SQLMAP

-GROUP 2-

Members

SE172607 - Nguyễn Nhật Phát

SE170526 - Trịnh Quốc Thái

SE172605 - Hoàng Văn Anh Nghĩa

SE170092 - Nguyễn Viết Nam Khánh

-OVERVIEW-

WHAT IS SQLMAP?

SQLmap is an open-source tool designed to automate the process of detecting and exploiting SQL injection vulnerabilities in web applications, assisting security professionals and penetration testers in assessing the security of systems.

-OVERVIEW-

WHY IS SQLMAP?

- Automatic Detection
- Time and Effort Savings
- Learning Support
- Versatile Performance
- System Security
- Cost-Effective

-OVERVIEW-

W H O ?

Sqlmap developed by

Bernardo Damele A. G. (@inquisb)
https://twitter.com/inquisb

Miroslav Stampar (@stamparm)
https://twitter.com/stamparm

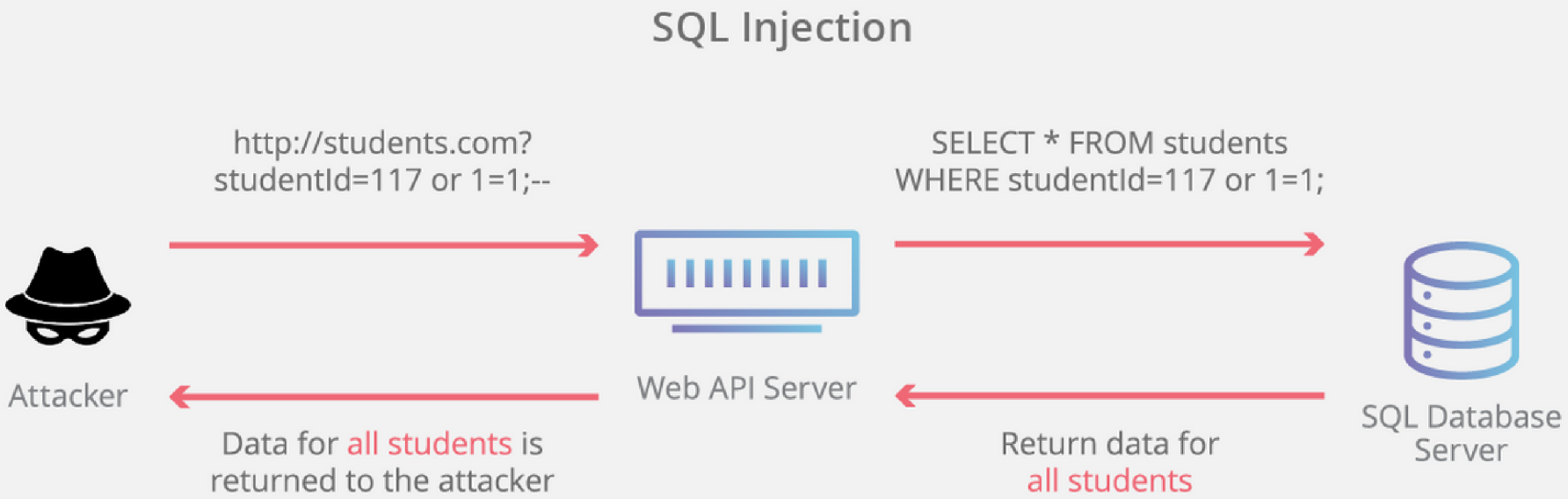
-OVERVIEW-

CUSTOMER REFERENCE

SQLmap is freely available to the public and is widely used by security professionals, ethical hackers, and penetration testers across the globe.

ARCHITECTURE

sqlmap is a software utility for automated discovering of SQL injection vulnerabilities in web applicatons



HIGHLIGHTS

An open source pentesting tool
An python based tool
Exploits vulnerabilities in databases
SQLMAP
Mostly used for web applicaton pentesting
Supports a wide range of databases
Comes pre-installed in kali linux

THE PROS AND CONS

PROS

- Automated Detection and Exploitation
- Open Source Community
- Command-line Flexibility
- Support for Various Database Management Systems

CONS

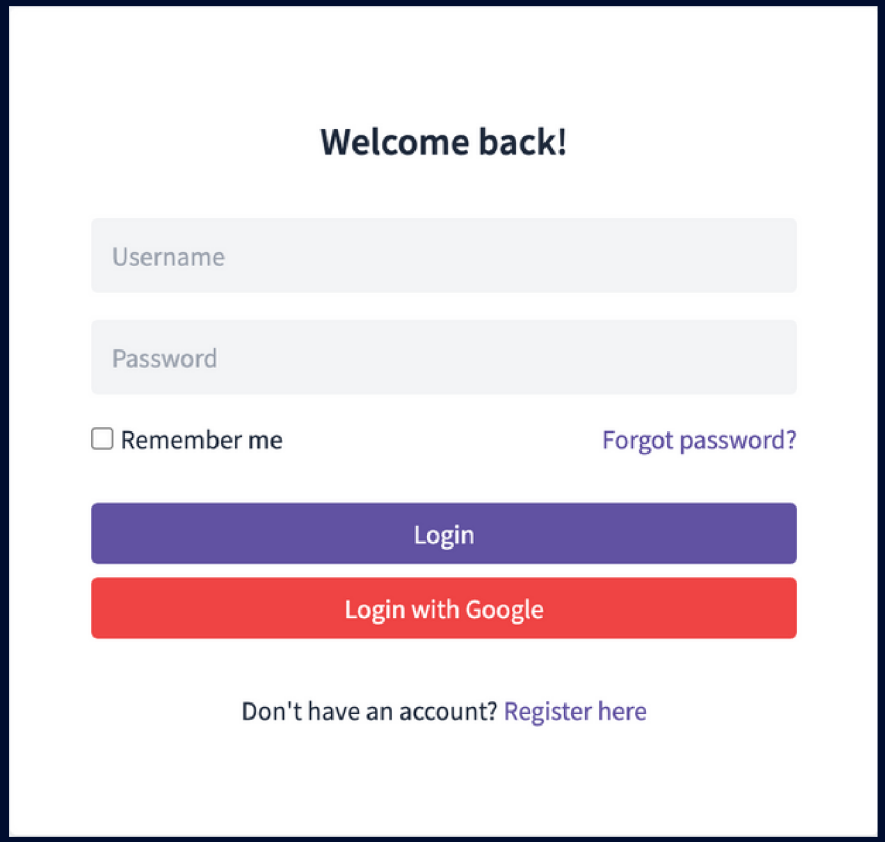
- Limited to SQL Injection Testing
- Potential Disruptions
- Requires Python
- Complex Output

Details of Features

1. Automated Analysis
2. Multi-Database Support
3. Automated Testing and Exploitation
4. Proxy Support
5. Sensitive Data Testing
6. Custom Querying
7. Network and Offline Attacks
8. File-Based Database Support
9. Fast and Accurate Testing

DEMO 1

Use SQLmap to detect vulnerability in login function



DEMO 2

Use SQLmap to take over DB System

THANK YOU!