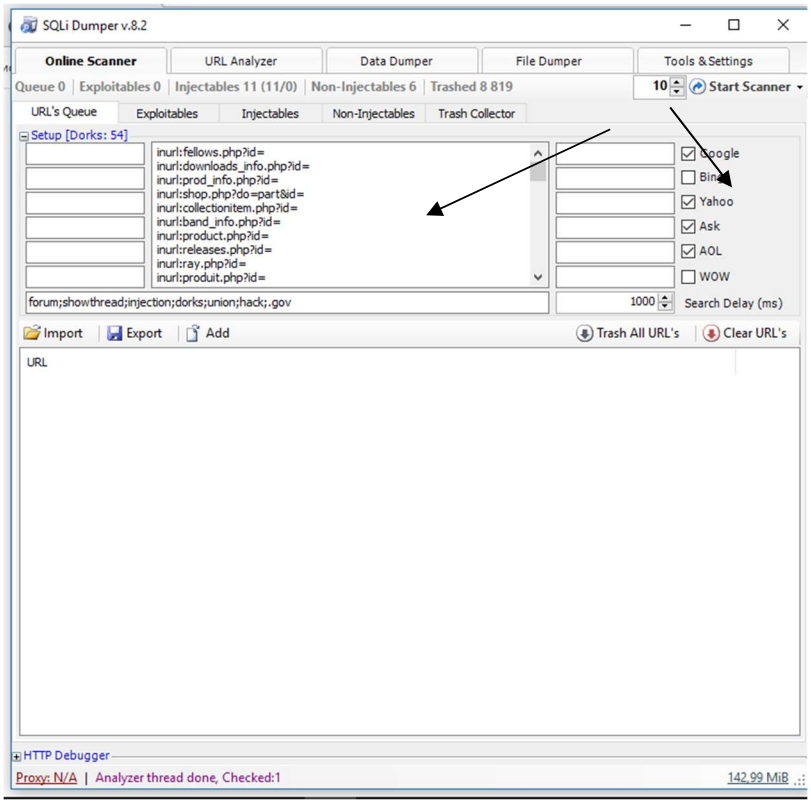
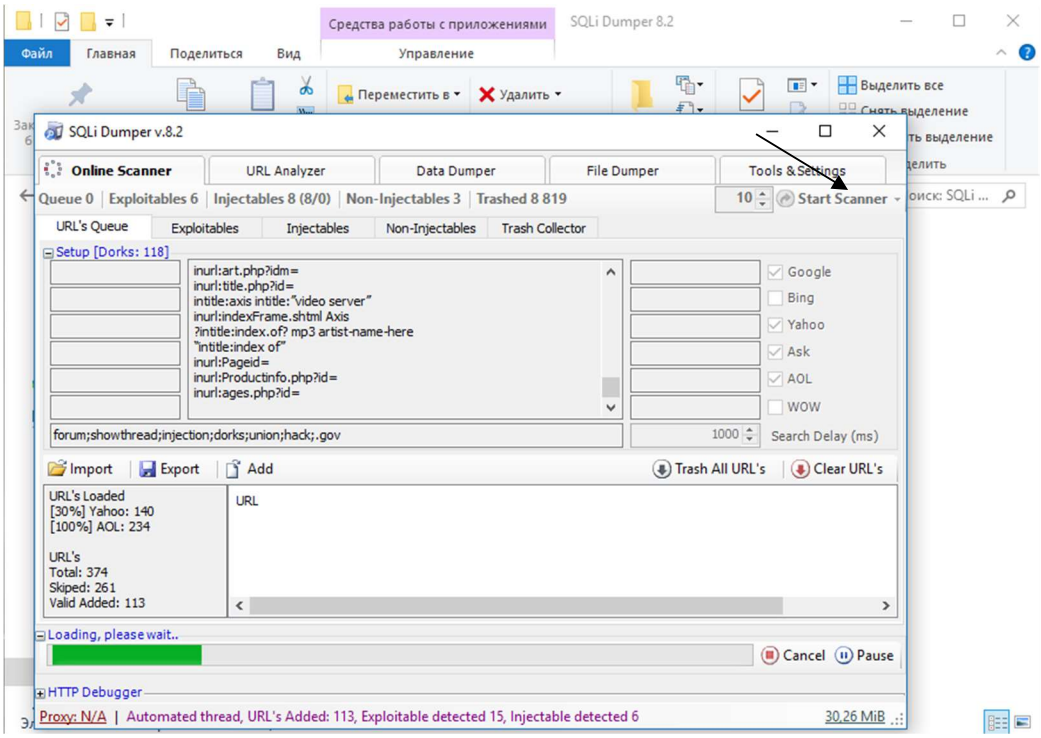
SQLi Dumper 8.2

