napadi na Marriott (2018.–2020.) pokazuju kako phishing poruka može poslužiti kao ulazna točka za instalaciju malicioznog softvera, krađu vjerodajnica i dugoročan pristup osjetljivim bazama podataka.

U slučaju Twittera (2020.), napadači su se oslonili na impersonaciju i spear-phishing kako bi kompromitirali verificirane račune s milijunima pratitelja, a zatim iskoristili njihov utjecaj za širenje prijevara. Financijski napadi poput incidenta nad Toyota Boshoku Corporation (2019.) i prijevare usmjerene na Shark Tank voditelja potvrđuju da su BEC (Business Email Compromise) napadi iznimno učinkoviti kad su poruke precizno usmjerene prema izvršnim funkcijama. Posebno je zabrinjavajući slučaj iz Ujedinjenog Kraljevstva, gdje je CEO prevaren deepfake glasovnom porukom – ranim primjerom zlouporabe generativne umjetne inteligencije unutar socijalnog inženjeringa. Konačno, višegodišnja prevara nad Googleom i Facebookom, vrijedna više od 100 milijuna USD, ukazuje da ni tehnološki giganti nisu imuni na sofisticirane manipulacije financijskim procesima.

Ovi slučajevi zajedno potvrđuju da je socijalni inženjering univerzalno učinkovit napadni vektor koji nadilazi branše, veličine i tehničku zrelost organizacija. Bez sustavne edukacije, stalnog testiranja i višeslojne obrane, čak i najnapredniji sigurnosni sustavi ostaju ranjivi na napade koji zaobilaze tehnologiju i ciljaju – čovjeka.

5. Jeshka

Jeshka predstavlja integrirani praktični framework razvijen za provedbu cjelovitih OSINT postupaka te izvođenje sofisticiranih phishing kampanja. Sustav objedinjuje modularne komponente za prikupljanje podataka, njihovu analizu, automatizirano generiranje personaliziranih poruka, upravljanje infrastrukturom za slanje e-mailova i praćenje metrika kampanje. U praktičnom dijelu rada prikazuje se arhitektura frameworka, funkcionalnosti pojedinih modula te tehnički procesi koji omogućuju da jeskha bude upotrebljiv u stvarnim operativnim scenarijima, uz minimalne dodatne nadogradnje.

5.1. Arhitektura baze podataka

Arhitektura baze podataka unutar jeskha sustava i dalje je temeljna komponenta cijelog frameworka. Sustav koristi jednu centraliziranu SQLite bazu definiranu putem config.DB_PATH, dok se logična izolacija postiže putem polja search_org_id i source_batch u gotovo svim tablicama. Na taj način baza funkcionira kao robusno informacijsko središte u kojem se podaci odvajaju po organizaciji i kampanji na logičkoj razini, ali ostaju unutar jedne optimizirane baze – što pojednostavljuje backup, analitiku, dijeljenje i razvoj.

Relacijski model i dalje je izgrađen oko dva osnovna entiteta - organizacija i osoba - ali je veći naglasak stavljen na domenu kao stabilan identifikator organizacije. Tablica organizations sada, uz jedinstveno ime, eksplicitno čuva i polje domain te pripadajući search_org_id. Organizacija se kreira ili pronalazi prvenstveno preko domene (npr. hpb.hr, otpbanka.hr), koju sustav automatski izvlači iz naziva firme, URL-a ili same email adrese. Funkcija normalize_org_id dodatno normalizira sve varijante (URL, email, čisti tekst) u kanonsku domenu - uklanja protokol, www, razmake i podvlake, a po potrebi dodaje i TLD (.hr). Time se različiti oblici iste organizacije (npr. www.hpb.hr, info@hpb.hr, hpb) u bazi svode na jedan konzistentan identitet.

Tablica persons proširena je poljem search_org_id i dodatnim metapodacima (source, source_batch, date_found), čime svaka osoba postaje precizno vezana uz organizaciju, izvor i kampanju. Poseban wrapper insert_person brine se da se full_name uvijek ispravno generira, dok funkcija insert_or_get_person osigurava da ista osoba unutar iste organizacije i istog search_org_id ne bude unesena više puta. Time se postiže stabilnost identiteta i konzistentnost baze čak i kada ista osoba dolazi iz različitih batch datoteka (scraping, LinkedIn, ručni import).

Kontakt podaci i dalje se pohranjuju u zasebne tablice: emails, phones, addresses, banks, oibs, ibans, pri čemu je svaki zapis vezan uz organization_id, opcionalni person_id, izvor, source_batch, datum i search_org_id. Tablica emails zadržava ključno polje is_pattern koje razlikuje stvarne, na webu pronađene adrese od onih koje su infiltrirane ili generirane prema uzorku (pattern). Novi mehanizmi, poput funkcija save_found_emails_to_db i import_pattern_results_to_db, omogućuju da se emailovi pronađeni Google/Brave pretragama ili generirani na temelju otkrivenog uzorka za ime i prezime automatski uvežu s odgovarajućom organizacijom i osobom. I u tom procesu koristi se kanonska domena i search_org_id, tako da svi podaci ostaju uredno grupirani.

Tablica social_profiles dodatno učvršćuje vezu između LinkedIn podataka i ostatka sustava. Svaki društveni profil (osobito LinkedIn) pohranjuje se uz person_id i organization_id, platformu, URL, poziciju, lokaciju, naziv kompanije, te source_batch i search_org_id. Funkcija insert_social_profile direktno upisuje profile iz LinkedIn batchova u ovu tablicu, čime se OSINT rezultati s društvenih mreža integriraju u isti graf odnosa kao i ostali identifikatori (emailovi, IBAN-i, adrese).

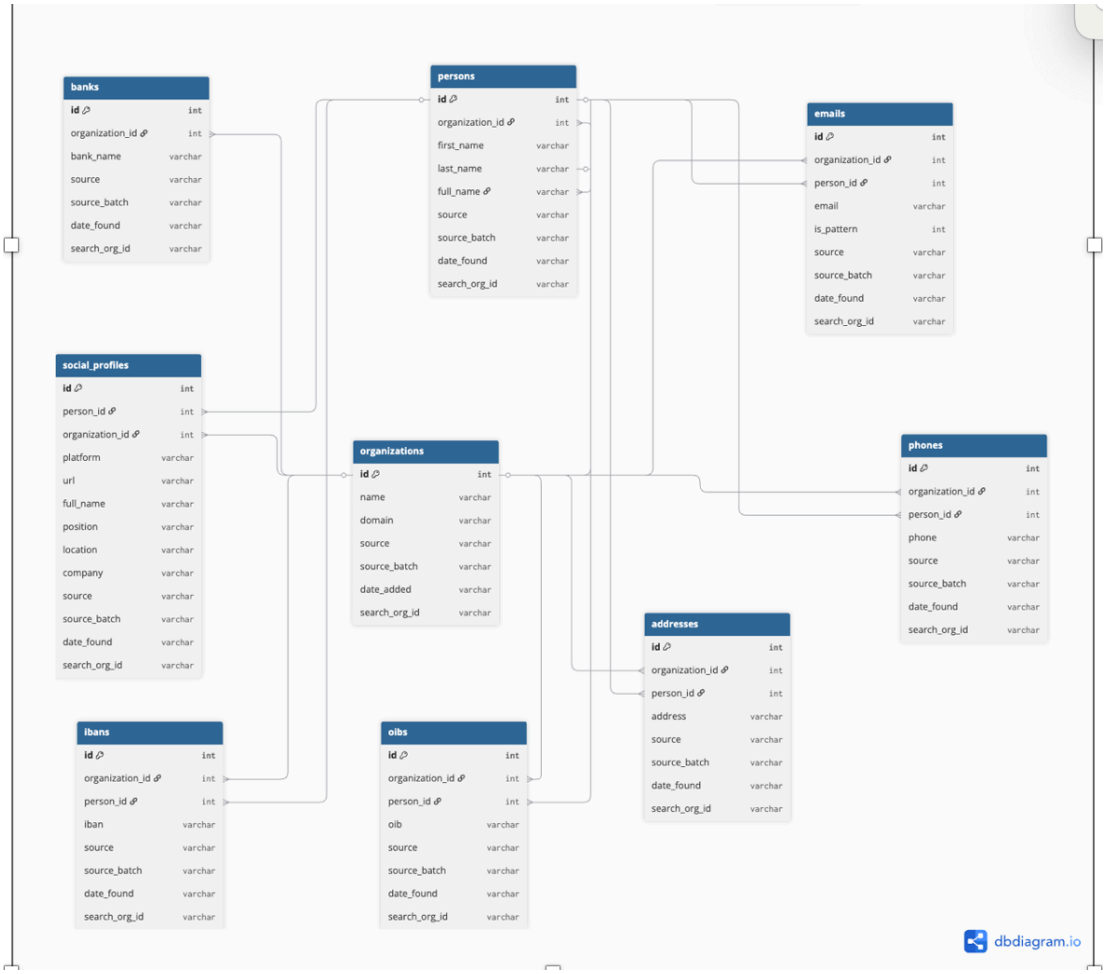
Tablice oibs i ibans imaju jedinstvena ograničenja na poljima oib i iban, što sprječava dupliciranje i čuva integritet financijskih identifikatora čak i kad se ponavljaju u više dokumenata i izvora. Tablica files_found evidentira sve pronađene dokumente (npr. PDF, XLSX) s njihovim URL-ovima, datumom i search_org_id, što omogućuje praćenje odakle su potekli određeni podaci i lakšu reviziju izvora.

Središnji tehnički element arhitekture više nije samo shema tablica, nego automatiziran i robustan uvozni pipeline koji stoji iza funkcije import_all_batches. Ona prolazi kroz sve .txt batch datoteke u zadanoj mapi, otvara ih jednu po jednu i procesira svaku liniju. Svaka linija se prvo sanitizira funkcijom sanitize_line, koja briše kontrolne znakove. Zatim funkcija line_already_imported izračunava MD5 hash linije i provjerava postoji li već u tablici imported_lines. Ako hash postoji, linija se potpuno preskače. Ako ne postoji, hash se upisuje i linija se po prvi put procesira. Time sustav postiže jaku idempotentnost: isti batch može biti pokrenut više puta, sustav se može rušiti, restartati ili dobiti duple ulaze - baza ipak ostaje čista, bez duplikata.

Nakon hash provjere, funkcija parse_line detektira format podatka. Ako je linija JSON, parsira se u Python objekt i, po potrebi, dodaju se polja emailovi, osobe i firma. Ako je linija tabličnog formata (email, ime, izvor), parser je pretvara u standardizirani zapis. U oba slučaja u strukturu se dodaje batch_file, što omogućuje kasnije vezanje na source_batch. Tako pripremljeni podaci predaju se funkciji insert_txt_batch, koja u strogo definiranom redoslijedu popunjava sve relevantne tablice: izračuna org_domain, pronađe ili kreira organizaciju, kreira

ili pronalazi osobe, povezuje emailove s osobama, dodaje telefone, IBAN-e, OIB-e, adrese, banke i eventualne društvene profile. U svakoj fazi koristi se INSERT OR IGNORE, čime se dodatno smanjuje rizik dupliciranja, a search_org_id se konzistentno postavlja na vrijednost izvedenu iz naziva batch datoteke (funkcija clean_batch_name).

Dodatnu zaštitu pruža i datoteka processed_batches.log, u koju se nakon uspješne obrade upisuje ime svakog batcha. Prilikom slijedećih pokretanja import_all_batches najprije čita taj log i preskače već obrađene batch fileove, što sprječava nenamjerno ponovno procesiranje istih izvora. U kombinaciji s hash provjerama na razini linije, ovaj mehanizam čini uvozni sustav izuzetno otpornim na korisničke pogreške, prekide rada i ponovne importe.



Slika 3: Shema baze podataka (Izvor: vlastita izrada)

5.2. Modul scraping interneta

Ovaj modul predstavlja centralni OSINT pretraživačko–scraperski sustav koji integrira više izvora podataka, inteligentnu obradu sadržaja i višeslojnu logiku filtriranja i ekstrakcije

informacija. Temeljna svrha modula jest omogućiti automatizirano prikupljanje javno dostupnih informacija o organizacijama i njihovim povezanim entitetima, uključujući e-mail adrese, telefonske brojeve, adrese, IBAN brojeve, podatke o tvrtkama, osobama te poveznice na dokumente kao što su PDF, Word i Excel datoteke. Ključna snaga sustava leži u kombiniranju više metoda pretraživanja, lokalnog cacheiranja, robustnog sustava parsiranja HTML-a i inteligentnog prepoznavanja hrvatskih imena, prezimena i adresa putem unaprijed pripremljenih nacionalnih baza.

Modul podržava dinamičko učitavanje API ključeva za Google Custom Search i Brave Search te LinkedIn vjerodajnica, čime se omogućuje fleksibilno upravljanje konfiguracijom tijekom izvođenja. Svaka funkcija koja ovisi o tim postavkama automatski ih osvježava kako bi se osiguralo korištenje aktualnih parametara. Nadalje, modul implementira sofisticiran sustav cacheiranja koji sprema prethodno pretražene URL-ove i ranije učitane HTML stranice, čime se značajno smanjuje broj mrežnih zahtjeva i ubrzava obrada velikih količina podataka. Osim toga, sustav može identificirati već procesirane URL-ove iz prethodnih scraping batch datoteka, što omogućuje izbjegavanje dupliciranja i optimizaciju izvođenja.

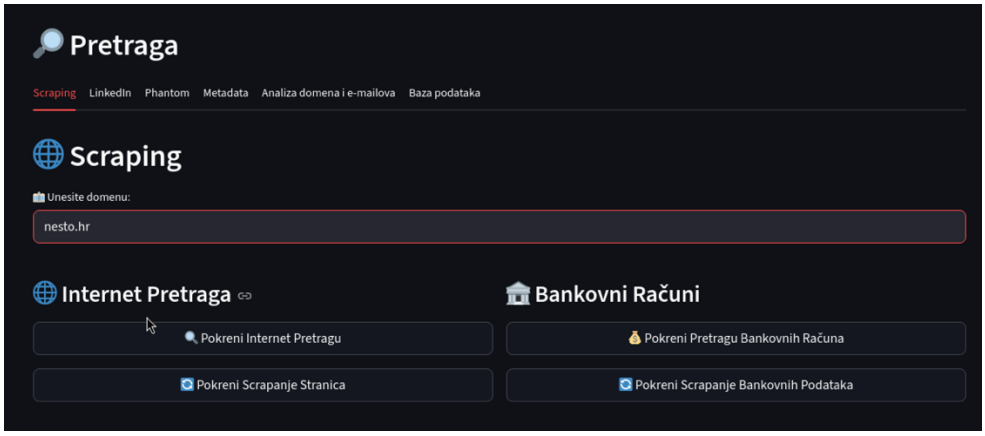
Pretraživanje interneta provodi se prvenstveno preko Google CSE API-a, uz opsežan set specifično konstruiranih upita usmjerenih na pronalaženje poslovnih e-mail adresa, imena zaposlenika, javnih dokumenata, financijskih podataka i kontaktnih informacija. U slučaju nedostupnosti Google API-ja automatski se aktivira Brave Search API kao backup. Rezultati se objedinjeni, filtriraju i spremaju u lokalni cache. Posebna varijanta pretraživanja namijenjena je otkrivanju IBAN-ova i žiro računa, što se postiže ciljanjem obrasca ključnih riječi povezanih s financijskim dokumentima i računima.

Scraper dio modula odgovoran je za dohvat, identifikaciju i obradu pojedinačnih URL-ova. Funkcija za scraping najprije analizira HTTP zaglavlja i heuristički detektira radi li se o dokumentu (npr. PDF-u) čak i u slučajevima kada poslužitelj lažno označi sadržaj kao HTML. Takvi dokumenti odmah se registriraju u SQLite bazu podataka kao pronađeni files. Ako se radi o HTML stranici, izvlače se svi tekstualni segmenti te se dodatno analiziraju poveznice koje unutar stranice vode na dokumente. Tek nakon toga se pristupa dubinskoj ekstrakciji korisnih informacija.

Najopsežniji dio modula čini funkcija za ekstrakciju korisnih informacija, koja uz pomoć BeautifulSoup-a, regularnih izraza i nacionalnih baza podataka prepoznaje sve relevantne entitete. Emailovi, IBAN-i, OIB-i i brojevi telefona identificiraju se preciznim regex pravilima. Adrese se otkrivaju naprednim algoritmom koji uspoređuje pojedine segmente teksta s hrvatskim ulicama i gradovima, validira kućne brojeve i uklanja lažne pozitivne rezultate. Sustav također prepoznaje nazive tvrtki putem višestupanjske logike koja analizira pravne

oznake, e-mail domene, HTML naslove, meta oznake i samu URL strukturu. Identifikacija osoba provodi se kombiniranjem hrvatskih imena i prezimena kako bi se prepoznale jedno-, dvo- i troslovne strukture osobnih imena.

Na kraju, cijeli proces batch scrapinga radi kao orkestrirani sustav koji filtrira neželjene URL-ove (npr. društvene mreže, medijske datoteke), obrađuje samo nove rezultate te sve pronađene podatke sprema u strukturirane .txt datoteke kako bi se omogućila daljnja analiza, uvoz u baze ili korištenje unutar phishing modula. Modul je projektiran tako da bude robustan, skalabilan i prilagođen velikim OSINT operacijama te pruža visoku preciznost u identifikaciji stvarnih osoba, entiteta i dokumenata unutar hrvatskog digitalnog prostora.



Slika 4: Prikaz modula scraping (Izvor: vlastita izrada)

Na slici vidimo korisničko sučelje modula *Scraping Pretrage*, koje predstavlja početni korak automatiziranog OSINT procesa. U gornjem dijelu nalazi se polje za unos domene ciljanog subjekta, a ispod njega četiri gumba koji pokreću različite faze internet pretrage. Ovaj modul povezan je s funkcijama implementiranim u datoteci *tools.py*, gdje se nalazi kompletna logika Google dorkinga, Brave API pretrage i scraping mehanizama.

Prvi gumb pokreće Internet Pretragu, gdje se nad unesenom domenom izvršava veliki skup unaprijed definiranih Google dorking upita. Ti upiti ciljaju kontakte, zaposlenike, PDF dokumente, poslovne direktorije i druge javne izvore. Rezultati se prikupljaju putem Google Custom Search API-ja i Brave Search API-ja te se zatim spremaju u lokalni cache kako bi se izbjegla ponovna pretraživanja.

Drugi gumb pokreće Pretragu Bankovnih Računa, specijalizirani skup dorkova usmjeren na pronalaženje IBAN-ova, računa, predračuna, uplata i ostalih financijskih dokumenata povezanih s organizacijom. Modul prepoznaje i dokumente poput PDF-ova te ih sprema u zasebnu internu bazu kako bi se kasnije mogli analizirati.

Treći gumb aktivira Scrapanje Stranica, proces koji prolazi kroz sve prethodno prikupljene URL-ove i za svaki poziva funkciju scrape_page(). Ona detektira kontakt podatke, adrese, brojeve telefona, IBAN-ove, OIB-eve, PDF datoteke i ostale korisne entitete. Sustav uključuje i napredne mehanizme prepoznavanja “skrivenih” dokumenata, provjere content-type zaglavlja i posebne filtere za eliminaciju nerelevantnih stranica.

Četvrti gumb koristi isti scraping mehanizam kao i standardno scrapanje stranica, ali se primjenjuje nad URL-ovima dobivenima iz specijalizirane pretrage bankovnih i financijskih dokumenata, čime se omogućuje izdvajanje IBAN-ova i povezanih financijskih podataka.

5.3. Modul Linkedin scrapanja

LinkedIn modul predstavlja cjeloviti podsustav unutar razvijene OSINT platforme i implementiran je u jednoj programskoj datoteci *linkedin.py*. Modul je dizajniran za automatizirano otkrivanje, prikupljanje i parsiranje LinkedIn profila zaposlenika ciljanih organizacija, uz naglasak na robusnost, skalabilnost i minimaliziranje detekcije od strane same platforme LinkedIn. Arhitektura modula temelji se na jasno definiranoj hijerarhiji metoda prikupljanja podataka, pri čemu se alati i tehnike aktiviraju sekvencijalno, ovisno o dostupnosti i ograničenjima pojedinog pristupa.

Primarni mehanizam LinkedIn OSINT-a u sustavu temelji se na Selenium automatizaciji uz korištenje stvarnog Firefox profila s aktivnom LinkedIn korisničkom sesijom. Ovaj pristup omogućuje pristup funkcionalnostima koje su nedostupne neautentificiranim korisnicima, poput pretraživanja zaposlenika unutar organizacija i prikaza rezultata temeljenih na internim LinkedIn parametrima.

Glavna ulazna točka modula je funkcija *run_linkedin_dorking*, koja orkestrira cijeli proces pronalaska LinkedIn profila. U prvom koraku modul pokušava identificirati službenu LinkedIn company stranicu ciljne organizacije korištenjem Google Custom Search i Brave Search dorking tehnika. Pretraga se provodi nad semantičkim varijantama naziva organizacije kako bi se povećala vjerojatnost pronalaska ispravne company stranice.

Ako je company stranica uspješno pronađena, aktivira se primarna metoda pretraživanja zaposlenika, koja koristi LinkedInov interni parametar *currentCompany*. U tom se koraku, koristeći Selenium i stvarni Firefox profil, generira stranica s rezultatima zaposlenika poveznih s identificiranom organizacijom. Stranica se dinamički scrolla, a iz HTML sadržaja se izdvajaju sve poveznice na LinkedIn profile oblika *linkedin.com/in/*. Ova metoda predstavlja najpouzdaniji i najpreciznij način prikupljanja profila te se koristi kao prvi izbor u hijerarhiji.

