SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 3057

ISPITIVANJE ALATA ZA PROVOĐENJE NAPADA DRUŠTVENIM INŽENJERINGOM I TRENIRANJE ZAPOSLENIKA

Iva Brcković

Zagreb, lipanj 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 3057

ISPITIVANJE ALATA ZA PROVOĐENJE NAPADA DRUŠTVENIM INŽENJERINGOM I TRENIRANJE ZAPOSLENIKA

Iva Brcković

Zagreb, lipanj 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 11. ožujka 2022.

DIPLOMSKI ZADATAK br. 3057

Pristupnica:	**Iva Brcković (0036509120)**
Studij:	Računarstvo
Profil:	Računarska znanost
Mentor:	doc. dr. sc. Stjepan Groš

Zadatak: **Ispitivanje alata za provođenje napada društvenim inženjeringom i treniranje zaposlenika**

Opis zadatka:

Jedan od temeljnih vektora napada na korisnike je slanje phishing poruka elektroničke pošte koje potom vode žrtvu na stranice na kojima se traže povjerljivi podaci. Zaštita od takvih napada je jako teška, a edukacija je svakako jedan od temeljnih načina na koji se to postiže. Iz tog razloga napravljen je niz alata koji služe za provođenje napada društvenim inženjeringom, ali i alata koji se koriste za treniranje zaposlenika kao i za provođenje napada. Ti alati dijele određene zajedničke karakteristike te su zbog toga srodni. U sklopu diplomskog rada potrebno je pronaći i proučiti alate za provođenje napada društvenim inženjeringom te za treniranje zaposlenika kako bi bili otporni od takvih napada. Demonstrirati rad tih alata na nekom kontroliranom primjeru, a također razviti mehanizme za procjenu rizika od napada društvenim inženjeringom. Citirati korištenu literaturu i navesti dobivenu pomoć.

Rok za predaju rada: 27. lipnja 2022.

Sadržaj

1. Uvod

Društveni inženjering je skup metoda s kojima napadači dobivaju pristup osjetljivim informacijama ili manipuliraju žrtvama da izvode određenu radnju što će rezultirati narušavanjem sigurnosti računalnog sustava. Umjesto da napadači iskorištavaju ranjivosti u računalnim sustavima, metodama društvenog inženjeringa iskorištavaju ljudsku psihologiju, točnije iskorištavaju ljudske mane u procesu donošenja odluka [1].

Jedan od vektora napada društvenim inženjeringom je phishing ili mrežna krađa podataka. Phishing je tehnika društvenog inženjeringa u kojoj napadač šalje poruke elektroničke pošte koje oponašaju pouzdane izvore. Cilj phishinga je pristup osjetljivim informacijama, isporuka maliciozne datoteke ili skupljanje vjerodajnica. Za provedbu phishing napada je potrebno manje tehničkog znanja nego za iskorištavanje ranjivosti sustava, a posljedice za organizacije su svejedno značajne. Posljedice mogu biti povreda osobnih podataka, kompromitiranje računa, gubitak intelektualne imovine, reputacijska šteta i tako dalje [2]. Zbog jednostavnosti napada i značajnih rezultata phishing napadi su sve češći te je u 2021. godini 86% organizacija bila meta phishing napada [2].

Zbog učestalosti phishing napada organizacije se moraju adekvatno zaštititi, a jedan dio zaštite je edukacija korisnika. Za edukaciju o phishingu organizacije provode simulacije phishing napada u kojima šalju phishing poruke elektroničke pošte zaposlenicima kako bi ispitali koliko zaposlenika će prepoznati phishing napad. Simulaciju phishing napada organizacijama mogu olakšati alati za provođenje napada jer automatski postavljaju određene funkcionalnosti poput web poslužitelja te omogućavaju pregled rezultata simulacije.

Tema ovog rada je pregled alata koji se koriste za postavljanje phishing simulacija. Cilj korištenja alata je utvrditi koliko alati olakšavaju pokretanje phishing simulacija te koliko su korisni za treniranje zaposlenika.

U drugom poglavlju objašnjeni su phishing napadi i obrana od njih. Opisane su različite metode, tipovi napada i teme koje napadači koriste u phishing napadima. Objašnjeni su različiti načini obrane od phishing napada te kako provesti kvalitetnu phishing simulaciju. Treće poglavlje je fokusirano na alate za edukaciju korisnika i penetracijsko ispitivanje.

Prikazano je korištenje alata te razlika između njih. U četvrtom poglavlju opisani su mehanizmi za procjenu phishing rizika organizacije.

2. Phishing

Prvi phishing napad se dogodio u 1995. godini na AOL aplikaciji za razmjenu poruka [3]. Tijekom napada napadači su se pretvarali da su AOL zaposlenici te tražili lozinke od žrtava. 25 godina nakon toga phishing je postao daleko najčešći napad na Internetu s čak dvostruko više napada od ostalih vrsta računalnih napada [3]. U 2021. godini 15 milijuna poruka elektroničke pošte je prijavljeno za pokušaj phishing napada u Proofpoint alatu [2].

Phishing napad se može razdvojiti u pet faza. Prva faza je planiranje koja uključuje pronalazak ciljanih korisnika, traženje informacija i pripremanje resursa potrebnih za napad. Druga faza je pokretanje napada sa stvorenim resursima. Treća faza je infiltracija u kojoj napadač pomoću dobivenih informacija dobiva pristup traženim osobnim podacima. Sljedeća faza je prikupljanje i iskorištavanje podataka u kojoj napadač izdvaja informacije i koristi ih za postizanje različitih ciljeva. Ciljevi mogu biti lažno predstavljanje kao žrtva ili prodaja osobnih podataka. U zadnjoj fazi napadači uklanjaju što je više moguće dokaza o napadu [4].

Phishing napadi se mogu podijeliti prema korištenom mediju, vektoru ili tehničkom pristupu [4].

Medij je metoda pomoću koje napadač komunicira s potencijalnim žrtvama. Za phishing napade napadač za medij može koristiti glas, SMS ili Internet [4].

Sljedeća podjela phishing napada je prema vektorima. Vektor je kanal kroz koji se provodi phishing napad. Prema vektoru phishing napadi se mogu podijeliti na *vishing* ili glas, *smishing* (SMS ili MMS), elektronička pošta, faks, trenutačne poruke, društvene mreže, web stranice i Wi-Fi [4].

Tehnički pristupi su metode koje se koriste tijekom napada [4]. Neki od tehničkih pristupa su masovni phishing, *spear phishing*, *whaling*, kompromitacija poslovnog računa elektroničke pošte i *QRishing*.

Masovni phishing je neselektivni phishing napad u kojem se ista poruka elektroničke pošte šalje mnogim korisnicima [2]. Poruke elektroničke pošte nisu personalizirane zbog čega uspješnost napada može biti manja. Nadalje, poruke elektroničke pošte u masovnoj krađi identiteta sadrže URL adresu phishing web stranice ili malicioznu datoteku koja

iskorištava stariju poznatu ranjivost. Umjesto ulaganja više truda u poruke elektroničke pošte, napadači se oslanjaju na veliki volumen da pronađu žrtve. Masovni phishing je najčešći tip phishing napada. U 2021. godini 86% organizacija se suočilo s masovnim phishingom [2].

Za razliku od masovnog phishing napada, *spear phishing* napadi su ciljani napadi upućeni odabranim osobama [2]. U *spear phishing* napadu napadači koriste personalizirane poruke elektroničke pošte kako bi se poboljšala vjerojatnost da će napad biti uspješan. Za personalizaciju poruke napadač se pretvara da je osoba koju žrtva poznaje ili koristi informacije o žrtvi u porukama elektroničke pošte. Cilj *spear phishing* napada je dobivanje pristupa sustavu organizacije ili isporuka ucjenjivačkog softvera (engl. *ransomware*) [4]. Ucjenjivački softver onemogućava korisniku pristup datotekama na računalu te traži plaćanje otkupnine za dobivanje pristupa.

Whaling je metoda slična *spear phishing* metodi, ali razlika je u tome što su mete visokopozicionirani zaposlenici čija im pozicija omogućuje privilegiran pristup podacima unutar organizacije [4]. Cilj *whaling* napada je isti kao kod *spear phishing* napada, to jest dobivanje pristupa sustavu organizacije.

Tijekom 2021. godine 79% organizacija se suočilo s dvije prethodno opisane vrste napada, odnosno sa *spear phishing* i *whaling* napadima [2].

Kompromitacija poslovnog računa elektroničke pošte (engl. *business email compromise*, BEC) je napad u kojem napadač, nakon što dobije pristup poslovnom računu elektroničke pošte, oponaša žrtvu u cilju prijevare organizacije, kupaca ili partnera. Prijevara je najčešće financijska te se napad sastoji od manipulacije žrtve da pošalje novac na račun napadača [5]. Jedna od tehnika korištenih u BEC napadima je lažiranje (engl. *spoofing*) adresa elektroničke pošte. Napadači koriste račun elektroničke pošte s domenom koja je što sličnija domeni organizacije kako bi povećali svoje šanse za uspješan napad. U BEC napadima najčešće se oponaša izvršni direktor organizacije te je on najčešća meta tih napada [4]. Ova vrsta napada je prvi put prijavljena u 2013. godini, a 2021. godine 77% organizacija se suočilo s tim napadom [2].

QRishing je phishing napad za koji napadač napravi QR kod koji sadrži URL adresu phishing web stranice ili URL adresu za preuzimanje maliciozne datoteke. Za korisnika je napad teži za otkriti jer nije moguće razumjeti sadržaj QR koda bez aplikacije kojom se on čita. Nadalje, neke aplikacije za čitanje QR kodova ne traže dopuštenje korisnika za

preusmjeravanje na stranicu već ju automatski otvore [4]. Također, napad može biti teže otkriti jer napadač može koristiti servise za skraćivanje linkova što otežava analizu URL adrese.

U phishing porukama elektroničke pošte napadači koriste različite tehnike uvjeravanja. Tehnike uvjeravanja pomažu napadaču da nagovori zaposlenika da zaobiđe procedure organizacije kako bi dobio željene informacije. Napadači mogu kao tehniku uvjeravanja koristiti autoritet, hitnost, tradiciju, prijetnju, privlačnost, sažaljenje, pristojnost ili formalnost. Najčešće tehnike uvjeravanja su autoritet i hitnost koje su ujedno i najučinkovitije [6] [7].

Phishing poruke elektroničke pošte se mogu analizirati i prema okidačima. Okidači se mogu definirati kao predmet ili tema phishing poruke. Najčešće teme u phishing porukama elektroničke pošte su razna upozorenja, verifikacija računa i neuspješni pokušaji prijave [6]. Međutim, to nisu najučinkovitije teme. Neke od najučinkovitijih tema su dostava, narudžba, nova faks poruka i pritužba [7]. Napadači koriste i aktualne teme poput pandemije koronavirusa, Olimpijskih igara i rata u Ukrajini [8].

Za skupljanje vjerodajnica napadači koriste phishing web stranice. Phishing web stranice mogu biti kopije poznatih web stranica ili lažne web stranice. Za kopije napadači mogu napraviti kopije web stranica društvenih mreža ili financijskih institucija, a za lažne web stranice u 2021. godini napadači su radili lažne servise za internetski prijenos (engl. *streaming*) [2]. Kod kopija web stranica napadači koriste URL adresu što sličniju onoj od legitimne web stranice kako bi zavarali korisnika. Postoji sedam tehnika za lažiranje URL adrese [9]. Prva tehnika je korištenje IP adrese u URL adresi, primjerice http:// 198.51.100.5. Kao druga tehnika koristi se nepovezana domena bez marke poput http://www.account.com. Treća tehnika je korištenje nepovezane domene gdje je marka u poddomeni, primjerice http://facebook.kdjsbd.com. Sljedeća tehnika je nepovezana domena, a marka se nalazi u putu URL adrese, primjerice http://www.account.com/www.facebook.com. Zatim, postoji tehnika u kojoj se koriste izvedene domene poput http://www.facebook-login.com. Šesta tehnika je korištenje domena koje imaju pravopisne pogreške, primjerice http://www.facebok.com. U zadnjoj tehnici napadači zamjenjuju određene znakove, primjerice http://www.faceb00k.com.

U slučaju kada je zaposlenik neke organizacije žrtva phishing napada, napad može imati velike posljedice za organizaciju. Najčešće posljedice za organizacije u 2021. godini su bile povreda podataka o klijentima, kompromitiranje računa, infekcija ucjenjivačkim

softverom i gubitak podataka ili intelektualnog vlasništva. Nadalje, sve više phishing napada je uspješno. U 2021. godini 83% napada na organizacije je bilo uspješno u odnosu na 2020. godinu u kojoj je 57% napada bilo uspješno [2]. Jedan od čimbenika koji nije bio prisutan u prijašnjim godinama je pandemijski umor. Pandemijski umor je definiran kao demotivacija da se slijede preporučene zaštitne mjere što se postupno pojavljuje tijekom vremena. Zbog pandemijskog umora zaposlenici imaju manji radni učinak što može utjecati i na podložnost phishing napadima [2].

2.1. Obrana od phishing napada

Zbog velikih posljedica i sve veće uspješnosti phishing napada organizacije trebaju imati djelotvornu obranu od njih. Obrana zaposlenika se sastoji od tehničkih pristupa i treniranja ili edukacije zaposlenika.

U tehničke pristupe pripadaju filtriranje phishing poruka elektroničke pošte, zaštita od phishing web stranica i korištenje alata za prijavu phishing napada. Poruke elektroničke pošte se mogu filtrirati prema raznim značajkama poput IP adrese ili domene pošiljatelja, adrese elektroničke pošte pošiljatelja ili umetnutih linkova. Za zaštitu od phishing web stranica potrebno je koristiti proširenja u web preglednicima koji blokiraju pristup URL adresama na kojima je detektiran phishing napad [10]. Alatima za prijavu phishing napada zaposlenici prijavljuju sumnjivu poruku elektroničke pošte sigurnosnom timu organizacije. U slučaju da je poruka elektroničke pošte pokušaj phishing napada, prijava omogućuje sigurnosnom timu da poduzme potrebne akcije poput promjene lozinke zaposlenicima.

Međutim, nijedno tehničko rješenje ne zaustavlja potpuno phishing napade, zbog čega je potrebno da ih korisnici znaju prepoznati. Međutim, većina korisnika ne zna ispravno identificirati phishing web stranice. Čak 90% korisnika za prepoznavanje phishing web stranice koristi izgled [7]. Izgled se ne treba koristiti za prepoznavanje phishing napada jer postoje alati koji imaju mogućnost kloniranja web stranica. Nadalje, korisnici misle da simbol zatvorenog lokota za HTTPS znači da je stranica legitimna [7]. Korisnike prvo treba naučiti da moraju biti pažljivi kada ih pošiljatelj traži osjetljive informacije, da kliknu na link ili da otvore priloženu datoteku. Sljedeće, korisnici trebaju znati uobičajene metode korištene u phishing napadima poput autoriteta i hitnosti. Zadnje, korisnici trebaju naučiti kako analizirati URL adresu i adresu elektroničke pošte pošiljatelja.

Organizacija može educirati zaposlenike materijalima za učenje ili phishing simulacijama. Materijali za učenje mogu biti tekstualni, videa, računalne igrice ili predavanja uživo. U jednom istraživanju je dokazano da su računalne igrice najučinkovitija metoda za edukaciju korisnika [11]. Neke od računalnih igrica za edukaciju korisnika o phishing napadima su *Anti-Phishing Phil*, *What.Hack* i *NoPhish*. *Anti-Phishing Phil* igrica uči korisnika kako identificirati phishing URL adrese [11]. U igrici cilj je da riba s kojom korisnik upravlja jede crve koji nad njima imaju legitimne URL adrese. Umjesto da se korisnika uči samo o phishing URL adresama, *What.Hack* je računalna igrica napravljena za učenje kako prepoznati phishing poruku elektroničke pošte [12]. Analizom poruke elektroničke pošte u igrici korisnik treba odlučiti hoće li na nju odgovoriti, prijaviti phishing napad ili zatražiti pomoć za analizu. Pri svakoj odluci korisnik ima pristup popisu pravila koje treba koristiti za identifikaciju phishing napada. *NoPhish* je mobilna aplikacija koja je usredotočena na učenje korisnika o phishing URL adresama [9]. Phishing URL adrese su podijeljene u sedam kategorija, to jest za korisnika u sedam razina. U svakoj razini korisnik prvo treba pročitati informacije o određenoj kategoriji phishing URL adresa, a zatim riješiti kviz. U kvizovima korisnik treba odlučiti je li zadana URL adresa phishing ili legitimna prema sadržaju koji je prethodno pročitao.

Međutim, materijali za učenje ne mogu potpuno reproducirati uvjete u stvarnom životu, zbog čega organizacije koriste phishing simulacije za treniranje zaposlenika. Tijekom phishing simulacija zaposlenici primaju poruke elektroničke pošte slične porukama korištenim u phishing napadima. Phishing simulacije se mogu provoditi na dva načina. Prvi način je da organizacija šalje poruke elektroničke pošte zaposlenicima u svrhu edukacije. Nakon što korisnik postane žrtva simuliranog napada, prikazuje mu se web stranica s informacijama o phishing napadima i kako ih izbjeći. Drugi način je tijekom penetracijskog ispitivanja. Penetracijsko ispitivanje je dozvoljena simulacija računalnog napada koja se provodi za procjenu sigurnosti sustava. Jedan od tipova penetracijskog ispitivanja je društveni inženjering koji uključuje simulaciju phishing napada [13]. Za razliku od simulacija koje pokreće organizacija, korisnik neće biti obaviješten da je žrtva phishing napada te se uhvaćene vjerodajnice mogu iskoristiti za pronalazak drugih sigurnosnih ranjivosti.

Tijekom planiranja phishing simulacija, organizacije trebaju pažljivo odrediti karakteristike simulacije jer neke od njih utječu na uspješnost učenja korisnika. Zbog toga organizacije trebaju slijediti nekoliko sljedećih uputa tijekom phishing simulacija.

Prvo, phishing simulacije potrebno je provoditi redovito. Između simulacija ne smije biti veći razmak od pet mjeseci inače će zaposlenici zaboraviti što su prethodno naučili [7].

