CP3418 Best Practice

-Roblox Bug bounty Problem

Group-1
Group Member: Muchun Wan, Benelyon Zoe Choo, Pyae Sone Soe Moe
Date: 15 April 2024

Outline

Introduction

Specific Findings and Recommendation

Conclusion

Part 1

Introduction

Scope

Project Name: Bug Bounty Program for Roblox
Client: Roblox
Topic: Bug Bounty Program targeting the *.roblox.com wildcard domain.

Out-of-Scope: This project will not address vulnerabilities related to the execution of non-technical attacks (e.g., social engineering, physical attacks) or issues already known to Roblox or disclosed publicly.

Project Strategy

This Project have been conducted in the spirit of industry best practices as recommended by Penetration Testing Execution Standard (PTES).

- Environment Setup Phase
- Subdomain Enumeration Phase
- Business Logic Assessment
- Vulnerbility Scanning
- CTF Training Phase
- Attack Testing Phase

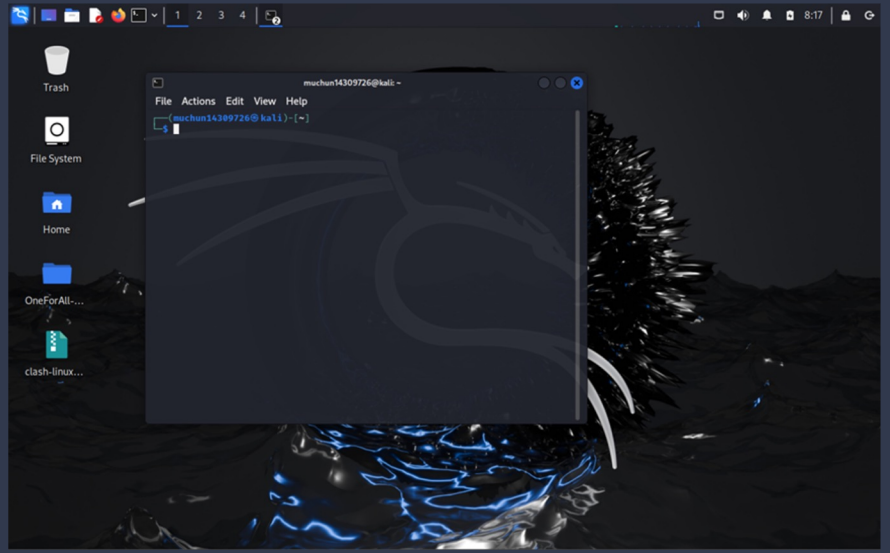
Environment

Virtual machine: VM Ware

Attack Environment: Kali

Version: kali-linux-2024.1-vmware-amd64

Tool: Dock, VPN, Burpsuite, One For All, Layer Subdomain Mining Machine, And Metasploit