- 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)**



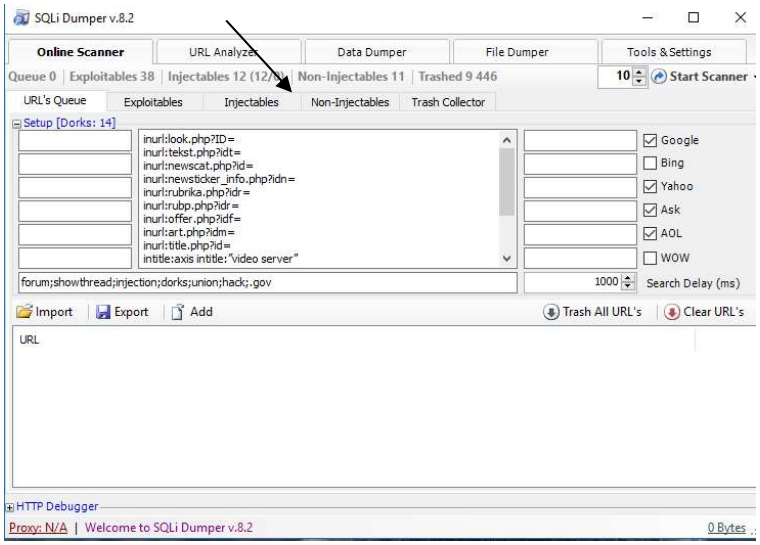
(fig. 10)

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



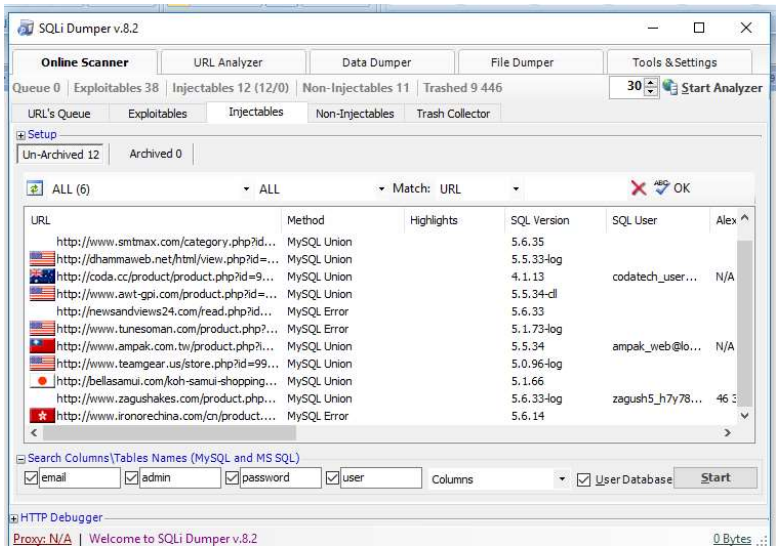
(fig. 11)

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



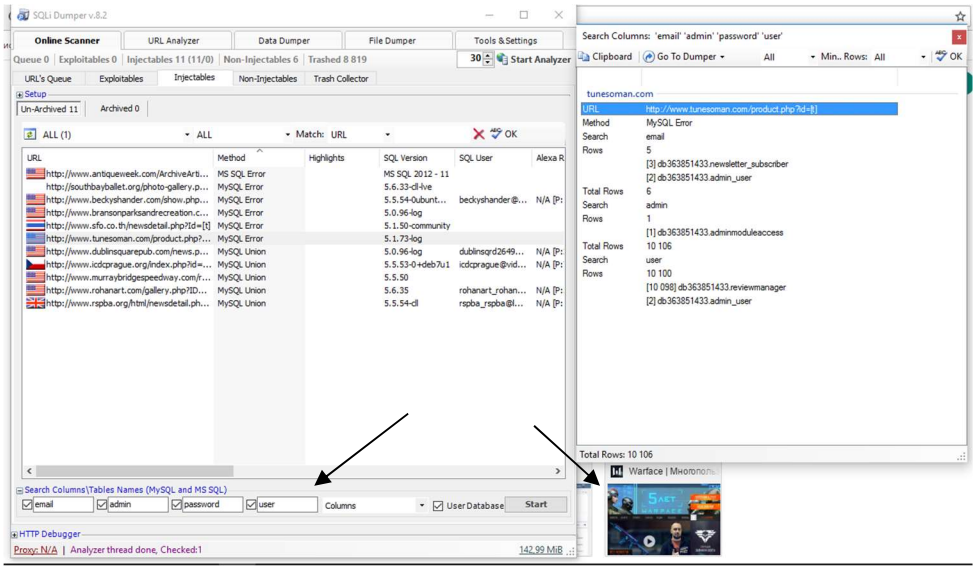
(fig. 12)