Zatim, phishing simulacije trebaju koristiti različite tehnike uvjeravanja jer se podložnost različitim tehnikama razlikuje po dobi. Mlađi ljudi su podložniji phishing napadu kada se koristi tehnika oskudice, a stariji ljudi kada se koristi tehnika uzvraćanja. U tehniku oskudice pripadaju poruke elektroničke pošte koje nude limitirani broj određenog proizvoda, a u tehniku uzvraćanja pripadaju poruke elektroničke pošte koje nagovaraju korisnika da instalira zlćudni program u zamjenu za besplatni proizvod [14].

Sljedeće, organizacije trebaju osmisliti phishing simulacije o različitim temama. Istraživanja koja su ispitivala koje su teme poruka elektroničke pošte najučinkovitije imaju različite rezultate. Primjerice, jedno istraživanje je dokazalo da su najučinkovitiji phishing napadi oni koji koriste poruke elektroničke pošte s pravnim temama, a najmanje učinkoviti su oni s financijskim temama, što je ujedno i najčešća tema u phishing napadima [14]. Međutim, drugo istraživanje je dokazalo da su dostava i narudžba najučinkovitije teme u phishing simulacijama [7]. Zbog različitih rezultata organizacije bi trebale proći različite teme u simulacijama.

Zaposlenici u organizaciji će imati različita predznanja i učit će različitom brzinom. Nadalje, korisnici bolje uče ako je težina phishing simulacije prilagođena njima jer je veća vjerojatnost da će uspješno prepoznati phishing napad [7]. Zbog toga je potrebno raspodijeliti zaposlenike u više grupa po njihovom znanju o phishing napadu. Kada zaposlenik nauči gradivo jedne skupine, potrebno ga je premjestiti u skupinu s težim simulacijama.

3. Phishing alati

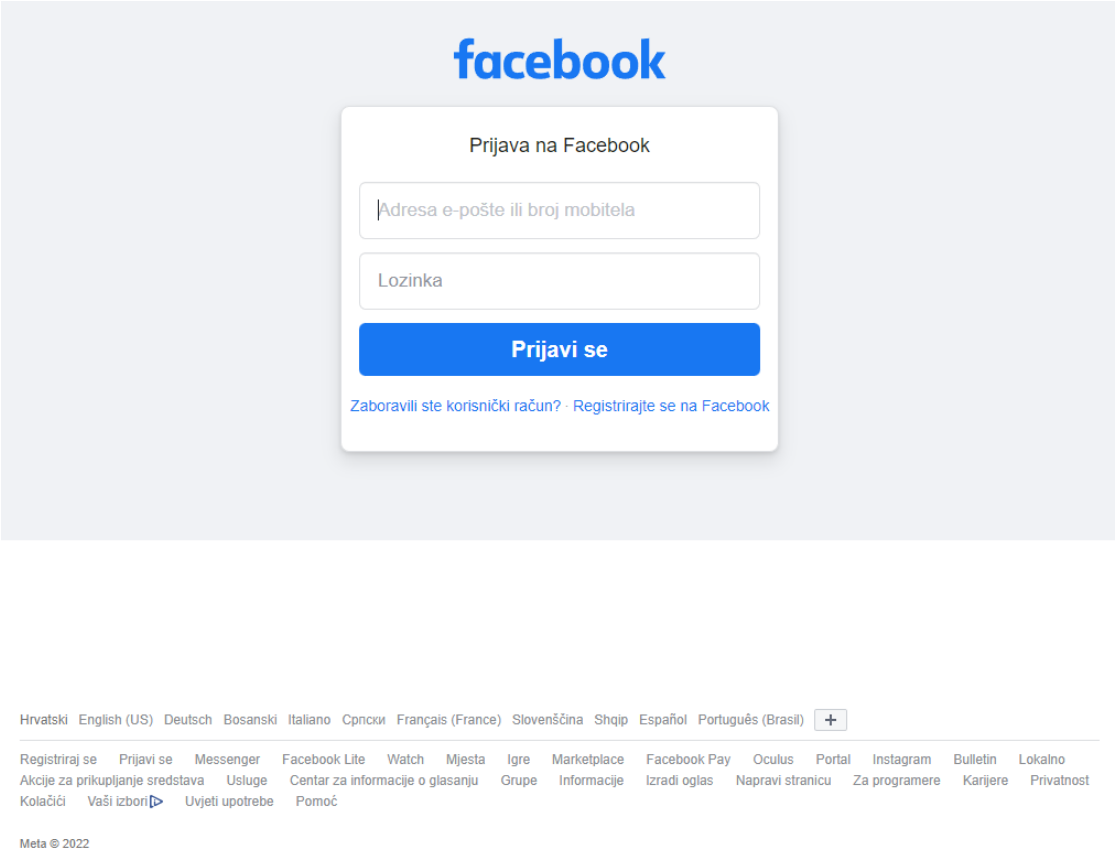
Kako bi si olakšale provođenje phishing simulacija, organizacije mogu koristiti razne phishing alate. Phishing alati imaju različite mogućnosti poput pokretanja web poslužitelja za phishing web stranicu, slanje phishing poruka elektroničke pošte, praćenje rezultata simulacije, generiranje phishing poruka elektroničke pošte ili web stranica i tako dalje. Alate je moguće podijeliti prema primarnoj svrsi na alate za edukaciju korisnika, alate za penetracijsko ispitivanje i ostale. U ostale alate su svrstani svi alati koji nemaju istaknutu primarnu svrhu.

Određeni alati imaju mogućnost pružanja vanjskog pristupa ili prosljeđivanja priključka (engl. *port*). Takvi alati koriste druge servise za pružanje te mogućnosti. Jedan od takvih servisa je *ngrok* [15]. *Ngrok* pruža vanjski pristup web aplikacijama koje su pokrenute lokalno. Nakon pokretanja, *ngrok* ispisuje javno dostupnu URL adresu koju je moguće koristiti u phishing napadima.

Kod dva alata koji imaju mogućnost slanja poruka elektroničke pošte promijenjen je SMTP poslužitelj s kojeg se šalju poruke u kodu alata. SMTP poslužitelj je u oba slučaja postavljen na Outlook SMTP poslužitelj, to jest *smtp-mail.outlook.com*. U *PhishMailer* alatu prethodno napisan poslužitelj je bio neispravan, a u *Phish-Me-Not* alatu poslužitelj je bio postavljen na Gmail SMTP poslužitelj. Gmail od 30.05.2022. ne dopušta prijavu u manje sigurne aplikacije zbog čega funkcionalnost slanja poruka elektroničke pošte na tom alatu više neće raditi [16]. Za slanje phishing poruka elektroničke pošte korištena je diplomski_rad_phish_0@outlook.com adresa elektroničke pošte. Za primanje phishing poruka elektroničke pošte korištene su sljedeće adrese elektroničke pošte:

- diplomski_rad_phish_1@outlook.com
- diplomski_rad_phish_2@outlook.com
- diplomski_rad_phish_3@outlook.com

Za demonstraciju alata korištena je Facebook web stranica. Kod alata koji nemaju mogućnost kopiranja web stranica, korištena je ručno napravljena kopija prikazana na slici 3.1.

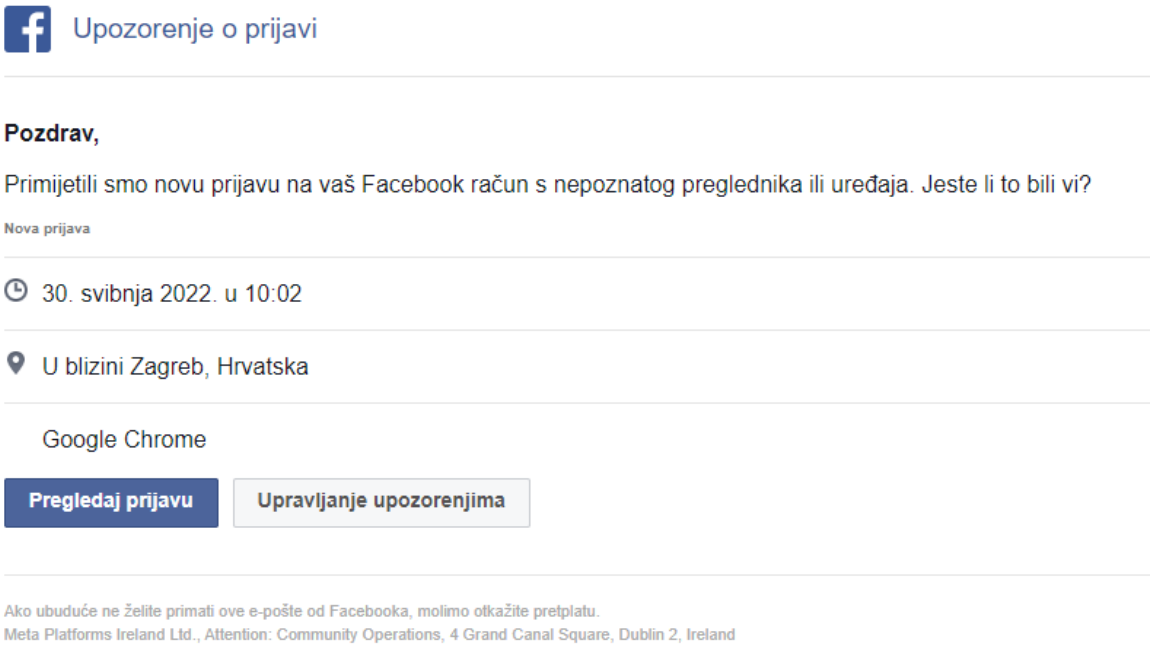


Slika 3.1. – Kopija Facebook web stranice za prijavu

Također, promijenjena je definicija forme za slanje vjerodajnica jer određeni alati rade samo s takvom definicijom. Nova definicija forme za slanje vjerodajnica je sljedeća:

```
<form id="login_form" action="" method="POST">
```

Neki alati imaju mogućnost korištenja proizvoljnog HTML koda za sadržaj poruke elektroničke pošte. Za demonstraciju je korištena lažirana poruka elektroničke pošte o upozorenju o prijavi na Facebook stranicu. HTML kod je generiran pomoću *PhishMailer* alata postupkom opisanim u poglavlju 3.3. Generirani sadržaj je preveden na hrvatski jezik te su izmijenjeni zastarjeli podaci o Facebooku na dnu poruke. Krajnji izgled poruke elektroničke pošte prikazan je na slici 3.2.



Slika 3.2. – Lažirana poruka elektroničke pošte upozorenja o prijavi na Facebooku

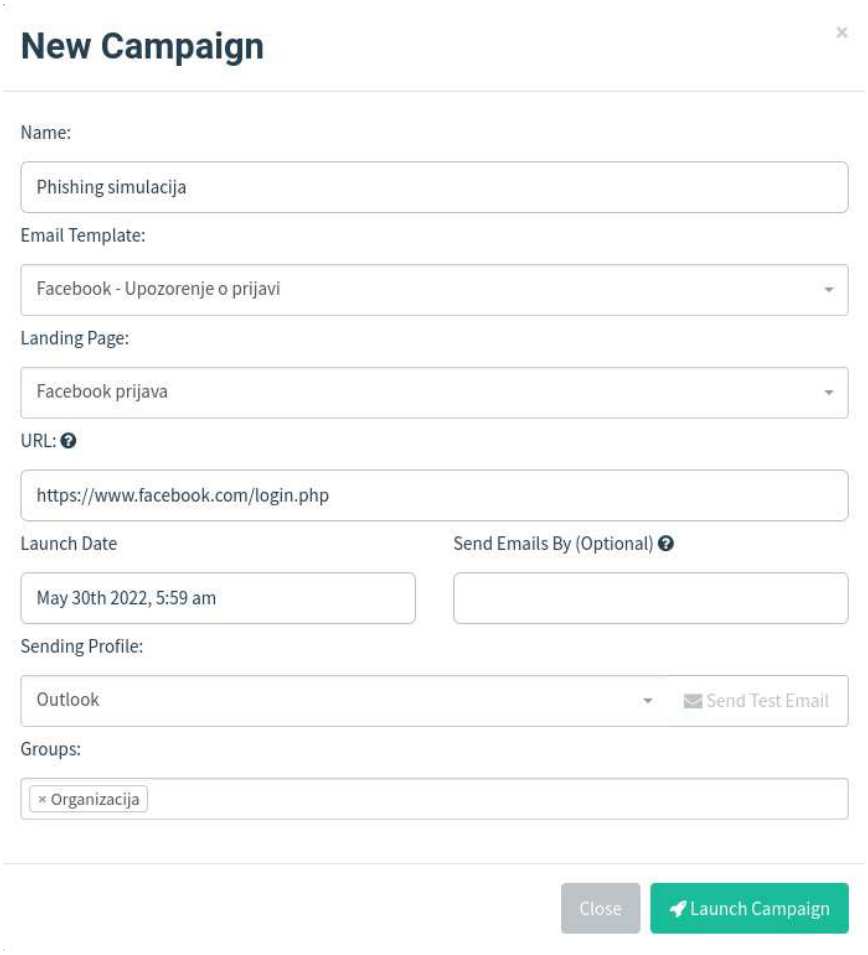
3.1. Phishing alati za edukaciju zaposlenika

Prvi alat za edukaciju zaposlenika je *Gophish* [17]. *Gophish* je phishing okvir napisan u programskom jeziku Go što omogućuje jednostavnu instalaciju. Nastao je s ciljem da pruži svima besplatnu i pristupačnu phishing edukaciju.

Korisnik alata postavlja sve što je potrebno za phishing simulaciju pomoću korisničkog sučelja koje je podijeljeno na pet kartica.

Prva kartica *Campaigns* omogućuje korisniku da postavi podatke o phishing kampanji. Tijekom konfiguracije kampanje moguće je odabrati predložak phishing poruke elektroničke pošte, HTML kod phishing web stranice, profil s kojeg se šalje i grupu zaposlenika. Također, treba upisati URL adresu na kojem je pokrenut *Gophish* poslužitelj te vrijeme početka i kraja kampanje. Postavljanje podataka o phishing kampanji u kartici *Campaigns* je prikazano na slici 3.3.

U drugoj kartici *Users & Groups* mogu se napraviti grupe korisnika kojima će se slati phishing poruke elektroničke pošte. Za svakog korisnika je moguće upisati ime, prezime, adresu elektroničke pošte i poziciju u organizaciji. Umjesto ručnog upisa, preko sučelja je moguć uvoz podataka o korisnicima iz CSV datoteke.



Slika 3.3. – Postavljanje phishing kampanje u *Gophish* alatu

Treća kartica *Email Templates* omogućuje izradu predložaka poruka elektroničke pošte za phishing simulaciju. Svaka poruka se može upisati kao tekstualna vrijednost ili HTML kod. Također, može se dodati slika za praćenje (engl. *tracking image*) preko koje će *Gophish* odrediti je li korisnik otvorio poruku elektroničke pošte.

Pomoću sljedeće kartice *Landing Pages* se dodaju HTML kodovi web stranica koji će se prikazati korisnicima nakon što kliknu na link u porukama elektroničke pošte. Osim HTML koda web stranice, može se postaviti treba li *Gophish* spremiti upisane podatke i lozinke te na koju URL adresu će se korisnika preusmjeriti nakon upisa podataka. Kako bi pratio koji korisnik je upisao podatke, *Gophish* generira *rid* parametar za svakog primatelja u phishing kampanji te dodaje taj parametar u URL adresu.

Zadnja kartica *Sending Profiles* se koristi za konfiguraciju profila s kojeg će se slati phishing poruke. Profil se sastoji od subjekta koji se prikazuje u porukama elektroničke pošte, SMTP poslužitelja, korisničkog imena i lozinke.

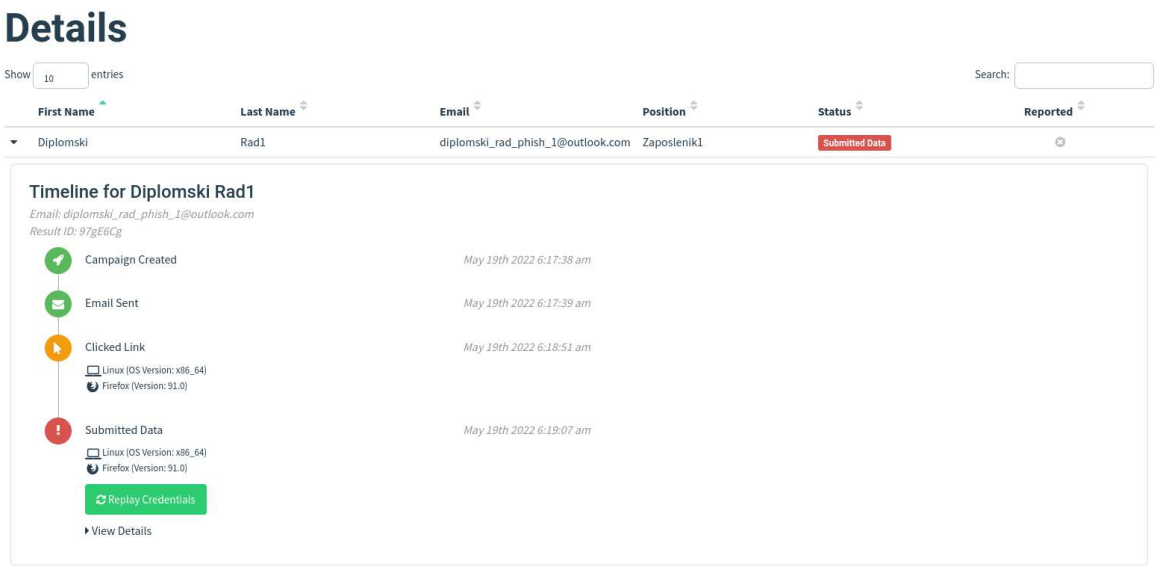
Kako bi phishing napad bio više personaliziran i uvjerljiviji, *Gophish* ima značajku koja korisniku omogućuje korištenje varijabli u predlošcima za poruke elektroničke pošte i u HTML kodovima web stranica. Primjerice, *{{.FirstName}}* je varijabla za ime zaposlenika, *{{.TrackingURL}}* za URL adresu slike preko koje se prati korisnika te *{{.URL}}* za URL phishing stranice [18].

