SIGURNOST RAČUNALNIH SUSTAVA, ak. god. 2022./2023.
Treća laboratorijska vježba: Ranjivosti web aplikacija

Virtualni stroj

Za treću i četvrtu laboratorijsku vježbu se koristi pripremljeni virtualni stroj s instaliranim operacijskim sustavom Linux Xubuntu 20.04 (64-bitni), 2048 MB memorije i 2 jezgre.

Za pokretanje na operacijskim sustavima **macOS, Linux i Windows se koristi VirtualBox**, a za **macOS Apple Silicon (M1/M2) UTM**.

Upute za pokretanje i priručnik za korištenje se nalaze u repozitoriju predmeta:

- Upute za dohvaćanje i pokretanje virtualnog stroja (VirtualBox): https://www.fer.unizg.hr/_download/repository/IMUNES_Ubuntu_upute.pdf
- Upute za dohvaćanje i pokretanje virtualnog stroja (macOS Apple Silicon M1/M2): https://www.fer.unizg.hr/_download/repository/IMUNES_Ubuntu_upute_m1.pdf
- Priručnik za korištenje virtualnog stroja: https://www.fer.unizg.hr/_download/repository/IMUNES_Ubuntu_prirucnik.pdf

Image za **macOS, Linux i Windows**:

- https://mrepro.tel.fer.hr/images/IMUNES-Ubuntu_20230222.ova

Image za **macOS Apple Silicon (M1/M2):**

- https://mrepro.tel.fer.hr/images/IMUNES-Ubuntu_20230209-M1.utm.zip

IP adresa

Za izvođenje treće laboratorijske vježbe potrebno je ispravno podesiti mrežne postavke kako bi se mogli spojiti na virtualni stroj. Obično sve radi standardno, no ako se ne možete spojiti na stroj putem mreže pokušajte promijeniti vrstu mrežnog adaptera virtualnog stroja (*bridged* ili NAT bi trebali raditi u svakom slučaju). Uz to, da bi mrežni adapter radio morate biti spojeni na Internet na matičnom računalu!

Logirajte se u virtualni stroj i provjerite dodijeljene IP adrese:

```
$ ip addr
...
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
...
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    inet 10.19.0.136/24 brd 10.19.0.255 scope global dynamic noprefixroute enp
0s8
...
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
```

```
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixrou
te enp0s9
```

U prikazanom ispisu je NAT sučelju dodijeljena adresa 10.0.2.15, "bridged" sučelju adresa 10.19.0.136, a "host- only" sučelju adresa 192.168.56.101.

U ovoj vježbi se spajate sa svog (glavnog) računala na ranjivi web poslužitelj na "bridged" ili "host-ony" adresi.

Docker

Kao korisnik root pokrenite docker instancu ranjivog web poslužitelja:

```
$ sudo docker run --rm -it -p 80:80 vulnerables/web-dvwa
```

Na operacijskom sustavu macOS Apple Silicon (M1/M2), umjesto vulnerables/web-dvwa dohvaćate petechua/docker-vulnerable-dvwa:

```
$ sudo docker run --rm -it -p 80:80 petechua/docker-vulnerable-dvwa:1.0
```

Spajanje na ranjivi web poslužitelj

Iz svog (glavnog) računala spojite se na ranjivi web poslužitelj na "bridged" ili "host-ony" adresi:

```
http://_vanjska_adresa_/
```

Kliknite na gumb pri dnu stranice: `Create / Reset Database` te ponovo otvorite istu stranicu na kojoj se sad traži upis korisničkog imena i lozinke.

```
http://_vanjska_adresa_/
```

Podaci za login su:

```
u: admin
p: password
```

U vježbi ćete proučavati ranjivosti web aplikacija (Commmand Execution, SQL injection, XSS i File inclusion). Cilj je iskoristiti ranjivosti kako biste ubuduće znali testirati i zaštiti web aplikaciju.

NAPOMENA: Prilikom izvođenja vježbe slobodno koristite opcije koje se kriju iza gumba `View Source` i `View Help` u donjem lijevom kutu pojedinih prozora.