U slučaju da identifikator tvrtke (*company_id*) nije moguće pouzdano izvući iz HTML-a ili LinkedIn ograniči pristup pretraživanju temeljenom na parametru *currentCompany*, modul automatski prelazi na sekundarnu metodu – People tab pretraživanje. Ova metoda koristi Selenium za otvaranje *People* podstranice company profila, uz simulaciju korisničkog ponašanja (scrollanje, pomicanje miša), te prikupljanje svih dostupnih LinkedIn profila prikazanih na stranici. Iako manje precizna od primarne metode, People tab predstavlja pouzdanu alternativu u slučaju ograničenja primarnog pristupa.

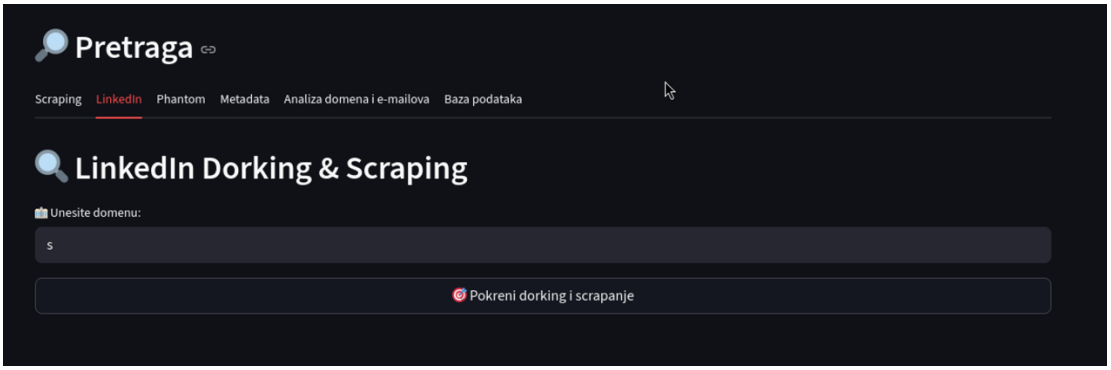
Ako niti jedna od metoda temeljenih na izravnoj interakciji s LinkedIn platformom nije dostupna, modul kao posljednju liniju obrane koristi dorking nad javnim webom. U tom slučaju generiraju se napredni Google i Brave pretraživački upiti koji ciljaju indeksirane LinkedIn profile povezane s organizacijom, koristeći kombinacije naziva tvrtke, radnih pozicija i geografskih pojmova. Ova metoda ima najniži prioritet u hijerarhiji i koristi se isključivo kao fallback kada autentificirani pristupi nisu mogući.

Svi pronađeni LinkedIn profili, neovisno o metodi prikupljanja, spremaju se u cache datoteku *search_linkedin_org_.json*, čime se omogućuje ponovna uporaba rezultata i izbjegavanje nepotrebnih ponovljenih pretraga.

Druga ključna funkcionalna cjelina modula implementirana je u funkciji *run_linkedin_scraping*, koja je zadužena za masovno scrapanje samih LinkedIn profila. Funkcija učitava URL-ove iz cache datoteke i sekvencijalno otvara svaki profil koristeći Selenium i isti Firefox profil s aktivnom sesijom. Iz HTML sadržaja profila parsiraju se osnovni atributi, uključujući puno ime, radni naslov, lokaciju i trenutnu organizaciju. Prikupljeni podaci spremaju se u strukturirane batch datoteke unutar direktorija *batches*, pri čemu svaki red predstavlja jedan JSON zapis profila.

U slučaju gubitka Selenium sesije, preusmjeravanja na LinkedIn login stranicu ili pojave tehničke greške tijekom učitavanja profila, modul automatski aktivira Playwright fallback mehanizam. U tom se scenariju profil učitava u headless Firefox instanci putem Playwrighta, ponovno parsira pomoću BeautifulSoup-a, te se - ako je dohvat uspješan - rezultat ravnopravno pohranjuje zajedno s ostalim podacima. Playwright se u sustavu koristi isključivo kao fallback i nikada ne zamjenjuje primarni Selenium pristup.

Opisani dizajn jasno definira hijerarhiju korištenih metoda: Selenium uz stvarni Firefox profil predstavlja primarni mehanizam, People tab i *currentCompany* pretraživanja služe kao sekundarne metode unutar LinkedIna, javni web dorking koristi se kao krajnja alternativa, dok Playwright ima isključivo ulogu tehničkog fallbacka. Takav pristup omogućuje stabilan, dugotrajan i skalabilan rad LinkedIn OSINT modula čak i u uvjetima pojačanih sigurnosnih ograničenja i aktivnih anti-bot mehanizama.



Slika 5: Prikaz modula Linkedin (Izvor: vlastita izrada)

Na slici je prikazano korisničko sučelje LinkedIn modula unutar OSINT platforme, namijenjenog dorkanju i scrapanju LinkedIn profila povezanih s određenom organizacijom. Modul je osmišljen kao jedinstvena ulazna točka za prikupljanje podataka o zaposlenicima tvrtki te objedinjuje fazu pretrage (dorking) i fazu analize profila (scraping).

U prvom koraku korisnik unosi domenu ciljne organizacije (npr. pbz.hr, otp.hr), koja se koristi kao polazna vrijednost za generiranje semantičkih varijanti naziva tvrtke. Te se varijante zatim koriste za automatsko pretraživanje LinkedIna i javnog weba s ciljem pronalaska povezanih LinkedIn profila zaposlenika, menadžera i drugih relevantnih osoba.

Klikom na gumb „Pokreni dorking i scrapanje“ aktivira se kompletan automatizirani proces. Sustav najprije pokušava pronaći službenu LinkedIn company stranicu ciljne organizacije koristeći Google Custom Search i Brave Search dorking. Ako je company stranica pronađena, modul koristi Selenium i Firefox preglednik sa stvarnim korisničkim profilom i aktivnom LinkedIn sesijom kako bi dohvaćao profile zaposlenika putem LinkedIn parametra currentCompany. U slučaju ograničenja ili neuspjeha ove metode, sustav se automatski prebacuje na People tab pretraživanje, koje se temelji na scrollanju stranice i ekstrakciji svih linkedin.com/in/ poveznica iz HTML sadržaja. Ako niti ta metoda nije dostupna, koristi se klasični web dorking kao završni fallback.

Svi pronađeni LinkedIn URL-ovi spremaju se u lokalni JSON cache, čime se osigurava da se sljedeće faze mogu pokretati bez ponavljanja pretrage. Nakon toga započinje faza scrapanja profila, u kojoj se svaki URL iz cachea pojedinačno posjećuje. Primarno se koristi Selenium s istim Firefox profilom, dok se u slučaju gubitka sesije, redirekcije na login ili tehničke greške automatski aktivira Playwright fallback. Playwright omogućuje stabilnije i brže učitavanje stranica te služi kao dodatni sloj otpornosti sustava.

Tijekom scrapanja iz svakog LinkedIn profila izdvajaju se ključni podaci kao što su puno ime, radni naslov (headline), lokacija i trenutna organizacija. Rezultati se zapisuju u strukturirane batch datoteke unutar sustava, čime se omogućuje daljnja analiza, pohrana u bazu podataka ili integracija s ostalim OSINT modulima.

5.4. Modul PhantomBuster

PhantomBuster modul je samostalan podsustav unutar OSINT arhitekture diplomskog rada, iako je u potpunosti kompatibilan i integriran s već postojećim LinkedIn modulom. Za razliku od tradicionalnih scraping metoda koje se oslanjaju na browser automatizaciju, ovaj modul koristi eksterni servis PhantomBuster za masovno dohvaćanje LinkedIn profila. Modul je koncipiran tako da automatizira sve faze rada - pripremu podataka, izgradnju Google Sheet ulazne tablice, pokretanje PhantomBuster agenata preko API-ja, praćenje njihovog statusa i preuzimanje rezultata. Ova razina automatizacije omogućuje stabilno i skalabilno prikupljanje podataka, ali zadržava potpunu samostalnost: modul može raditi odvojeno, bez potrebe da ostatak LinkedIn modula bude aktivan.

U uvodnoj fazi rada modul učitava lokalni cache LinkedIn URL-ova i pretvara ga u Google Sheet dokument pomoću Google Drive API-ja. Ovaj korak je nužan jer PhantomBuster zahtijeva da ulazni podaci budu predočeni putem javno dostupne Google tablice. Modul stvara novu tablicu, puni je URL-ovima i automatski ju postavlja kao javno čitljivu, čime se uklanja potreba za ručnim posredovanjem i ubrzava cjelokupan proces. Ujedno se vodi i lokalni cache linkova prema tablicama kako bi se omogućio ponovni rad bez nepotrebnog dupliciranja.

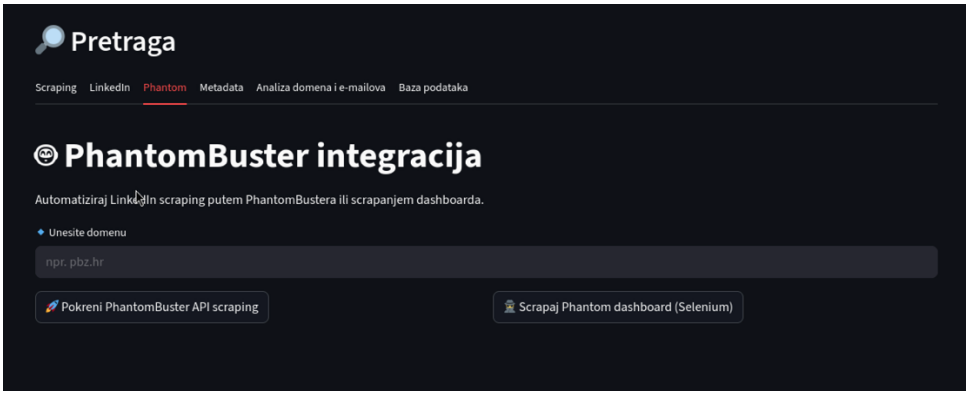
Središnji dio modula oslanja se na PhantomBuster API. Modul provjerava dostupnost agenta, čeka njegovo oslobađanje, pokreće novo izvršenje i prati status koristeći dva različita API endpointa - jedan za provjeru trenutačnog stanja, a drugi za povijest izvršavanja. Time se postiže potpun uvid u životni ciklus zadatka, uključujući detekciju faza *running*, *success* i *failed*. Nakon završetka scraping kampanje, modul koristi API kako bi pokušao preuzeti CSV datoteku s rezultatima. Međutim, ključan detalj je da PhantomBuster CSV eksport nije dostupan na besplatnom planu, što znači da u praksi korisnik često ne može preuzeti rezultate kroz službeni API.

Upravo zbog tog ograničenja modul uključuje i alternativni mehanizam - Selenium scraper za PhantomBuster dashboard. Scrapanje dashboarda omogućuje dobivanje rezultata čak i kada CSV eksport nije dostupan, odnosno kada korisnik koristi samo besplatni PhantomBuster račun. Modul automatski ulazi u korisnički panel, pronalazi tablicu s rezultatima, otkriva sve redove i prepoznaje strukturu bez obzira na to je li dashboard smješten unutar iframea. Implementirani su i pouzdani mehanizmi paginacije koji klikaju gumb “Next” i

prelaze na sljedeće stranice rezultata, sve dok ne iscrpe zadani dataset. Ova funkcionalnost omogućuje visoku razinu pokrivenosti dostupnih rezultata.

Parser dashboard tablice koristi više heuristika za pronalaženje relevantnih polja: imena, prezimena, radne pozicije, kompanije, lokacije, headlinea i LinkedIn URL-a. Rezultati se dedupliciraju i spremaju u batch datoteke u istom formatu koji koristi ostatak OSINT sustava. Time se osigurava potpuna interoperabilnost bez obzira potječu li podaci iz API-ja, CSV-a ili direktnog scrapanja web sučelja.

U konačnici, PhantomBuster modul funkcionira kao neovisna i skalabilna komponenta može raditi potpuno samostalno, ali i kao napredni dodatak LinkedIn scraperu. Njegova najveća prednost je sposobnost masovnog prikupljanja LinkedIn podataka bez opasnosti od LinkedIn blokada, uz istovremenu mogućnost zaobilaženja ograničenja besplatnog PhantomBuster plana putem Selenium scrapanja dashboarda. Modul tako predstavlja najpouzdaniji i najautomatiziraniji mehanizam unutar cijelog OSINT pipelinea.



Slika 6: Prikaz modula PhantomBuster (Izvor: vlastita izrada)

Na priloženoj slici prikazano je sučelje modula *PhantomBuster integracija*, koje omogućuje automatizirano prikupljanje LinkedIn podataka koristeći PhantomBuster. Modul je dizajniran tako da pokriva oba scenarija rada: standardni scraping putem API-ja te alternativni scraping dashboarda u slučajevima kada PhantomBuster CSV eksport nije dostupan.

Korisnik najprije unosi domenu organizacije kako bi odredio skup LinkedIn URL-ova koji će se procesirati. Nakon toga su ponuđene dvije funkcije. Gumb *Pokreni PhantomBuster API scraping* koristi službeni PhantomBuster API za pokretanje LinkedIn extractora. Korisnik ručno unosi svoj API ključ, Phantom ID i li_at cookie, nakon čega modul automatski pokreće agenta, čeka dovršetak i preuzima sve rezultate u JSON formatu. Ova metoda predstavlja primarni i najpouzdaniji način rada.

Druga opcija, *Scrapaj Phantom dashboard (Selenium)*, namijenjena je upravo situacijama kada se CSV datoteke ne mogu preuzeti – što je čest slučaj kod besplatnog PhantomBuster plana. Budući da dashboard omogućuje pregled rezultata, ali ne i izvoz, implementiran je Selenium scraper koji se automatski prijavljuje u PhantomBuster korisnički račun, otvara odgovarajući dashboard, prolazi kroz sve stranice tablice i prikuplja podatke direktno iz HTML-a. Time se nadomješta funkcionalnost CSV eksport-a bez potrebe za plaćenim planom.

Ovaj modul tako omogućuje potpunu fleksibilnost LinkedIn scrapanja – bilo korištenjem API-ja kada je dostupan, bilo zaobilaskom ograničenja besplatne verzije putem dashboard scrapanja.

5.5. Metadata modul

Metadata modul predstavlja samostalnu komponentu OSINT sustava namijenjenu obradi i analizi datoteka pronađenih tijekom pretraživanja internetskih izvora. Iako je u potpunosti odvojen od LinkedIn i PhantomBuster modula, integriran je u širi OSINT pipeline tako što koristi zajedničku SQLite bazu podataka i automatizirano preuzima sve URL-ove prikupljene scraping procesima. Primarna svrha modula jest sustavno analizirati dokumente i slike, izdvojiti njihove metapodatke te ih strukturirano pohraniti u namjensku tablicu files_metadata, omogućujući naknadnu analizu, verifikaciju podataka i korelaciju informacija unutar OSINT nadzorne ploče.

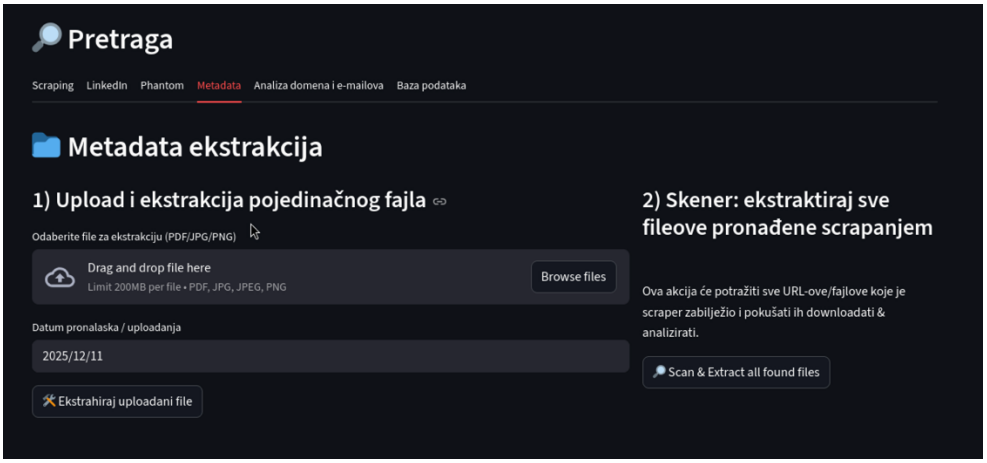
Modul radi u dvije osnovne paradigme. Prva se odnosi na obradu lokalno učitanih datoteka, primjerice PDF-ova ili slika koje korisnik učita kroz OSINT dashboard. Takve datoteke spremaju se u lokalni cache, identificiraju po sigurnoj hash vrijednosti te prolaze kroz specijalizirane interpretere poput PyPDF2 za PDF dokumente i exifread biblioteke za EXIF podatke slika. Iz PDF-ova se izvlače osnovni metapodaci, uključujući naslov, autora, vrijeme kreiranja, kao i tekstualni isječak s prve stranice. Kod slika se prikupljaju EXIF tagovi, ako postoje, što može uključivati informacije o korištenom uređaju, vremenu snimanja i geolokaciji. Svi dobiveni podaci pohranjuju se kao JSON zapis, čime se osigurava dosljednost i fleksibilnost pohrane različitih vrsta metapodataka.

Drugi način rada modula odnosi se na automatsko procesiranje eksternih datoteka pronađenih tijekom web scrapinga. Modul pretražuje sve tablice u SQLite bazi i identificira stupce koji sadrže URL-ove. Svaki URL koji upućuje na potencijalni dokument preuzima se u lokalni cache, a datoteka se zatim analizira kao i kod lokalnih uploadova. Posebna pažnja posvećena je detekciji lažnih ili irelevantnih datoteka - primjerice, HTML redirect stranica koje se maskiraju kao dokumenti, posebno kod servisa poput LinkedIna ili servisa sa zaštitnim

“authwall” mehanizmima. Modul takve datoteke automatski filtrira i izbjegava pohranu, čime se povećava točnost i efikasnost cijelog OSINT procesa.

Svaka obrađena datoteka dobiva jedinstvenu hash vrijednost, metapodatke, vrijeme preuzimanja, veličinu i originalni URL, te ulazi u tablicu files_metadata. Na taj način modul omogućuje centralizirano praćenje svih dokumenata koji se pojavljuju tijekom OSINT istrage, uključujući interne PDF-ove organizacija, obrasce, financijske dokumente, ugovore, skenove i slike. Budući da se metadata modul može pokretati samostalno, u batch modu, ili kroz korisničko sučelje, omogućuje fleksibilnost u radu i služi kao važan korak u automatiziranom izvlačenju informacija i strukturiranju podataka iz nestrukturiranih izvora.

U konačnici, metadata modul pridonosi OSINT sustavu tako što nadopunjuje standardne scraping metode dubinskom analizom sadržaja, što značajno proširuje mogućnosti identifikacije obrazaca, razotkrivanja izvora dokumenata i razumijevanja digitalnih tragova pronađenih tijekom istrage. Njegova samostalnost omogućuje jednostavno održavanje i skaliranje, a njegova integracija s bazom podataka omogućuje njegovu uporabu kao temeljne komponente unutar većih OSINT operacija.



Slika 7: Prikaz modula Metadata (Izvor: vlastita izrada)

Na prikazanoj slici nalazi se sučelje modula *Metadata ekstrakcija*, koje omogućuje analizu dokumenata pronađenih tijekom OSINT postupka. Modul je podijeljen u dva funkcionalna dijela, jasno označena brojevima.

U lijevom dijelu nalazi se opcija *Upload i ekstrakcija pojedinačnog fajla*. Korisnik može povući ili učitati PDF, JPG, JPEG ili PNG datoteku, odabrati datum pronalaska te pokrenuti analizu klikom na *Ekstrahiraj uploadani file*. Na taj se način obrađuju pojedinačni dokumenti koji možda nisu došli iz automatskog scrapinga. Nakon učitavanja, sustav sprema datoteku u

lokalni cache, iz nje izvlači metapodatke (PDF meta-info, EXIF podaci za slike, hash, veličinu, tekstualni snippet) te ih trajno zapisuje u SQLite tablicu *files_metadata*.

Desni dio sučelja nudi mogućnost *Skeniranja i ekstrakcije svih fajlova pronađenih scrapanjem*. Ova funkcija pretražuje sve URL-ove koje je scraper prethodno označio kao dokumente, pokušava ih automatski preuzeti te izvući odgovarajuće metapodatke. Posebna logika detektira i preskače HTML redirecte i authwall stranice (primjerice LinkedIn login), kako bi se izbjegla pogrešna obrada. Svaki uspješno obrađeni fajl također se zapisuje u bazu zajedno s pripadajućim metapodacima.

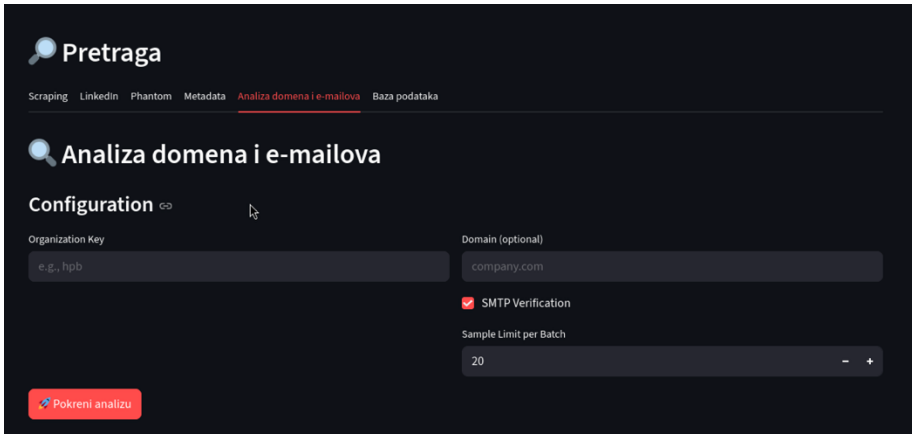
5.6. Modul analize domena i mailova

Modul za analizu domena i e-mail adresa predstavlja jednu od najkompleksnijih i najinteligentnijih komponenti OSINT sustava. Njegova je uloga višestruka: provjerava valjanost i postojanje domena, otkriva e-mail obrasce organizacija (pattern inference), pronalazi stvarne e-mail adrese dostupne na internetu, automatski generira nove adrese za kompletnu listu zaposlenika te validira njihov status korištenjem DNS-a, reputacijskih servisa i SMTP testova. Iako je u potpunosti samostalan modul, duboko je integriran s LinkedIn scrapingom i bazom podataka - koristi LinkedIn batch datoteke za detekciju imena zaposlenika, a rezultate automatski sprema u centraliziranu bazu radi daljnje OSINT obrade.