Nakon pokretanja kampanje, na kartici *Dashboard* je moguće vidjeti rezultate simulacije koji uključuju broj poslanih i otvorenih poruka elektroničke pošte, broj korisnika koji su kliknuli na link u phishing poruci, broj upisanih podataka te broj prijavljenih poruka elektroničke pošte. Primjer rezultata za phishing simulaciju je prikazan na slici 3.4.

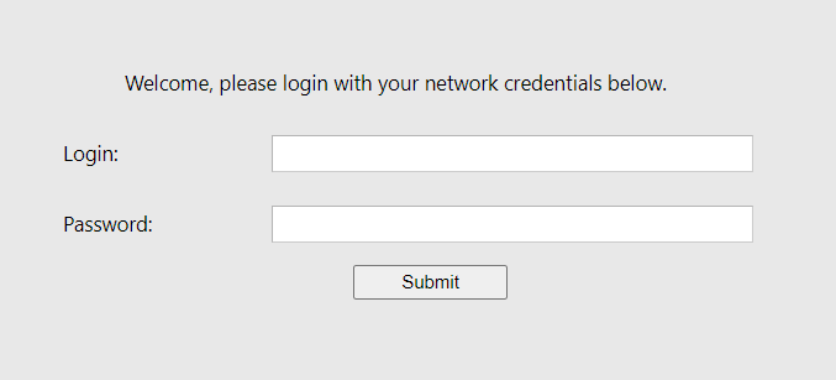
Slika 3.4. – Rezultati phishing simulacije u *Gophish* alatu

Također je moguć pregled detalja rezultata po zaposlenicima. Za svakog zaposlenika, osim osobnih podataka korisnika, moguće je vidjeti status i je li prijavio da je poruka elektroničke pošte mogući phishing napad. Kod korisnika gdje je phishing napad bio uspješan, status je *Submitted Data* ako je korisnik upisao podatke ili *Clicked Link* ako je samo kliknuo na link. Za oba statusa će se zapisati koji operacijski sustav i web preglednik korisnik koristi, a za *Submitted Data* će zapisati i upisane podatke ako je ta opcija prethodno odabrana. Primjer dijela kartice gdje je moguće vidjeti detalje je prikazan na slici 3.5.

Drugi alat za edukaciju korisnika je *MSISimplePhish* [19] koji pruža jednostavan mehanizam za pokretanje phishing simulacija u organizacijama. Nakon pokretanja alata, na priključku 8080 će se postaviti jednostavna generička stranica za prijavu, prikazana na slici 3.6.



Slika 3.5. – Detalji rezultata phishing simulacije u *Gophish* alatu

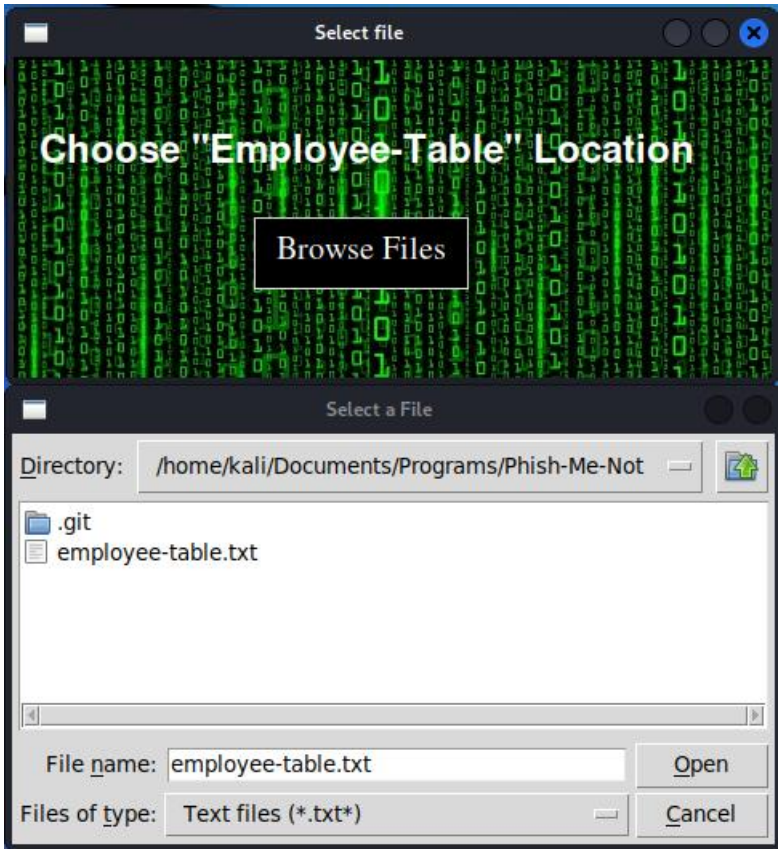


Slika 3.6. – *MSISimplePhish* phishing web stranica

Alat ne pruža mogućnost slanja phishing poruka pa će organizacija morati poslati poruke koje će sadržavati URL adresu phishing stranice izvan alata. *MSISimplePhish* sprema podatke o žrtvama phishing napada u tekstualnu datoteku. U toj datoteci se zapisuje IP adresa ako je korisnik posjetio URL adresu ili IP adresa, korisničko ime i prva tri znaka lozinke ako je korisnik upisao svoje vjerodajnice. Zapisivanjem samo prva tri znaka onemogućuju se daljnji napadi, ali moguće je dokazati korisnicima da su podaci uspješno zapisani [20].

Zadnji alat za edukaciju zaposlenika je *Phish-Me-Not* [21]. Alat koristi Apache web poslužitelj te pruža vanjski pristup web stranici pomoću *ngrok* alata. Za raspoznavanje korisnika generira se link na *pingb* web stranici koja zapisuje IP adrese korisnika koje posjete generirani link [22].

Za korištenje alata potrebno je postaviti ime organizacije i tablicu s podacima o zaposlenicima. Tablica zaposlenika sadrži ime, adresu elektroničke pošte, IP adresu i zadnji projekt zaposlenika. IP adresa se koristi za raspoznavanje korisnika. Korisnik može napraviti novu tablicu zaposlenika upisom podataka u terminal ili koristiti postojeću tablicu. U slučaju korištenja postojeće tablice, otvara se prozor s korisničkim sučeljem za odabir datoteke s podacima o zaposlenicima prikazan na slici 3.7.



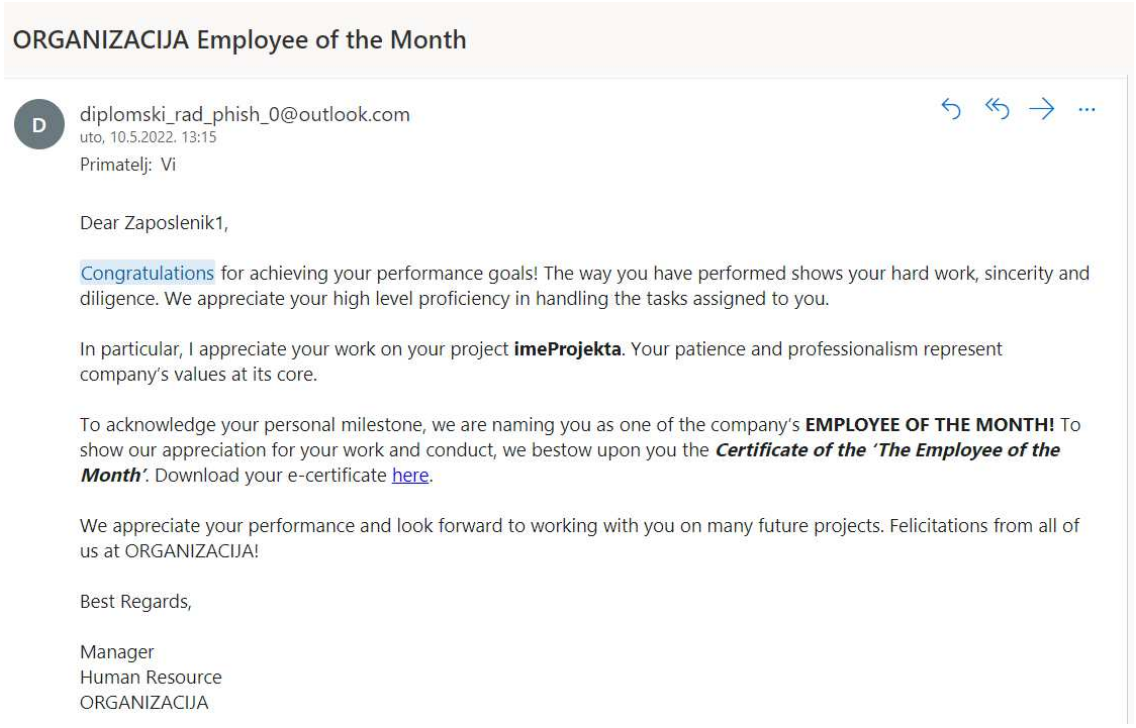
Slika 3.7. – Prozor za odabir tablice zaposlenika u *Phish-Me-Not* alatu

Nakon postavljanja podataka o zaposlenicima, alat šalje phishing poruke te čeka upis korisnika alata da je simulacija gotova. Poruka elektroničke pošte koju alat koristi za phishing simulacije se ne može mijenjati interakcijom s alatom, a prikazana je na slici 3.8. U slučaju da korisnik klikne na link u poruci elektroničke pošte, prikazat će mu se web stranica s informacijama o phishing napadima i kako ih izbjeći.

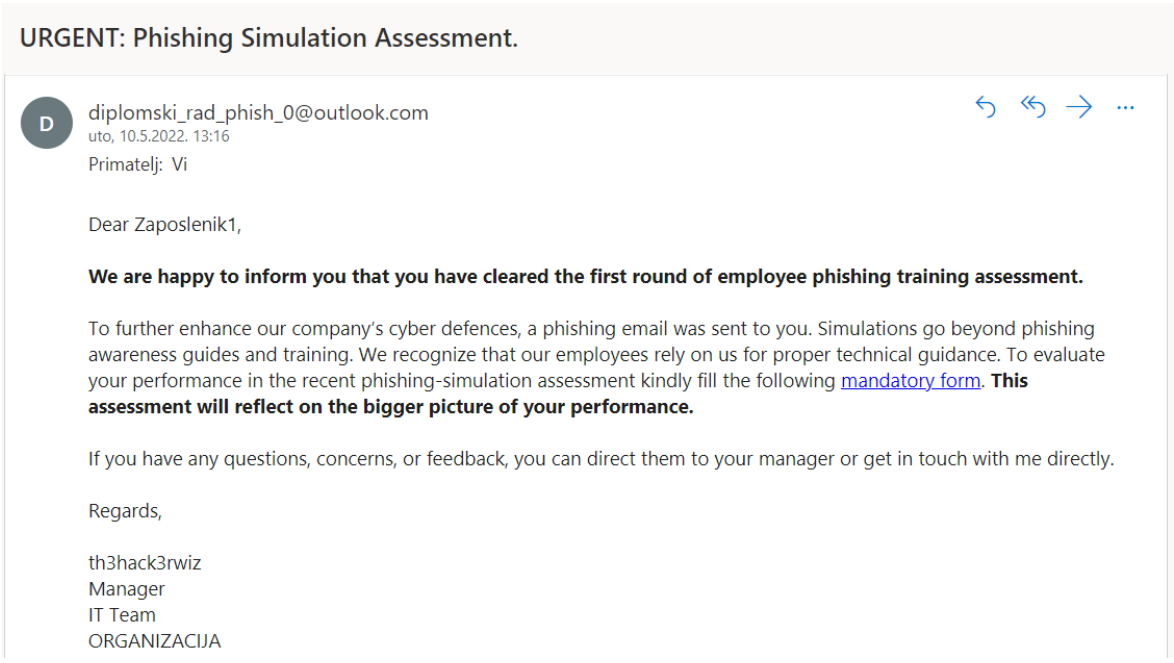
Nakon što je simulacija gotova, *Phish-Me-Not* kreće s pokretanjem tri značajke koje su korisne tijekom phishing simulacija u organizaciji. Te značajke su slanje poruka elektroničke pošte žrtvama sa savjetima kako izbjeći phishing napade, slanje poruka elektroničke pošte s URL adresom na obavezni kviz koji ispituje znanje o phishing napadima zaposlenicima koji nisu kliknuli na link te generiranje XLSX datoteke s

rezultatima simulacije. Poruka elektroničke pošte s linkom na obavezni kviz je prikazana na slici 3.9., a generirana XLSX datoteka je na slici 3.10.

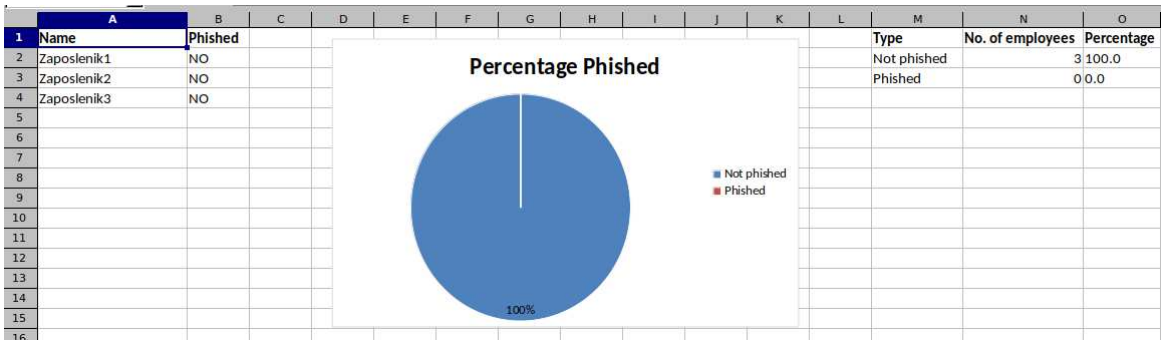
Cijeli proces korištenja alata opisan gore prikazan je i na slici 3.11.



Slika 3.8. – Poruka elektroničke pošte za phishing korištena u *Phish-Me-Not* alatu

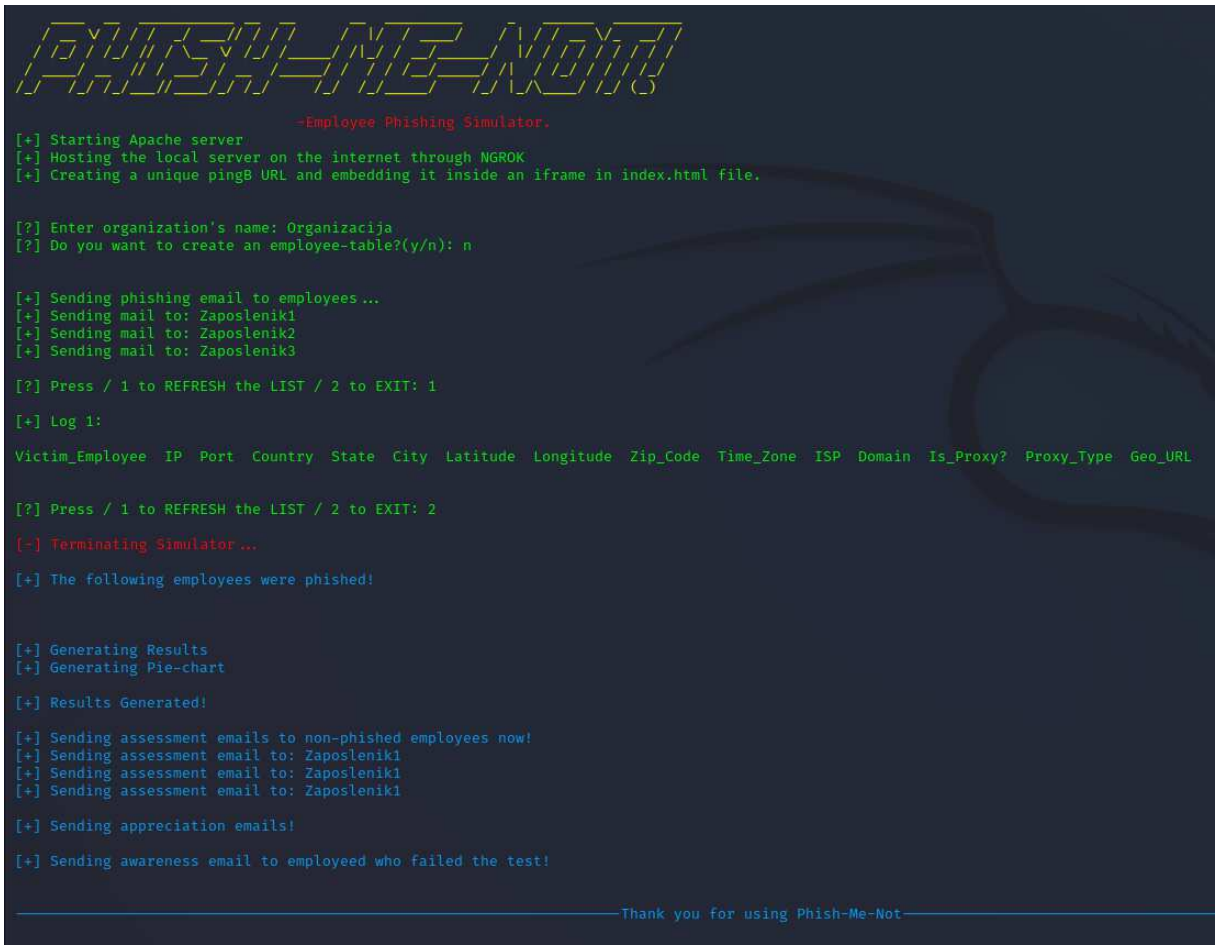


Slika 3.9. – Poruka elektroničke pošte poslana korisnicima koji su prošli phishing simulaciju



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Name	Phished											Type	No. of employees	Percentage
2	Zaposlenik1	NO											Not phished	3	100.0
3	Zaposlenik2	NO											Phished	0	0.0
4	Zaposlenik3	NO													

Slika 3.10. – Generirana XLSX datoteka s rezultatima phishing simulacije



Slika 3.11. – Korištenje *Phish-Me-Not* alata

Iako alat ima korisne značajke za simulaciju phishing napada, alat ima nedostatak što se poruke elektroničke pošte i sadržaj web stranice ne mogu mijenjati interakcijom s alatom.