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



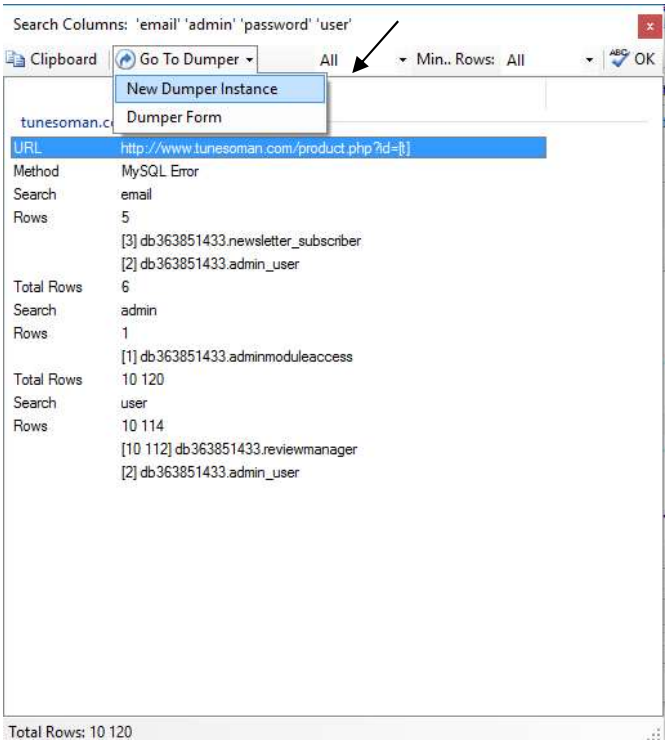
(fig. 13)

- 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)**



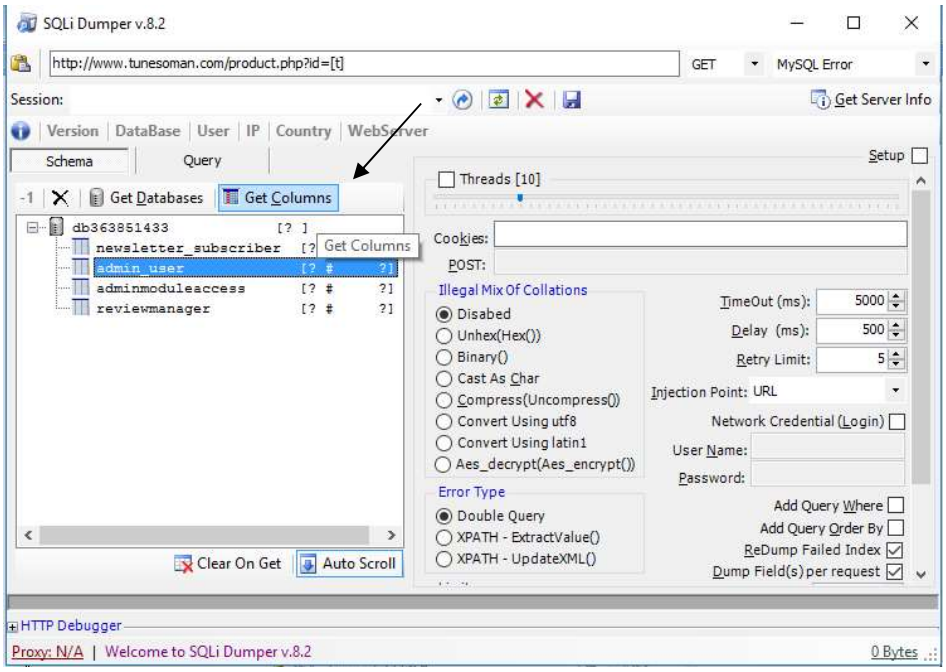
(fig. 14)