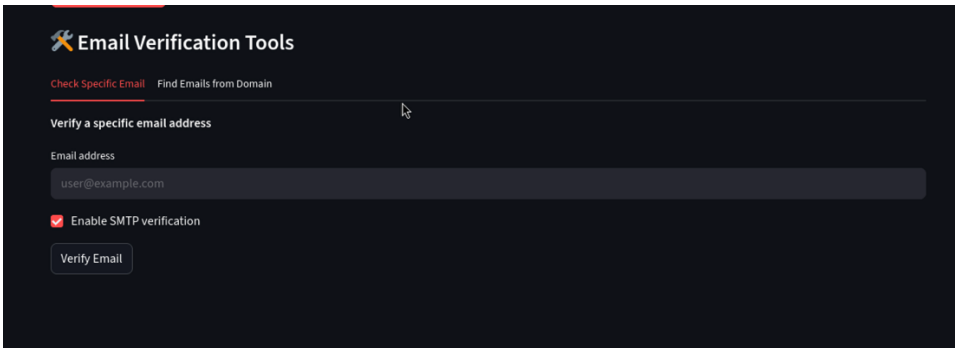
Analiza započinje provjerom domene organizacije. Modul izdvaja sve moguće domene iz preuzetih batch datoteka, provodi DNS analizu (uključujući MX zapise) i detektira postoji li aktivni web poslužitelj. Time se eliminiraju lažne, tipografski pogrešne ili nepostojeće domene koje se često pojavljuju u OSINT projektima, osobito kod phishing priprema. Nakon toga modul prelazi na identifikaciju postojećih e-mailova na internetu koristeći Google Custom Search API, Brave Search API i više fallback mehanizama. Ti rezultati služe kao “ground truth” na temelju kojeg modul izvlači stvarni obrazac građenja e-mail adresa unutar određene organizacije. Detekcija patterna uključuje analizu lokalnog dijela adrese i njegovo usklađivanje s normaliziranim LinkedIn imenima, uz prepoznavanje obrazaca poput *ime.prezime*, *iimeprezime*, *i.prezime*, *prezime.ime* i mnogih drugih. Kada se prepoznati obrazac ponavlja u dovoljnom broju, modul automatizirano generira e-mail adrese za sve osobe iz LinkedIn batcha.

U slučajevima kada se obrazac ne može zaključiti iz web rezultata, modul aktivira napredni SMTP brute-force mehanizam. Taj algoritam u realnom vremenu testira različite kombinacije e-mail formata koristeći RCPT TO naredbu na MX poslužitelju organizacije. Ako poslužitelj potvrdi postojanje barem jedne verzije adrese, modul proglašava obrazac detektiranim i primjenjuje ga na sve zaposlenike. Sustav sadrži i višeslojne mehanizme zaštite,

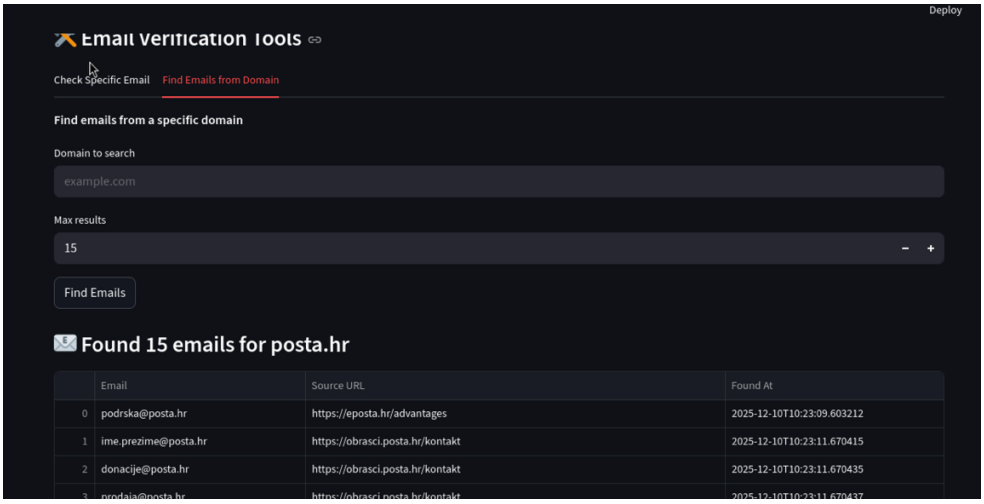
uključujući hlađenje (cooldown) nakon određenog broja neuspješnih upita kako bi se izbjegla blokada pošiljatelja i detekcija spam aktivnosti.



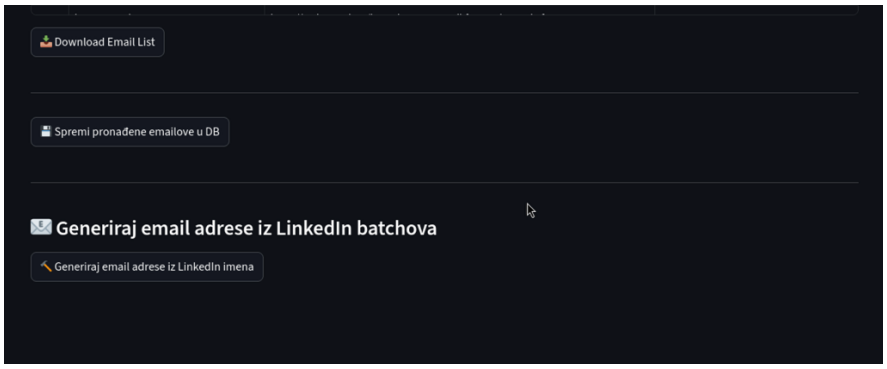
Slika 8: Prikaz dijela modula analize domena i emaila – analiza postojanja(Izvor: vlastita izrada)



Slika 9: Prikaz dijela modula analize domena i emaila – provjera postojanja pojedinačnog maila (Izvor: vlastita izrada)



Slika 10: Prikaz dijela modula analize domena i emaila – analiza postojanja po domeni 1.dio (Izvor: vlastita izrada)



Slika 11: Prikaz dijela modula analize domena i emaila – analiza postojanja po domeni 2.dio (Izvor: vlastita izrada)

Na prikazanim ekranima vidljiv je cjeloviti modul za analizu domena i e-mail adresa, koji objedinjuje provjeru tehničke ispravnosti domena, validaciju pojedinačnih adresa te pretragu i ekstrakciju većeg broja e-mailova iz javnih izvora. Modul je podijeljen u tri funkcionalne cjeline.

Prvi dio, Domain & Email Analysis konfiguracija, omogućuje unos organizacijskog ključa i opcionalne domene, nakon čega se provodi automatizirana provjera postojanja domene, pripadajućih DNS zapisa, dostupnosti web stranice te MX zapisa koji indiciraju postoji li valjana e-mail infrastruktura. Ovaj korak služi kao inicijalni “health-check” organizacijske domene prije bilo kakve daljnje analize. Dodatno se može uključiti i SMTP verifikacija, čime se procjenjuje može li domena prihvatiti poruke prema standardnom SMTP handshakeu. Parametar *Sample Limit per Batch* služi kao kontrola opterećenja prilikom analize većeg broja rezultata.

Drugi dio modula čini sekcija Email Verification Tools, u kojoj se nude dvije mogućnosti. Prva opcija omogućuje provjeru postojanja jedne konkretne e-mail adrese putem SMTP provjere. Ovo je korisno kada se želi pojedinačno potvrditi je li određeni korisnik aktivan ili je adresa nevažeća. Druga opcija, *Find Emails from Domain*, omogućuje pretragu javnih izvora (dorkanjem) za sve e-mail adrese povezane s određenom domenom. Korisnik unosi naziv domene i broj maksimalnih rezultata, nakon čega se prikazuje tablica pronađenih adresa, pripadajućih URL-ova te vremena pronalaska.

Nakon toga slijede dodatne funkcionalnosti nad rezultatima: preuzimanje tablice u CSV formatu, spremanje pronađenih adresa u bazu podataka, te pokretanje analize e-mail patterna i generiranje novih adresa. Na dnu modula nalazi se i opcija za generiranje e-mail adresa iz LinkedIn batchova, gdje se na temelju LinkedIn imena i ustanovljenog formata (ime.prezime@domena.hr, i.prezime@ itd.) automatski generiraju potencijalne e-mail adrese zaposlenika.

5.7. Modul za kloniranje web stranica

Modul za simulirano kloniranje web-stranica predstavlja centralni tehnički mehanizam sustava, razvijen isključivo za potrebe istraživanja, edukacije i demonstracije automatiziranih phishing tehnika u kontroliranom, neškodljivom i jasno označenom akademskom okruženju. Njegova je uloga omogućiti generiranje realističnih, ali potpuno bezopasnih i transparentnih replika postojećih web-stranica kako bi se proučavali vizualni elementi, obrasci interakcije korisnika i opća struktura modernih web-sučelja koja se u praksi često zloupotrebljavaju u pravim phishing napadima. Modul ne kreira funkcionalne kopije niti pokušava reproducirati originalne servisne funkcije - umjesto toga izrađuje statičnu HTML repliku s ugrađenim upozorenjima, akademskim disclaimerom i vlastitom simulacijskom formom koja ne prikuplja stvarne podatke.

Proces započinje Playwright renderiranjem stranice, čime se omogućuje dohvat potpunog HTML-a nakon što se svi dinamički elementi učitaju. Modul automatski detektira i prihvaća ili odbija cookie bannere kako bi dobio čistu i stabilnu verziju stranice. Nakon toga uklanja sve skripte i sigurnosne slojeve koji bi mogli utjecati na offline prikaz ili izazvati interakciju s izvornim serverom. Budući da moderni web intenzivno koristi vanjske CSS datoteke, modul te stilove automatski dohvaća i inline-a te prepravlja sve relativne putanje u apsolutne kako bi stranica ostala vizualno identična i kada se otvara lokalno ili na kontroliranom hosting poslužitelju. Paralelno se uklanjaju svi elementi koje bi korisnik mogao zamijeniti za originalne – osobito kolačićni slojevi, interaktivni widgeti i JS skripte.

Ključni sigurnosni element ovog modula je ugrađeni dvostruki banner s upozorenjem (na hrvatskom i engleskom jeziku) koji se automatski pojavljuje na vrhu svake simulirane stranice. Banner jasno naglašava da stranica nije stvarna, da se koristi isključivo u svrhe diplomskog rada te da ne prikuplja nikakve autentične podatke. Ovaj korak je nužan kako bi se modul uskladio s etičkim standardima i akademskim pravilima te spriječila svaka mogućnost pogrešne interpretacije.

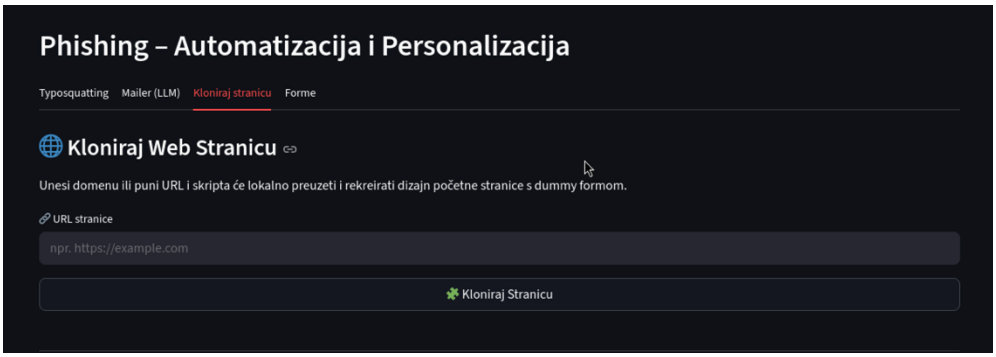
Nakon pripreme vizualnog okvira, modul ubacuje vlastitu kontakt formu estetski prilagođenu izvornom dizajnu stranice, koristeći analizu dominantnih boja. Forma šalje podatke lokalnom ili izoliranom poslužitelju koji simulira prikupljanje unosa, ali ne vrši nikakvu obradu stvarnih korisničkih informacija. To omogućuje testiranje tehničkih tokova, analizu korisničkog ponašanja i demonstraciju phishing mehanike bez ikakvog rizika ili narušavanja privatnosti. Modul također nudi mogućnost automatskog odabira vizualno najprikladnije boje gumba analizom slike iz zaglavlja ili unaprijed definirane pozadinske fotografije, čime se postiže uvjerljiv, ali i dalje simulirani izgled.

Drugi dio sustava čini hosting modul implementiran unutar *api.py*, koji omogućuje automatsko objavljivanje simuliranih stranica na posebno pripremljenoj akademskoj domeni. Kroz klasu *PhishingHostClient* korisnički sustav komunicira sa serverom putem definiranog API-ja koji podržava dva načina objave: upload pojedinačne HTML datoteke ili upload ZIP arhive cijelog foldera stranice. API na poslužitelju kreira direktorij prema nazivu kampanje, raspakira sadržaj te automatski generira javni URL u formatu *https://{site_name}.{HOSTING_DOMAIN}/*. Time se postiže jednostavan i dosljedan workflow objave: „kreiraj > pošalji > objavljeno“.

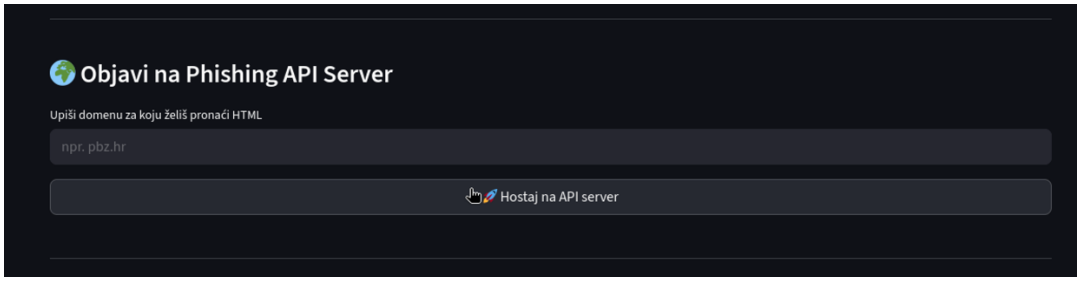
Hosting modul uključuje i funkcije za upravljanje objavljenim simulacijama, poput dohvaćanja popisa svih kampanja, njihovog brisanja te pregleda podataka poslanih kroz simulacijsku formu. Time se održava čisto i kontrolirano radno okruženje, bez nakupljanja starih pokusa. Budući da svaka objavljena stranica sadrži ugrađenu formu i jasno istaknuta etička upozorenja, moguće je simulirati kompletan tok phishing interakcija bez ugrožavanja privatnosti ili sigurnosti korisnika.

U cjelini, hosting modul predstavlja nužan nastavak modula za kloniranje: omogućuje da statična simulacija postane dostupna u stvarnom okruženju, gdje se može koristiti za istraživanje interakcija, demonstraciju phishing tehnika i analizu sigurnosnih prijetnji. U kombinaciji s webhook modulom za metrike, sustav čini zatvorenu cjelinu koja obuhvaća sve faze simulirane phishing kampanje - izgradnju stranice, objavljivanje, dostavu e-poruka i praćenje reakcija korisnika u realnom vremenu. Modul za simulirano kloniranje web-stranica tako funkcionira kao samostalna komponenta OSINT sustava, ali se logički naslanja na druge

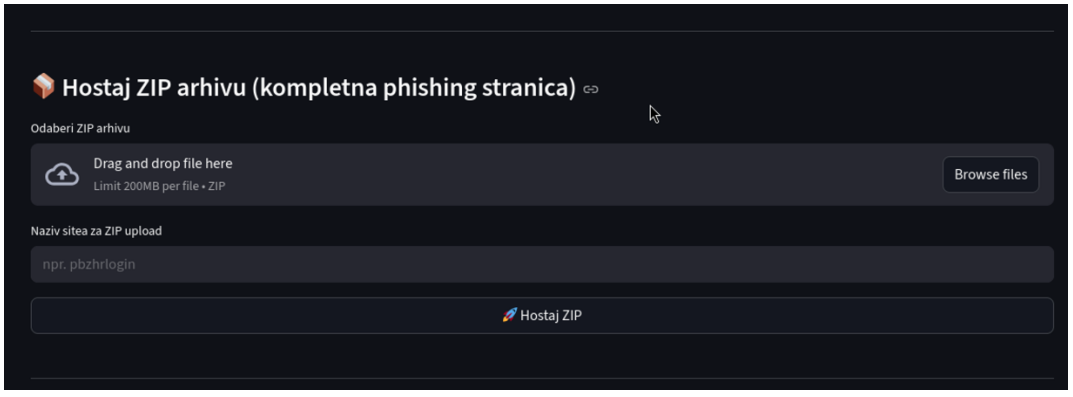
module poput LinkedIn scraping sustava i generatora e-poruka. Njegova svrha nije replicirati funkcionalnost izvornih stranica, nego pružiti visoko realističan, ali siguran model web-sučelja za istraživačke eksperimente, analizu sigurnosnih prijetnji i edukaciju o obrambenim tehnikama protiv phishing napada. Ovime se stvara kontrolirano okruženje u kojem je moguće proučavati automatizaciju phishing kampanja bez narušavanja zakonskih ili etičkih okvira.



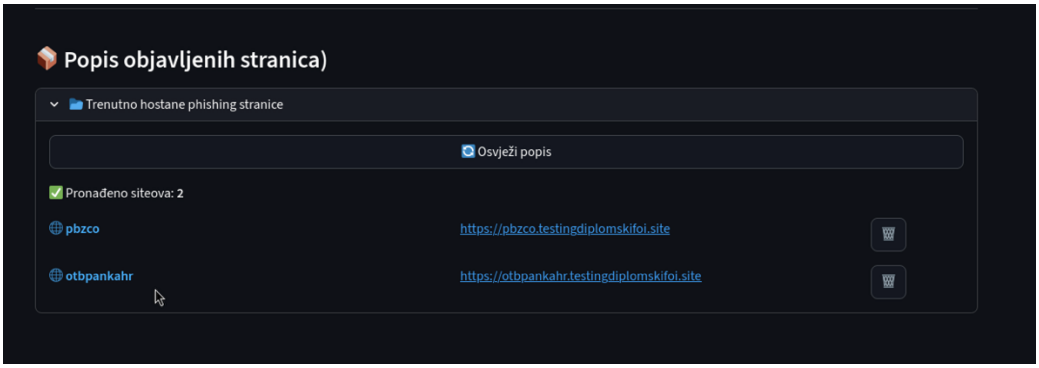
Slika 12: Prikaz dijela modula za kloniranje stranica – Kloniranje stranica (Izvor: vlastita izrada)



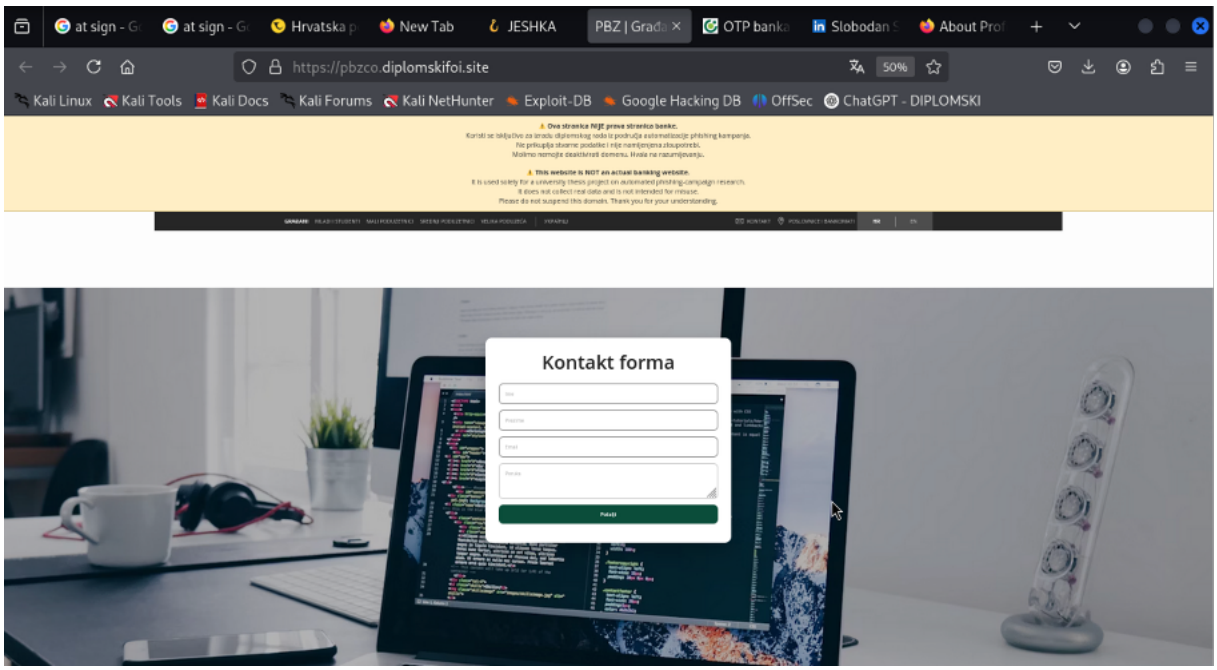
Slika 13: Prikaz dijela modula za kloniranje stranica – Objavljivanje kloniranih stranica (Izvor: vlastita izrada)



Slika 14: Prikaz dijela modula za kloniranje stranica – Objavljivanje zip datoteka (Izvor: vlastita izrada)



Slika 15. Prikaz dijela modula za kloniranje stranica – Popis objavljenih stranica (Izvor: vlastita izrada)



Slika 16: Prikaz klonirane stranice (Izvor: vlastita izrada)

Na prvoj slici prikazano je sučelje za kloniranje web stranice, gdje korisnik jednostavno unosi URL ciljanog weba, a skripta automatski preuzima HTML, stilove i slike kako bi lokalno generirala vizualno identičnu početnu stranicu. Umjesto stvarne forme, sustav ubacuje *dummy formu* koja omogućuje kasniju personalizaciju i povezivanje s backendom za phishing kampanju. Modul služi kao polazište za brzu izradu kopija legitimnih stranica, bez potrebe za ručnim pisanjem koda.