3.2. Phishing alati za penetracijsko ispitivanje

Jedan od alata koji se koristi za napade društvenim inženjeringom u penetracijskim testiranjima je *The Social-Engineer Toolkit* (SET) [23].

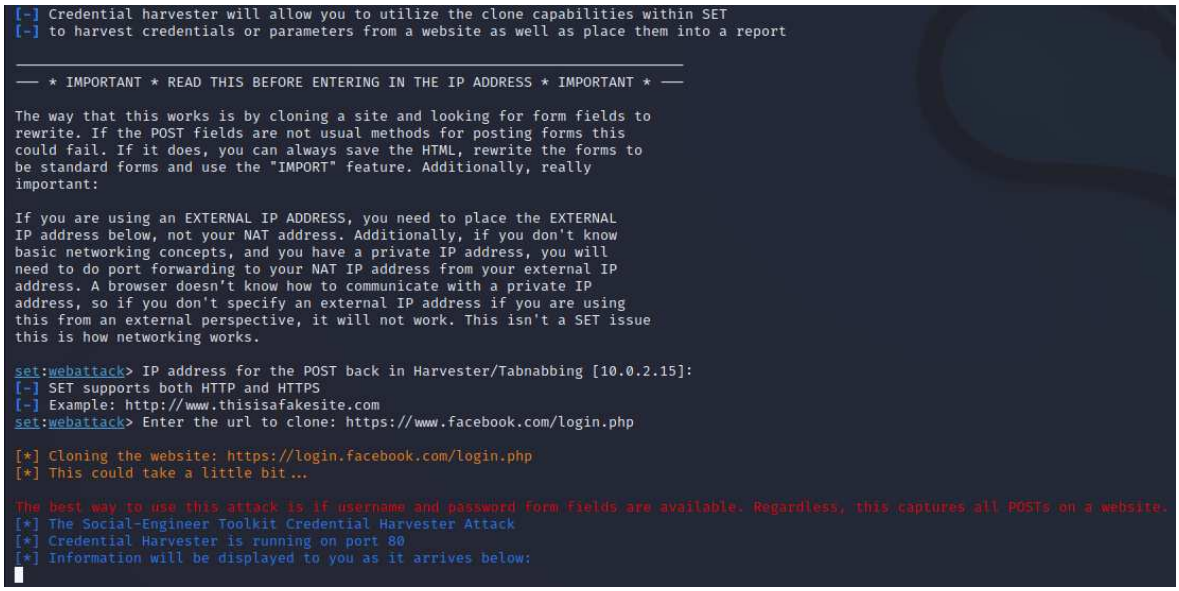
Glavna značajka SET-a je pokretanje tehnički sofisticiranih napada društvenim inženjeringom uz pružanje jednostavnog korisničkog sučelja [24]. Korisničko sučelje se sastoji od višerazinskih izbornika u kojima korisnik odabire vektor napada i postavlja različite opcije konfiguracije za odabrani napad.

Za napade društvenim inženjeringom postoji deset različitih opcija koje su prikazane na slici 3.12., a neke od njih su *Website Attack Vectors*, *Mass Mailer Attack* i *QRCode Generator Attack Vector*.

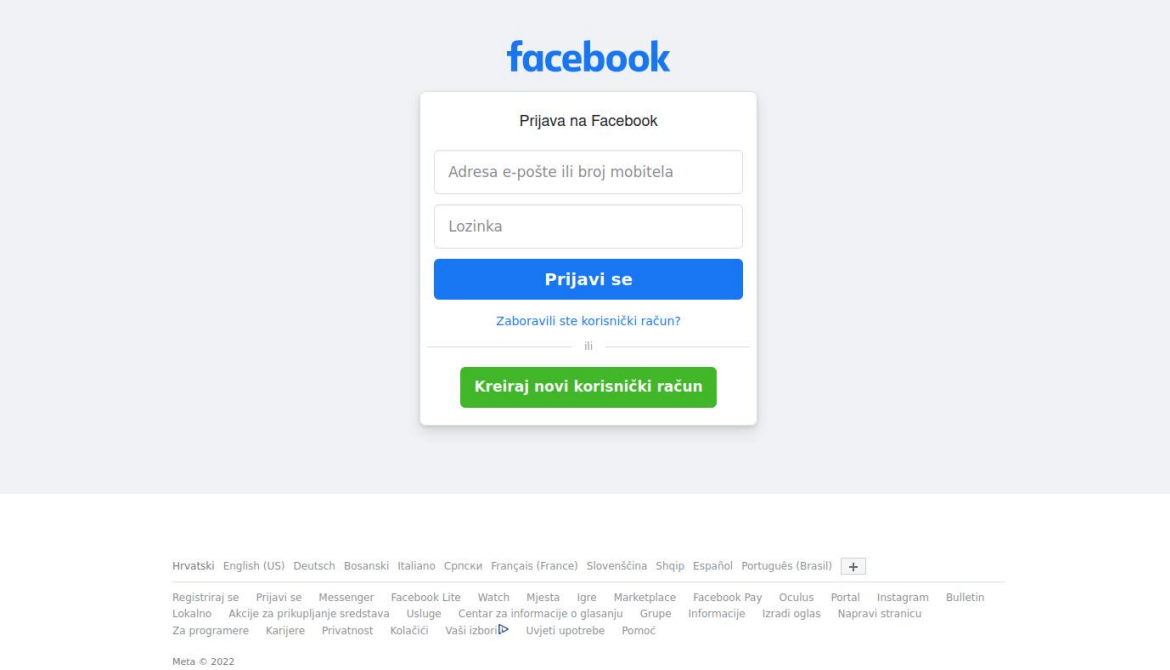
Slika 3.12. – Opcije napada društvenim inženjeringom u SET alatu

Website Attack Vectors opcija uključuje sve vektore napada koji koriste generiranu web stranicu za kompromitiranje žrtava. Jedan od vektora napada u toj opciji je *Credential Harvester Attack Method* koji pomoću lažirane web stranice zapisuje vjerodajnice žrtava koje upišu svoje podatke [24].

Kako bi se konfigurirao alat da napravi lažiranu Facebook stranicu, potrebno je postaviti IP adresu web poslužitelja i URL adresu koju SET treba kopirati kao što je prikazano na slici 3.13. Generirana lažirana Facebook web stranica je prikazana na slici 3.14.



Slika 3.13 – Postavljanje *Credential Harvester Attack Method* napada



Slika 3.14. – Generirana Facebook web stranica pomoću SET alata

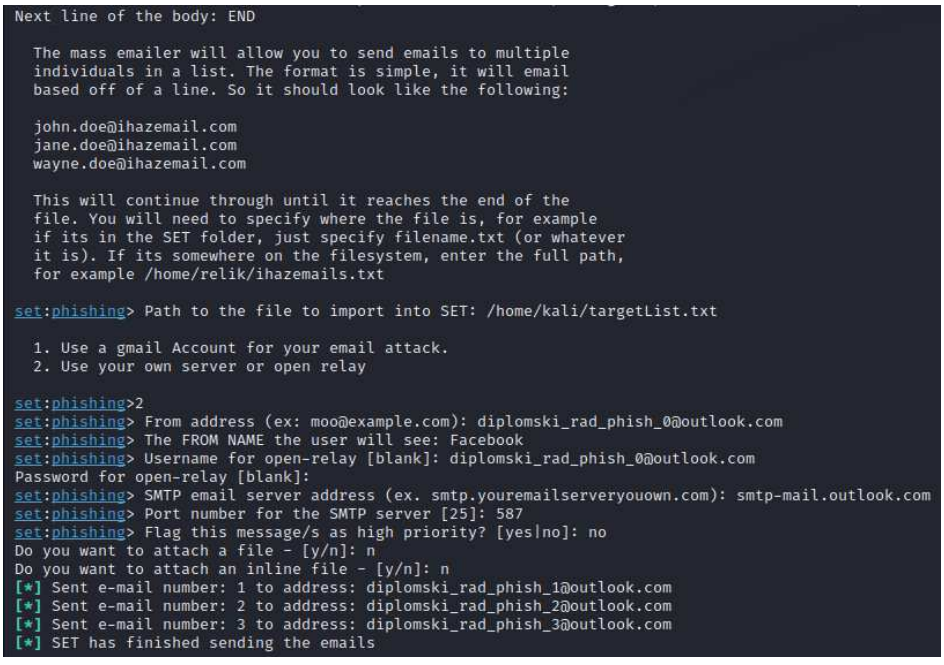
Nakon konfiguracije opcija, alat čeka upis podataka žrtve. Upisani podaci se ispisuju u prozoru terminala i zapisuju u XML datoteku.

Druga isprobana opcija na glavnom izborniku je *Mass Mailer Attack* koja služi za slanje phishing poruka elektroničke pošte. Prvi korak u toj opciji je odabrati šalje li se poruka elektroničke pošte jednoj ili više osoba. U drugom koraku treba odabrati koristi li se već napravljeni predložak sadržaja poruke elektroničke pošte ili se radi novi jednokratni. U slučaju novog predloška treba upisati subjekt poruke te sadržaj u tekstualnom ili HTML

obliku. Također, treba postaviti još neke podatke o poruci elektroničke pošte poput priloženih datoteka, ime pošiljatelja te hoće li poruka biti označena kao visoki prioritet. Korisnik treba postaviti i podatke o računu s kojeg će se poslati poruke elektroničke pošte poput SMTP poslužitelja i priključka, korisničkog imena i lozinke.

Primjer postavljanja te opcije je prikazan na slikama 3.15 i 3.16. Izostavljen je upis HTML sadržaja poruke elektroničke pošte zbog preglednosti.

Slika 3.15. – Prvi dio postavljanja *Mass Mailer Attack* napada

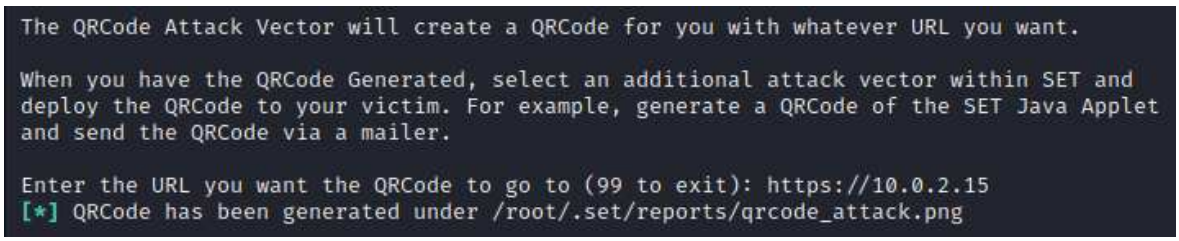


Slika 3.16. - Drugi dio postavljanja *Mass Mailer Attack* napada

Sljedeća opcija koja je na glavnom izborniku je *QRCode Generator Attack Vector* koja generira QR kod za upisanu URL adresu. Generirani QR kod se kasnije može koristiti u

phishing poruci kako bi se smanjila vjerojatnost detekcije phishing napada i vjerojatnost da će žrtva uočiti sumnjivu URL adresu.

Generiranje QR koda za internu IP adresu virtualnog operacijskog sustava koji se koristio za isprobavanje alata je prikazano na slici 3.17.



Slika 3.17. – Postavljanje *QRCode Generator Attack Vector* napada

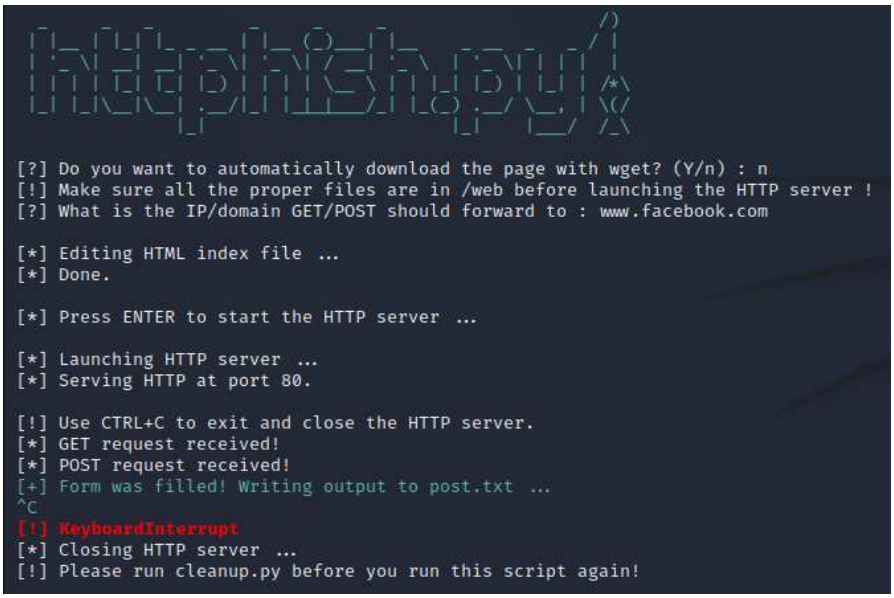
Sljedeći alat za penetracijska testiranja je *httphish* koji ima mogućnost kopiranja web stranica i pokretanja HTTP poslužitelja.

Najveća prednost ovog alata je jednostavnost jer su potrebna samo dva koraka za postavljanje phishing napada. Konfiguracija se sastoji od upisa URL adrese web stranice koja se želi kopirati ili kopiranja postojeće kopije u *web* direktorij koji se nalazi u istom direktoriju kao i Python skripta alata. Zatim, treba upisati na koju IP adresu ili domenu treba preusmjeriti korisnika nakon upisa podataka. Alat nakon toga čeka upis podataka i zapisuje ih u tekstualnu datoteku.

Nakon kraja korištenja alata potrebno je pokrenuti *cleanup* Python skriptu koja će obrisati *web* direktorij i tekstualnu datoteku s upisanim podacima.

Za demonstraciju korištenja alata je korištena ručno modificirana verzija Facebook stranice za prijavu što je prikazano na slici 3.18.

Zatim, za penetracijsko testiranje se može koristiti i *Modlishka* alat [25]. *Modlishka* je HTTP reverzni posrednik, to jest *Modlishka* poslužitelj se nalazi između ciljane web stranice i žrtve te prosljeđuje sve zahtjeve žrtve ciljanoj web stranici. Ta pozicija omogućava *Modlishka* alatu da zapiše sve podatke koje je žrtva upisala.



Slika 3.18. – Korištenje *httphish* alata

Modlishka alat je moguće konfigurirati preko opcija u terminalu ili pomoću JSON datoteke. Primjer JSON konfiguracijske datoteke s kojom će Facebook biti ciljana web stranica je u nastavku:

```
{
  "proxyDomain": "loopback.modlishka.io",
  "listeningAddress": "0.0.0.0",
  "proxyAddress": "",
  "target": "www.facebook.com",
  "targetResources": "static.xx.fbcdn.net",
  "rules": "",
  "terminateTriggers": "",
  "terminateRedirectUrl": "",
  "trackingCookie": "fr",
  "trackingParam": "ident",
  "jsRules":"",
  "jsReflectParam": "",
  "debug": false,
```

```
    "forceHTTPS": false,
    "forceHTTP": false,
    "dynamicMode": false,
    "logPostOnly": false,
    "disableSecurity": false,
    "log": "facebook.log",
    "plugins": "all",
    "credParams":
  "ZW1haWw9KFteXFddKyk=,ZW5jcGFzcz0oW15cbl0rKQ==",
    "cert": "",
    "certKey": "",
    "certPool": ""
  }
```

Prve tri varijable se odnose na domenu koju posjeduje korisnik. Varijabla *proxyDomain* je domena na kojem će se nalaziti phishing stranica. Varijabla *listeningAddress* je adresa sučelja na kojem *Modlishka* čeka zahtjeve. Ako je vrijednost 0.0.0.0, *Modlishka* sluša na svim sučeljima. Sljedeća varijabla *proxyAddress* je adresa posrednika koja se koristi [25].

Sljedeće tri varijable su povezane s ciljanom web stranicom. Varijablu *target* treba postaviti na vrijednost URL adrese ciljane web stranice. Druga varijabla *targetResources* treba sadržavati dodatne domene na kojima se nalaze resursi potrebni ciljanoj web stranici. Varijabla *rules* definira listu atributa i vrijednosti s kojima se treba zamijeniti prethodne vrijednosti tih atributa u HTTP odgovorima ciljane web stranice [25].

Dvije varijable u JSON datoteci konfiguriraju podatke o dnevniku. Varijablom *logPostOnly* može se odrediti da se zapisuju samo POST HTTP zahtjevi, a *log* varijabla sadrži ime datoteke u koju će se zapisivati uhvaćeni HTTP zahtjevi.

Modlishka uhvaćene vjerodajnice zapisuje na krajnjoj točki *SayHello2Modlishka*. Navedena krajnja točka sadrži *UUID* identifikacijski broj, korisničko ime i lozinku žrtve, a to se može postaviti sa sljedeće dvije varijable. Prvo, u varijabli *trackingParam* se postavlja ime HTTP parametra za praćenje žrtve. Taj parametar se koristi u URL adresi phishing stranice, a vrijednost tog parametra će se upisati pod stupac *UUID*. Drugo,

varijabla *credParams* sadrži base64 šifriran popis uzoraka podudaranja (engl. *regex*) korisničkog imena i lozinke. U primjeru za Facebook prva vrijednost je *email=([^\W]+)* koja prihvaća sve vrijednosti do prvog znaka koji nije slovo, a druga *encpass=([^\n]+)* koja prihvaća sve vrijednosti do novog reda.