Part 2

Specific Findings and Recommendation

Subdomain Enumeration - Findings

Layer子域名挖掘机4.1 重构版

域名: roblox.com　端口: 80,443　扫描端口　DNS: DNSPOD-119.29.29.29　枚举　接口　启动

域名	解析IP	开放端口	来源
c2.roblox.com	52.217.203.184,16.182.34.240,52.217.226.152,16.182.41.192,54.231.203.192,52.217.117.24,52.216.251.118,54.231.192.8	80,443	暴力枚举
c5.roblox.com	52.217.228.240,52.217.205.184,52.217.48.238,52.217.164.112,52.217.137.96,52.216.111.69,54.231.162.64,54.231.193.136	80,443	暴力枚举
c4.roblox.com	54.231.132.168,16.182.33.208,54.231.199.152,52.217.232.128,52.216.210.144,54.231.169.192,52.217.134.232	80,443	暴力枚举
c1.roblox.com	52.216.210.144,54.231.169.192,52.217.134.232,54.231.132.168,16.182.33.208,54.231.199.152,52.217.232.128	80,443	暴力枚举
c3.roblox.com	16.182.100.200,54.231.192.248,54.231.163.152,52.216.89.166,54.231.193.144,52.216.207.205,52.216.160.69,54.231.236.248	80,443	暴力枚举
m.roblox.com	128.116.118.4	80,443	暴力枚举
www.roblox.com	128.116.118.4	80,443	暴力枚举
blog.roblox.com	104.74.21.13	80,443	暴力枚举
mail.roblox.com	172.217.160.115	80,443	暴力枚举
help.roblox.com	3.141.133.52,3.132.2.44,3.18.13.7	80,443	暴力枚举
apis.roblox.com	128.116.118.4	80,443	暴力枚举
static.roblox.com	128.116.118.4	80,443	暴力枚举
news.roblox.com	3.132.2.44,3.18.13.7,3.141.133.52	80,443	暴力枚举
forum.roblox.com	128.116.118.4	80,443	暴力枚举
developer.roblox.com	54.192.18.43,54.192.18.53,54.192.18.84,54.192.18.32	80,443	暴力枚举
corp.roblox.com	118.215.11.69	80,443	暴力枚举
content.roblox.com	128.116.118.3	80,443	暴力枚举
groups.roblox.com	128.116.118.4	80,443	暴力枚举
css.roblox.com	52.217.163.88,52.216.214.40,52.217.131.248,52.217.41.118,16.182.72.48,54.231.128.64,52.217.46.94,52.216.33.176	80,443	暴力枚举
web.roblox.com	128.116.118.4	80,443	暴力枚举
js.roblox.com	52.216.62.168,52.216.130.197,54.231.194.224,52.217.10.238,52.217.192.112,52.217.204.8,52.216.26.198,52.216.28.6	80,443	暴力枚举
share.roblox.com	128.116.118.3	80,443	暴力枚举
ads.roblox.com	128.116.118.4	80,443	暴力枚举
wiki.roblox.com	54.192.18.43,54.192.18.32,54.192.18.84,54.192.18.53	80,443	暴力枚举
search.roblox.com	128.116.118.4	80,443	暴力枚举
affiliates.roblox.com	128.116.118.4	80,443	暴力枚举
auth.roblox.com	128.116.118.4	80,443	暴力枚举
billing.roblox.com	128.116.118.4	80,443	暴力枚举
catalog.roblox.com	128.116.118.4	80,443	暴力枚举
shop.roblox.com	8.42.96.20	-	暴力枚举
chat.roblox.com	128.116.118.4	80,443	暴力枚举
bronze.roblox.com	128.116.102.3	80,443	暴力枚举
careers.roblox.com	23.200.152.254	80,443	暴力枚举
community.roblox.com	3.141.133.52,3.18.13.7,3.132.2.44	80,443	暴力枚举
corporate.roblox.com	23.200.152.254	80,443	暴力枚举
develop.roblox.com	128.116.118.4	80,443	暴力枚举
data.roblox.com	128.116.118.4	80,443	暴力枚举
de.roblox.com	3.132.2.44,3.18.13.7,3.141.133.52	80,443	暴力枚举
discussions.roblox.com	128.116.118.3	80,443	暴力枚举
education.roblox.com	23.200.152.254	80,443	暴力枚举
es.roblox.com	3.132.2.44,3.141.133.52,3.18.13.7	80,443	暴力枚举
fr.roblox.com	3.141.133.52,3.132.2.44,3.18.13.7	80,443	暴力枚举
events.roblox.com	54.192.18.97,54.192.18.62,54.192.18.67,54.192.18.76	80,443	暴力枚举
gold.roblox.com	128.116.118.3	80,443	暴力枚举

状态：完成，共发现108个子域名　访问Sean博客

Layer Subdomain Mining Machine

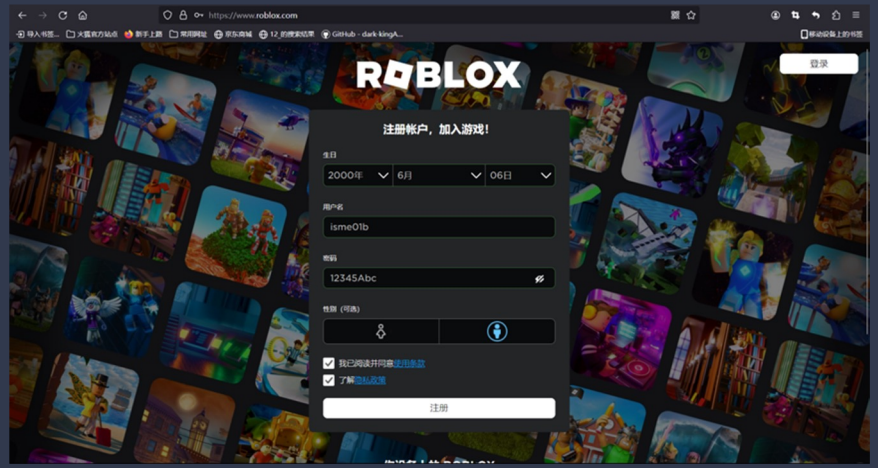
A total of 108 subdomain information were collected