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



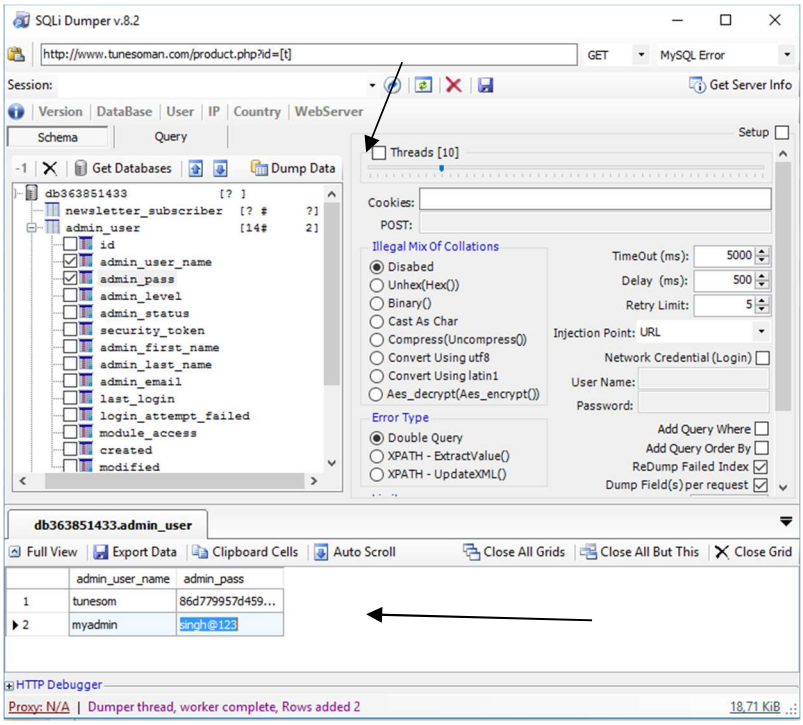
(fig. 15)

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



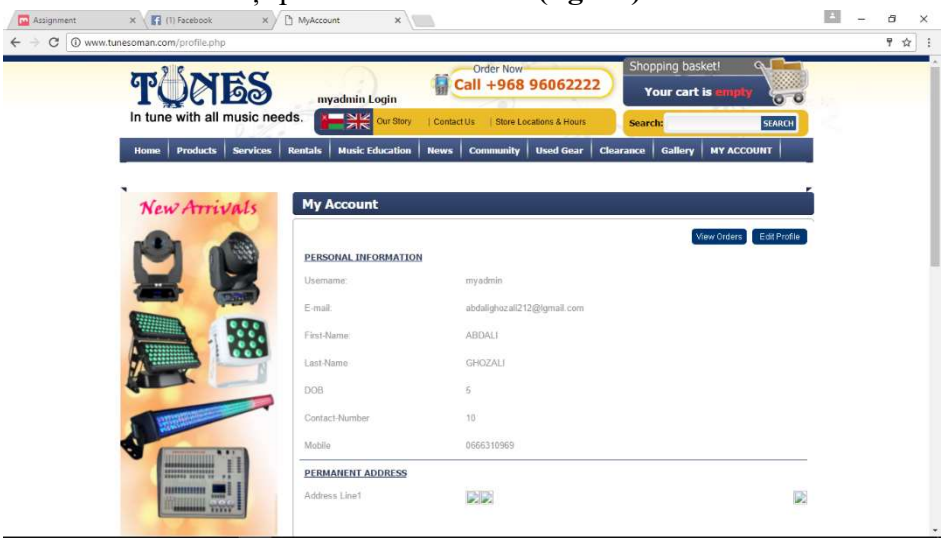
(fig. 16)

- Astfel noi obținem ce cîmpuri conține tabelul **admin_users** . După informația primită bifăm cîmpuri cu informația necesara 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