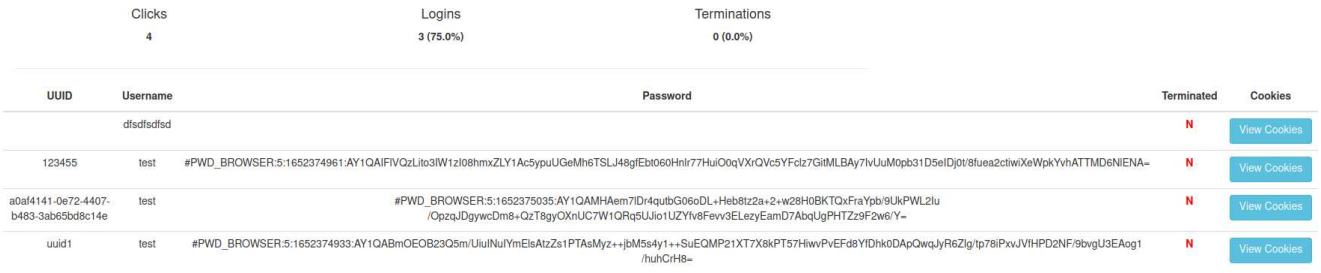
Sljedeće tri varijable konfiguriraju podatke o certifikatu phishing stranice. Varijabla *cert* sadrži vrijednost PEM certifikata, *certKey* vrijednost SSL ključa certifikata, a *certPool* ime tijela za izdavanje certifikata. Sve vrijednosti moraju biti base64 šifrirane.

Ostale varijable postavljaju ostatak mogućih konfiguracija. Varijabla *terminateTriggers* sadrži listu URL adresa čijom posjetom će se prekinuti sesija žrtve, a nakon toga će se korisnik preusmjeriti na URL adresu u varijabli *terminateRedirectUrl*. U varijabli *trackingCookie* je ime HTTP kolačića koji se koristi za praćenje žrtve. Sljedeća varijabla *jsRules* sadrži listu JavaScript tereta i URL adresa na koje će se ubaciti taj teret. Varijable *forceHTTPS* i *forceHTTP* određuju treba li posrednik koristiti samo HTTPS, odnosno HTTP. Varijabla *dynamicMode* pokreće način rada u kojem *Modlishka* prihvaća sve dolazne HTTP zahtjeve. Varijabla *plugins* sadrži popis svih omogućenih dodataka. Zadana vrijednost omogućava sve dodatke, a korisnik može dodati i svoje dodatke.

Nakon upisa podataka u datoteku, alat se može pokrenuti u početnom direktoriju alata s naredbom:

```
sudo ./dist/proxy -config templates/facebook.json
```

Nakon pokretanja, uhvaćene vjerodajnice se mogu vidjeti na *SayHello2Modlishka* krajnjoj točki, kao što je prikazano na slici 3.19.



Slika 3.19. – *SayHello2Modlishka* krajnja točka od *Modlishka* alata

Prednost *Modlishka* alata je što za rad alata ne treba kopija web stranice. U slučaju da se promijeni izgled originalne stranice, promjena će se odmah prikazati na *Modlishka* phishing stranici. Istovremena promjena na phishing stranici smanjuje vjerojatnost da će korisnik primijetiti phishing napad.

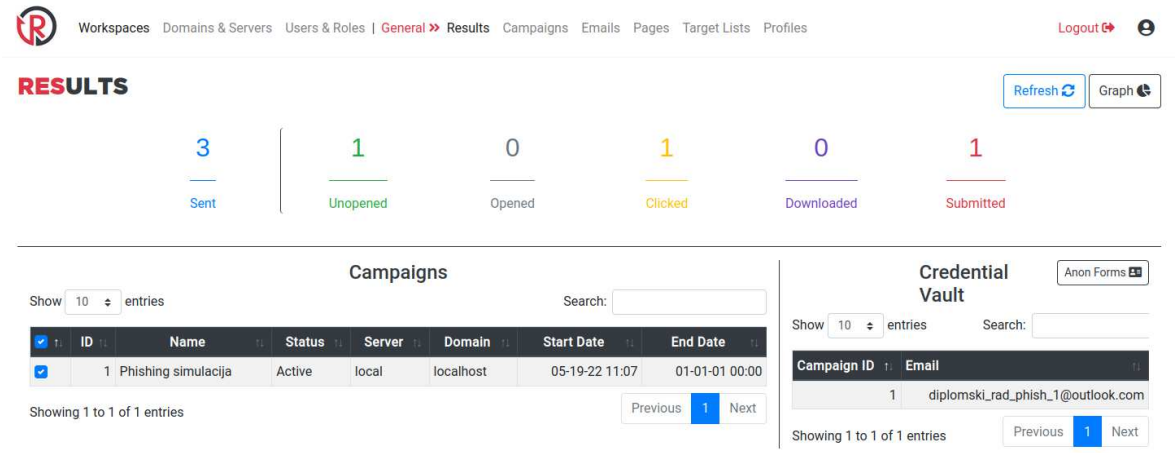
Sljedeći alat za penetracijski test je *redlure*. Glavna značajka *redlure* phishing okvira je što omogućava upravljanje više phishing kampanja koje su pokrenute na različitim poslužiteljima, priključcima ili domenama. Također, *redlure* omogućava povezivanje više predložaka web stranica za lažiranje web stranica koje imaju više koraka u prijavi korisnika.

Sastoji se od tri komponente: *redlure-console*, *redlure-worker* i *redlure-client* [27] [28] [29]. Prva komponenta *redlure-console* je centralizirani API koji sprema predloške, prati phishing kampanje i upravlja *redlure-worker* komponentama [27]. Sljedeća komponenta *redlure-worker* upravlja web poslužiteljem za phishing kampanje. Komponenta *redlure-client* je web sučelje za interakciju s *redlure-console* komponentom.

Korisničko sučelje se sastoji od tri glavne komponente: *Workspaces*, *Domains & Servers* i *Users & Roles*. *Workspaces* komponenta pomaže korisniku pri organizaciji kampanja, predložaka poruka elektroničke pošte i web stranica i tako dalje. U komponenti *Domains & Servers* korisnik treba postaviti podatke o poslužitelju na kojem se nalazi *redlure-worker* komponenta te upisati domene koje će se koristiti u phishing kampanjama. Pomoću komponente *Users & Roles* administrator može upravljati korisnicima i pravima koje imaju.

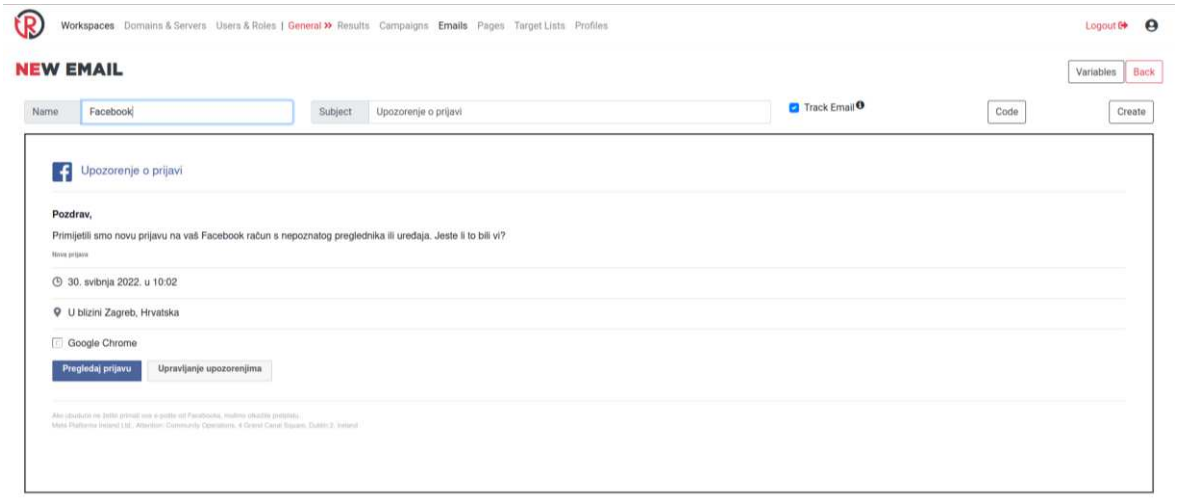
U *Workspaces* komponenti se nalazi šest kartica. Prva kartica je *Results* koja prikazuje rezultate phishing kampanja koje se nalaze u trenutnom radnom prostoru. Rezultati prikazuju broj poslanih poruka elektroničke pošte, broj neotvorenih i otvorenih poruka, broj korisnika koji su kliknuli na link u poruci, broj korisnika koji su preuzeli datoteku u poruci elektroničke pošte te broj podataka upisanih na phishing stranici. Primjer kartice *Results* prikazan je na slici 3.20.

U drugoj kartici *Campaigns* korisniku je omogućeno upravljanje i stvaranje phishing kampanja. Kod upravljanja phishing kampanjama može se vidjeti status kampanje i prethodno odabrane postavke te kopirati, zaustaviti ili obrisati kampanju. Za stvaranje nove kampanje korisnik mora postaviti tri grupe postavki. Prva grupa je vezana uz postavke poslužitelja poput domene, IP adrese, priključka i koristi li se SSL. Druga grupa postavlja podatke o phishing scenariju poput predloška poruke elektroničke pošte i web stranice, URL adresa na koju treba preusmjeriti korisnika i tako dalje. Zadnja grupa postavki se odnosi na slanje phishing poruka elektroničke pošte, odnosno lista primatelja, pošiljatelj, slanje u skupinama i početak slanja poruka.



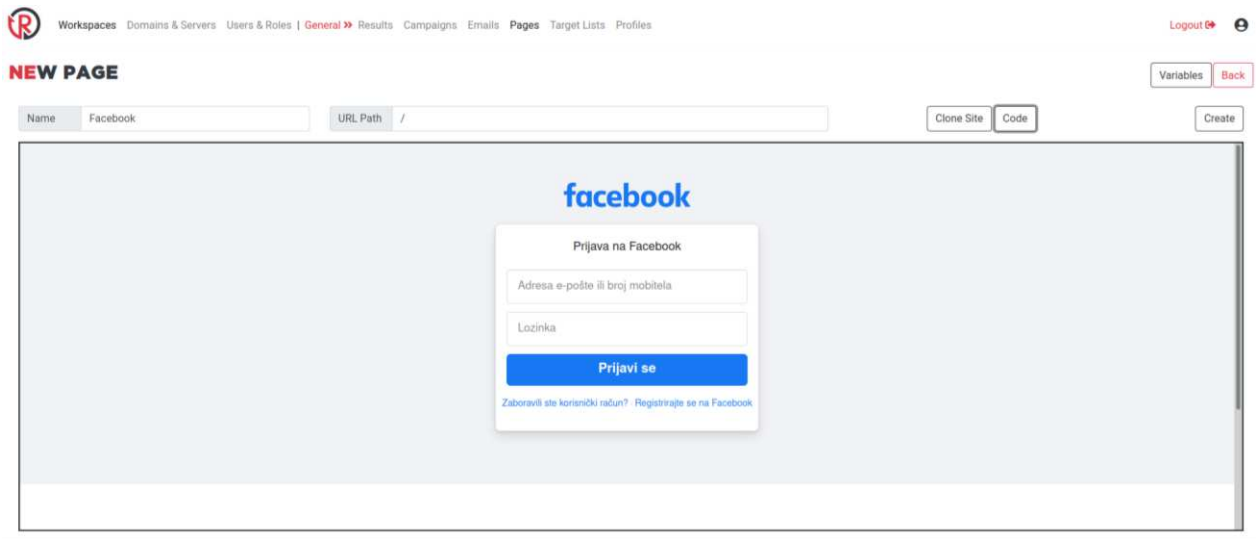
Slika 3.20. - Rezultati phishing simulacije u *redlure* alatu

Emails kartica služi za stvaranje HTML predložaka poruka elektroničke pošte. Korisnik može omogućiti praćenje poruka elektroničke pošte što će ubaciti sliku u HTML sadržaj poruke. Također, postoji mogućnost korištenja varijabli koje ubacuju tekst ovisno o podatku primatelja. Primjerice, *{{ fname }}* je varijabla za ime primatelja, a *{{ url }}* je URL adresa phishing stranice [30]. Primjer *Emails* kartice za Facebook poruku elektroničke pošte je prikazan na slici 3.21.



Slika 3.21. – Postavljanje poruke elektroničke pošte u *redlure* alatu

Na *Pages* kartici se stvaraju HTML predlošci web stranicu za phishing. Moguće je i napraviti automatsku kopiju web stranice. Izgled *Pages* kartice za web stranicu za prijavu na Facebook je na slici 3.22. Kako bi se ispravno zapisivale upisane vjerodajnice potrebno je promijeniti vrijednost *action* atributa u *{{ next_url }}* kod HTML forme za prijavu u ručno napravljenoj kopiji Facebook web stranice.



Slika 3.22. – Postavljanje phishing web stranice u *redlure* alatu

Kartica *Target Lists* služi za stvaranje popisa primatelja phishing poruka. Korisnik može ručno upisivati podatke ili uvesti ih pomoću CSV datoteke. Podaci primatelja koji se trebaju upisati su ime, prezime i adresa elektroničke pošte.

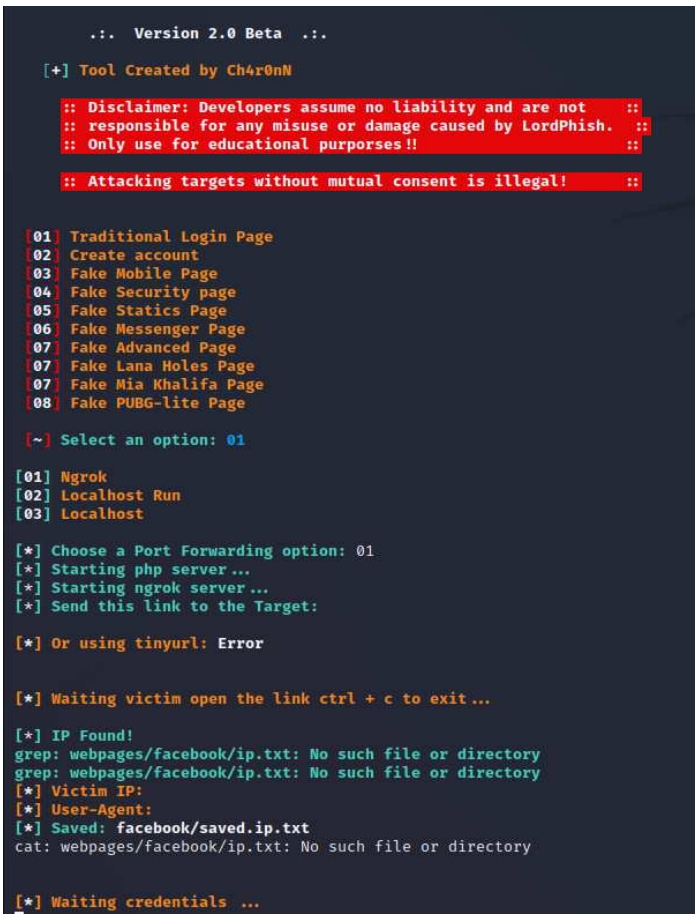
Kartica *Profiles* omogućuje korisniku da konfigurira račun s kojeg će se slati poruke elektroničke pošte. Jedan profil se sastoji od imena pošiljatelja, SMTP poslužitelja i priključka, korisničkog imena i lozinke.

3.3. Ostali phishing alati

Prvi alat je *LordPhish* [31]. *LordPhish* sadrži 52 gotova predloška web stranica među kojima su razne društvene mreže. Sve opcije su prikazane na slici 3.23. Za neke web stranice, poput Facebooka, korisnik može odabrati između više predložaka različitog sadržaja. Alat pruža tri opcije za prosljeđivanje priključka, a to su *ngrok*, *Localhost Run* i lokalni pristup. U slučaju da korisnik odabere *ngrok* opciju, alat neće ispisati generiranu URL adresu zbog pogreške u kodu, ali se adresa može pronaći na http://127.0.0.1:4040/api/tunnels.

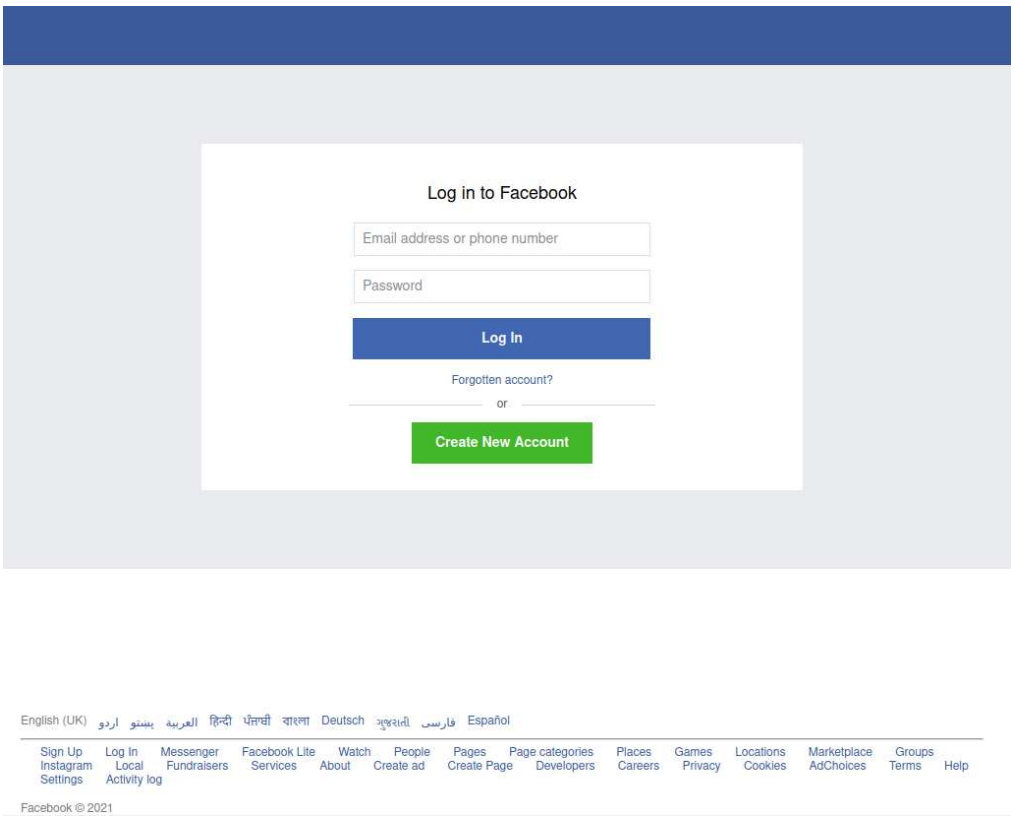
Slika 3.23. – Predlošci web stranica na *LordPhish* alatu

Nakon odabira Facebooka na prvom izborniku, korisnik može birati između osam predloška. Zatim, treba se odabrati način za prosljeđivanje priključka te tada alat čeka upis podataka. Cijeli proces konfiguracije alata prikazan je i na slici 3.24.