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	id	alive	request	resolve	url	subdomain	level	cname	ip	public	cdn	port	status
2	1	1	1	1	http://corp.roblox.com	corp.roblox.com	1	e7229.dscl	23.42.124.	1	1	80	40
3	2	1	1	1	https://nrt2-128-116-120-4.roblox.com	nrt2-128-116-120-4.roblox.com	1	nrt2-128-1	128.116.12	1	1	443	40
4													
5													
6													

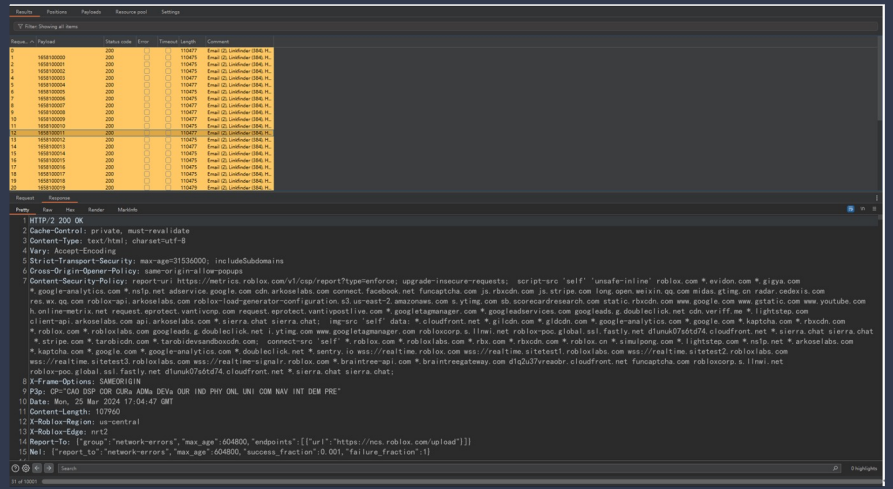
OneForAll

Collected a total of 2 subdomain name information

Business Logic Assessment - Findings



Registration feature lacked identity verification



Potential user enumeration vulnerabilities

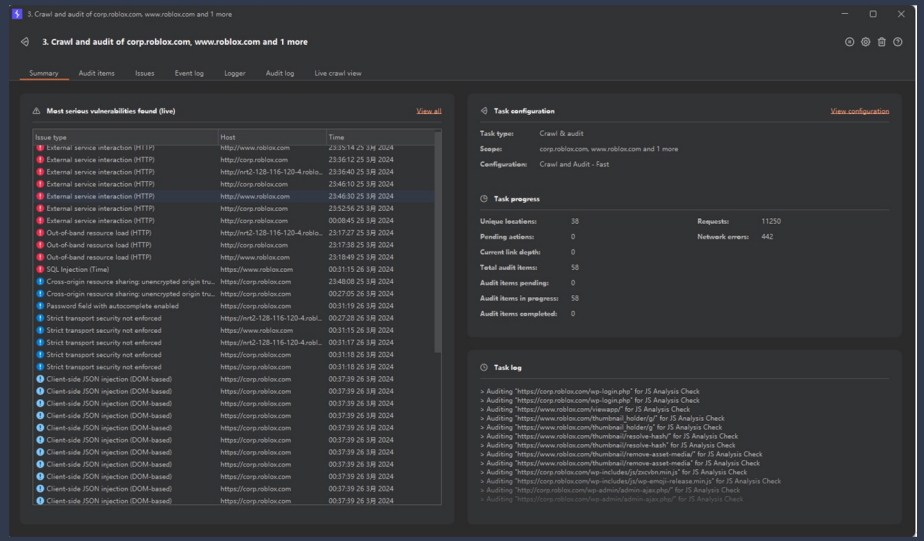
Business Logic Assessment - Recommendation