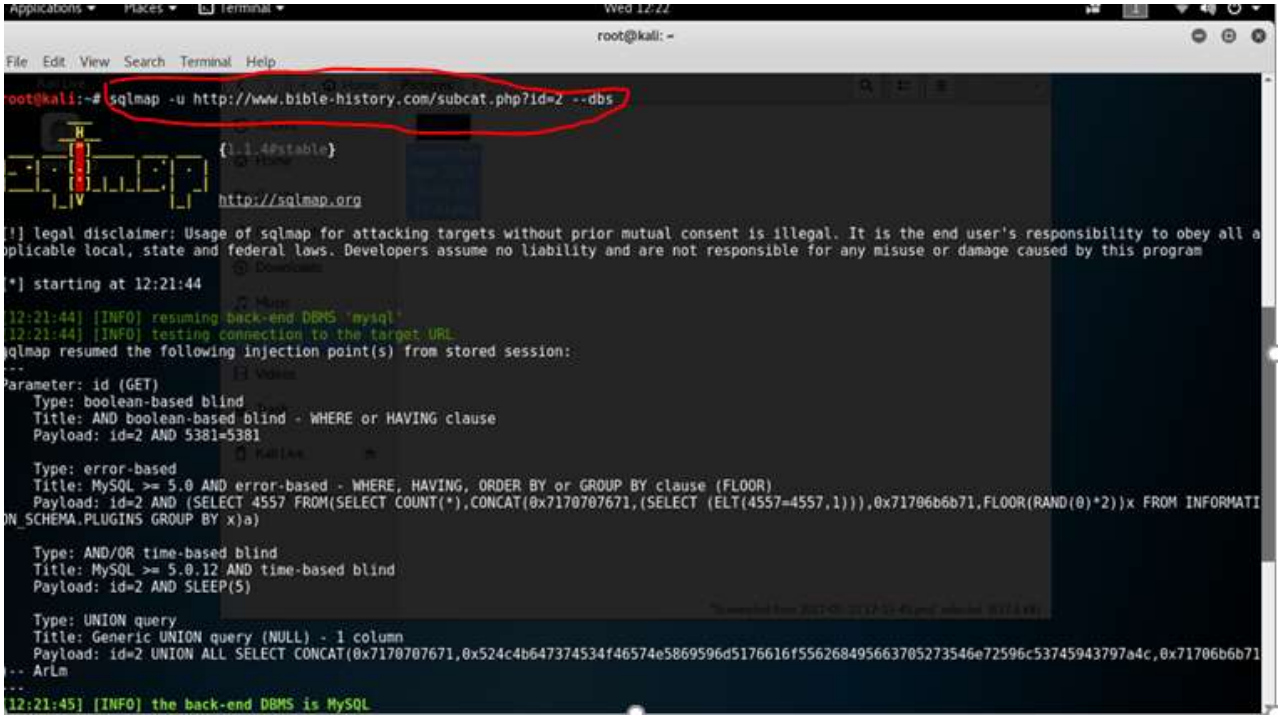
Pornim sistemul de operare kali linux, apoi deschidem terminalul,

Dup ce alegem tinta, introducem urmatoarea comanda in terminal:

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

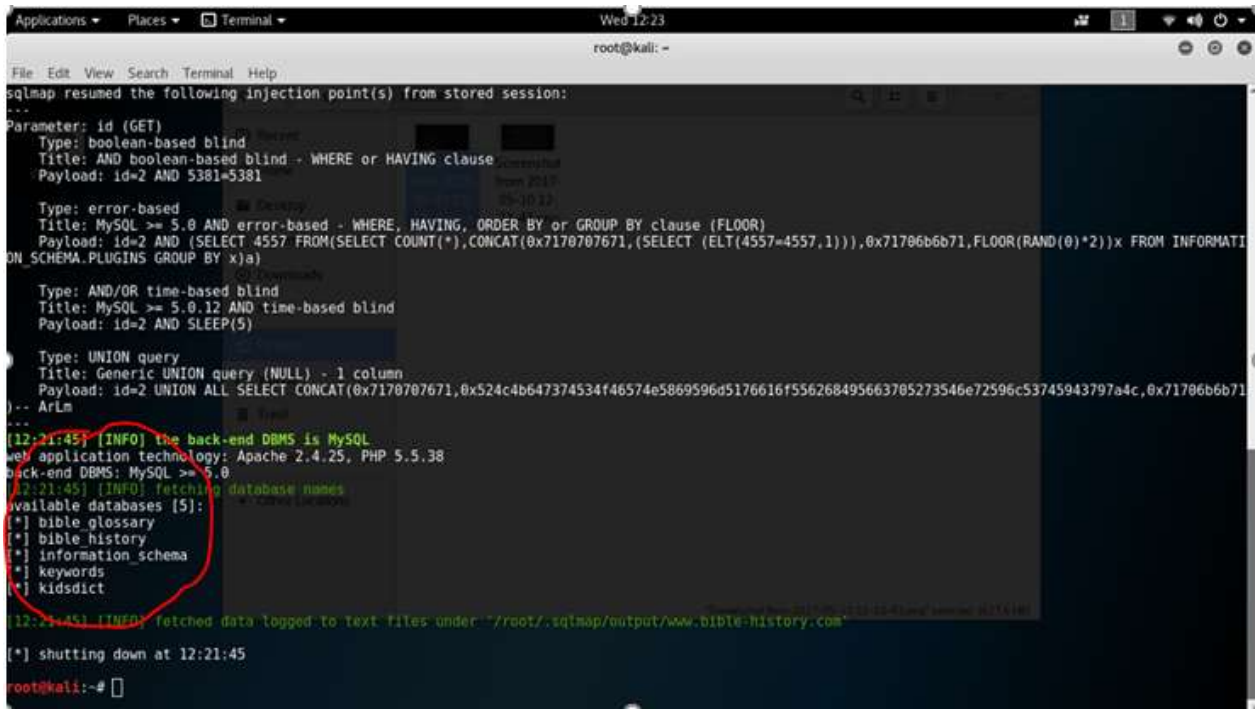
-u – semnifica ca urmeaza o adresa url

--dbs – semnifica ca avem nevoie de baza de date



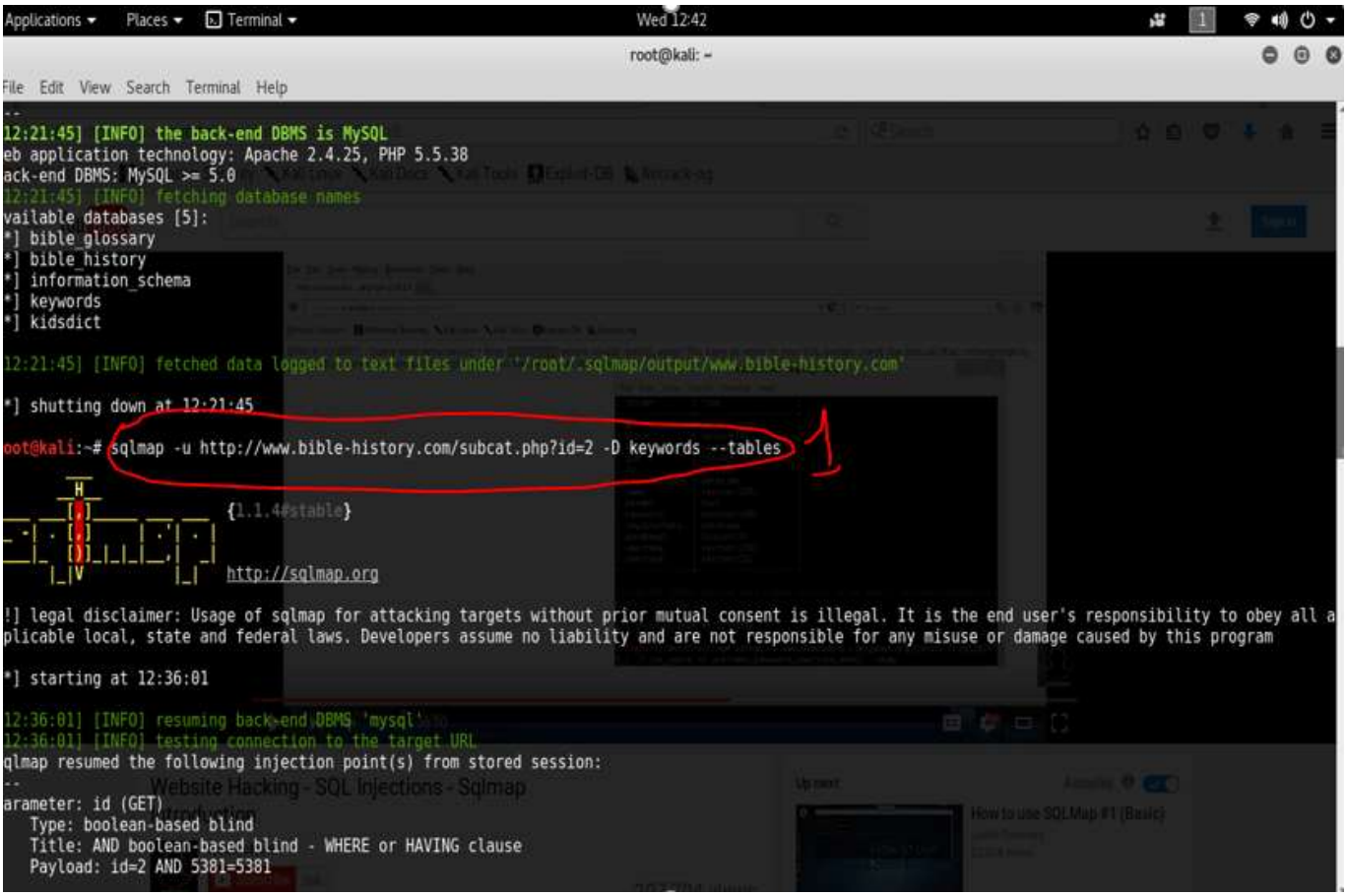
După cum se observă, aplicația în timp ce rulează testele, afișează informația despre testul ce se rulează și unele informații care ar putea fi utile pentru utilizator. În cazul dat, se vede că aplicația este vulnerabilă și la atac corss-site scripting.