Slika 3.24. – Postavljanje *LordPhish* alata

Izgled predloška Facebook stranice za prijavu je zastario prema čemu bi određen broj korisnika mogao prepoznati phishing napad. Zastarjeli predložak je prikazan na slici 3.25.



Slika 3.25. – Ugrađeni predložak za Facebook web stranicu za prijavu u *LordPhish* alatu

Facebook predlošci su imali pogrešku u kodu zbog koje se nisu zapisivali upisani podaci. Pogreška je pronađena u *login.php* datoteci u *facebook* direktoriju. U PHP datoteci koristi se *$_POST* za skupljanje podataka koji su upisani u HTML obrazac i poslani s POST metodom. Međutim, napisana su kriva imena parametara. Umjesto *id* treba pisati *username*, a umjesto *pass* treba biti *password*.

Sljedeći alat je *Zphisher* [1]. Alat pokreće web poslužitelj za phishing stranicu te zapisuje upisane vjerodajnice.

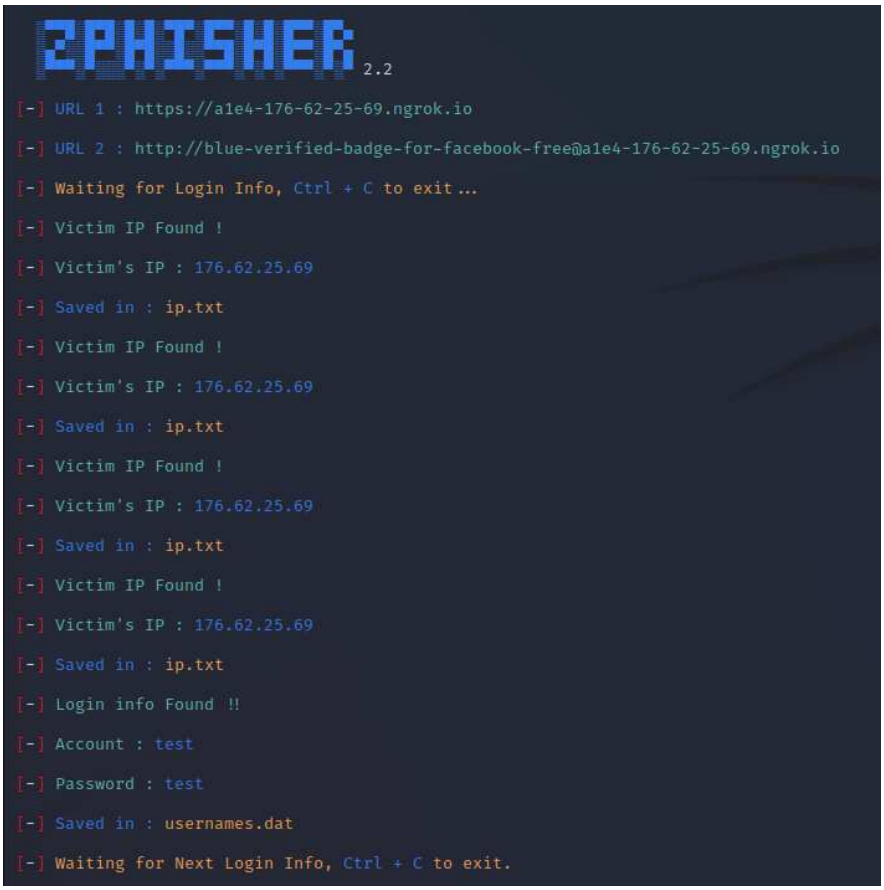
Korisničko sučelje se sastoji od dva izbornika. U prvom izborniku alat omogućuje izbor između 34 web stranica, a za neke postoji više različitih predložaka. Za Facebook postoje četiri predloška prikazani na slici 3.26., a to su uobičajena stranica za prijavu, prijava na glasačku anketu, stranica za sigurnosnu prijavu i prijava na Messenger servis. Ugrađena verzija uobičajene Facebook stranice za prijavu je izgledom ista kao sadašnja verzija pa korisnici ne mogu na taj način prepoznati phishing napad.

Drugi izbornik prikazan na slici 3.27 služi za odabir servisa za prosljeđivanje priključka. Moguće opcije su lokalni pristup, *Ngrok* i *Cloudflared*.

Nakon konfiguracije, alat čeka upis podataka te na terminalu ispisuje pronađene IP adrese i vjerodajnice, što je prikazano na slici 3.28.

Slika 3.26. – Opcije za Facebook predloške za web stranicu u *Zphisher* alatu

Slika 3.27. – Odabir servisa za prosljeđivanje priključka u *Zphisher* alatu



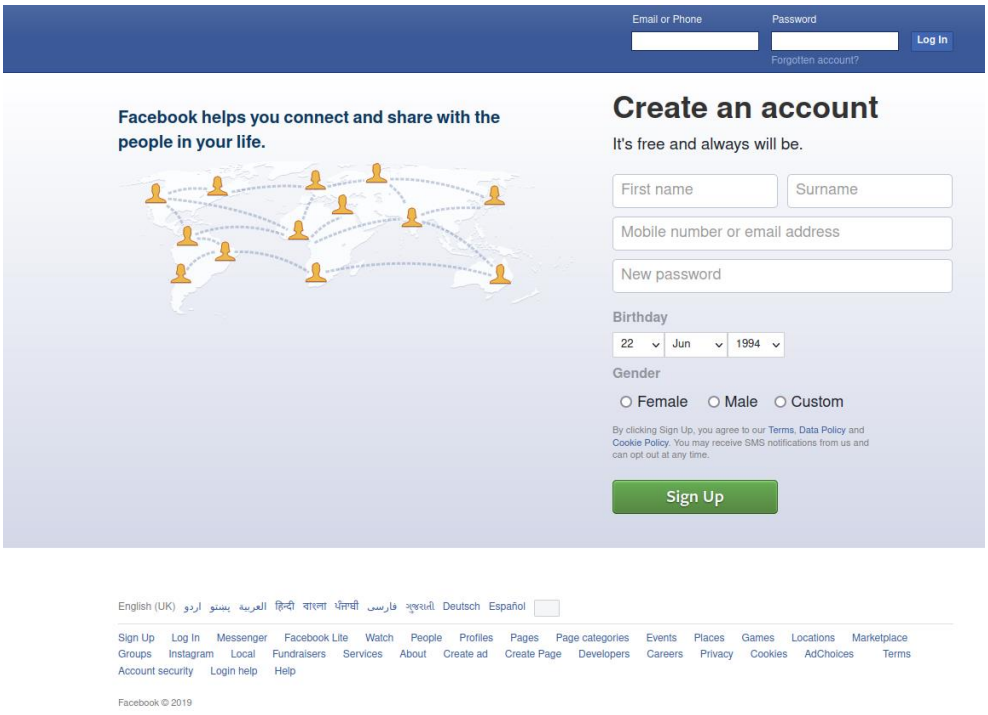
Slika 3.28. – Ispis *Zphisher* alata nakon upisanih vjerodajnica

Sljedeći alat je *AdvPhishing* [33]. Alat, kao i prethodni, pokreće web poslužitelj za phishing stranicu i zapisuje vjerodajnice. Za razliku od prijašnjih alata, predlošci web stranica u *AdvPhishing* alatu traže upis jednokratne lozinke (engl. *one-time password*, OTP).

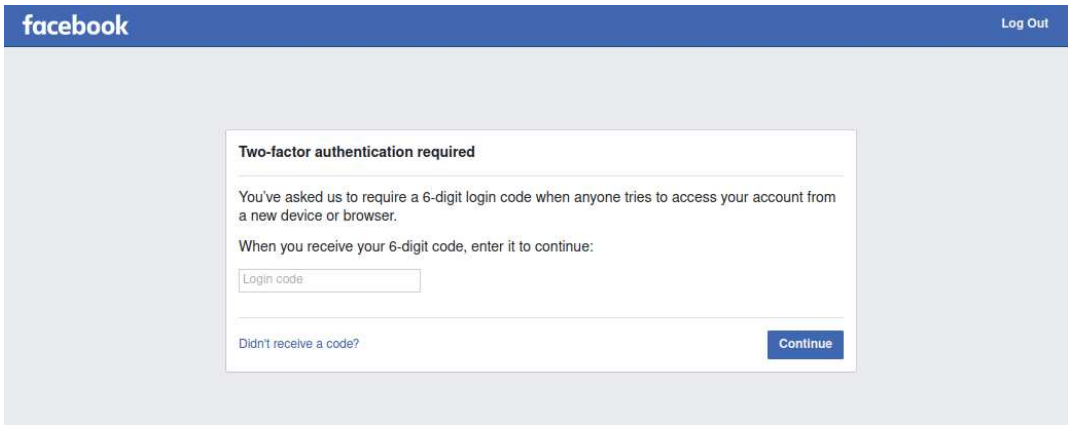
Za postavljanje alata potrebno je odabrati web stranicu koja se želi koristiti za phishing napad. Taj korak prikazan je na slici 3.29. U slučaju odabira Facebook opcije, za phishing napad će se koristiti starija verzija Facebook web stranice te je prva stranica prikazana na slici 3.30. Nakon što žrtva upiše korisničko ime i lozinku, prikazuje se stranica za upis jednokratne lozinke na slici 3.31.

Nakon upisa podataka, oni se ispisuju u terminalu što je prikazano na slici 3.32.

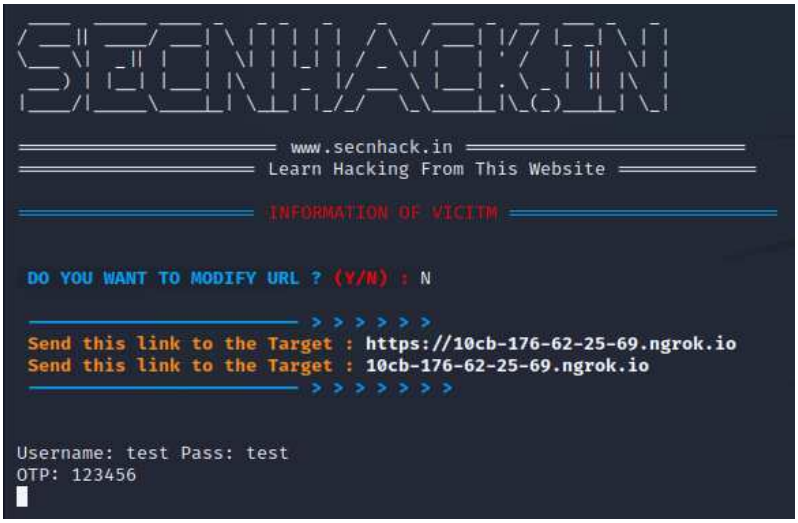
Slika 3.29. – Postavljanje *AdvPhishing* alata



Slika 3.30. – Ugrađena Facebook web stranica za prijavu u *AdvPhishing* alatu



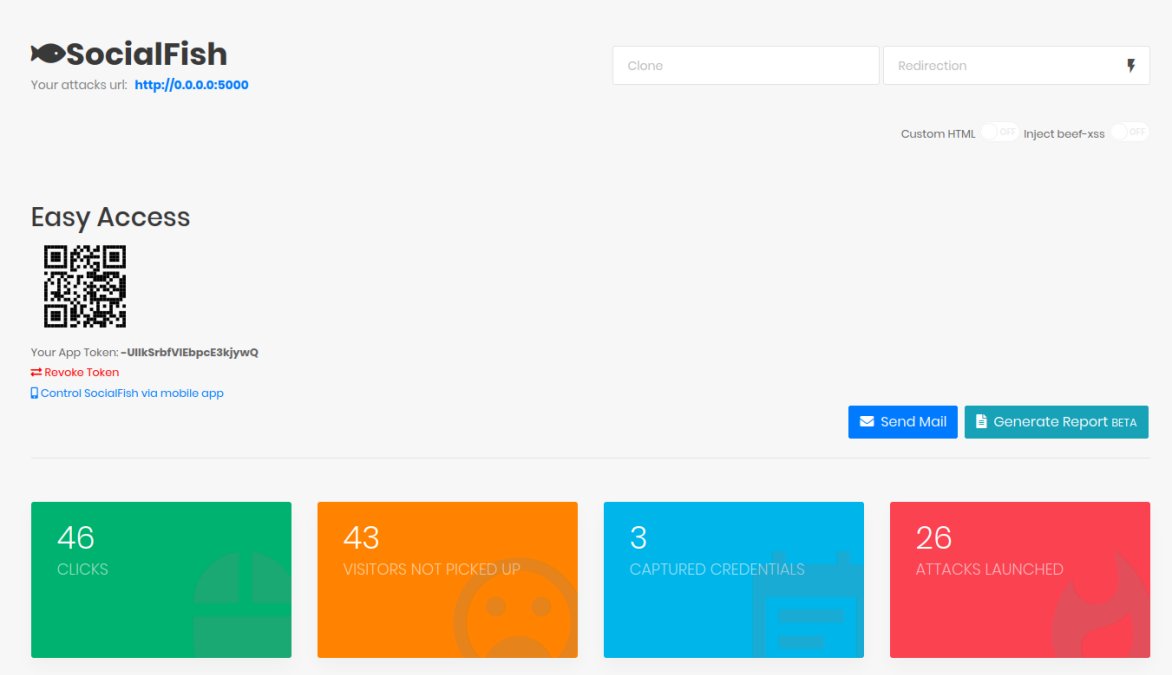
Slika 3.31. – Ugrađena Facebook web stranica za upis jednokratne lozinke u *AdvPhishing* alatu



Slika 3.32. – Ispis *AdvPhishing* alata nakon upisanih vjerodajnica

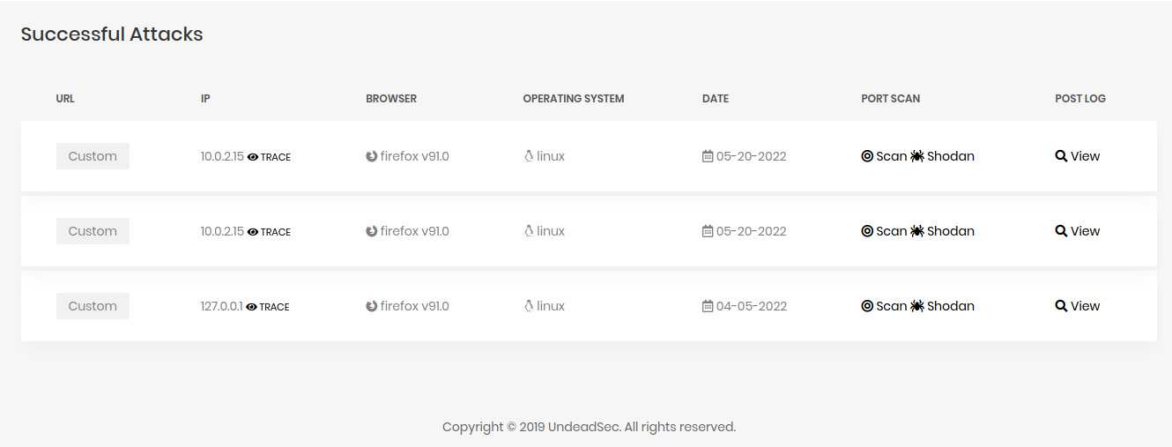
Sljedeći alat je *SocialFish* [34]. Alat omogućuje postavljanje web stranice za phishing i slanje phishing poruka elektroničke pošte.

Alat se pokreće u terminalu, a ostala interakcija s alatom je moguća pomoću korisničkog sučelja prikazanog na slici 3.33. U gornjem dijelu sučelja se postavlja phishing web stranica. Korisnik može napraviti automatsku kopiju web stranice na upisanoj URL adresi te postaviti na koju URL adresu preusmjeriti žrtvu ili odabrati korištenje prilagođenog HTML koda. U donjem dijelu sučelja prikazani su rezultati phishing napada, to jest broj klikova na link phishing web stranice, broj posjetitelja koji nisu upisali podatke, broj uhvaćenih vjerodajnica i broj pokrenutih phishing napada.



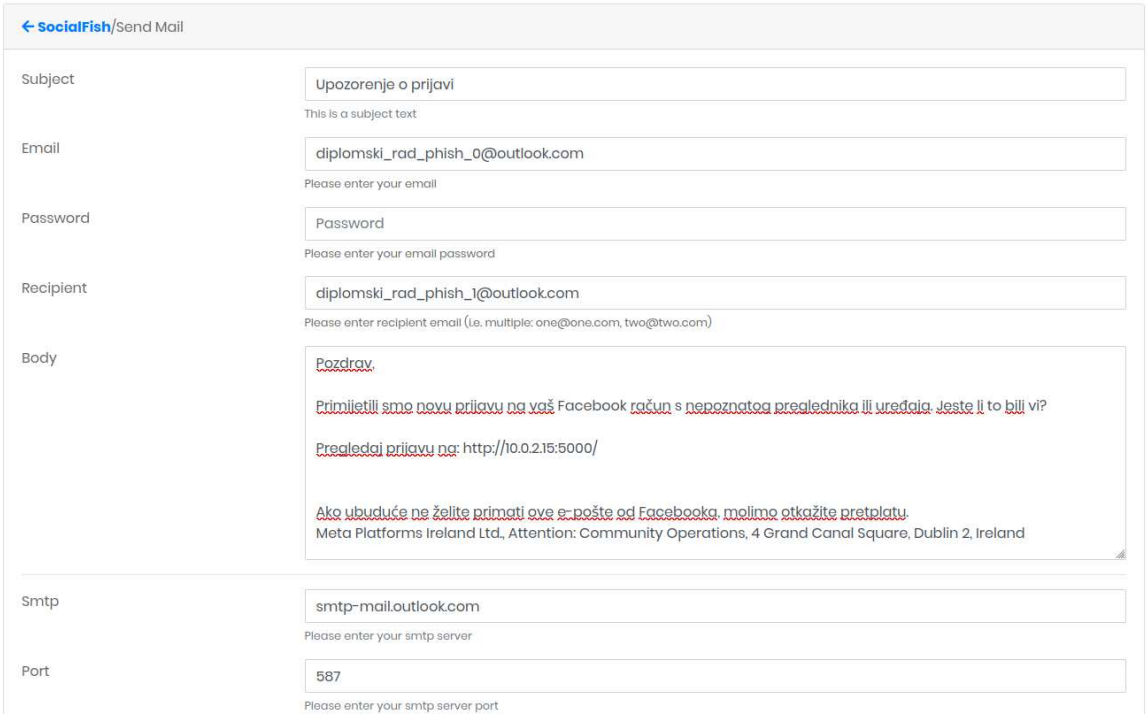
Slika 3.33. – Korisničko sučelje *SocialFish* alata

U slučaju da su uhvaćene vjerodajnice, na korisničkom sučelju će se ispisati podaci o korisniku poput IP adrese, korištenog web preglednika i operacijskog sustava te svi napravljeni POST zahtjevi. Dio korisničkog sučelja koji prikazuje uhvaćene vjerodajnice je prikazan na slici 3.34.