Druga sekcija omogućuje objavu generirane HTML stranice na phishing API server. Korisnik unosi naziv željene domene (najčešće typosquattana verzija originala), nakon čega se klikom na gumb HTML automatski šalje preko API-ja i postavlja na hosting sustav. Rezultat je potpuno funkcionalna phishing stranica dostupna javno putem poddomene koju korisnik

definira. Ovaj modul u potpunosti automatizira prijenos klonirane stranice iz lokalnog okruženja na operativni server.

Sljedeći dio sučelja omogućuje upload ZIP arhive kompletne phishing stranice. To je alternativa automatskom kloniranju i koristi se kada korisnik želi postaviti unaprijed pripremljenu, naprednu ili ručno modificiranu phishing stranicu. ZIP se učita u sustav, doda se naziv sitea, a API ga automatski raspakira i objavi kao novu phishing domenu. Na ovaj način moguće je hostati i kompleksnije stranice koje zahtijevaju dodatne resurse ili interaktivnost.

Zadnja slika prikazuje popis svih objavljenih phishing stranica. Sučelje omogućuje pregled trenutnog stanja hostanih poddomena, uključujući njihov naziv i direktan URL. Za svaku objavljenu instancu dostupna je opcija brisanja, kao i gumb za ručno osvježavanje popisa. Ova sekcija pruža centraliziranu kontrolu nad svim aktivnim phishing siteovima i omogućuje jednostavno upravljanje kampanjama.

5.8. Modul za generiranje mailova

Sustav za generiranje i distribuciju phishing-poruka implementiran je kao jedinstveni aplikacijski modul, sastavljen od više međusobno povezanih Python datoteka, od kojih svaka obavlja jasno definiranu ulogu unutar cjelokupnog procesa. Unutar tog modula objedinjene su funkcionalnosti za generiranje sadržaja, slanje poruka, upravljanje konfiguracijom i evidenciju događaja, čime se omogućuje potpuna automatizacija phishing kampanje – od pripreme poruka do njihove distribucije i analize.

Funkcionalnost slanja poruka realizirana je kroz datoteku manual_send_mail.py, koja implementira logiku za pojedinačno i masovno slanje e-mailova putem SMTP poslužitelja. Funkcija send_manual_smtp omogućuje slanje jedne poruke prema unaprijed definiranom primatelju, pri čemu se SMTP parametri (host, port, korisničko ime, lozinka i TLS postavke) dinamički učitavaju iz korisničke konfiguracije aplikacije. Radi povećanja vjerodostojnosti poruka, adresa pošiljatelja automatski se prilagođava tako da lokalni dio ostaje nepromijenjen, dok se domena rekonstruira iz naziva ciljane organizacije, čime se simulira komunikacija iz legitimnog poslovnog okruženja.

Masovno slanje poruka implementirano je funkcijom send_bulk_emails, optimiziranom za rad s većim skupovima primatelja. SMTP veza otvara se samo jednom, a sve se poruke šalju unutar iste sesije, čime se smanjuje broj autentikacija prema poslužitelju i rizik od blokiranja ili ograničenja prometa. Poruke se šalju u HTML formatu, a sustav ne implementira

dodatne mehanizme za praćenje otvaranja ili interakcije s porukama, budući da se takve funkcionalnosti u realnim okruženjima najčešće rješavaju na razini samog e-mail providera.

Generiranje sadržaja poruka ostvareno je unutar iste aplikacijske cjeline kroz datoteku ollama_mailer.py, koja je zadužena za izradu personaliziranih phishing-poruka pomoću velikih jezičnih modela. Sustav ne koristi statične predloške, već dinamički generira sadržaj na temelju dostupnih podataka o primatelju (ime i prezime, e-mail adresa, domena organizacije, pripadajući phishing URL i opcionalne korisničke upute).

Za potrebe realističnije simulacije socijalnog inženjeringa implementirana su dva semantički različita prompta, ovisno o odnosu primatelja prema organizaciji:

- prompt za zaposlenike, koji simulira internu komunikaciju (npr. IT sigurnosne obavijesti, obvezne treninge ili proceduralne zahtjeve),
- prompt za klijente, koji simulira vanjsku korisničku komunikaciju (npr. obavijesti o ažuriranju kontaktnih podataka ili sigurnosnim provjerama računa).

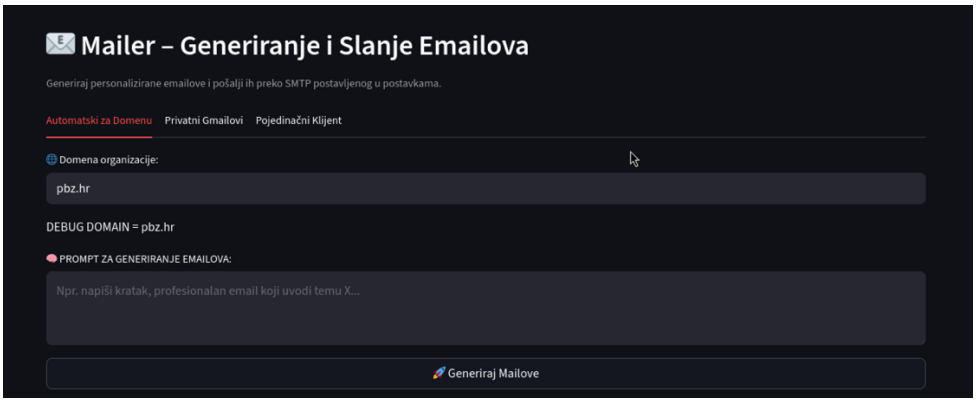
Odabir odgovarajućeg prompta ne vrši se ručno, već se automatski određuje analizom domene e-mail adrese primatelja. Ako se domena primatelja podudara s domenom unesene organizacije, poruka se generira korištenjem prompta za zaposlenike. U suprotnom slučaju (privatne e-mail adrese poput Gmaila ili e-mail adrese drugih organizacija) koristi se prompt za klijente. Takav pristup omogućuje kontekstno prilagođavanje poruka bez potrebe za dodatnom logikom na razini korisničkog sučelja.

U sklopu mehanizma za generiranje sadržaja implementirana je podrška za dva LLM providera: Groq API (model *llama-3.1-8b-instant*) i DeepSeek API (model *deepseek-chat*). Odabir jezičnog modela provodi se automatski na temelju dostupnosti API ključeva u konfiguraciji sustava. Ako je prisutan DeepSeek API ključ, sustav koristi DeepSeek kao primarni izvor za generiranje sadržaja, dok se u suprotnom automatski koristi Groq API kao zadana opcija. Takav pristup omogućuje fleksibilno upravljanje troškovima i dostupnošću bez potrebe za izmjenama u ostatku aplikacije.

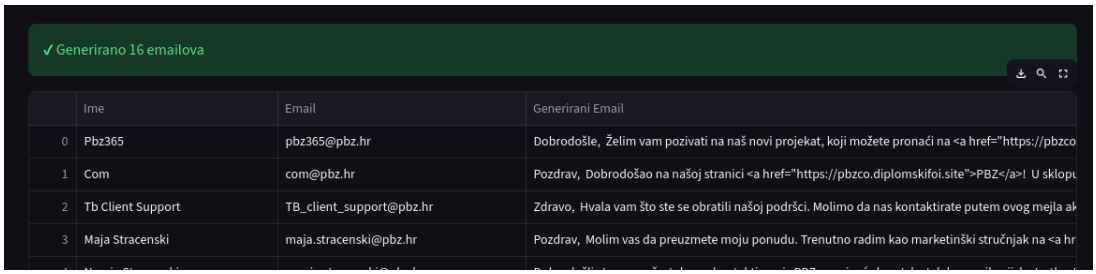
Sustav podržava generiranje pojedinačnih poruka (generate_email_single), poruka namijenjenih svim zaposlenicima određene organizacije (generate_emails_for_domain), kao i poruka usmjerenih prema privatnim e-mail adresama povezanim s organizacijom (generate_emails_for_related_gmail). Kako bi se optimizirala potrošnja API resursa i osigurala konzistentnost rezultata unutar jedne kampanje, svi generirani sadržaji pohranjuju se u lokalni cache.

Dodatno je implementiran mehanizam za automatsko pronalaženje pripadajuće phishing stranice (resolve_phishing_link), koji koristi lokalni popis hostanih stranica i fuzzy

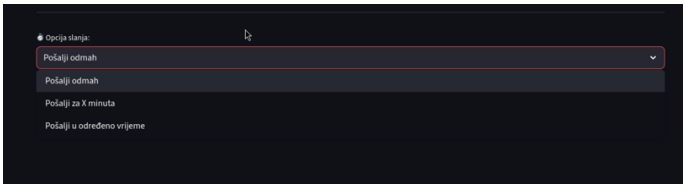
matching nad nazivom organizacije. Time se osigurava da svaka generirana poruka sadrži odgovarajući URL u ispravnoj HTML sintaksi. Upravljanje API ključevima riješeno je robusnim mehanizmom koji omogućuje dohvat vrijednosti iz aktivne sesije aplikacije, lokalne konfiguracijske datoteke ili konfiguracijskog modula, čime se smanjuje mogućnost pogrešaka u autentikaciji.



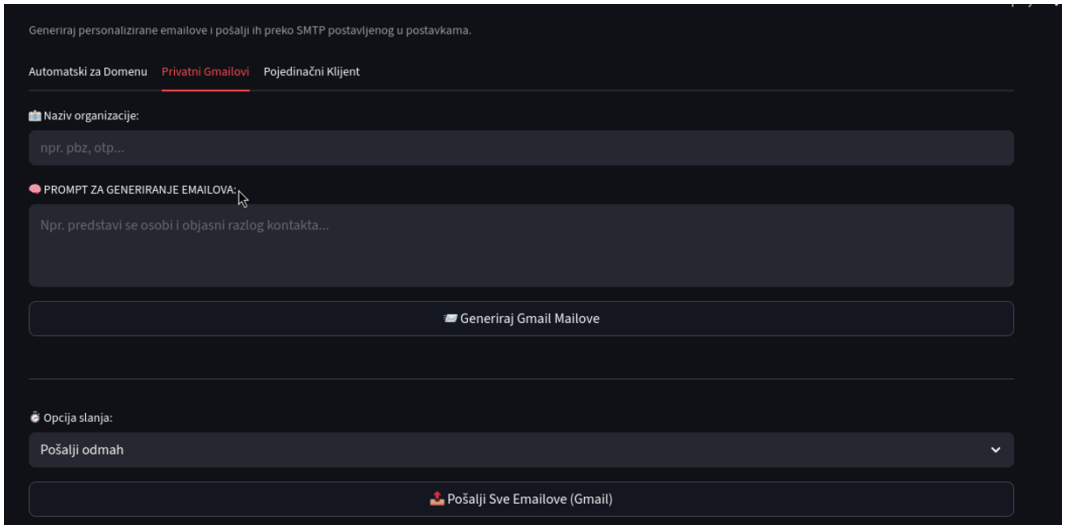
Slika 17: Prikaz dijela modula za generiranje mailova - 1. dio automatski za domenu kartice(Izvor: vlastita izrada)



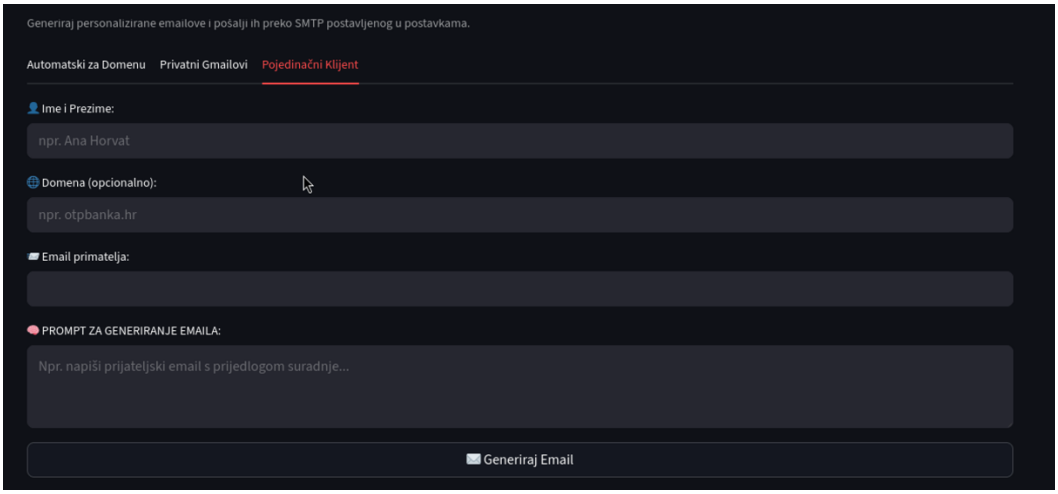
Slika 18: Prikaz dijela modula za generiranje mailova - 2. dio automatski za domenu kartice – prikaz generiranih mailova(Izvor: vlastita izrada)



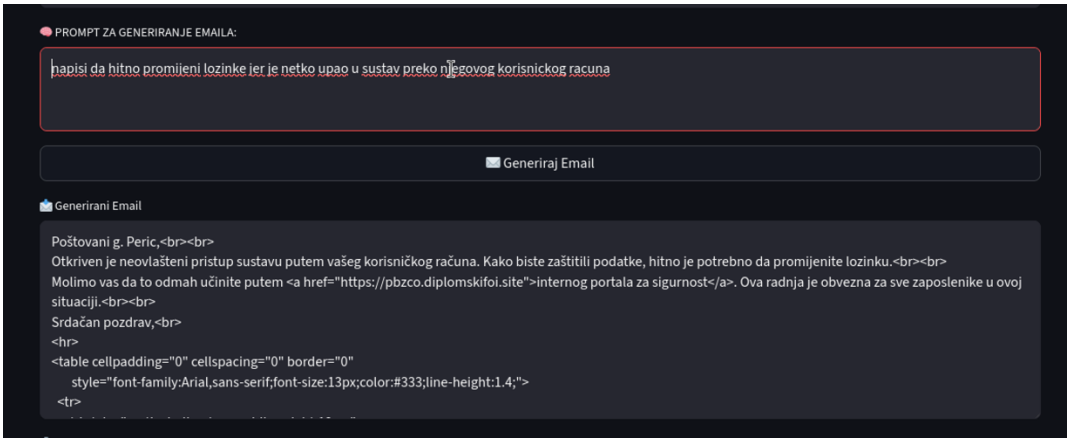
Slika 19:Prikaz dijela modula za generiranje mailova - 3. dio automatski za domenu kartice – zakazano slanje (Izvor: vlastita izrada)



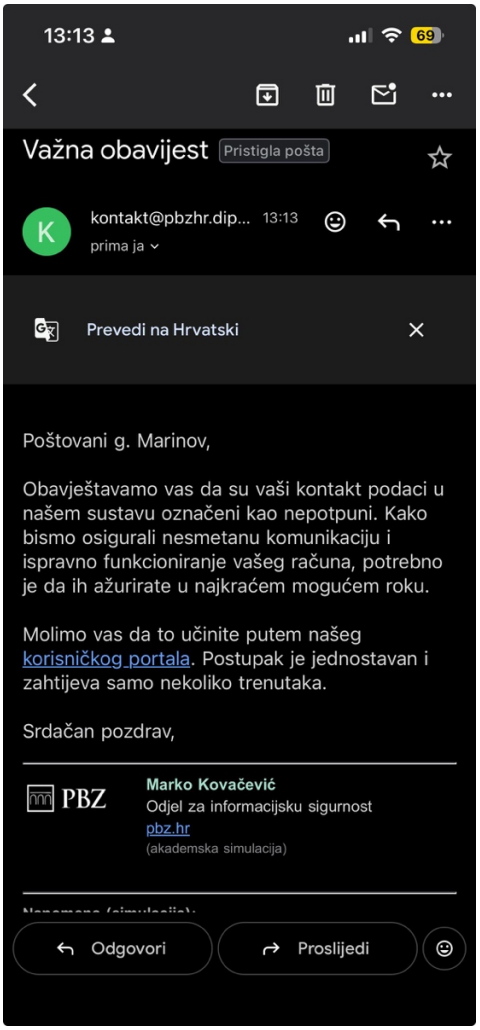
Slika 20: Prikaz dijela modula za generiranje mailova - Privatni gmailovi (Izvor: vlastita izrada)



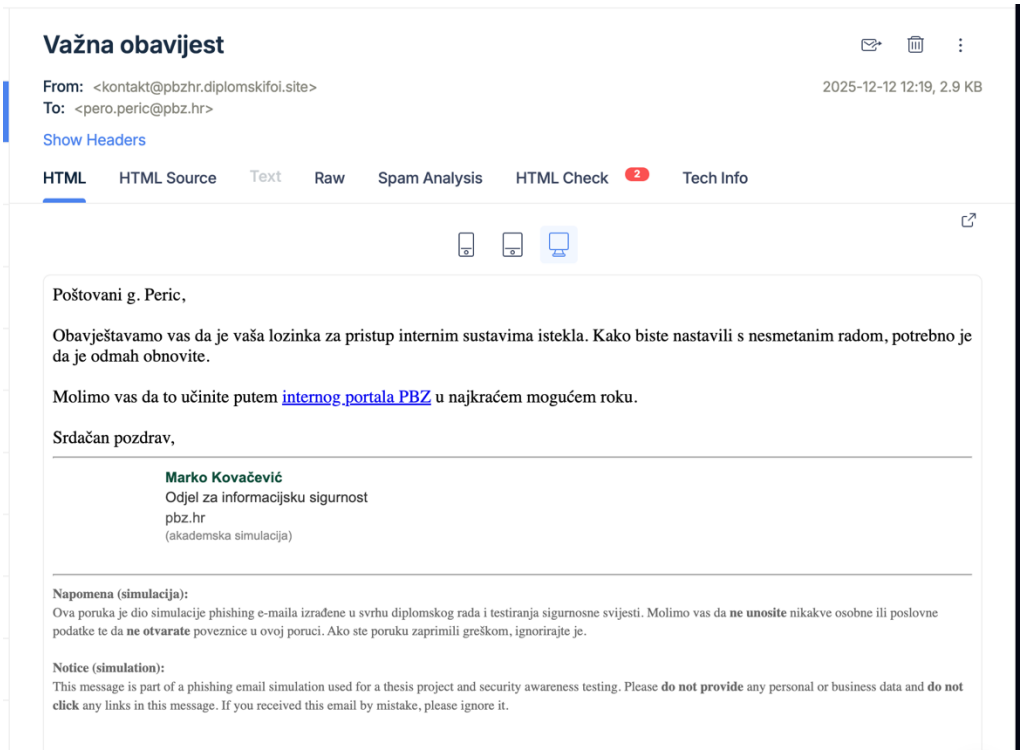
Slika 21: Prikaz dijela modula za generiranje mailova - Pojedinačni klijenti (Izvor: vlastita izrada)



Slika 22: Prikaz dijela modula za generiranje mailova – Pojedinačni klijenti - prikaz prompta i izgeneriranog maila (Izvor: vlastita izrada)



Slika 23: Prikaz poslanog maila klijentu (Izvor: vlastita izrada)



Slika 24: Prikaz poslanog maila zaposleniku(Izvor: vlastita izrada)

Na prikazanim slikama nalazi se Mailer modul, centralno mjesto za generiranje i automatsko slanje phishing emailova prema ciljanim korisnicima. Modul je podijeljen u tri kartice, od kojih svaka pokriva specifičan scenarij slanja, čime omogućuje fleksibilno izvođenje phishing kampanja različitog opsega i namjene.

Prva kartica, Automatski za Domenu, namijenjena je slanju emailova svim korisnicima čije su adrese povezane s određenom organizacijom. Korisnik unosi domenu, primjerice *pbz.hr*, nakon čega sustav učitava sve raspoložive kontakte iz baze. Ispod toga se nalazi polje za unos prompta - uputa koju se predaje modelu Grok/Deepseek, a na temelju koje se generiraju personalizirani emailovi. Sustav prikazuje tablicu s rezultatima u kojoj je vidljivo ime primatelja, email adresa, te automatski generirani sadržaj. Nakon toga moguće je odabrati način slanja: odmah, za određeni broj minuta ili u unaprijed definiranom terminu.