Dupa finisarea scanarii avem urmatorul rezultat:



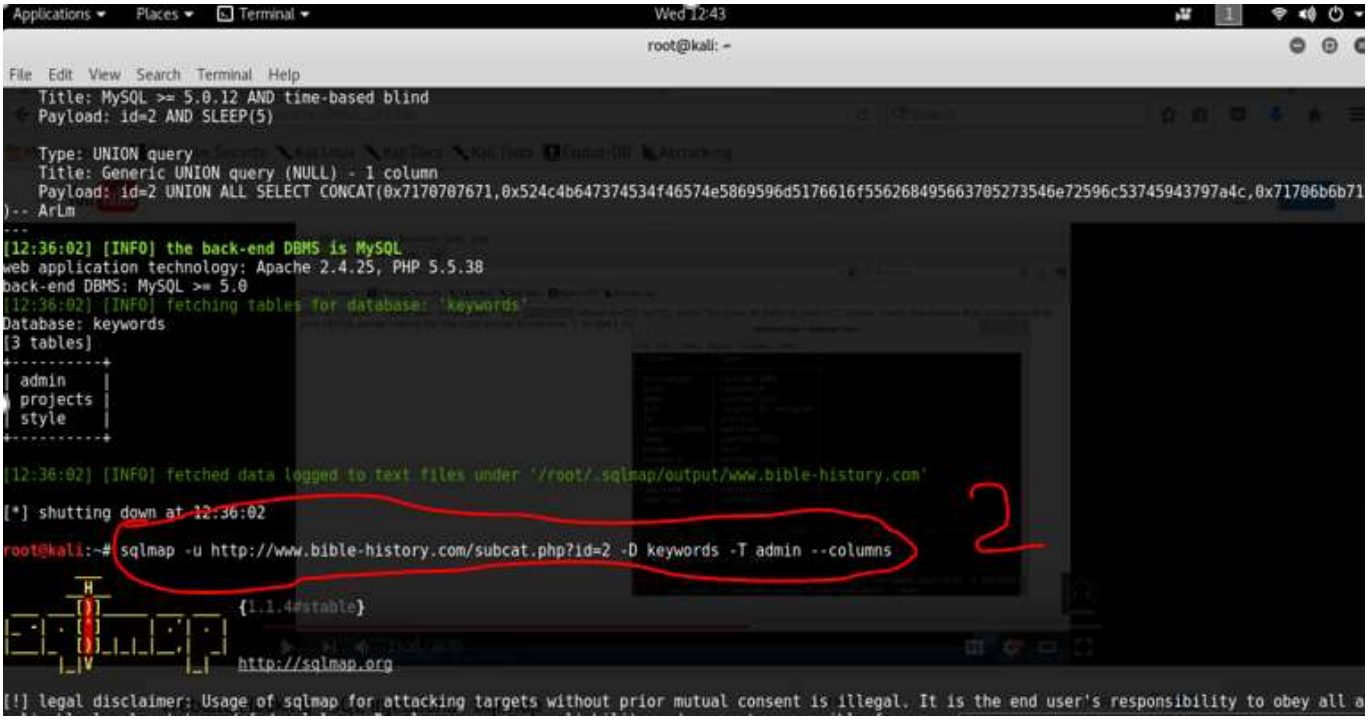
- De asemenea, aplicația afișează informația despre atacul săvârșit, care a fost parametrul injectat, tipul atacului, titlul și payload-ul utilizat, rezultatul atacului, denumirile bazelor de date prezente în aplicația dată
- Ca rezultat poate fi solicitată afișarea unei baze de date sau poate fi determinat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

