Machine Learning in Cyber Security

2024/2025

Class Project: SQL Injection with SQLmap

1. Objective

The aim of this class project is to experiment with **SQLmap** how to find SQL injection vulnerabilities in web applications.

In this class project, students will use the virtual machine (VM) installed previously. Using this VM, the goal is to find SQL injection (SQLi) vulnerabilities in the MODC-DB web application and retrieve the database structure and data from the database that supports that application. However, before attacking the application, students should first work with it and perform some attacks manually to understand how SQLi works, and which vulnerable points exist in the application.

2. Exploiting vulnerabilities manually

The VM contains the MODC-DB web application, our target web application. It is accessed through the URL http://127.0.0.1/modc-db/ or http://localhost/modc-db/.

Explore the application by doing the following actions and in order to understand its functioning and some vulnerable points.

1. Create an account, by defining your username and password credentials, and then login with them
2. Explore some Operations provided by the application:
    a. DNS Lookup: provide the VM's IP (127.0.0.1) and see the result
    b. Add to Your Blog: write some text you want insert in your blog
    c. Show User Info: provide your credentials and see your information
3. Through the option **Show User Info**, it is possible to exploit a SQL injection vulnerability. Explain how you proceed to exploit the SQLi. Also, provide the URL that is sent by the browser to the application. You can use the Browser Developer Tools (F12 key) and access the Network separator to get this information.

4. The operation **DNS Lookup** is vulnerable to OS command injection, i.e., it is possible inject other linux commands besides the required IP address. Explain how you can exploit this vulnerability in order to obtain the content of the /etc/passwd file.

3. Running SQLmap

Execute the following commands in a terminal to test and run the SQLmap tool. Change into the directory and run the python script to ensure all looks good.

```
$ cd /home/modc/apps/sqlmap-dev
$ python3 sqlmap.py
```

To get a full list of the options available run `python3 sqlmap.py -h`

To show advanced help and options available run `python3 sqlmap.py -hh`

In the **Bibliography** section a set of small tutorials is available to help you in performing the following tasks.

4. Database structure and SQLi vulnerabilities

One of the most powerful features of SQLmap is its capability of retrieving the structure (tables, columns) of the target database, as well as the data contained in their tables. To understand how you can use SQLmap to get this data, you should read the tutorials listed in Section 5. The tutorials are very similar, but they complement each other. Also, you can resort to Browser Developer Tools in case, for example, you need to access to the requests sent to the web application in order to obtain malicious inputs to be used with SQLmap. (HINT: For the next tasks, you can use the URL of question 3, from Section 2)

Task 1:

Using SQLmap, identify and indicate:

- Which DBMS is associated with the MODC-DB database and which databases it stores;
- After identifying the MODC-DB's database, indicate which are its tables and their structures;
- Which is the table that contains the most sensitive data; retrieve the data from this table.

Task 2:

Using SQLmap and the information and data retrieved in Task 1, find the SQL injections vulnerabilities existing in MODC-DB.

5. Bibliography

SQLmap official website: https://sqlmap.org/

SQLmap tutorials:

https://techyrick.com/sqlmap-full-tutorial/

https://www.sqlinjection.net/sqlmap/tutorial/

https://hackertarget.com/sqlmap-tutorial/

Delivery of the Report

The output of the class project is a report answering all the questions and including the justifications for the responses. Each group should deliver the report either by submitting it in the course moodle page, or if there is some difficulty with this method, by emailing it to professor. The file type should be a pdf.

Deadline: 20 September 2024 (there will be no extensions)