Slika 3.34. – Uhvaćene vjerodajnice prikazane u *SocialFish* alatu

SocialFish omogućuje slanje poruka elektroničke pošte preko korisničkog sučelja. Potrebno je upisati subjekt i sadržaj poruke u tekstualnom obliku, primatelja i podatke o pošiljatelju i SMTP poslužitelju kao što je prikazano na slici 3.35. za lažiranu Facebook poruku elektroničke pošte.



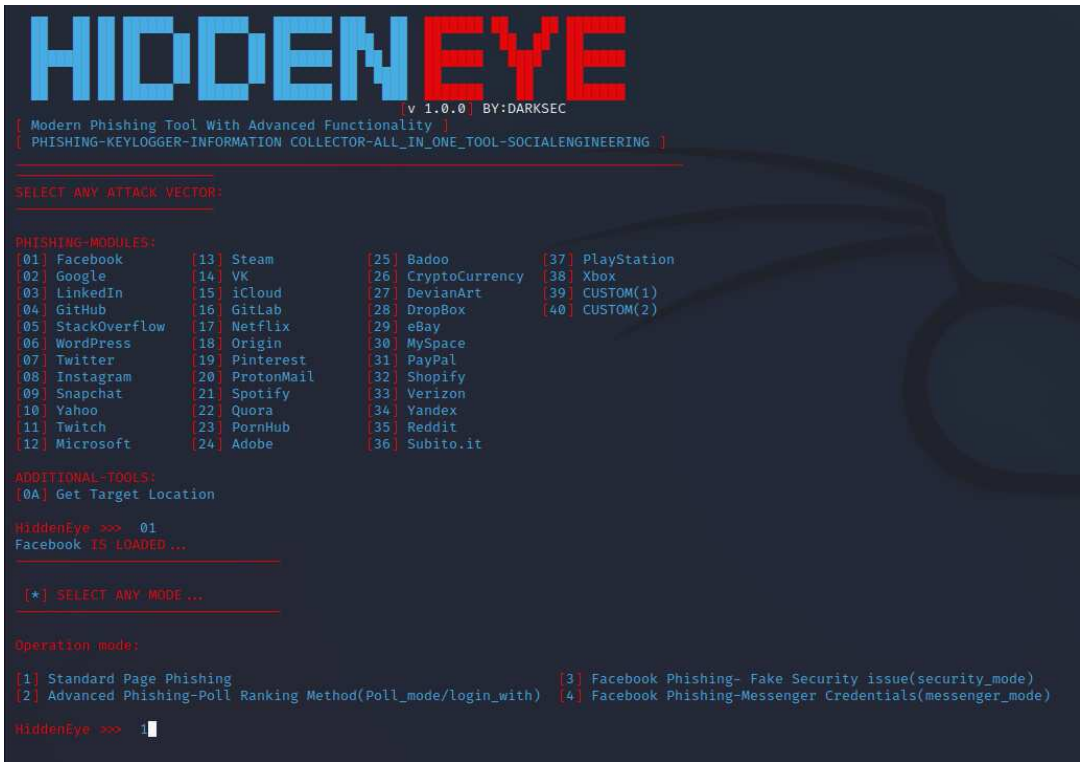
Slika 3.35. – Postavljanje lažirane Facebook poruke elektroničke pošte na *SocialFish* alatu

Funkcionalnost kopiranja web stranice ne radi ispravno na primjeru Facebook stranice za prijavu pa je potrebno koristiti funkcionalnost korištenja prilagođenog HTML koda. Kako bi *SocialFish* ispravno zapisivao upisane vjerodajnice potrebno je dodati sljedeći kod u HTML kod kopije Facebook stranice:

```
<script type="text/javascript">
  var forms = document.forms;
  for (var i = 0, iLen = forms.length; i < iLen; i++) {
    var form = forms[i];
    form.action = '/login';
  }
</script>
```

Sljedeći alat je *HiddenEye* [35]. Ovaj alat omogućuje korisniku odabir između 40 web stranica za phishing te postavlja web poslužitelj za odabranu stranicu.

Konfiguracija alata se sastoji od pet izbornika. Na prvom izborniku na slici 3.36. odabire se web stranica za phishing napad. Za određene web stranice postoji više predložaka.



Slika 3.36. – Predlošci web stranica na *HiddenEye* alatu

Drugi izbornik omogućuje uporabu dodatnih funkcionalnosti kao što je prikazano na slici 3.37. Prva funkcionalnost dodaje *keylogger* koja bilježi sve unose preko tipkovnice na phishing web stranici. Druga funkcionalnost dodaje lažnu *Cloudflare* stranicu prije učitavanja phishing web stranice. *Cloudflare* je reverzni posrednik kojeg koriste legitimne web stranice za zaštitu od napada uskraćivanjem usluge (engl. *denial of service attack*). Zadnja dodatna funkcionalnost je mogućnost slanja zabilježenih podataka na zadanu adresu elektroničke pošte.

Slika 3.37. – Dodatne funkcionalnosti na *HiddenEye* alatu

Treći izbornik se koristi za unos URL adrese na koju će se preusmjeriti žrtva nakon upisa podataka na phishing web stranicu. Prikazan je na slici 3.38.

Slika 3.38. – Postavljanje preusmjeravanja žrtve u *HiddenEye* alatu

HiddenEye na četvrtom izborniku, koji je prikazan na slici 3.39, omogućuje unos priključka na kojem će se pokrenuti web poslužitelj s phishing web stranicom.

Slika 3.39. – Postavljanje priključka za phishing web stranicu u *HiddenEye* alatu

Zadnji izbornik prikazan na slici 3.40. omogućuje odabir servisa za prosljeđivanje priključka. Jedine dvije opcije koje trenutno ispravno rade su lokalni pristup i *ngrok*.

Slika 3.40. – Postavljanje servisa za prosljeđivanje priključka u *HiddenEye* alatu

Nakon upisa podataka u prethodnih pet izbornika, *HiddenEye* čeka upis podataka na phishing web stranici. U slučaju upisa ispisuje IP adresu, *User-Agent* HTTP zaglavlje, trenutno prijavljenog korisnika i upisane vjerodajnice. Takav ispis je prikazan na slici 3.41.

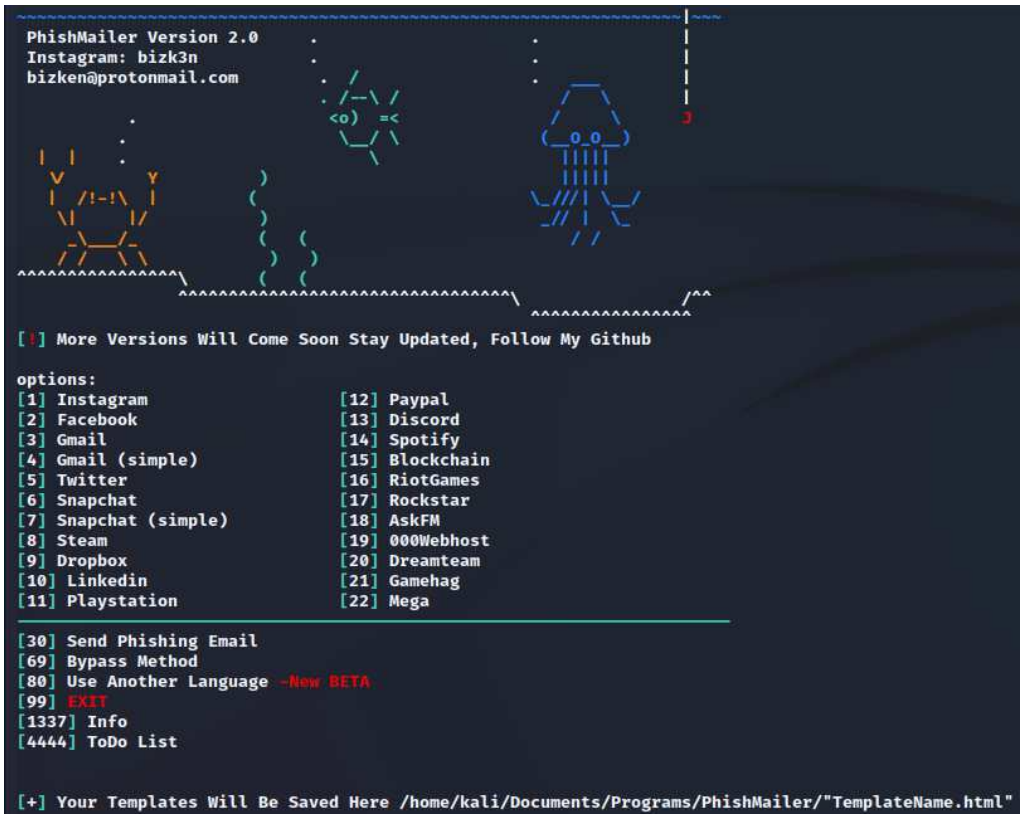
Slika 3.41. – Ispis *HiddenEye* alata nakon upisanih vjerodajnica

Sljedeći alat je *PhishMailer* [36]. Služi za generiranje i slanje phishing poruka elektroničke pošte. Alat generira poruke elektroničke pošte za 22 web stranice.

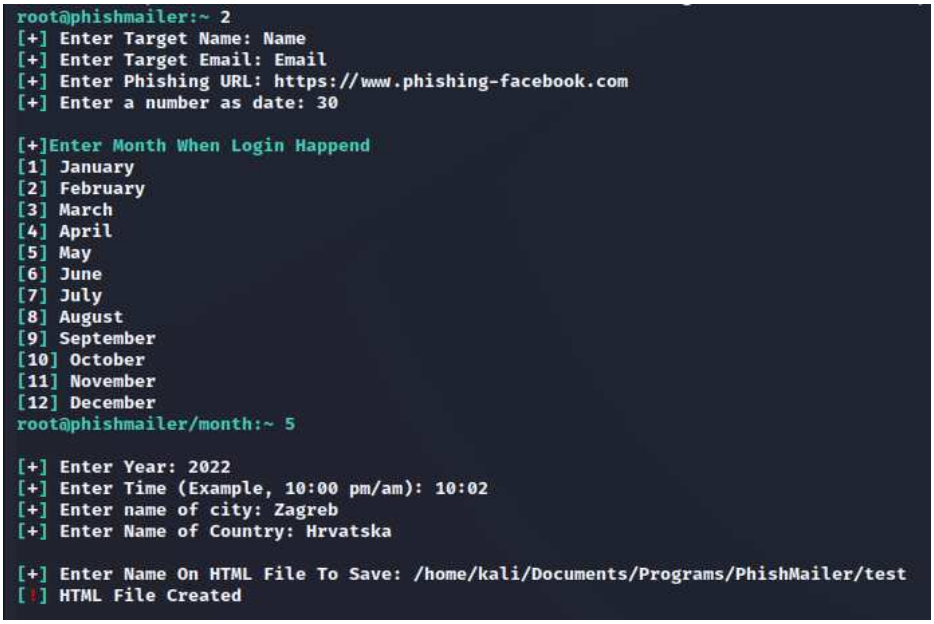
Na prvom izborniku se odabire za koju web stranicu se želi generirati poruka elektroničke pošte. Prvi izbornik i sve moguće opcije su prikazane na slici 3.42.

Nakon odabira predložaka, potreban je upis podataka koji će se upisati u sadržaj poruke te upis lokacije gdje će se spremiti generirana HTML datoteka. Za Facebook poruku elektroničke pošte potrebni su podaci o žrtvi, URL adresa phishing web stranice, te proizvoljni datum i mjesto. Upis tih podataka u korisničkom sučelju je prikazan na slici 3.43.

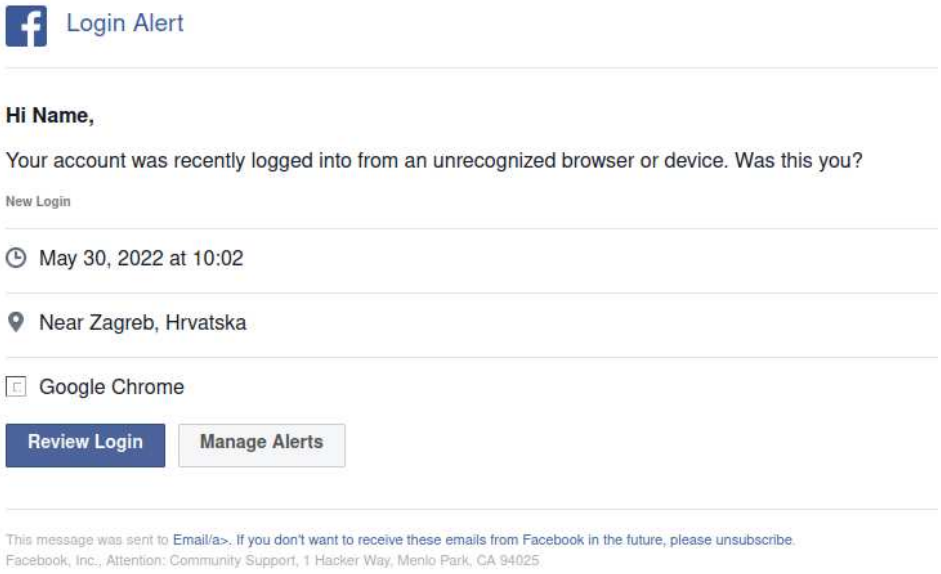
Nakon upisa potrebnih podataka, generirat će se HTML datoteka za Facebook koja je prikazana na slici 3.44.



Slika 3.42. – Predlošci poruka elektroničke pošte u *PhishMailer* alatu



Slika 3.43. – Postavljanje poruke elektroničke pošte u *PhishMailer* alatu



Slika 3.44. – Generirana Facebook poruka elektroničke pošte u *PhishMailer* alatu

3.4. Razlike u phishing alatima

Prethodno opisane alate je moguće usporediti pomoću šest značajki. Takva usporedba prikazana je u tablici 3.1.

	Slanje poruka elektroničke pošte	Proizvoljne phishing web stranice	Kloniranje web stranica	Vanjski pristup phishing web stranici	Otvoreni kod	Grafičko korisničko sučelje
Gophish	Da	Da	Da	Ne	Da	Da
MSISimplePhish	Ne	Ne	Ne	Ne	Ne	Ne
Phish-Me-Not	Da	Ne	Ne	Da	Da	Djelomično
SET	Da	Da	Da	Da	Da	Ne
httphish	Ne	Da	Da	Ne	Da	Ne
Modlishka	Ne	Da	Ne	Ne	Da	Ne
redlure	Da	Da	Da	Da	Da	Da
LordPhish	Ne	Ne	Ne	Da	Da	Ne
Zphisher	Ne	Ne	Ne	Da	Da	Ne
AdvPhishing	Ne	Ne	Ne	Da	Da	Ne
SocialFish	Ne	Da	Da	Ne	Da	Da
HiddenEye	Ne	Da	Ne	Da	Da	Ne
PhishMailer	Da	Ne	Ne	Ne	Da	Ne

Tablica 3.1. – Razlika phishing alata

Prvi stupac u tablici prikazuje koji alati imaju mogućnost slanja phishing poruka elektroničke pošte. Takvi alati su *Gophish*, *Phish-Me-Not*, SET, *redlure* i *PhishMailer*.

Drugi stupac se odnosi na mogućnost korištenja proizvoljnih web stranica za phishing napad. Određeni alati imaju već napravljene predloške web stranica te je moguće koristiti samo te web stranice. Alati koji dopuštaju korištenje samo ugrađenih web stranica su *MSISimplePhish*, *Phish-Me-Not*, *LordPhish*, *Zphisher* i *AdvPhishing*. *PhishMailer* alat je također naznačen da nema tu opciju jer uopće nema mogućnost za postavljanje web poslužitelja za phishing web stranicu.

Određeni alati imaju ugrađenu funkcionalnost za kloniranje proizvoljnih web stranica. U tom slučaju korisnik ne mora napraviti ručne kopije željene web stranice što olakšava postavljanje phishing napada. Ugrađeno kloniranje imaju *Gophish*, SET, *httphish*, *redlure* i *SocialFish* što je prikazano u trećem stupcu.

Vanjski pristup phishing web stanici u četvrtom stupcu pokazuje alate u kojima je moguće postaviti da je phishing web stranica javno dostupna na Internetu. *Phish-Me-Not*, *LordPhish*, *Zphisher*, *AdvPhishing* i *HiddenEye* imaju ugrađene servise koji omogućuju vanjski pristup poput *ngrok* servisa. SET i *redlure* omogućuju korisniku da upiše javnu IP adresu tijekom konfiguracije poslužitelja na kojem se nalazi phishing web stranica.

U petom stupcu je prikazano koji alati su softveri otvorenog koda. Samo jedan alat, to jest *MSISimplePhish*, nije otvorenog koda.

Alati koji imaju grafičko korisničko sučelje su prikazani u zadnjem stupcu. Alati s potpunim grafičkim sučeljem su *Gophish*, *redlure* i *SocialFish*. *Phish-Me-Not* alat ima djelomično grafičko sučelje. Kada korisnik treba odabrati datoteku iz koje se učitavaju podaci ili u koju će se spremiti podaci, otvara se prozor što je jedina interakcija grafičkim sučeljem.