2. Analizam rezultatul obtinut si selectam baza de date dorita pentru explorare, alegem keywords indroducind urmatoarea comanda(**1**):



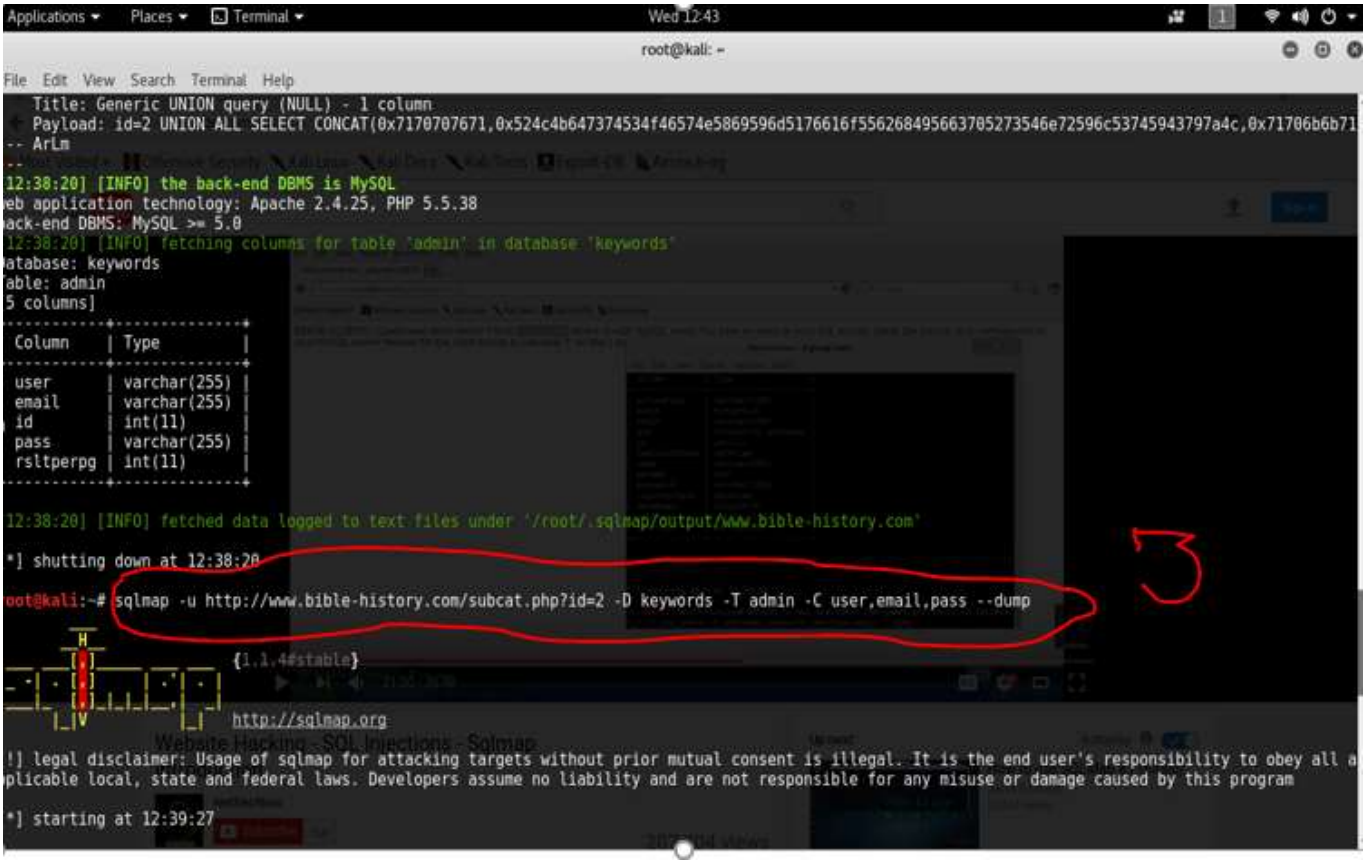
--tables – smnifica ca vom acesa tabela

Am obtinut rezulatatul 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 **--colums**



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

-C – coloanele.



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