Password Cracking

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

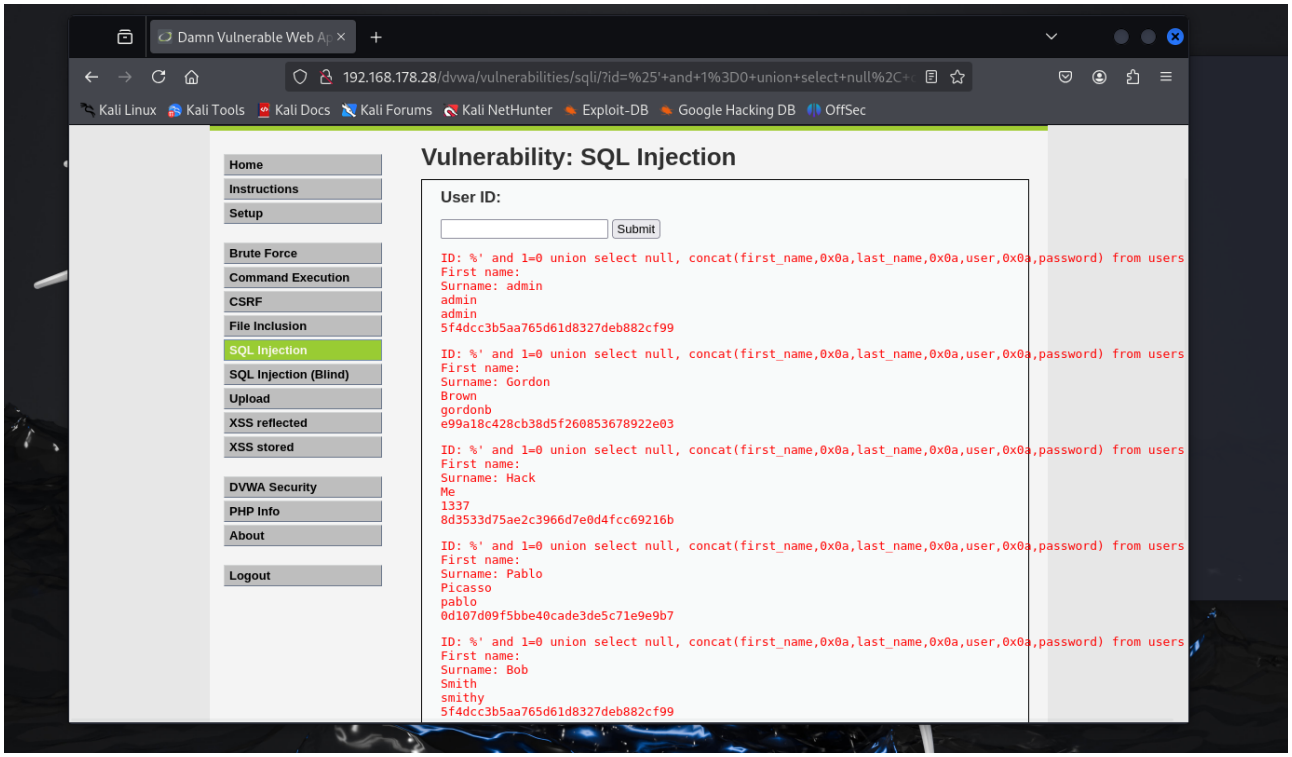
Il primo passo è stato quello di recarsi sul sito della **DVWA**, la quale è vulnerabile agli attacchi **SQL Injection**, in modo da poter iniettare un codice SQL che ci consentisse di visualizzare tutti gli admin e le relative password presenti all'interno. Il problema di fare ciò è che le password 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 #