4. Mehanizmi za procjenu phishing rizika

Nakon provođenja phishing simulacija, organizacije koriste različite mehanizme za procjenu rizika od napada društvenim inženjeringom. Osim što ti mehanizmi organizacijama pokazuju phishing rizik, pokazuju i efikasnost edukacije zaposlenika u organizaciji.

4.1. Pregled mehanizama

Najčešći korišteni mehanizam za procjenu phishing rizika je stopa klikova. Stopa klikova je postotak zaposlenika koji su kliknuli na URL adresu phishing web stranice. Mehanizam stope klikova je jednostavan, međutim nije učinkovit način za praćenje phishing rizika jer ovisi o sadržaju i temi poruke elektroničke pošte. Za poruke elektroničke pošte sa sadržajem o financijama će više ljudi kliknuti na phishing link u odnosu na link u poruci elektroničke pošte o telekomunikacijama [37]. Također, niske stope klikova ne moraju nužno ukazivati na dobru edukaciju zaposlenika već mogu biti pokazatelji na nedostatke u phishing simulaciji. Nedostatci mogu biti da je phishing napad bio lagan za prepoznavanje, da nije primjenjiv na većinu osoblja ili da su se zaposlenici susreli sa sličnim napadom na prethodnim simulacijama [38]. Nadalje, ovaj mehanizam ne koristi nijednu metriku koja je usredotočena na poželjno ponašanje korisnika tijekom phishing napada niti metriku koja uključuje druge tipove phishing napada poput zloćudnih datoteka priloženih u poruci elektroničke pošte.

Drugi mehanizam je faktor otpornosti od Proofpointa koji u računanje rizika uključuje i uzorno ponašanje korisnika, odnosno prijavu mogućeg phishing napada. Prijava phishing napada ima veliku važnost u smanjenju štete phishing napada u organizaciji. Prijavom phishing napada sigurnosni tim organizacije može poduzeti potrebne akcije poput promjene lozinki korisnika ili uklanjanje zloćudnog programa s računala. Faktor otpornosti se računa kao rezultat dijeljenja postotka prosječne stope prijava i postotka prosječne stope klikova. Proofpoint preporuča faktor otpornosti 14 kao cilj organizacijama, to jest 70% za stopu prijave i 5% za stopu klikova [37].

Sljedeći postojeći mehanizam uz stopu klikova prikazuje metrike koje opisuju phishing simulaciju. Koristeći te metrike uklonit će se nedostatak u mehanizmu stope klikova da niska stopa može ukazivati na nedostatke u phishing simulaciji. Metrike o phishing simulaciji koje se trebaju odrediti su broj znakova i usklađenost premise [38]. Broj znakova se odnosi na znakove u porukama elektroničke pošte pomoću kojih su zaposlenici trebali otkriti phishing napad. Usklađenost premise opisuje učinkovitost phishing simulacije za određene ciljane žrtve. Pomoću broja znakova i usklađenosti premise se određuje težina detekcije. Kada se odrede težine phishing simulacija, organizacijama će biti lakše analizirati dobivene rezultate simulacija.

Sljedeći mehanizam je metoda izračunavanja phishing rizika od Affinity IT-a [39]. Ideja metode je dodijeliti svakom zaposleniku ocjenu koja će prikazivati njihovo ponašanje tijekom phishing simulacije. Drugim riječima, ocjena zaposlenika pokazuje koliki je rizik da zaposlenik bude žrtva u phishing napadu. Ako zaposlenik pokazuje poželjno ponašanje, ocjena će mu se smanjiti. U suprotnom, ako zaposlenik bude žrtva phishing napada, ocjena će mu se povećati. U početku je svim zaposlenicima dodijeljena početna ocjena pet. Ako zaposlenik ne poduzme ništa vezano uz phishing napad, ocjenu treba umanjiti za jedan. Za prijavu phishing napada, ocjena zaposlenika će se umanjiti za dva. Za žrtve phishing napada, ocjena se povećava za jedan ako su kliknuli na link ili za dva ako su upisali svoje podatke na phishing web stranici. Nakon više phishing simulacija krajnja ocjena zaposlenika je između nula i deset. Zaposlenici s ocjenom od nula do tri imaju mali rizik da budu žrtve phishing napada, od četiri do sedam imaju srednji, a od osam do deset visoki rizik.

4.2. Predloženi mehanizam

Od mehanizama u poglavlju 4.1. zadnji mehanizam od Affinity IT-a je najpotpuniji jer za određivanje krajnje ocjene zaposlenika uzima u obzir poželjna i nepoželjna ponašanja. Također, razlikuje ponašanja unutar poželjnih ponašanja. Odnosno, bolju ocjenu će imati zaposlenici koji su prijavili phishing napad nego oni koji nisu ništa poduzeli.

Međutim, metoda ima nekoliko nedostataka. Prvo, svakom zaposleniku se dodjeljuje početna ocjena pet što u toj metodi označuje srednji rizik. Međutim, neki zaposlenici mogu predstavljati veći rizik zbog određenih vlastitih karakteristika. Neke od takvih karakteristika su one psihološke poput otvorenosti, savjesnosti ili ekstraverzije [40]. Drugi

nedostatak je što metoda ne boduje dovoljno ponavljanje nepoželjnog ponašanja u više phishing simulacija. Postoji mali broj korisnika koji će biti žrtva svakog phishing napada bez obzira na kompleksnost napada [41]. Takvi korisnici predstavljaju najveći rizik u organizaciji te njihova ocjena treba to prikazivati. Bodovanjem nepoželjnog ponašanja također se povećava ocjena korisnicima koji nisu dovoljno naučili tijekom phishing simulacija. Zadnji nedostatak je što metoda nema definirano kako odrediti ukupni phishing rizik organizacije već samo rizik svakog pojedinačnog zaposlenika.

Umjesto da svaki zaposlenik ima početnu ocjenu pet, početna ocjena se može odrediti prema određenim karakteristikama zaposlenika zbog kojih bi mogli biti podložniji phishing napadima. Te karakteristike se mogu ispitati anketom prije početka phishing simulacija. Prva karakteristika korisnika podložnijih na phishing napade je korištenje intuicije umjesto razuma za donošenje odluka [42]. Korištenjem intuicije korisnici donose odluku pomoću nepotpunih informacija ili emocionalnih reakcija. Zbog toga mogu propustiti znakove phishing napada u porukama elektroničke pošte. Drugo, prema istraživanjima, žene i mladi ljudi od 18 do 24 godina su podložniji phishing napadima [14] [43]. Sljedeće, za ljude sa psihološkim karakteristikama poput savjesnosti, otvorenosti, ekstraverzije i emocionalne nestabilnosti je vjerojatnije da će biti žrtve phishing napada [40]. Zatim, za korisnike koji podcjenjuju vjerojatnost da budu žrtve phishing napada je vjerojatnije da se to ostvari. Takvi korisnici mogu imati previše samopouzdanja te zbog toga nisu svjesni svih mogućih scenarija phishing napada [44]. Sljedeće, u organizacijama sa snažnom hijerarhijom korisnici su podložniji phishingu. Korisnici u takvim organizacijama će zbog poštivanja hijerarhije prije odgovoriti na phishing poruke elektroničke pošte koje koriste autoritet i hitnost u sadržaju [45]. Sljedeća karakteristika koja ukazuje da je korisnik podložniji na phishing napad je da nije prošao prijašnje edukacije o phishingu u organizaciji [43]. Također, treba provjeriti jesu li korisnici naučili kako prepoznati phishing napad, to jest hoće li koristiti sadržaj poruke elektroničke pošte ili analizirati URL adresu. Korisnici koji koriste sadržaj poruke elektroničke pošte za prepoznavanje phishing napada će vjerojatnije biti žrtve [46]. U slučaju da korisnik ima neku od opisanih karakteristika, za svaku treba dobiti 1.25 boda. Prema tome može se odrediti početna ocjena koja će biti između nula i deset.

Kako bi se uklonio drugi nedostatak Affinity IT mehanizma za procjenu phishing rizika može se bodovati ponavljanje nepoželjnog ponašanja. Ponavljanje nepoželjnog ponašanja se može promatrati na zadnje četiri phishing simulacije što je dovoljno da se pokaže koliko

su korisnici naučili tijekom edukacije. Bodovi se mogu dodijeliti tako da korisnik koji u tom razdoblju klikne na link dva puta dobije jedan bod više, za tri puta 1.5 boda, a za četiri puta dva boda. Korisnik koji upiše podatke dva puta tijekom četiri phishing simulacije može dobiti dva boda, za tri puta tri boda, a za četiri puta četiri boda više.

Za uklanjanje zadnjeg nedostatka potrebno je definirati kako odrediti phishing rizik cijele organizacije, a ne samo pojedinog zaposlenika. Rizik cijele organizacije se može odrediti kao prosjek rizika svakog zaposlenika, no može doći do pogreške jer određeni zaposlenici neće pročitati phishing poruku elektroničke pošte. Zbog toga bolje je odrediti rizik organizacije kao prosjek rizika zaposlenika koji su otvorili poruku elektroničke pošte.

5. Zaključak

Phishing je najčešća vrsta napada koji je prošle godine imao vrlo visoku uspješnost. Neki od uzroka uspješnosti su slaba informiranost korisnika i nedovoljno učinkovita tehnička obrana. Dok se ne razvije djelotvorna tehnička obrana, organizacije moraju phishing simulacijama trenirati svoje zaposlenike. Phishing simulacije su dobar način za edukaciju zaposlenika jer najbliže oponašaju stvarne phishing napade.

Alati za phishing simulacije olakšavaju postavljanje simulacija s različitim značajkama poput postavljanja web poslužitelja i slanja personaliziranih poruka elektroničke pošte. Također, neki alati omogućavaju potpuno prilagođavanje phishing simulacije. Organizacije u nekim alatima mogu koristiti web stranice koje lažiraju stranice koje zaposlenici koriste. U određenim alatima je moguć jednostavan pregled rezultata phishing simulacija što olakšava organizacijama da izračunaju svoj phishing rizik.

Alati za phishing simulacije imaju jednu manu vezanu uz korištenje Outlooka za slanje poruka elektroničke pošte u phishing simulacijama. Ponekad će Outlook označiti te poruke kao pokušaj phishing napada zbog čega će manje zaposlenika postati žrtvom u simulaciji. Označavanje poruke pomaže korisniku u zaštiti od stvarnih napada, ali napadači će uvijek pronaći način kako izbjeći označavanje te se ne treba oslanjati potpuno na tu metodu. Nadalje, alati koji koriste samo već napravljene predloške web stranica imaju manu što za određene web stranice koriste zastarjele verzije. Korištenje zastarjelih verzija web stranica može smanjiti uspješnost phishing simulacije.

Proces postavljanja phishing napada pomoću alata je vrlo jednostavan za organizacije, ali i za napadače. Napadači će uvijek imati prednost nad organizacijama jer im je potreban samo jedan uspješan napad za postizanje cilja, dok organizacije moraju educirati sve svoje zaposlenike. Međutim, phishing simulacijama organizacije mogu smanjiti vjerojatnost uspješnog napada i povećati znanje zaposlenika. Inače, bez treniranja zaposlenika uspješnost phishing napada će ostati visoka.

6. Literatura

[1] Social engineering (security), 28.04.2022., https://en.wikipedia.org/wiki/Social_engineering_(security), pristupano: 30.05.2022.

[2] Proofpoint, 2022 State of the Phish Report, 01.2022., https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-uk-tr-state-of-the-phish-2022.pdf, pristupano: 10.06.2022.

[3] Phishing, 12.6.2022., https://en.wikipedia.org/wiki/Phishing, pristupano: 30.05.2022.

[4] Alabdan R., Phishing Attacks Survey: Types, Vectors, and Technical Approaches, Future Internet 2020, 27.09.2020., svezak 12

[5] Barracuda, Business Email Compromise (BEC), https://www.barracuda.com/glossary/business-email-compromise, pristupano: 07.06.2022.

[6] Atkins B., Huang W., A Study of Social Engineering in Online Frauds, Open Journal of Social Sciences, 21.08.2013., svezak 1

[7] Jampen D., Gur G., Sutter T., Tellenbach B., Don't click: towards an effective anti-phishing training. A comparative literature review, Hum. Cent. Comput. Inf. Sci., 09.08.2020., svezak 10

[8] Trustwave, Cyber Attackers Leverage Russia-Ukraine Conflict in Multiple Spam Campaigns, 25.03.2022., https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cyber-attackers-leverage-russia-ukraine-conflict-in-multiple-spam-campaigns/, pristupano: 07.06.2022.

[9] Canova G., Volkamer M., Bergmann C., Borza R., NoPhish: An Anti-Phishing Education App, 09.2014.

[10] Gupta B. B., Arachchilage N. A. G., Psannis K. E., Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions, Telecommuncation Systems, 02.2018., svezak 67

[11] Sheng S., Magnien B., Kumaraguru P., Acquisti A., Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish, Proceedings of the 3rd Symposium on Usable Privacy and Security, 01.2007., svezak 229

[12] Wen A. Z., Lin Z., Chen R., Andersen E., What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 04.2019.

[13] Penetration test, 10.06.2022., https://en.wikipedia.org/wiki/Penetration_test, pristupano: 08.06.2022.

[14] Lin T., Capecci D. E., Ellis D. M., Rocha H. A., Dommaraju S., Oliveira D. S., Ebner N. C., Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content, ACM Trans Comput Hum Interact., 09.2019., svezak 26

[15] ngrok, https://ngrok.com/, pristupano: 09.06.2022.

[16] Google, Less secure apps & your Google Account, https://support.google.com/accounts/answer/6010255, pristupano: 09.06.2022.

[17] GoPhish, https://getgophish.com/, pristupano: 30.05.2022.

[18] GoPhish, Template Reference, 2019., https://docs.getgophish.com/user-guide/template-reference, pristupano: 30.05.2022.

[19] MicroSolved, Tools and research, https://www.microsolved.com/free-tools, pristupano: 30.05.2022.

[20] MSISimplePhish, *readme* tekstualna datoteka, pristupano: 30.05.2022.

[21] Phish-Me-Not : Employee Phishing Simulator, https://github.com/th3hack3rwiz/Phish-Me-Not, pristupano: 30.05.2022.

[22] pingb, http://pingb.in, pristupano: 30.05.2022.

[23] The Social-Engineer Toolkit (SET), https://github.com/trustedsec/social-engineer-toolkit, pristupano: 31.05.2022.

[24] Pavković N., Perkov L., Social Engineering Toolkit - A Systematic Approach To Social Engineering, 01.2011.

[25] ..Modlishka.., https://github.com/drk1wi/Modlishka, pristupano: 31.05.2022.

[26] Modlishka, How to use, 25.05.2019., https://github.com/drk1wi/Modlishka/wiki/How-to-use, pristupano: 31.05.2022.

[27] The redlure Distributed Phishing Framework, https://github.com/redlure/redlure-console, pristupano: 01.06.2022.

[28] redlure-worker, https://github.com/redlure/redlure-worker, pristupano: 01.06.2022.

[29] redlure-client, https://github.com/redlure/redlure-client, pristupano: 01.06.2022.

[30] redlure, Emails, https://docs.redlure.io/redlure-console/emails.html, pristupano: 01.06.2022.

[31] LordPhish, https://github.com/Black-Hell-Team/LordPhish, pristupano: 01.06.2022.

[32] Zphisher, https://github.com/htr-tech/zphisher, pristupano: 01.06.2022.

[33] AdvPhishing, https://github.com/mohantirumalasetti/AdvPhishing, pristupano: 02.06.2022.

[34] SocialFish, https://github.com/UndeadSec/SocialFish, pristupano: 02.06.2022.

[35] HiddenEye, https://github.com/Morsmalleo/HiddenEye, pristupano: 02.06.2022.

[36] PhishMailer, https://github.com/BiZken/PhishMailer, pristupano: 03.06.2022.

[37] Mike Bailey, Reporting Phishing Simulations: The Essential Metric to Measure in Phishing Awareness, 01.11.2021., https://www.proofpoint.com/us/blog/email-and-cloud-threats/reporting-phishing-simulations-essential-metric-measure-phishing, pristupano: 06.06.2022.

[38] Steves M., Greene K., Theofanos M., Categorizing human phishing difficulty: a Phish Scale, Journal of Cybersecurity, 14.09.2020., svezak 6

[39] Affinity IT, Measuring Phishing Risk., https://affinity-it-security.com/measuring-phishing-risk/, pristupano: 06.06.2022.

[40] Yang R., Zheng K., Wu B., Li D., Wang Z., Wang X., Predicting User Susceptibility to Phishing Based on Multidimensional Features, 17.01.2022.

[41] Omer Taran, ssessing Your Phishing Risks: More Than Just Click Rate, 17.12.2018., https://cyberready.com/phishing-simulation-training-right-metrics, pristupano: 06.06.2022.

[42] Jones H. S., Towse J. N., Race N., Harrison T., Email fraud: The search for psychological predictors of susceptibility, PLoS ONE, 16.01.2019., svezak 14

[43] Sheng S., Lanyon M. B., Kumaraguru P., Cranor L, Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions, Conference on Human Factors in Computing Systems – Proceedings, 01.2010., svezak 1

[44] Halevi T., Memon N., Nov O., Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks, SSRN Electronic Journal, 01.2015.

[45] Williams E. J., Hinds J., Joinson A. N., Exploring susceptibility to phishing in the workplaceInternational Journal of Human-Computer Studies, 12.2018, svezak 120

[46] Jayatilaka A., Arachchilage N. A. G., Babar M. A., Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors, 08.2021.

Sažetak

Ispitivanje alata za provođenje napada društvenim inženjeringom i treniranje zaposlenika

Phishing je najčešća vrsta napada te je obrana od istih postala važan dio računalne sigurnosti organizacija. U ovom radu opisani su alati za postavljanje phishing simulacija za edukaciju zaposlenika. Opisan je mehanizam za procjenu phishing rizika organizacija.

Ključne riječi: društveni inženjering, phishing

Summary

Evaluation of tools for social engineering attacks and training of employees

Phishing is the most common cyberattack and defending against it has become an important part of the organizations' cybersecurity. This paper describes tools for setting up phishing simulations used to educate employees. The mechanism for assessing the phishing risk of the organizations is described.

Keywords: social engineering, phishing