Druga kartica, Privatni Gmailovi, služi za ciljanu komunikaciju prema adresama koje ne pripadaju domenama organizacija - tipično privatnim Gmail računima. Princip rada je isti kao kod slanja prema domenama: korisnik unosi naziv organizacije te prompt kojim definira stil i sadržaj emaila (primjerice: predstavljanje, obavijest, zahtjev za akcijom). Sustav generira emailove za sve pronađene Gmail adrese te ih, uz odabranu opciju slanja, automatski distribuira putem konfiguriranog SMTP poslužitelja.

Treća kartica, Pojedinačni Klijent, omogućuje potpuno individualizirani pristup. Ovdje korisnik ručno unosi ime i prezime primatelja, opcionalnu domenu, njegovu email adresu te prompt koji definira sadržaj poruke. Model generira jedinstveni spear-phishing email prilagođen baš toj osobi. U prikazanom primjeru sustav generira poruku o sumnjivoj transakciji i hitnoj potrebi za ažuriranjem lozinke, zajedno s ugrađenim phishing linkom. I u ovom slučaju moguće je odmah poslati poruku ili zakazati slanje za kasniji termin.

Prva prikazana poruka odnosi se na simulirani phishing e-mail poslan klijentu, pri čemu je poruka isporučena na privatnu Gmail adresu autora rada. U tom scenariju sustav automatski prepoznaje da primatelj ne pripada domeni ciljne organizacije te koristi poseban prompt namijenjen vanjskim korisnicima. Sadržaj poruke oblikovan je tako da imitira legitimnu obavijest o ažuriranju kontaktnih podataka, uz poveznicu na kloniranu stranicu i jasno istaknut disclaimer, čime se osigurava etički i akademski okvir testiranja.

Druga poruka prikazuje e-mail generiran za zaposlenika, koji je isporučen unutar sandbox okruženja organizacijske domene. U ovom slučaju sustav detektira da je domena primatelja jednaka unesnoj domeni organizacije te automatski primjenjuje prompt namijenjen internim korisnicima. Poruka simulira obavijest vezanu uz sigurnosne procedure (istek lozinke, interni portal), uz realističan stil komunikacije koji odgovara uobičajenoj internoj poslovnoj korespondenciji.

Iako prikazane poruke djeluju uvjerljivo, njihova konačna kvaliteta i razina vjerodostojnosti ovise o generiranju sadržaja od strane korištenog jezičnog modela. U testiranju se DeepSeek pokazao nešto prikladnijim za hrvatski jezik u odnosu na Grok, no sustav je namjerno dizajniran fleksibilno - korisnik može dodatno prilagoditi sadržaj unutar korisničkog sučelja prije slanja, kao i definirati vlastiti prompt koji se kombinira s unaprijed definiranim (hardkodiranim) pravilima. Važno je naglasiti da se u okviru rada poruke ne šalju stvarnim korisnicima bez kontrole, da sve poruke sadrže jasan disclaimer, te da i e-mailovi i klonirane web stranice služe isključivo u svrhu simulacije i testiranja sigurnosne svijesti

5.9. Modul metrike

Modul za metrike predstavlja mehanizam za prikupljanje, pohranu i analizu podataka o uspješnosti simuliranih phishing kampanja. Za razliku od ranijih ili lokalno implementiranih pristupa mjerenju, u ovom sustavu isključivo se koriste webhook mehanizmi e-mail providera, bez ikakvog lokalnog bilježenja događaja unutar klijentske aplikacije. Time se u potpunosti uklanja potreba za zasebnim modulima poput metrics.py te se osigurava veća pouzdanost i točnost prikupljenih podataka.

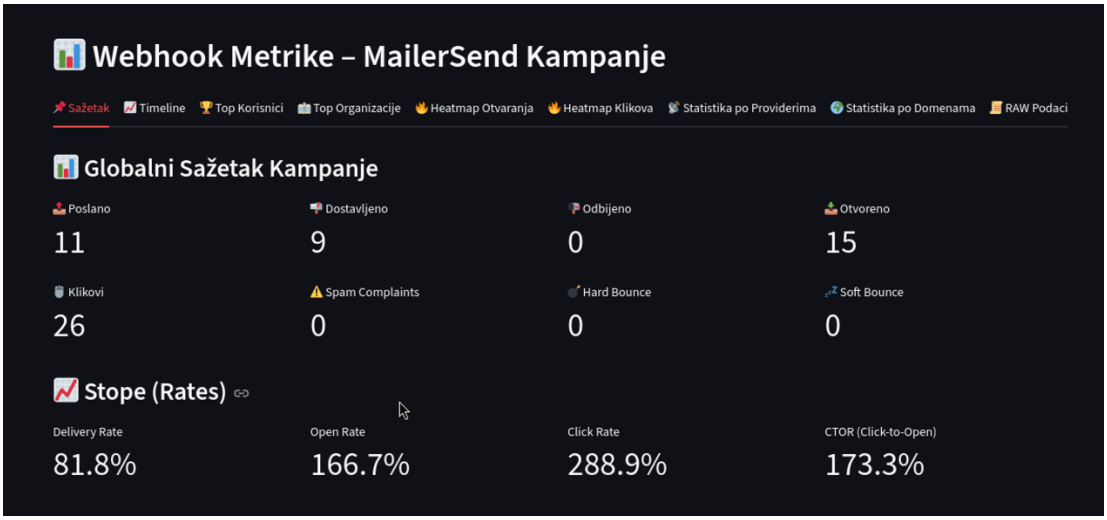
Modul se oslanja na webhook integracije s e-mail servisima MailerSend, Mailgun i Postmark, koji automatski šalju obavijesti o stvarnim događajima kao što su dostava poruke, otvaranje e-maila, klik na poveznicu, odbijanje poruke ili prijava spama. Ovakav pristup omogućuje prikupljanje verificirane telemetrije izravno od e-mail infrastrukture, neovisno o korisničkom pregledniku, operacijskom sustavu ili lokalnoj aplikaciji, što je ključno za analitičku vjerodostojnost diplomskog rada.

Središnja komponenta modula implementirana je u serverskoj datoteci api.py. Prilikom pokretanja poslužitelja inicijalizira se jedina baza podataka u sustavu za metrike, lokalna SQLite baza webhook_events.db, koja se nalazi isključivo na serverskoj strani. U bazi se automatski stvara tablica mail_events, dizajnirana kao univerzalni model za pohranu događaja iz različitih e-mail providera. Svaki zapis sadrži vrstu događaja (npr. delivered, opened, clicked, bounced), adresu primatelja, jedinstveni identifikator poruke, vremensku oznaku događaja te, ako je primjenjivo, URL na koji je korisnik kliknuo.

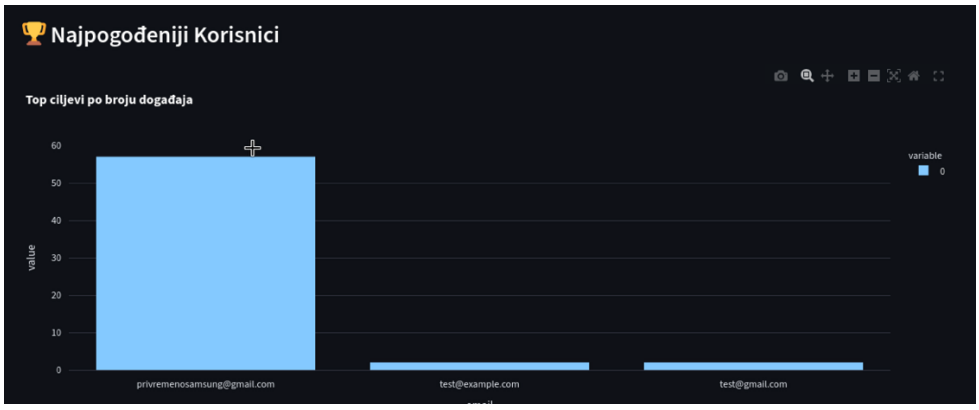
Za svaki podržani e-mail servis implementiran je zaseban webhook endpoint (/mailersend_webhook, /mailgun_webhook, /postmark_webhook). Endpointi prihvaćaju JSON payload koji provider automatski šalje u trenutku nastanka događaja. Nakon validacije i parsiranja zaprimljenih podataka, događaji se normalizirano zapisuju u tablicu mail_events. Na taj način svi podaci o kampanji dolaze iz jedinstvenog i pouzdanog izvora, bez lokalne interpretacije ili heuristika.

Korisničko sučelje, implementirano u Streamlit aplikaciji, nema vlastitu bazu metrika niti mehanizme praćenja korisničkih interakcija. Umjesto toga, sučelje dohvaća podatke isključivo putem API endpointa (npr. /mailersend_logs), koji vraća sve zabilježene webhook događaje sortirane po vremenu. Na temelju tih podataka aplikacija generira vizualne analize, uključujući sažetak kampanje, vremensku liniju aktivnosti, najaktivnije korisnike i domene te heatmape za otvaranja i klikove. Dostupan je i sirovi prikaz webhook zapisa, kao i mogućnost izvoza podataka u CSV formatu.

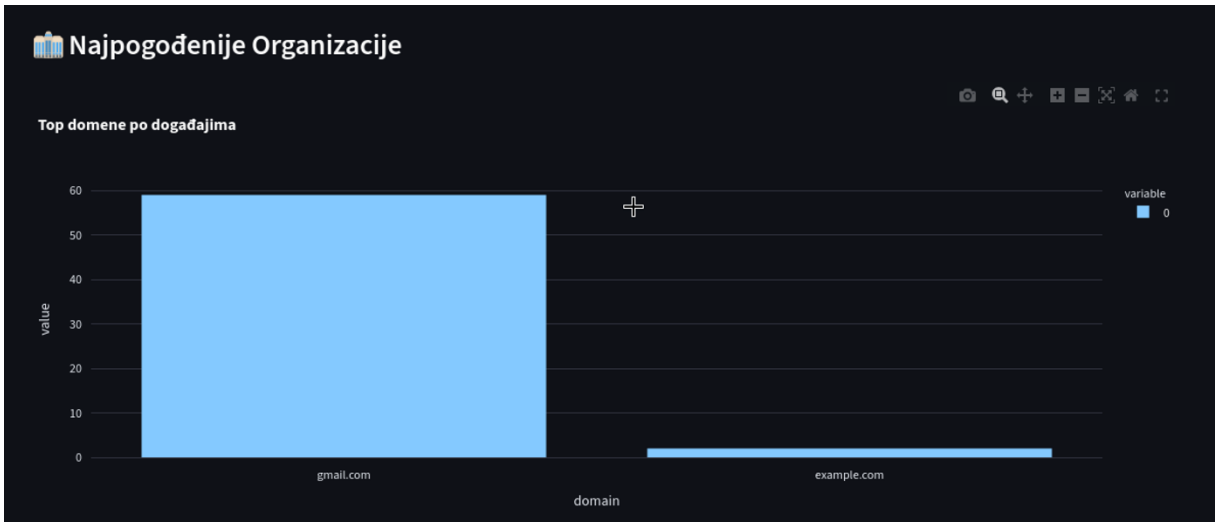
Prednost ovakve arhitekture je u potpunom razdvajanju prikupljanja metrika od klijentske aplikacije. Lokalni sustav za slanje e-mailova ne mora održavati vlastitu logiku za praćenje otvaranja ili klikova, već se oslanja na provjeren i industrijski standardiziran mehanizam e-mail servisa. Time se arhitektura sustava pojednostavljuje, smanjuje se mogućnost pogrešaka i osigurava visoka pouzdanost prikupljenih podataka.



Slika 25: Prikaz dijela modula za metrike – globalni sažetak (Izvor: vlastita izrada)

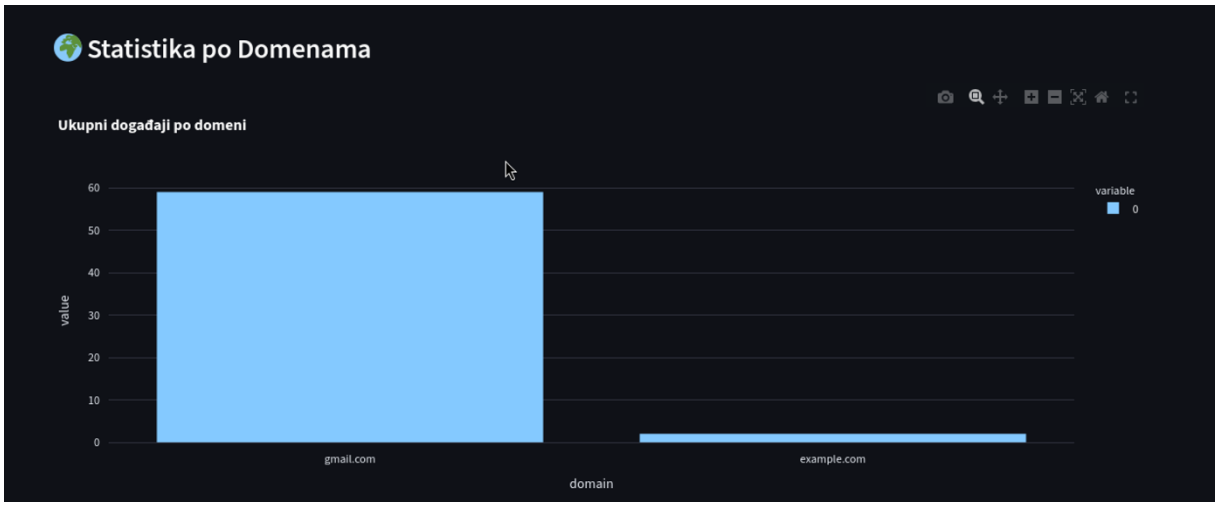


Slika 26: Prikaz dijela modula za metrike – najpogođeniji korisnici (Izvor: vlastita izrada)

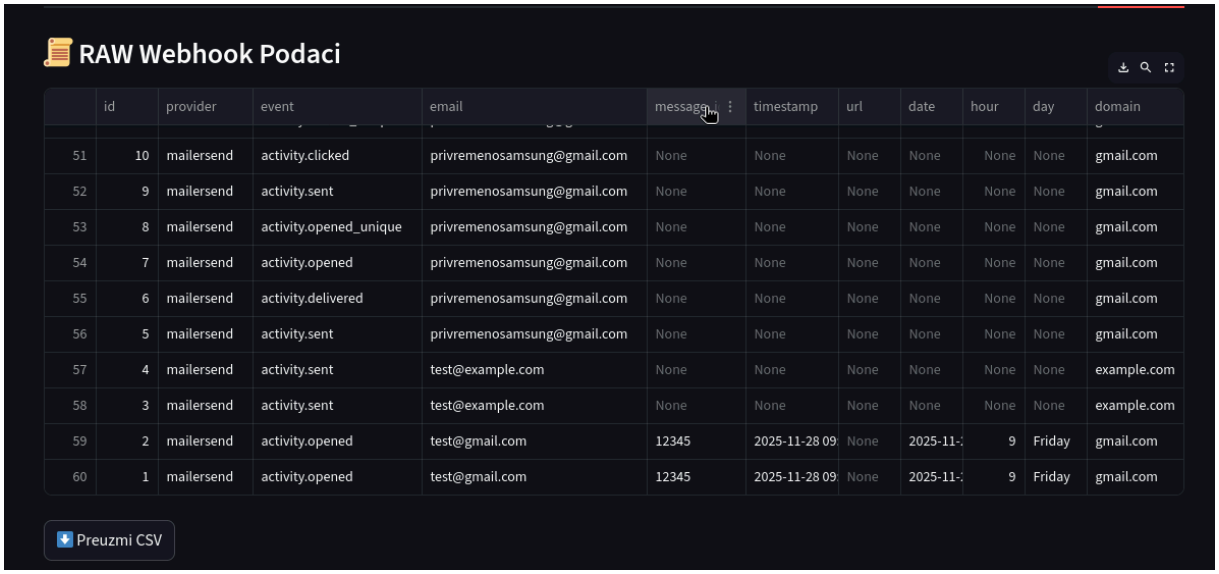


Slika 27: Prikaz dijela modula za metrike – najpogođenije organizacije (Izvor: vlastita izrada)

Slika 28: Prikaz dijela modula za metrike – statistika po providerima (Izvor: vlastita izrada)



Slika 29: Prikaz dijela modula za metrike – statistika po domenama (Izvor: vlastita izrada)



Slika 30: Prikaz dijela modula za metrike – raw webhook podaci (Izvor: vlastita izrada)

Sučelje je organizirano kroz više kartica pri vrhu ekrana, kao što su *Sažetak*, *Timeline*, *Top Korisnici*, *Top Organizacije*, različite *heatmap* vizualizacije te statistike po domenama i providerima. Na ovaj način korisnik može brzo prelaziti između različitih perspektiva i analizirati rezultate kampanja iz više kutova.

Na početnom ekranu nalazi se Globalni Sažetak Kampanje, koji prikazuje ključne metrike u čistom, preglednom i vizualno naglašenom formatu. Tu su prikazani ukupni brojevi poslanih emailova, isporučenih poruka, otvaranja, klikova te eventualnih odbijenih pokušaja dostave. Ispod njih istaknute su stope (rates), uključujući delivery rate, open rate, click rate i CTOR, čime korisnik odmah dobiva uvid u uspješnost kampanje bez potrebe za dodatnim filtriranjem ili pretraživanjem.

Sljedeće kartice omogućuju detaljnije analize. U sekciji Najpogođeniji Korisnici nalazi se grafički prikaz korisnika koji su generirali najviše događaja (npr. otvaranja ili klikova). Prikaz je realiziran kao jednostavan stupčasti graf, što omogućuje intuitivnu interpretaciju - već nakon jednog pogleda jasno je koji je korisnik najviše puta reagirao na phishing sadržaj.

Iduća kartica, Najpogođenije Organizacije, prikazuje sličan graf, ali grupiran prema domenama. Ovo je korisno kada se radi s većim brojem ciljanih organizacija ili kada se želi usporediti razine ranjivosti između njih.

Sekcija Statistika po Providerima prikazuje udio događaja s obzirom na email servis koji je koristio primatelj (npr. MailerSend, Gmail, Outlook). Vizualizacija je ponovno jednostavna i pregledna, s naglaskom na volumen događaja za pojedini servis.

Kartica Statistika po Domenama dodatno razlaže učinke kampanje prema domenama primatelja te vizualno prikazuje broj interakcija za svaku od njih. Ovo omogućuje brzo prepoznavanje koji je segment ciljne publike bio najaktivniji.

Na dnu sučelja nalazi se kartica RAW Webhook Podaci, gdje je svaka pojedinačna interakcija prikazana tablično: provider, event, email, timestamp, domena i drugi metapodaci. Tablica se može sortirati, filtrirati i preuzeti u obliku CSV datoteke, čime modul omogućuje i detaljnu forenzičku analizu.

Kroz kombinaciju agregiranih grafova, sažetaka i detaljnih zapisa, ovaj UI omogućuje korisniku da u samo nekoliko minuta stekne jasnu sliku o tome koliko je kampanja bila učinkovita te koji su korisnici ili organizacije najosjetljiviji na phishing pokušaje. Cjelokupan dizajn naglašava brzinu uvida, preglednost i intuitivno korištenje, bez potrebe za tehničkim predznanjem.

5.10. Ostale kartice

Implementacija kartice *Postavke* temelji se na funkciji show_settings(), koja u potpunosti generira korisničko sučelje putem Streamlit okvira. Funkcija je strukturirana kao niz logičkih cjelina koje odgovaraju različitim skupinama postavki. Organizacija modula omogućuje jasnu separaciju odgovornosti, dok se za pohranu vrijednosti u tijeku sesije koristi objekt st.session_state, čime se postiže trajnost podataka tijekom korištenja aplikacije. Dodatno, odabrane vrijednosti upisuju se u konfiguracijski modul config.py, što omogućuje njihovo trajno spremanje i ponovno učitavanje pri svakom pokretanju aplikacije.

Konfiguracija baze podataka ostvarena je jednostavnim unosom putanje do SQLite datoteke. Funkcija čita početni DB_PATH iz modula config te korisniku prikazuje trenutačnu aktivnu vrijednost. Po spremanju, varijabla config.DB_PATH se ažurira kako bi se reflektirala nova postavka. Time se postiže fleksibilnost, jer korisnik može koristiti zasebne baze za različite sesije ili projekte.

Sekcija za API postavke implementirana je korištenjem Streamlitove forme, što osigurava da se svi uneseni podaci obrađuju tek nakon potvrde korisnika. Google API ključevi i CSE identifikatori obrađuju se kao nizovi odvojenih vrijednosti, dok se Brave API ključ i LinkedIn vjerodajnice spremaju kao jednostavni stringovi. Nakon obrade, sve vrijednosti pohranjuju se u session_state, no funkcija također pokušava ažurirati razine u config.py kako bi se zadržale između pokretanja aplikacije.

PhantomBuster sekcija proširuje ovaj mehanizam dodavanjem dodatnih parametara - API ključa, Phantom ID-a, LinkedIn cookieja, konzolnog URL-a te pristupnih podataka za

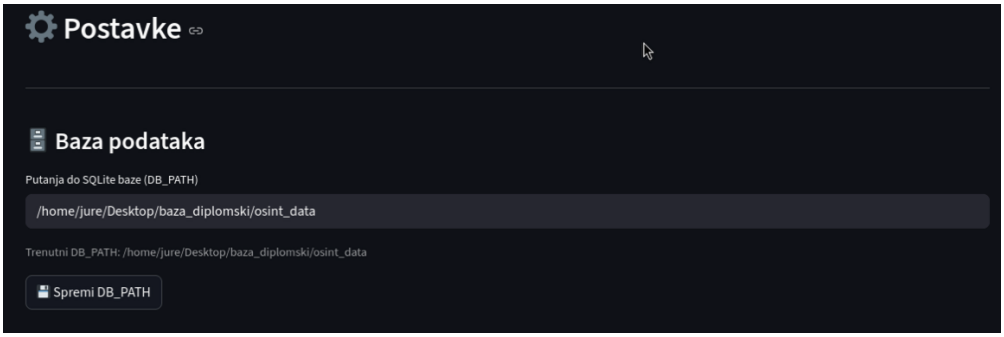
Selenium login. Vrijednosti se spremaju u sesiju i po potrebi u konfiguracijsku datoteku. Ova sekcija posebno prati sigurnosne smjernice te osigurava da osjetljivi podaci ne budu prikazani u čistom obliku u sučelju.