1) Izvođenje naredbi (Command Injection)

- Otvorite prozor `Command Injection`
- Isprobajte naredbu: `1 | echo sui`
- Ako se ispod forme ispisalo `sui`, nastavite - ako nije, provjerite je li u izborniku `DVWA Security` postavljena razina `low`.
- Nadalje, možete upisati bilo koju naredbu nakon početnih `1 |`. Višestruke naredbe odvajate znakom &. Primjeri: `1 | ls`, `1 | pwd & whoami & ps`...
- Potrebno je ispisati sadržaj datoteke `/etc/passwd` i priložiti ga u rješenju zadatka uz opisani postupak i korištene naredbe.

2) Napadi SQL umetanjem (SQL injection)

- Otvorite prozor `SQL Injection`.

- Isprobajte osnovne primjere prema predavanjima iz predmeta.
- Cilj je dohvatiti sažetak lozinke korisnika Pablo Picasso. Kako bi došli do sažetka trebate poznavati strukturu i naziv tablice u kojoj su pohranjeni korisnički podaci. Iako je do toga moguće doći upisivanjem niza SQL naredbi u formu pod `SQL injection`, zbog jednostavnosti možete pogledati kako tablica izgleda izravno u bazi podataka:

```
mysql> show columns from users;
+------------+-------------+------+-----+---------+-------+
| Field      | Type        | Null | Key | Default | Extra |
+------------+-------------+------+-----+---------+-------+
| user_id    | int(6)      | NO   | PRI | 0       |       |
| first_name | varchar(15) | YES  |     | NULL    |       |
| last_name  | varchar(15) | YES  |     | NULL    |       |
| user       | varchar(15) | YES  |     | NULL    |       |
| password   | varchar(32) | YES  |     | NULL    |       |
| avatar     | varchar(70) | YES  |     | NULL    |       |
+------------+-------------+------+-----+---------+-------+
```

- Sažetak lozinke dohvaćen napadom "SQL injection" spremite u datoteku na virtualnom stroju. Primjer za lozinku `admin`:

```
$ echo "21232f297a57a5a743894a0e4a801fc3" > hashes.txt
```

Sažetak lozinke je u izračunat s algoritmom MD5.

Otkrivanje lozinke možete izvesti pomoću neke besplatne "on-line" usluge.
(A možete i instalirati i koristiti program "John the Ripper")

- Potrebno je navesti sve naredbe koje ste umetali i opisati cijeli postupak. Konačno rješenje zadatka je lozinka korisnika Pablo Picasso. (Hint: u upitima koristite ključnu riječ `UNION`)

3) XSS (Cross Site Scripting)

- Otvorite prozor `XSS Stored`. Ovdje je omogućen unos skripti u dijelu `Message` koje se potom pohranjuju u bazu podataka, tj. u tablicu `guestbook`.
- Isprobajte unijeti jednostavn javascript kod - ponovnim učitavanjem stranice skripta bi se automatski trebala izvršiti (npr. javascript naredba `alert()`).
- Potrebno je pročitati kolačiće korisnika koji pregledava stranicu s pomoću javascript naredbe `alert()`. Vrijednost varijable `PHPSESSID` navedite u izvještaju u jednoj liniji sljedećeg oblika:

```
PHPSESSID=f04m0i20nek10volimtep6e9irji5
```

- Sve kolačiće potrebno je s pomoću `GET` zahtjeva predati kao parametar na `http://public.tel.fer.hr/sui`. (npr. `http://public.tel.fer.hr/sui?cookie=security=low;%20PHPSESSID=f04m0i20nek10volimtep6e9irji5`) Opišite cijeli postupak i priložite korištene skripte.
- Kako biste zaštitili aplikaciju od ovakvih ranjivosti?

4) Inkluzija datoteka (File inclusion)

- Otvorite prozor File Inclusion i pratite upute (moguće je mijenjati HTTP `GET` parametar `page`)

- Ispišite datoteku `/etc/passwd`, priložite sliku ekrana s ispisanom datotekom i objasnite zašto je to moguće izvesti.
- Kako biste zaštitili navedenu aplikaciju od ovakve vrste napada?

Rezultati laboratorijske vježbe

Kao rezultat laboratorijske vježbe, kroz sustav Ferko trebate predati **ZIP arhivu** koja sadrži **izvještaj** u txt formatu (najviše **1500 riječi**) s postupkom rješavanja zadatka i odgovorima na pitanja te **sliku ekrana** iz 4. zadatka.