**Lab 6- Automating SQL injection using SQLmap**

**What Was Learned:**This lab provided hands-on experience in automating SQL injection attacks using SQLmap, an open-source tool widely used for penetration testing. Participants learned how to identify vulnerabilities in web applications and use SQLmap to exploit those vulnerabilities efficiently.

**Key Learnings:**

1. **Introduction to SQLmap:**
   * SQLmap is a powerful tool designed to automate the detection and exploitation of SQL injection vulnerabilities.
   * It saves time and increases accuracy by systematically testing various injection techniques.
2. **Lab Setup and Environment:**
   * Used TryHackMe’s AttackBox, a virtual environment equipped with SQLmap and other penetration testing tools.
   * Explored SQL injection vulnerabilities via a sample login page hosted on a target system.
3. **Basic SQL Injection Test:**
   * Tested the login form for SQL injection by inputting 1 or 1=1-- - into the Profile ID field and observing that access was granted.
   * This simple test demonstrated the vulnerability of the application to SQL injection.
4. **Automating SQL Injection with SQLmap:**

Ran SQLmap with the following command to target and analyze the vulnerable parameter:  
bash  
Copy code  
sqlmap -u 'http://10.10.101.165:5000/sesqli1/login?profileID=q&password=a' -p 'profileID' --level=3 --risk=3

* + Key flags used:
    - -u: Specifies the target URL.
    - -p: Identifies the parameter to test for SQL injection.
    - --level=3: Increases the depth of techniques tested.
    - --risk=3: Makes the injection attempts more aggressive.

1. **SQLmap Results:**
   * SQLmap identified the profileID parameter as vulnerable to SQL injection.
   * The tool also provided detailed information about the backend database, including the version and other metadata, enabling further exploitation.

**Takeaways:**

* **SQL Injection Testing:**Learned how to test for and confirm SQL injection vulnerabilities manually and automatically.
* **Automation Benefits:**SQLmap significantly speeds up the testing process by applying a wide range of injection techniques.
* **Critical Information Gathered:**The database version and additional insights from SQLmap enable security professionals to craft more targeted and effective SQL queries for further exploitation.
* **Ethical Considerations:**Emphasized the importance of only conducting SQL injection tests with explicit permission from the system owner and within ethical hacking boundaries.
* **Defense Against SQL Injection:**Highlighted the need for developers to implement robust input validation, parameterized queries, and other security best practices to protect against SQL injection attacks.

This lab demonstrated the power of SQLmap as a penetration testing tool, making it an essential resource for professionals tasked with securing web applications.