Dio funkcije koji se odnosi na upravljanje hosting serverom usko je povezan s modulom setup_server.py. U slučaju ručne konfiguracije, aplikacija samo sprema unijeti ključ i wildcard domenu. Međutim, u automatskom načinu rada poziva se funkcija setup_server(), koja putem SSH-a izvodi niz konfiguracijskih koraka na udaljenom poslužitelju. To uključuje instalaciju potrebnih paketa, kreiranje virtualnog okruženja, instalaciju FastAPI i uvicorn biblioteka, generiranje samopotpisanog certifikata, konfiguraciju systemd servisa, generiranje početne HTTP konfiguracije Nginxa, izdavanje wildcard SSL certifikata putem DNS-01 validacije i konačno prebacivanje na HTTPS s punom Let's Encrypt podrškom. Tijekom izvođenja, Streamlit koristi callback za prikaz poruka u stvarnom vremenu, čime korisnik dobiva jasan uvid u status instalacije.

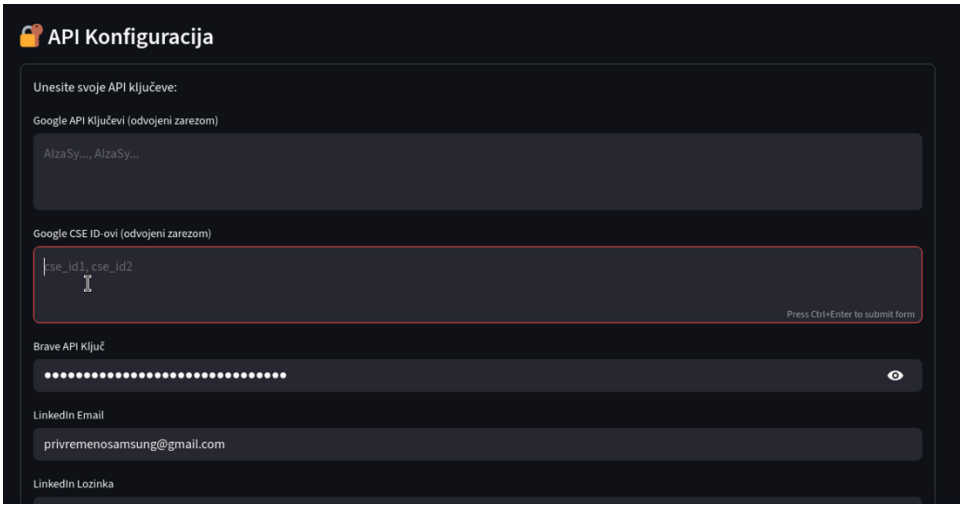
SMTP dio implementiran je kao jednostavna forma koja prikuplja parametre za slanje e-pošte. Podaci se spremaju u obliku rječnika u session_state, što omogućuje centralizirano upravljanje konfiguracijom email servisa.

Administrativne funkcije - uvoz batch datoteka i generiranje izvještaja - implementirane su kao gumbi koji pokreću pomoćne funkcije. Uvoz batch-eva odvija se u zasebnom threadu kako bi se izbjegla blokada aplikacije, dok čišćenje cache-a uključuje brisanje i ponovno kreiranje direktorija. Izvještaj koristi podatke iz SQL baze kako bi izračunao broj prikupljenih organizacija, osoba, email adresa i LinkedIn profila te generirao Markdown dokument spreman za preuzimanje.

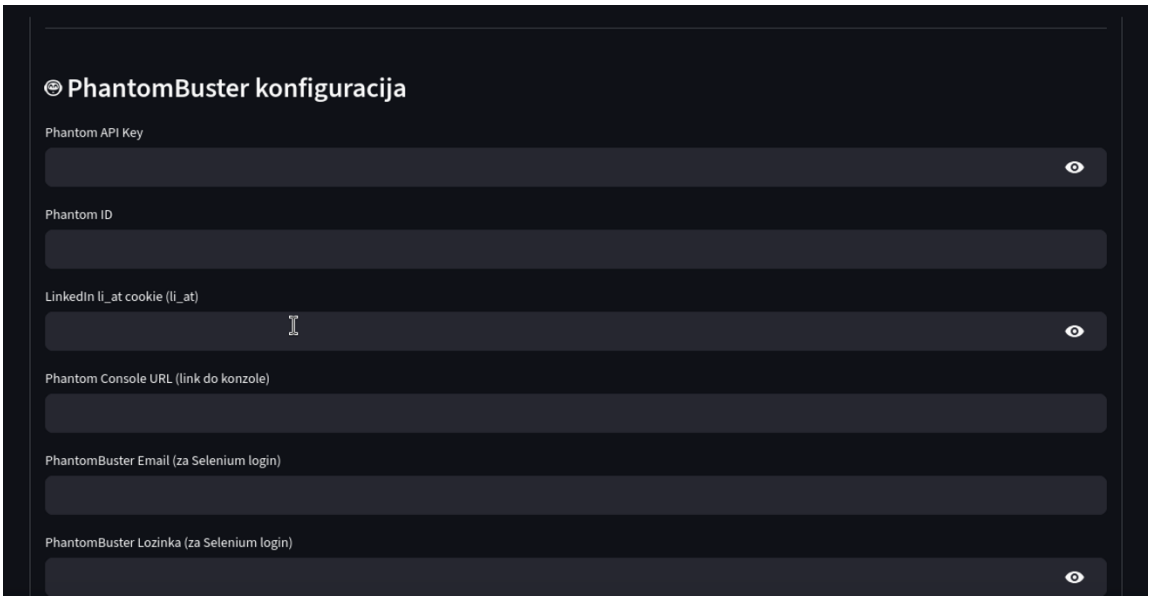
Završni dio funkcije odgovoran je za prikaz osnovnih sustavskih informacija, a koristi standardne Python biblioteke za dohvat verzija i parametara okruženja. Time se korisniku pruža uvid u radno okruženje te se olakšava otklanjanje pogrešaka. Na ovaj način, modul *Postavke* predstavlja cjelovito i tehnički koherentno rješenje koje omogućuje fleksibilno upravljanje svim aspektima aplikacije.



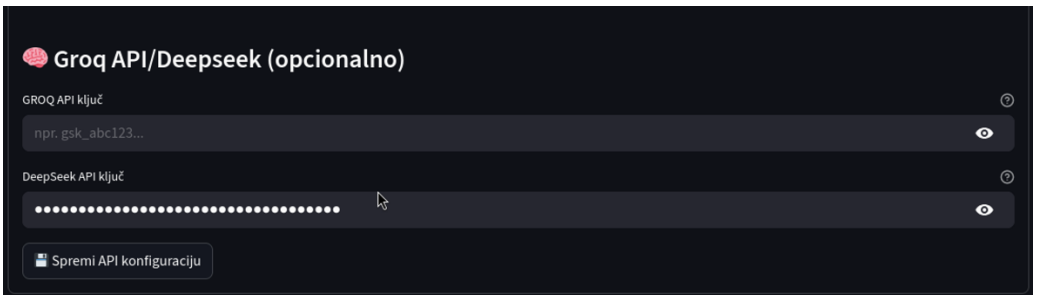
Slika 31: Prikaz dijela kartice postavke - baza podataka (Izvor: vlastita izrada)



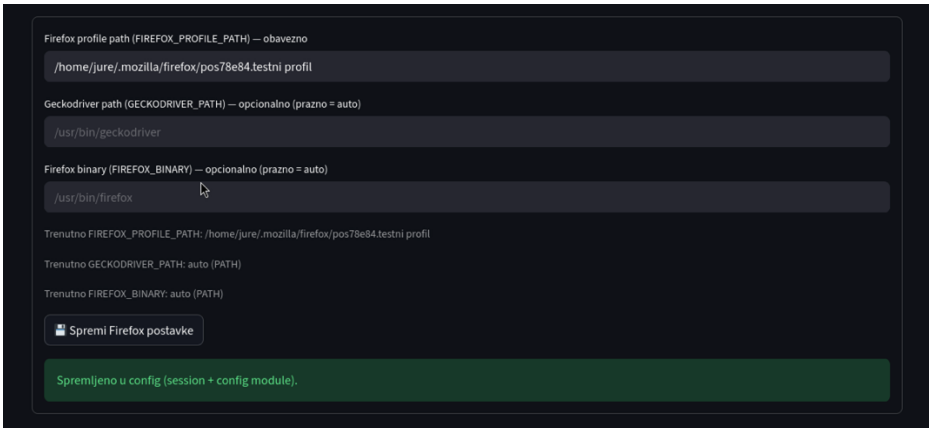
Slika 32: Prikaz dijela kartice postavke - postavljanje API ključeva za scraping(Izvor: vlastita izrada)



Slika 33: Prikaz dijela kartice postavke - konfiguracija PhantomBustera(Izvor: vlastita izrada)

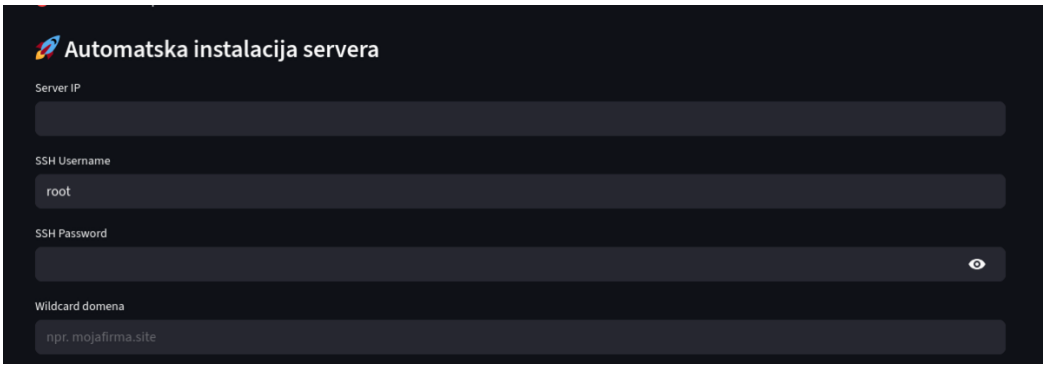


Slika 34: Prikaz dijela kartice postavke – unos Groq Api i Deepseek(Izvor: vlastita izrada)

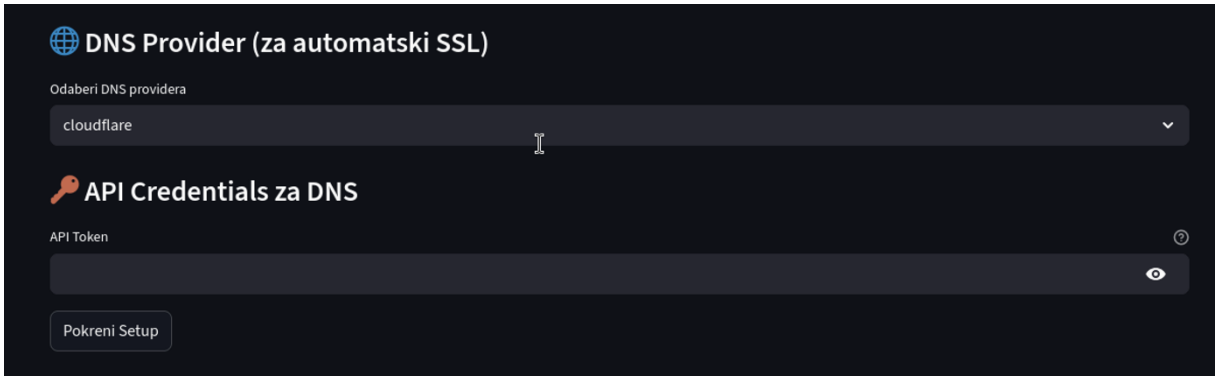


Slika 35: Prikaz dijela kartice postavke – unos Firefox/Selenium (Izvor: vlastita izrada)

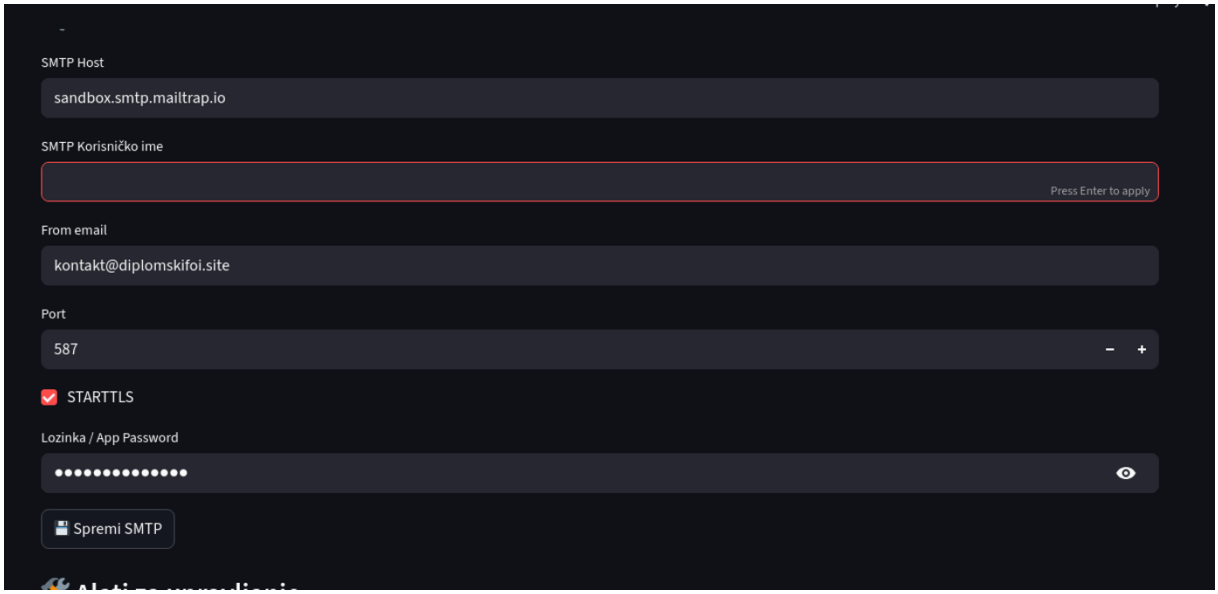
Slika 36: Prikaz dijela kartice postavke – ručno postavljanje servera (Izvor: vlastita izrada)



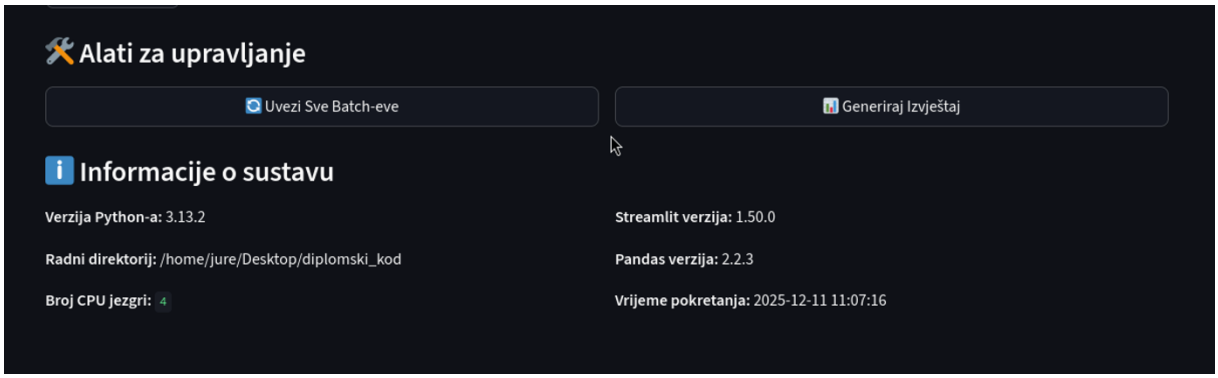
Slika 37: Prikaz dijela kartice postavke – 1. dio automatsko postavljanje servera (Izvor: vlastita izrada)



Slika 38: Prikaz dijela kartice postavke - 2. dio automatsko postavljanje servera (Izvor: vlastita izrada)



Slika 39: Prikaz dijela kartice postavke– postavljanje SMTP postavci (Izvor: vlastita izrada)



Slika 40: Prikaz dijela kartice postavke– alati za upravljanje (Izvor: vlastita izrada)

Kartica *Postavke* predstavlja centralno upravljačko sučelje aplikacije i omogućuje korisniku konfiguraciju svih ključnih komponenti sustava na jednom mjestu. Sučelje je organizirano u nekoliko tematskih cjelina, pri čemu se svaka odnosi na specifičan dio funkcionalnosti sustava, a naglasak je stavljen na preglednost i jednostavnost korištenja. Prva cjelina odnosi se na konfiguraciju baze podataka, gdje korisnik može definirati putanju do SQLite baze podataka. Nakon unosa, prikazuje se trenutno aktivna putanja, čime se smanjuje mogućnost pogreške i omogućuje brza provjera ispravnosti konfiguracije.

Središnji dio kartice čini opsežna sekcija za unos API ključeva i vjerodajnica. U njemu korisnik unosi Google API ključeve, Google CSE identifikatore, Brave API ključ te LinkedIn korisničke podatke potrebne za Selenium autentikaciju. Sučelje omogućuje unos više vrijednosti odvojenih zarezom, a sve postavke spremaju se unutar tekuće sesije, ali se po potrebi mogu trajno zapisati u konfiguracijsku datoteku. Nakon spremanja, korisniku se prikazuje pregled svih unesenih vrijednosti s jasnim indikatorima o tome koje su postavke ispravne, a koje nedostaju.

Zaseban dio posvećen je integraciji sa servisom PhantomBuster, koji omogućuje automatizirano preuzimanje podataka s LinkedIna. Ovdje se unose API ključ, identifikator agenta, LinkedIn li_at cookie te pristupni podaci za PhantomBuster konzolu. Ova sekcija jasno odvaja različite vrste vjerodajnica kako bi se smanjila mogućnost zamjene podataka i kako bi postavke bile intuitivne za korisnika.

Dodatno je uključena i opcionalna postavka za unos Groq (Grok) API I Deepseek API ključeva koji se koriste za generiranje personaliziranih phishing poruka uz pomoć LLM-a. Time se omogućuje proširenje funkcionalnosti aplikacije bez potrebe za dodatnim modulima.

Dodatna sekcija kartice namijenjena je konfiguraciji Firefox okruženja za Selenium scraping. U ovom dijelu korisnik unosi putanju do vlastitog Firefox profila, čime se omogućuje korištenje postojeće autentikacijske sesije prilikom pristupa LinkedInu. Putanje do Firefox binarne datoteke i geckodrivera definirane su kao opcionalne te se, ukoliko nisu zadane, automatski određuju putem sistemske varijable PATH. Ovakav pristup omogućuje visoku razinu prenosivosti aplikacije i smanjuje potrebu za ručnom konfiguracijom na različitim operacijskim sustavima.

Posebno važan dio kartice odnosi se na konfiguraciju hosting servera. Korisniku su ponuđena dva načina konfiguracije: ručni i automatski. Ručni način predviđen je za korisnike koji već posjeduju vlastiti poslužitelj te omogućuje jednostavan unos wildcard domene i API ključa. Automatski način omogućuje potpunu instalaciju poslužiteljske infrastrukture jednim klikom, uključujući instalaciju potrebnih paketa, postavljanje FastAPI servisa, generiranje SSL certifikata i konfiguraciju Nginx proxy servera. Nakon unosa IP adrese, SSH vjerodajnica i DNS

podataka, sustav prikazuje proces instalacije u stvarnom vremenu, čime korisnik dobiva transparentan uvid u sve korake konfiguracije.

U sklopu kartice nalazi se i odjeljak za postavljanje SMTP postavki, čime korisnik definira parametre za slanje e-pošte, uključujući adresu poslužitelja, korisničko ime, “from” adresu, port i sigurnosne opcije. Time se omogućuje potpuna kontrola nad mehanizmom slanja phishing poruka.

Na kraju su uključeni i alati za administraciju, među kojima su automatski uvoz svih batch datoteka, generiranje izvještaja o prikupljenim OSINT podacima. Sve ove funkcionalnosti pokreću se iz korisničkog sučelja bez potrebe za ručnim izvršavanjem skripti. Kartica završava prikazom sustavskih informacija, gdje su navedene verzije ključnih biblioteka, radni direktorij, broj procesorskih jezgri i vrijeme pokretanja aplikacije, što olakšava dijagnostiku i nadzor rada sustava.

Kartica *Datoteke i Cache* predstavlja centralno mjesto za upravljanje svim datotekama i direktorijima koje aplikacija generira tijekom procesa prikupljanja, obrade i analize OSINT podataka. Kako alat tijekom rada stvara veliki broj privremenih i trajnih datoteka – uključujući batch rezultate, cache zapise, spremljene HTML stranice, logove, generirane phishing stranice i različite JSON strukture – bilo je potrebno implementirati intuitivno grafičko sučelje koje korisniku omogućuje lak pristup svim datotekama bez potrebe za ručnim pretraživanjem direktorija na disku.