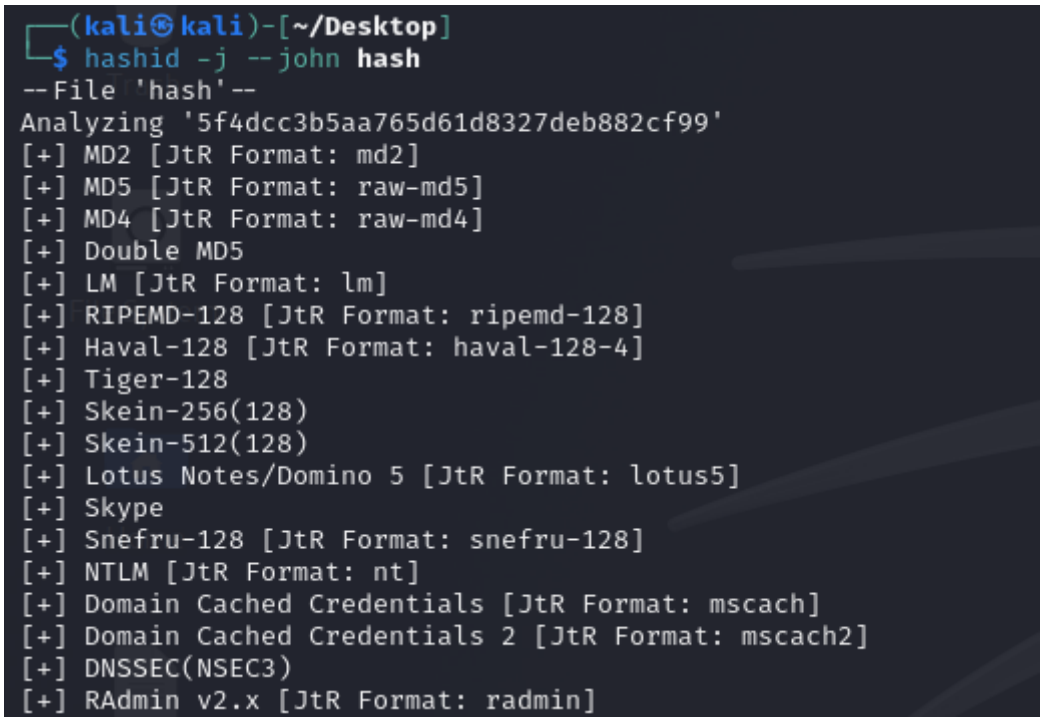
Tramite questo attacco abbiamo ottenuto tutte le informazioni degli user presenti:



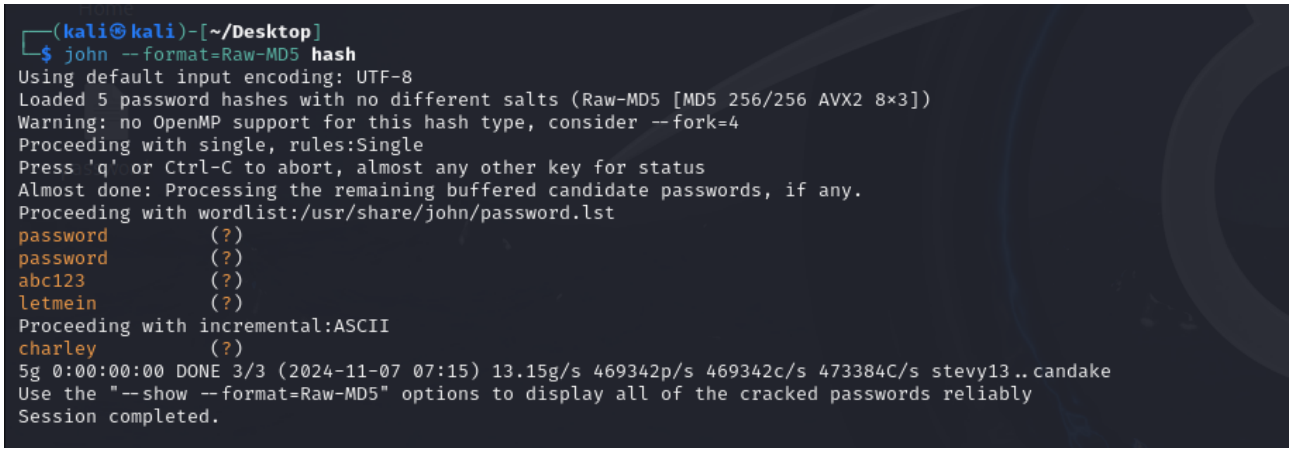
Tra cui le informazioni sulla password, salvata in codice hash su un file di testo.

```
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.



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.



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
```