SQLMap

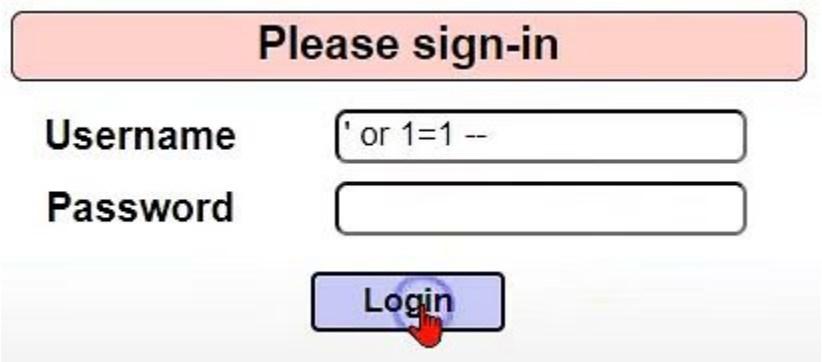
Jaylan Howden

Overview

- Conducting SQL injection attacks manually can be a time consuming and tedious process.
- As one of the most common and dangerous vulnerabilities in web applications, SQL injection is a critical concern for security professionals.
- SQLMap is an open-source penetration testing tool that automates the detection and exploitation of SQL injection vulnerabilities.
- Web applications can greatly improve their safety precautions and avoid data breaches by knowing how what SQL injection is and how to prevent it..
- SQL injection attacks threaten the CIA Triad by compromising the confidentiality, integrity, and availability of data and systems, leading to unauthorized access, data manipulation, and service disruptions.

What is SQL Injection

- SQL Injection is a type of security vulnerability that occurs when an attacker is able to manipulate with the queries that an application makes to into database.
- SQL Injection can lead to unauthorized access to sensitive data such as personal information, intellectual property, and financial details.
- It allows attackers to view data that they are not normally able to retrieve from regular queries.
- SQL Injection is one of the most widespread and critical security threats to web applications.



SQLMap

- SQLMap is a open source automated SQL Injection tool.
- SQLMap is an application that can be used on the Linux Command line
- SQLMap can find and exploit SQL vulnerabilities on a web application
- SQLMap can perform numerous attacks such as database fingerprinting, data extraction, file system access and OS command execution.
- SQLMap can be used for a variety of SQL Injection attacks.

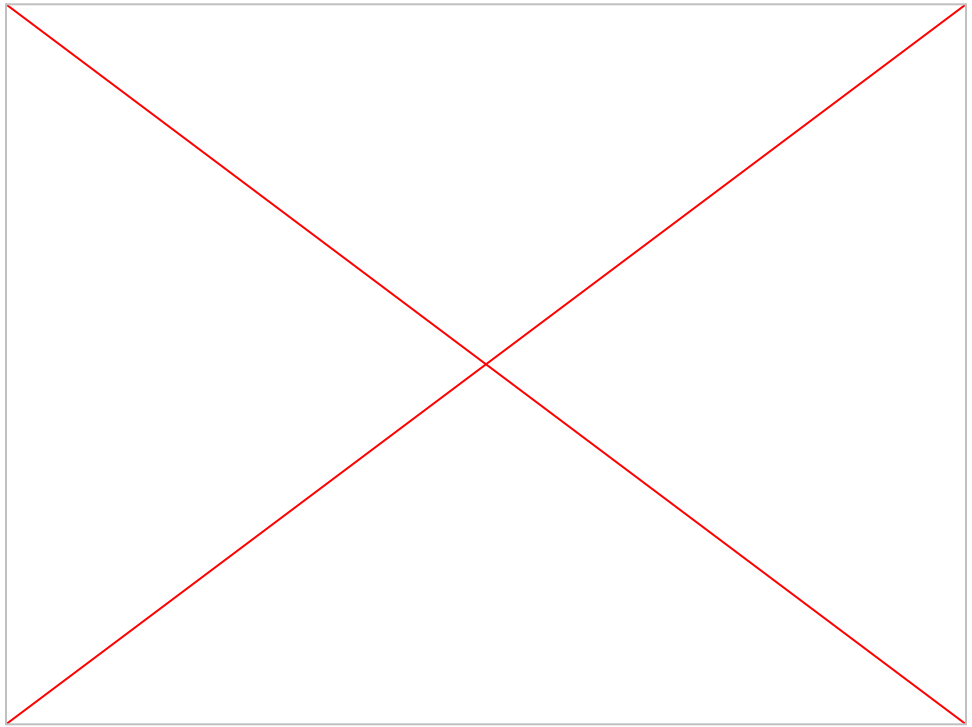
Tools

- SQLMap on linux
- Damn Vulnerable Web Application
- Virtual Machine with Apache Guacamole on Ubuntu
- Burp Suite (Linux)
- Web Browser (Firefox)
- Linux Command Line Terminal

Demonstration Preview

- Setting up DVWA(Damn Vulnerable Web Application) and testing queries
- Using the Burp Suite proxy to get HTTP request
- Setting parameters on SQLMap to start the SQL injection
- SQLMap uses the parameters to inject and attack the SQL database
- SQLMap then launches the attack and can get data such as database names, table names, usernames, and password hashes

SQLMap Demonstration



Demonstration Summary

- Using SQLmap on DVWA it shows how SQLMap can automate an attack on a vulnerable web application
- Using the HTTP proxy on Burp Suite you can see GET request which shows the request from the web application which SQLMap uses for the injection
- SQLMAP then launches the injection which enumerates the databases, dumps the tables in the database, and dumps the data from the table which includes usernames and password hashes which can be cracked.
- In Summary SQLMap can be a very useful tool for penetration testers when testing for web vulnerabilities and also be used by Security Analysts to identify and remediate SQL vulnerabilities on a web application.

Mitigation Against SQL Injection

- Input validation and sanitization
- Web application firewalls
- Prepared Statements and Parameterized Queries which treat statements as data, not as executable code
- Keeping Web applications and databases up to date with updates and patches
- Provide thorough security awareness training to all relevant employees, including as system administrators, software developers, quality assurance teams, and DevOps engineers.
- Having a Incident response plan if a SQL Injection attack were to happen

The End

Thank You