Na vrhu kartice nalazi se informativna sekcija koja korisniku objašnjava razliku između trajnih i privremenih direktorija. Direktoriji poput *logs/* i *cache_pages/* prepoznati su kao privremene radne mape koje aplikacija koristi za pohranu međurezultata. Korisnik ih može u potpunosti obrisati bez rizika za rad sustava, jer će se automatski ponovno napuniti prilikom sljedećeg procesa scrapinga ili analize. Slično tome, direktoriji *cache/* i *osint_project/cache/* služe isključivo kao radna predmemorija, te se njihovo čišćenje preporučuje kako bi se oslobodio prostor i optimizirala izvedba alata.

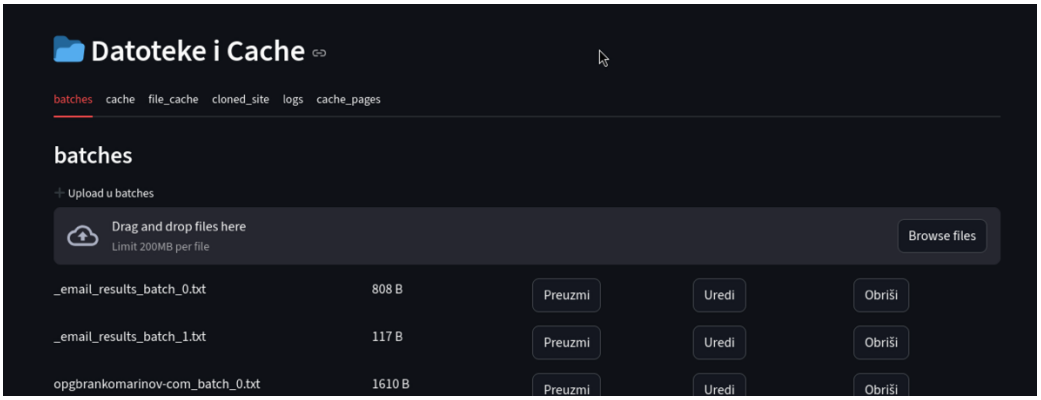
Ispod početnog objašnjenja nalazi se horizontalna navigacijska traka s karticama koje predstavljaju različite radne direktorije: *batches*, *cache*, *file_cache*, *cloned_site*, *logs* i *cache_pages*. Svaki od ovih direktorija prikazan je kao interaktivna lista datoteka u kojoj korisnik može pregledavati sadržaj, preuzimati pojedine datoteke ili ih trajno brisati. Ova struktura omogućuje jasnu preglednost kompleksnog sustava datoteka koje se generiraju tijekom rada OSINT modula.

Odabirom taba *cache* korisniku se prikazuje dodatno upozorenje da se radi o privremenoj mapi koju je sigurno obrisati. Funkcionalnost *Upload u cache* omogućuje korisniku učitavanje datoteka izravno u aktivni direktorij putem „drag-and-drop“ sučelja ili odabirom

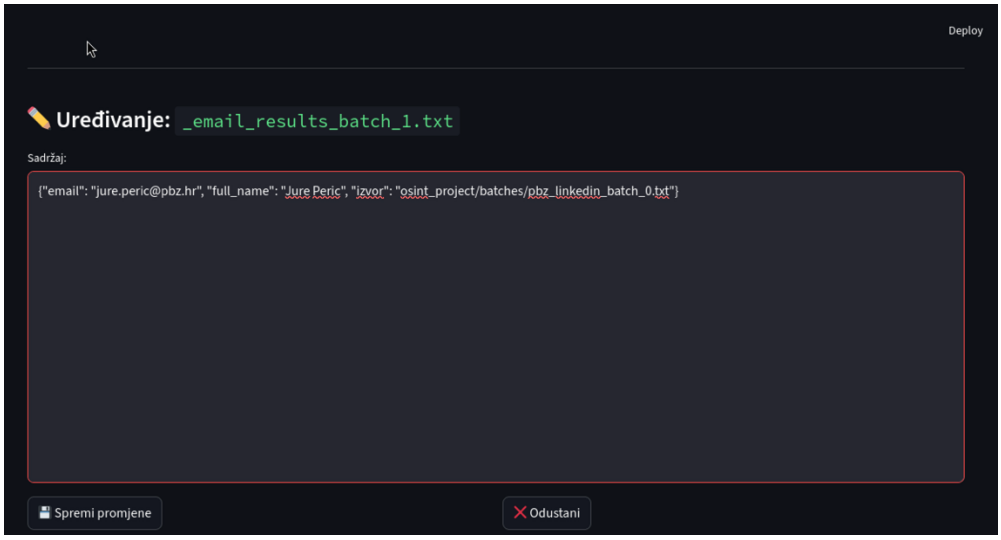
datoteke ručno. Time aplikacija dobiva i mogućnost ručnog unošenja datoteka potrebnih za daljnju analizu ili testiranje sustava. Podržane su datoteke veličine do 200 MB, što omogućuje rad i s većim HTML ili JSON zapisima dobivenima tijekom scrapinga.

Posebno značajna komponenta kartice *Datoteke i Cache* je mogućnost uređivanja datoteka izravno unutar sučelja. Kada korisnik odabere opciju „Uredi“, otvara se posebno uređivačko okruženje s istaknutim nazivom datoteke i velikim tekstualnim editorom koji prikazuje njezin cjelokupan sadržaj. Ovaj editor omogućuje uređivanje različitih tekstualnih formata, uključujući .txt, .json i .log datoteke. Korisnik tako može jednostavno ispraviti pogreške u batch rezultatima, dodati nove vrijednosti, ukloniti redundantne podatke ili ručno prilagoditi rezultate scrapinga. Ovo je osobito važno u OSINT radu, gdje automatsko prikupljanje nerijetko zahtijeva naknadnu ručnu validaciju i korekciju.

Na dnu uređivača nalaze se dvije ključne kontrole: gumb „Spremi promjene“, koji ažurira originalnu datoteku na disku, te gumb „Odustani“, koji prekida uređivanje bez spremanja. Ovaj mehanizam integriran je tako da ne narušava strukturu direktorija te omogućuje brzu i sigurnu izmjenu postojećih podataka.



Slika 41: Prikaz dijela kartice Datoteke i Cache (Izvor: vlastita izrada)



Slika 42: Prikaz dijela kartice Datoteke i Cache – uređivanje sadržaja (Izvor: vlastita izrada)

Kartica Pregled podataka, smještena unutar glavnog izbornika *Pretraga*, predstavlja centralni modul za rad s SQLite bazom podataka te omogućuje korisniku detaljan uvid, pretraživanje i uređivanje svih podataka koje je OSINT sustav prikupio tijekom izvršavanja različitih faza scrapinga. Sučelje je implementirano kao interaktivni DB Browser te je dizajnirano da spoji jednostavnost korištenja s funkcionalnostima tipičnima za specijalizirane SQL alate.

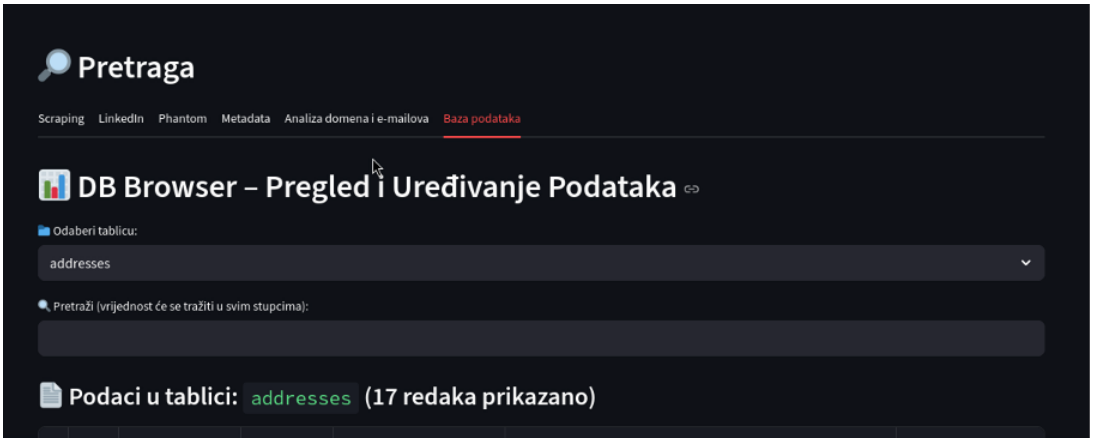
Na vrhu kartice nalazi se padajući izbornik za odabir tablice iz baze, pri čemu sustav automatski učitava sve postojeće tablice poput *emails*, *organizations*, *persons*, *social_profiles* i ostalih koje čine model podataka aplikacije. Nakon odabira tablice, korisniku se prikazuje kompletan sadržaj u obliku interaktivne tablice, uključujući sve retke i stupce. Tablica podržava horizontalno i vertikalno skrolanje te omogućuje jednostavno pregledavanje i ručno uređivanje pojedinih ćelija - što je korisno za ispravak pogrešaka, ručne anotacije ili dodavanje nedostajućih informacija.

Kako bi olakšala rad s većim količinama podataka, kartica uključuje i ugrađeni sustav pretraživanja: korisnik može upisati bilo koju vrijednost, a sustav će je potražiti u svim stupcima odabrane tablice. Osim toga, moguće je ručno uređivanje podataka kroz obrazac ispod tablice, gdje korisnik može spremiti promjene ili obrisati određeni redak jednostavnim upisivanjem njegovog identifikatora. Time se eliminira potreba za vanjskim alatima poput DB Browser for SQLite, jer sve osnovne funkcije uređivanja baze postaju dio aplikacije.

Napredniji korisnici imaju na raspolaganju i opciju izvršavanja ručno pisanih SQL upita. U posebno označenom polju moguće je pisati *SELECT*, *UPDATE*, *DELETE* i *INSERT* naredbe, što omogućuje potpunu kontrolu nad bazom podataka. Rezultat upita prikazuje se

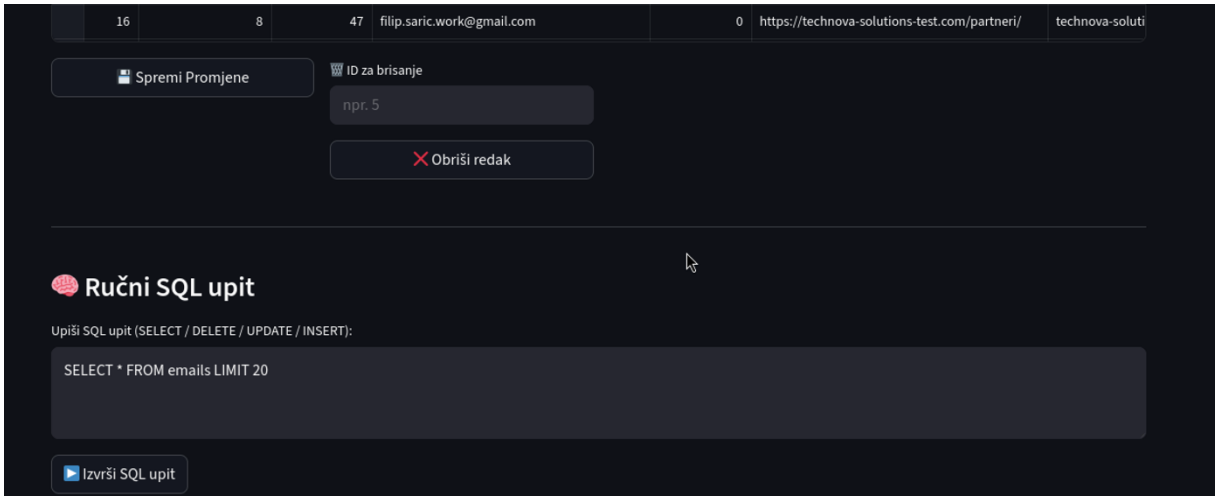
odmah ispod, što pruža fleksibilnost u analizi podataka i otklanjanju pogrešaka tijekom razvoja i testiranja.

Konačno, kartica prikazuje i statistiku tablice, uključujući ukupan broj redaka, ukupan broj stupaca te popis njihovih naziva. Ova funkcionalnost olakšava razumijevanje strukture podataka i daje brzi uvid u opseg prikupljenih informacija. Kartica Pregled podataka time predstavlja ključni alat za upravljanje podacima unutar OSINT sustava, kombinirajući vizualnu preglednost, fleksibilnost SQL jezika i jednostavnost interaktivnog grafičkog sučelja.

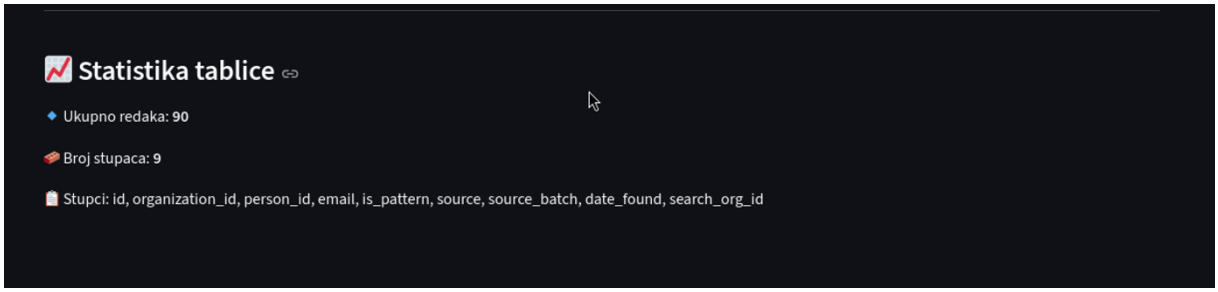


Slika 43: Prikaz dijela kartice Pregled podataka – Odabir tablice i pretraživanje (Izvor: vlastita izrada)

Slika 44: Prikaz dijela kartice Pregled podataka – Pregleda tablice (Izvor: vlastita izrada)



Slika 45: Prikaz dijela kartice Pregled podataka – Ručni SQL upit (Izvor: vlastita izrada)



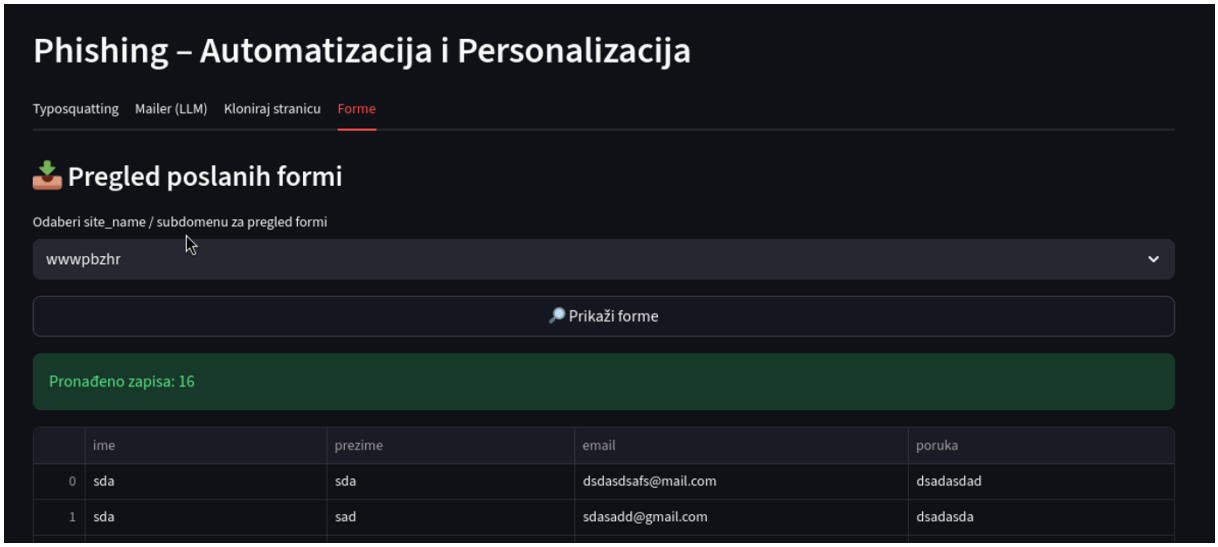
Slika 46: Prikaz dijela kartice Pregled podataka – Statistika tablice (Izvor: vlastita izrada)

Kartica Forme u okviru izbornika *Phishing* služi isključivo za pregled svih obrazaca (formi) koje su korisnici ispunili na postavljenim phishing stranicama. Na vrhu se nalazi polje za unos naziva poddomene (*site_name*), odnosno direktorija u kojem se nalaze spremljene forme. Nakon što korisnik upiše naziv i klikne na gumb „Prikaži forme“, aplikacija učitava sve zapisane forme povezane s tom poddomenom.

Ako su forme pronađene, prikazuje se informacija o njihovom ukupnom broju, primjerice *„Pronađeno zapisa: 16“*. Ispod toga nalazi se tablica u kojoj je svaki redak jedan zaprimljeni obrazac. Tablica prikazuje stvarne podatke koje je korisnik unio na phishing stranici, uključujući polja poput *ime*, *prezime*, *email*, *poruka* i ostale vrijednosti definirane u HTML formi. Tablica je čitljiva, uredno strukturirana i omogućuje pregled svih zaprimljenih podataka, ali ne sadrži napredne statističke funkcije niti grafičke metrike - služi isključivo kao pregled stvarnih unosa.

Ova kartica tako pruža jednostavan i izravni uvid u sve prikupljene forme koje su pristigle tijekom phishing simulacije, bez automatske analize ili obrade podataka. Korisnik

ručno odabire koju poddomenu želi provjeriti i dobiva točan prikaz svih zaprimljenih formi vezanih uz nju.



Slika 47: Prikaz kartice Forme (Izvor: vlastita izrada)

6. Ograničenja sustava i usporedba s postojećim rješenjima

Jeshka razvijeni sustav predstavlja cjelovitu OSINT i phishing simulacijsku platformu namijenjenu edukaciji i red team vježbama, no kao i svako tehničko rješenje, posjeduje određena ograničenja. Najznačajnija ograničenja proizlaze iz ovisnosti o vanjskim servisima i izvorima podataka. Dostupnost i kvaliteta OSINT podataka uvelike ovise o promjenama strukture web stranica, primjeni anti-scraping mehanizama te ograničenjima poput rate-limitinga ili CAPTCHA zaštite, osobito kod društvenih mreža kao što je LinkedIn.

Dodatno, iako sustav koristi mehanizme za cacheiranje, batch obradu i fallback metode (Selenium i Playwright), dugotrajno i intenzivno korištenje može dovesti do smanjenja pouzdanosti određenih modula zbog vanjskih promjena koje nisu pod kontrolom autora sustava. Također, generiranje phishing sadržaja uz pomoć velikih jezičnih modela podložno je ograničenjima kvalitete ulaznih podataka te mogućim varijacijama u generiranom tekstu.

U usporedbi s postojećim rješenjima, poput alata GoPhish, razvijeni sustav nudi širu integraciju OSINT procesa i automatiziranog izviđanja ciljeva, dok se GoPhish primarno fokusira na upravljanje phishing kampanjama i metrike. S druge strane, alati poput Maltega pružaju snažne vizualne mogućnosti analize podataka, ali zahtijevaju ručnu interakciju i ne nude cjelovitu automatizaciju phishing simulacija. Razvijena platforma kombinira prednosti oba pristupa kroz automatizirano prikupljanje podataka, generiranje prilagođenog sadržaja i centraliziranu analitiku, uz naglasak na lokalno pokretanje i edukativnu namjenu.

Unatoč navedenim ograničenjima, sustav ispunjava postavljene ciljeve rada te predstavlja fleksibilnu osnovu za daljnji razvoj i nadogradnju u području OSINT analitike i simulacije napada.

7. Zaključak

Informacijska sigurnost danas predstavlja jedno od najkompleksnijih i najdinamičnijih područja tehnološkog ekosustava. Organizacije, bez obzira na veličinu i djelatnost, svakodnevno su izložene prijetnjama koje kombiniraju tehničku sofisticiranost i psihološku manipulaciju, a među njima posebno se ističu OSINT napadi i phishing kampanje. Upravo zato je cilj ovog diplomskog rada bio prikazati, implementirati i tehnički zaokružiti sustav sposoban objediniti prikupljanje informacija, njihovu analizu i provedbu sigurnosnih simulacija kroz jedinstven, konzistentan i automatiziran alat - jeshka. Uspješnom realizacijom ovog sustava postignuti su rezultati koji otvaraju nove mogućnosti za razumijevanje, testiranje i unapređivanje sigurnosnih politika u stvarnom okruženju.

Teorijski dio rada obradio je ključne elemente koji su temelj svakog modernog pristupa informacijskoj sigurnosti: od osnova socijalnog inženjeringa, ljudske psihologije, motivacije i ranjivosti, pa sve do tehničkih vektora napada, evolucije phishing taktika te razlika između ciljanih i masovnih napada. Posebno je istaknuto kako su danas napadi sve manje rezultat puke tehničke sile, a sve više posljedica precizne analize ljudskog ponašanja i dostupnih informacija o cilju. Upravo tu se nalazi OSINT, koji igra ključnu ulogu u fazi izviđanja. To je faza koja određuje vjerodostojnost, uspješnost i učinkovitost svake iduće akcije, a time i cjelokupne sigurnosne prijetnje ili simulacije.

Na temelju toga, praktični dio rada prikazao je kako se sve te teorijske komponente mogu spojiti u jedan ujednačen proces. Razvoj frameworka jeshka reprezentira sve faze suvremenog OSINT-phishing lanca: dorkanje na pretraživačima, scraping sadržaja, validaciju prikupljenih osobnih i organizacijskih podataka, izgradnju baze znanja, generiranje phishing predložaka, upravljanje kampanjama, kreiranje realističnih lažnih stranica, implementaciju hostinga putem vlastite infrastrukture i praćenje rezultata kroz metrike. Time sustav više nije samo tehnički alat, nego i metodološki okvir koji omogućuje ponovljivost, standardizaciju i kontrolu čitavog procesa.

