Chapter 5

Understanding SQL Injection & SQL Map

Today, we are exploring the fascinating world of SQL Injection, a powerful technique used to uncover vulnerabilities in websites. SQL injection plays a critical role in hacking by targeting the weak points in a website's database security.

WHAT IS SQL INJECTION

Every website is backed by a database—a virtual storage room that holds essential information like usernames, passwords, product details, and more. Accessing this database typically requires authorization, like using a **secret key** to unlock a room. But what if someone could bypass this security key? This is where SQL injection comes into play.

SQL injection is a method used to manipulate a website's database by injecting malicious SQL (Structured Query Language) code into vulnerable input fields. By doing this, hackers can gain unauthorized access to sensitive data or even take control of the database.

UNDERSTANDING THROUGH REAL LIFE EXAMPLE

Imagine you're shopping online and see a "Coupon Code" field at checkout. When you enter a code, the website communicates with its database to check if the code is valid:

- If valid, it returns a **True** response, and you get a discount.
- If invalid, it returns a **False** response, showing “Coupon code is invalid.”

Now, if the website is poorly secured, a hacker can input malicious SQL code like *OR 1=1*. Mathematically, *1=1* is always **True**, so the database interprets it as valid and provides unauthorized access or discounts. This is the magic of SQL injection—tricking the database into doing something unintended.

THE ROLE OF SQL MAP

To perform SQL injection efficiently, ethical hackers and cybercriminals rely on tools like SQL Map. SQL Map is an advanced, automated tool designed specifically to find and exploit SQL injection vulnerabilities in websites.

What Does SQL Map Do

Scans the Website:

- SQL Map starts by interrogating the website, asking it various questions (like a detective interrogating a suspect).
- It observes the responses to identify weak points in the website’s database queries.

Tests Inputs:

- SQL Map sends different types of inputs and commands to the website (like trying different keys in a lock).

- ❖ If the website reacts strangely or provides unexpected responses, it indicates a vulnerability.

Exploits Vulnerabilities:

- ❖ Once SQL Map identifies a weak point, it digs deeper.
- ❖ It can extract sensitive information, modify data, or even take full control of the system, depending on the severity of the vulnerability.

How SQL Map Works in Simple Terms

1. You provide the URL of a target website to SQL Map.
2. SQL Map scans the site, analyzing how it responds to various inputs.
3. If the responses deviate from normal behavior, SQL Map flags the input field as vulnerable.
4. Finally, it extracts (or "dumps") data from the database by running queries and analyzing the responses.

SQL MAP BASIC COMMANDS

Learn how to identify website vulnerabilities with SQL Map using these essential commands:

Targeting a Website

Specify the website to test using the *-u* command:

sqlmap -u "https://targetwebsite.com"

Replace *https://targetwebsite.com* with the URL of the website you want to scan. This tells SQL Map which website to analyze for vulnerabilities.

Crawling Pages

Use the *--crawl* command to detect linked pages for vulnerabilities:

sqlmap -u "https://targetwebsite.com" --crawl=3

Choose a number between 1 (light scan) to 5 (deep scan).

Avoid Detection

Disguise requests using the *--random-agent* command:

```
sqlmap -u "https://targetwebsite.com" --random-agent
```

This command ensures that the server cannot easily detect that the scan is being conducted by a tool like SQL Map.

Adjust Risk Levels

Control scan aggressiveness with *--risk*:

```
sqlmap -u "https://targetwebsite.com" --risk=2
```

Risk levels: 1 (low), 2 (medium), 3 (high).

Deep Scanning

Analyze more parameters using *--level*:

sqlmap -u "https://targetwebsite.com" --level=4

Levels: 1 (shallow) to 5 (deep).

Combine for Best Results

Example command:

```
sqlmap -u "https://targetwebsite.com" --crawl=3
--random-agent --risk=2 --level=4
```

This approach helps you explore vulnerabilities while balancing depth, risk, and stealth.

CONCLUSION

SQL injection is like a double-edged sword—it can be used maliciously or ethically to strengthen security. With the help of tools like SQL Map, we can uncover vulnerabilities, secure websites, and protect sensitive data.
Always remember: With great knowledge comes great responsibility. Let's continue to learn and grow responsibly as ethical hackers.

By ScripterJee