Jedna od najvećih vrijednosti razvijenog sustava jest eliminacija potrebe za korištenjem velikog broja zasebnih alata koji bi se inače morali ručno instalirati, konfigurirati i međusobno povezivati. Tradicionalne OSINT i phishing kampanje uključuju ručni rad u pretraživačima, naprednu analizu podataka, korištenje više platformi za scraping, različite API-je, prilagođene web poslužitelje te čak i zasebne sustave za slanje emailova. Jeshka taj složeni sustav svodi na jedan panel, jednu bazu podataka, jedinstveni upravljački sloj i kompletno automatizirane operacije. To u praksi znači da korisnik u svega nekoliko minuta može pokrenuti cijeli ciklus

sigurnosnog testiranja, od početne analize cilja do slanja prilagođenih phishing poruka i bilježenja reakcija korisnika.

Posebnu vrijednost u ovom radu predstavlja i tehnička implementacija. Infrastruktura koja omogućuje automatsko stvaranje servera, implementirana preko SSH komunikacije i skripti za instalaciju NGNIX-a, FastAPI-ja, certifikata i DNS konfiguracija, omogućuje da se korisnik ne mora baviti ručnim podešavanjem servera. Time se uklanja jedan od najkompleksnijih pragova ulaska u realne phishing simulacije – hosting lažnih stranica. Automatizacija stvara produkcijski spreman server, s podrškom za SSL, wildcard certifikate i dinamičke poddomene, čime se vjerodostojnost phishing kampanja značajno povećava.

Još jedan važan segment rada je i implementacija sustava za praćenje metrika. Omogućeno je detaljno praćenje svakog emaila koji je poslan - uključujući dostavu, otvaranje, klikove, vrijeme reakcije i distribuciju aktivnosti po domenama, vremenskim intervalima ili organizacijama. Te metrike imaju iznimnu važnost, jer predstavljaju temelj za stvarne sigurnosne procjene, analizu ponašanja korisnika i razvoj učinkovitijih edukacijskih programa. Bez takvog sustava, cijeli proces phishing simulacija bio bi nepotpun, jer ne bi davao stvarni uvid u razinu ugroženosti organizacije.

Framework jeshka dodatno osnažuje vrijednost rada kroz svoju modularnost. Svaka komponenta razvijena je tako da se može proširiti ili zamijeniti bez utjecaja na ostatak sustava. API sustavi, scraping mehanizmi, moduli za dorkanje i upravljanje kampanjama mogu se nadograditi novim funkcijama ili prilagoditi različitim sigurnosnim scenarijima. Time jeshka nije statičan alat, već platforma koja se može razvijati sukladno rastućim potrebama sigurnosne zajednice.

Praktični doprinos ovog rada nije samo tehnički, nego i pedagoški. Kroz razvoj sustava i dokumentaciju, čitatelj uči kako funkcionira OSINT, što su ključni rizici u sigurnosnoj arhitekturi organizacija, kako napadači razmišljaju i kako se prikupljeni podaci mogu pretvoriti u konkretne, mjerljive simulacije. Framework time postaje alat ne samo za testiranje, već i za edukaciju zaposlenika, analitičara i studenata koji žele razumjeti stvarne prijetnje i obranu u cyber sigurnosti.

Sustav, iako funkcionalan i spreman za korištenje, predstavlja i polazište za niz budućih nadogradnji. Potencijalni daljnji razvoj uključuje integraciju umjetne inteligencije za automatsko klasificiranje prikupljenih podataka, poboljšano prepoznavanje entiteta u tekstu, napredne module za detekciju obrazaca ponašanja žrtava, generiranje prilagođenih phishing stranica uz pomoć LLM modela, kao i direktno povezivanje s enterprise SIEM sustavima radi korelacije događaja u stvarnom okruženju. Također, mogućnost izvoza rezultata u standardizirane

sigurnosne formate (kao što su STIX/TAXII) predstavlja sljedeći logičan korak prema profesionalnoj uporabi u velikim organizacijama.

Važno je istaknuti da je primarni cilj svih funkcionalnosti jeshke usmjeren na poboljšanje sigurnosti, a ne na zlouporabu. Sustav omogućuje sigurnosnim timovima da provode legalne i etičke phishing simulacije, analiziraju ranjivosti i treniraju korisnike, čime se povećava otpornost organizacije na stvarne napade. U vremenu kada su socijalni inženjering i phishing među najčešćim vektorima proboja, ovakvi alati omogućuju da se organizacije pripreme, testiraju i unaprijede svoje sigurnosne mjere bez rizika narušavanja integriteta.

Cijeli rad prikazuje mogućnost povezivanja teorijskih koncepata i praktične implementacije u području informacijske sigurnosti. Kombinacija psiholoških aspekata socijalnog inženjeringa, tehničkih mehanizama i automatizacije omogućila je izradu sustava koji ilustrira cjelokupan tijek sigurnosnog napada, od prikupljanja informacija do faze interakcije s korisnikom. Time se naglašava važnost razumijevanja napadačkog procesa u cjelini, kako u svrhu zaštite organizacija, tako i u kontekstu edukacije sigurnosnih stručnjaka.

Razvijeni framework jeshka predstavlja funkcionalni prototip koji demonstrira primjenu sustavnog i modularnog pristupa u analizi i simulaciji suvremenih prijetnji. Uz teorijsku podlogu i praktičnu realizaciju, rad doprinosi boljem razumijevanju metoda socijalnog inženjeringa i automatizacije unutar sigurnosnih istraživanja te ukazuje na mogućnosti daljnjeg unaprjeđenja i proširenja sustava u budućim istraživanjima.

Popis literature

[1] Poslovni.hr, “U pet godina kibernetički kriminal u RH udvostručen,” 2025. Online. Dostupno na: https://www.poslovni.hr/hrvatska/u-pet-godina-kiberneticki-kriminal-u-rh-udvostrucen-4505134. Preuzeto 2.12.2025.

[2] Sigurnosno-obavještajna agencija Republike Hrvatske, “Značajan napredak Republike Hrvatske u 2025. godini u kibernetičkoj sigurnosti,” 2024. Online. Dostupno na: https://soa.hr/hr/znacajan-napredak-republike-hrvatske-u-2025-godini-u-kibernetickoj-sigurnosti-i-digitalnoj-otpornosti/325. Preuzeto 2.12.2025.

[3] Wahl, “Kibernetička sigurnost u Republici Hrvatskoj: izazovi implementacije,” 2024. Online. Dostupno na: https://www.wahl.hr/hr/insight/cybersecurity-in-the-republic-of-croatia-implementation-challenges. Preuzeto 2.12.2025.

[4] Tportal.hr, “Kibernetička sigurnost u Hrvatskoj: Svijest raste, ali stručnjaka nedostaje,” 2025. Online. Dostupno na: https://www.tportal.hr/tehno/clanak/kiberneticka-sigurnost-u-hrvatskoj-svijest-raste-ali-strucnjaka-i-ulaganja-jos-uvijek-nedost. Preuzeto 2.12.2025.

[5] Nacionalni CERT, “ožujak 2025,” CERT-HR, 2025. Online. Dostupno na: https://www.cert.hr/2025/03/. Preuzeto 2.12.2025.

[6] Nacionalni CERT, “listopad 2025,” CERT-HR, 2025. Online. Dostupno na: https://www.cert.hr/2025/10/. Preuzeto 2.12.2025.

[7] Nacionalni CERT, “Tag: Upozorenje,” CERT-HR, 2025. Online. Dostupno na: https://www.cert.hr/tag/upozorenje/. Preuzeto 2.12.2025.

[8] Nacionalni CERT, “svibanj 2025,” CERT-HR, 2025. Online. Dostupno na: https://www.cert.hr/2025/05/. Preuzeto 2.12.2025.

[9] Nacionalni CERT, “2025,” CERT-HR, 2025. Online. Dostupno na: https://www.cert.hr/2025/. Preuzeto 2.12.2025.

[10] Nacionalni CERT, “ECSM 2025: Kibernetički kriminalci iskorištavaju vaše javne podatke i vaše emocije,” CERT-HR, 2025. Online. Dostupno na: https://www.cert.hr/ecsm-2025-kiberneticki-kriminalci-iskoristavaju-vase-javne-podatke-i-vase-emocije/. Preuzeto 2.12.2025.

[11] M. Miletić, “Illegal Cyber Activities,” Balkan Criminology, 2019. Online. Dostupno na: https://www.balkan-criminology.eu/wp-content/uploads/2019/02/Miletic.pdf. Preuzeto 3.12.2025.

[12] INSECM, “Phishing Vishing Smishing: Beneficial Actions for Detection and Prevention,” 2024. Online. Dostupno na: https://insecm.ca/en/newsletter/phishing-vishing-smishing-beneficial-actions-for-detection-and-prevention/. Preuzeto 3.12.2025.

[13] Bug.hr, “Godišnji izvještaj Nacionalnog CERT-a: Manje je incidenata, phishing i dalje vodeći,” 2025. Online. Dostupno na: https://www.bug.hr/sigurnost/godisnji-izvjestaj-nacionalnog-cert-a-manje-je-incidenata-phishing-i-dalje-48767. Preuzeto 2.12.2025.

[14] Nacionalni CERT (CERT-HR), “Phishing,” 2023. Online. Dostupno: https://www.cert.hr/phishing/. Preuzeto: 3.12.2025.

[15] Fakultet organizacije i informatike, “OSINT - Open Source Intelligence,” *SIS Wiki - FOI*, 2012. Online. Dostupno na: https://security.foi.hr/wiki/index.php/OSINT_-_Open_Source_Intelligence.html. Preuzeto: 3.12.2025.

[16] M. Petr, “Analiza sigurnosnih prijetnji preko OSINT-a,” *LSS*, 2018. Online. Dostupno na: http://nevena.lss.hr/recordings/fer/predmeti/racfor/2018/seminari_2018_2019/mpetr/seminar.pdf. Preuzeto: 3.12.2025.

[17] Lupa, “OSINT (Open Source Inteligence),” *Mrežni leksikon*, n.d. Online. Dostupno na: https://lupa.lupiga.com/mrezni-leksikon/osint-open-source-inteligence. Preuzeto: 4.12.2025.

[18] Eduza, “Andrea Stepić: Open Source Intelligence (OSINT) nova je digitalna kompetencija,” *Eduza*, 2025. Online. Dostupno na: https://www.eduza.hr/blog/andrea-stepic-open-source-intelligence-osint-nova-je-digitalna-kompetencija-za-sve-koji-zele-donositi-. Preuzeto: 4.12.2025.

[19] Portal Interno, “Obavještajni ciklus,” 2023. Online. Dostupno na: https://internocg.me/opservacija/obavjestajni-ciklus/. Preuzeto: 4.12.2025.

[20] Hrčak, “Informacije Iz Otvorenih Izvora - Osnova Za Poslovno-obavještajnu Analitiku,” n.d. Online. Dostupno na: https://hrcak.srce.hr/clanak/418673. Preuzeto: 4.12.2025.

[21] Eduza, “Kako prepoznati prijetnje i smanjiti rizike,” n.d. Online. Dostupno na: https://www.eduza.hr/kako-prepoznati-prijetnje-i-smanjiti-rizike-prije-nego-sto-postanu-problemi/639/. Preuzeto: 6.12.2025.

[22] OSINTCOE, “Odjel za metodologiju i doktrinu,” n.d. Online. Dostupno na: https://www.osintcoe.hr/odjeli/odjel-za-metodologiju-i-doktrinu/81. Preuzeto: 6.12.2025.

[23] OSINTCOE, “O Centru,” n.d. Online. Dostupno na: https://www.osintcoe.hr/o-centru/9. Preuzeto: 6.12.2025.

[24] Repozitorij FPZG, “Obavještajna analiza i donošenje odluka,” n.d. Online. Dostupno na: https://repozitorij.fpzg.unizg.hr/islandora/object/fpzg:2257/datastream/PDF/view. Preuzeto: 6.12.2025.

[25] NaVKiS, “OSINT,” CTF.xfer.hr, n.d. Online. Dostupno na: https://ctf.xfer.hr/lekcije/osint/o_osintu/. Preuzeto: 7.12.2025.

[26] NSK Zir, “OSINT – analiza društvenih mreža i blogova kao izvora,” n.d. Online. Dostupno na: https://zir.nsk.hr/islandora/object/vvg:241/datastream/PDF/view. Preuzeto: 7.12.2025.

[27] Unite.ai, “10 najboljih alata Open Source Intelligence (OSINT),” 2024. Online. Dostupno na: https://www.unite.ai/hr/best-open-source-intelligence-osint-tools/. Preuzeto: 7.12.2025.

[28] Maltego, “Maltego – Transformacija podataka u inteligenciju,” 2025. Online. Dostupno na: https://www.maltego.com/. Preuzeto: 8.12.2025.

[29] SpiderFoot, “SpiderFoot – Automatizirani OSINT sustav,” 2025. Online. Dostupno na: https://www.spiderfoot.net/. Preuzeto: 8.12.2025.

[30] theHarvester Project, “theHarvester – OSINT alat za prikupljanje e-mailova i domena,” 2025. Online. Dostupno na: https://github.com/laramies/theHarvester. Preuzeto: 8.12.2025.

[31] Shodan, “Shodan – tražilica za internetom povezane uređaje,” 2025. Online. Dostupno na: https://www.shodan.io/. Preuzeto: 8.12.2025.

[32] Censys, “Censys – pretraživanje internetske infrastrukture,” 2025. Online. Dostupno na: https://search.censys.io/. Preuzeto: 8.12.2025.

[33] FOCA, “FOCA – alat za analizu metapodataka i dokumenata,” 2025. Online. Dostupno na: https://github.com/ElevenPaths/FOCA. Preuzeto: 8.12.2025.

[34] Recon-ng, “Recon-ng – modularni OSINT framework,” 2025. Online. Dostupno na: https://github.com/lanmaster53/recon-ng. Preuzeto: 8.12.2025.

[35] OWASP, “OWASP Amass – projekt za mapiranje domena i infrastrukture,” 2025. Online. Dostupno na: https://github.com/owasp-amass/amass. Preuzeto: 8.12.2025.

[36] A. Stepić, “OSINT: Tajno oružje korporativne sigurnosti,” LinkedIn, 14.5.2025. Online. Dostupno na: https://www.linkedin.com/pulse/osint-tajno-oru%C5%BEje-korporativne-sigurnosti-za-koje-mo%C5%BEda-stepi%C4%87-dfd2f. Preuzeto: 8.12.2025.

[37] Kaspersky, “OSINT: what’s the danger, and how to stay safe,” 31.8.2023. Online. Dostupno na: https://www.kaspersky.com/blog/osint-open-source-intelligence/48911/. Preuzeto: 8.12.2025.

[38] Eithos, “Open Source Intelligence (OSINT): Its Legal and Ethical Aspects,” 2025. Online. Dostupno na: https://eithos.eu/open-source-intelligence-osint-its-legal-and-ethical-aspects. Preuzeto: 8.12.2025.

[39] American Journal of International Law, “Ethical Considerations for Open-Source Investigations Into International Crimes,” Cambridge University Press, 2023. Online. Dostupno na: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ethical-considerations-for-opensource-investigations-into-international-crimes/FE78D42FD4D344F6B1EE98413C20B5DF. Preuzeto: 9.12.2025.

[40] P. Alsharnouby, F. Alaca i S. Chiasson, “Phishing attacks: Past, present and future,” *Journal of the Economy of the Household*, vol. XX, 2021. Online. Dostupno na: https://journals.sagepub.com/doi/full/10.1177/10567879221082966. Preuzeto: 9.12.2025.

[41] Fortinet, “Types of phishing attacks,” n.d. Online. Dostupno na: https://www.fortinet.com/uk/resources/cyberglossary/types-of-phishing-attacks. Preuzeto: 9.12.2025.

[42] *Applied Sciences*, “Social Engineering Attacks and Human Factors,” MDPI, 2022. Online. Dostupno na: https://www.mdpi.com/2076-3417/12/12/6042. Preuzeto: 9.12.2025.

[43] *Journal of Information Security and Applications*, “Human vulnerabilities in social engineering: cognitive and emotional triggers,” ScienceDirect, 2021. Online. Dostupno na: https://www.sciencedirect.com/science/article/pii/S2451958821000749. Preuzeto: 9.12.2025.

[44] ResearchGate, “The Psychology of Social Engineering,” 2024. Online. Dostupno na: https://www.researchgate.net/publication/382581466_The_psychology_of_social_engineering. Preuzeto: 10.12.2025.

[45] International Journal of Advanced and Applied Sciences, “Social Engineering Behavioural Patterns,” 2024. Online. Dostupno na: https://www.science-gate.com/IJAAS/2024/V11I4/1021833ijaas202404016.html. Preuzeto: 10.12.2025.

[46] *Research and Reviews: Journal of Engineering and Technology*, “Social Engineering as a Driving Force for Innovation in Cybersecurity,” 2023. Online. Dostupno na: https://www.rroij.com/open-access/social-engineering-as-a-driving-force-for-innovation-in-cybersecurity.php?aid=93744. Preuzeto: 10.12.2025.

[47] zvelo, “The Anatomy of a Phishing Attack,” 2023. Online. Dostupno na: https://zvelo.com/anatomy-of-a-phishing-attack. Preuzeto: 10.12.2025.

[48] Tegodata, “The Anatomy of a Phishing Attack – Part 1,” 2023. Online. Dostupno na: https://tegodata.com/the-anatomy-of-a-phishing-attack-part-1. Preuzeto: 10.12.2025.

[49] Varonis, “Whitepaper – Anatomy of a Phish,” 2023. Online. Dostupno na: https://info.varonis.com/whitepaper-anatomy-of-a-phish. Preuzeto: 10.12.2025.

[50] NordVPN, “URL spoofing: što je i kako ga izbjeći,” NordVPN Blog, 2024. Online. Dostupno na: https://nordvpn.com/blog/url-spoofing/. Preuzeto: 10.12.2025.

[51] McAfee, “What Is Typosquatting?,” McAfee Learn, 2024. Online. Dostupno na: https://www.mcafee.com/learn/what-is-typosquatting. Preuzeto: 10.12.2025.

[52] Digital.ai, “How to Obfuscate JavaScript Code,” Digital.ai Blog, 2023. Online. Dostupno na: https://digital.ai/catalyst-blog/obfuscate-javascript-code. Preuzeto: 10.12.2025.

[53] TheCoinZone, “HTML Code Obfuscator – Protect Your Source Code,” TheCoinZone Software, n.d. Online. Dostupno na: https://www.thecoinzone.com/software/html-code-obfuscator. Preuzeto: 10.12.2025.

[54] NordLayer, “Browser-in-the-Browser (BitB) attack: kako radi i kako se zaštititi,” NordLayer Learn, 2024. Online. Dostupno na: https://nordlayer.com/learn/browser-security/bitb-attack. Preuzeto: 11.12.2025.

[55] Heroku, “SSL Certificate Self,” Heroku Dev Center, n.d. Online. Dostupno na: https://devcenter.heroku.com/articles/ssl-certificate-self. Preuzeto: 11.12.2025.

[56] Urllo, “Why You Should Not Use URL Masking / Forwarding / Cloaking,” Urllo Resources, n.d. Online. Dostupno na: https://www.urllo.com/resources/learn/why-you-should-not-use-url-masking-forwarding-cloaking. Preuzeto: 11.12.2025.

[57] Let’s Encrypt, “Let’s Encrypt – Free SSL/TLS Certificates,” 2025. Online. Dostupno na: https://letsencrypt.org/. Preuzeto: 12.12.2025.

[58] Proofpoint, “Malicious Email Attachments: Threat Reference,” Proofpoint Threat Center, n.d. Online. Dostupno na: https://www.proofpoint.com/au/threat-reference/malicious-email-attachments. Preuzeto: 12.12.2025.

[59] SecureWorld, “Top 7 MFA Bypass Techniques,” SecureWorld News, 2023. Online. Dostupno na: https://www.secureworld.io/industry-news/top-7-mfa-bypass-techniques. Preuzeto: 12.12.2025.

[60] ResearchGate, “Study of Phishing Attack and their Prevention Techniques,” 2024. Online. Dostupno na: https://www.researchgate.net/publication/385083853_Study_of_Phishing_Attack_and_their_Prevention_Techniques. Preuzeto: 12.12.2025.

[61] PubMed Central, “A Systematic Review of Phishing Attacks and Defenses,” 2021. Online. Dostupno na: https://pmc.ncbi.nlm.nih.gov/articles/PMC8478002. Preuzeto: 12.12.2025.

[62] ACM Digital Library, “Phishing Detection and Prevention in E-mail Systems,” 2020. Online. Dostupno na: https://dl.acm.org/doi/abs/10.1145/3410352.3410825. Preuzeto: 13.12.2025.

[63] Journal of Network and Computer Applications, “Comprehensive Frameworks for Phishing Attack Mitigation,” ScienceDirect, 2025. Online. Dostupno na: https://www.sciencedirect.com/science/article/pii/S092054892500011X. Preuzeto: 13.12.2025.

[64] Warmup Inbox, “SPF, DKIM, DMARC: Complete Guide to Email Authentication,” Warmup Inbox Blog, 2025. Online. Dostupno na: https://www.warmupinbox.com/blog/email-marketing/spf-dkim-dmarc/. Preuzeto: 14.12.2025.

[65] DNS Made Easy, “Domain Management Resources,” DNS Made Easy, 2025. Online. Dostupno na: https://dnsmadeeasy.com/resources/domain-management. Preuzeto: 15.12.2025.

Popis slika

Popis tablica