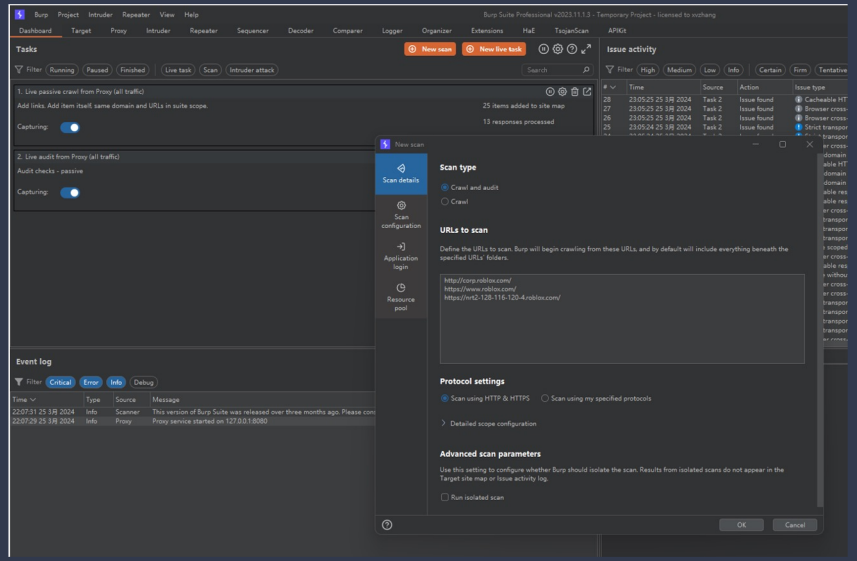
Based on the findings from the logical vulnerability testing, we recommend the following actions to mitigate identified risks and enhance the security posture of the Roblox platform:

1. Enhance Input Validation and Authentication Checks: Implement more rigorous checks to verify user information during registration and login processes to prevent unauthorized access.

1. Secure User Enumeration Points: Address vulnerabilities that allow user enumeration, potentially by implementing rate limiting, enhancing error messages to be less informative about the existence of user accounts, and employing more robust authentication mechanisms.

Vulnerability Scanning





The system has 11 high-risk vulnerabilities
and 22 low-risk vulnerabilities.

Vulnerability Scanning - Findings

CVE-2022-30004 Detail

Description

Sourcecodester Online Market Place Site v1.0 suffers from an unauthenticated blind SQL Injection Vulnerability allowing remote attackers to dump the SQL database via time-based SQL injection..

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

CVE-2018-16307 Detail

Description

An "Out-of-band resource load" issue was discovered on Xiaomi MIWiFi Xiaomi_55DD Version 2.8.50 devices. It is possible to induce the application to retrieve the contents of an arbitrary external URL and return those contents in its own response. If a domain name (containing a random string) is used in the HTTP Host header, the application performs an HTTP request to the specified domain. The response from that request is then included in the application's own response.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

CVE-2016-9692 Detail

Description

IBM WebSphere Cast Iron Solution 7.0.0 and 7.5.0.0 is vulnerable to External Service Interaction attack, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to induce the application to perform server-side DNS lookups or HTTP requests to arbitrary domain names. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. IBM X-Force ID: 119516.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 8.6 HIGH **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

External Service Interaction (HTTP) - CVE-2016-9692

Out-of-band Resource Load (HTTP) - CVE-2018-16307

SQL Injection (Time) - CVE-2022-30004

Critical Vulnerbility - Recommendation

External Service Interaction (CVE-2016-9692):

- Immediate Action
- Patch Management
- Configuration Review
- Input Validation
- Monitoring and Logging

SQL Injection (Time-based - CVE-2022-30004):

- Input Sanitization
- Prepared Statements and Parameterized Queries
- ORM Usage
- Regular Audits and Code Reviews
- Web Application Firewall (WAF)

Out-of-band Resource Load (CVE-2018-16307)

- Patching
- URL Whitelisting
- Secure Coding Practices
- Defense in Depth

For all these recommendations, it is crucial to:

1. Perform Regular Updates
2. Educate Development Teams
3. Incident Response Plan

XSS Attack - Findings

- CTF Training

- Manual Testing
  "https://www.roblox.com/" correctly sanitizes user input to prevent reflected XSS

- Auto Testing
  The tests did not reveal any XSS vulnerabilities on roblox.com.

XSS Attack - Recommendation

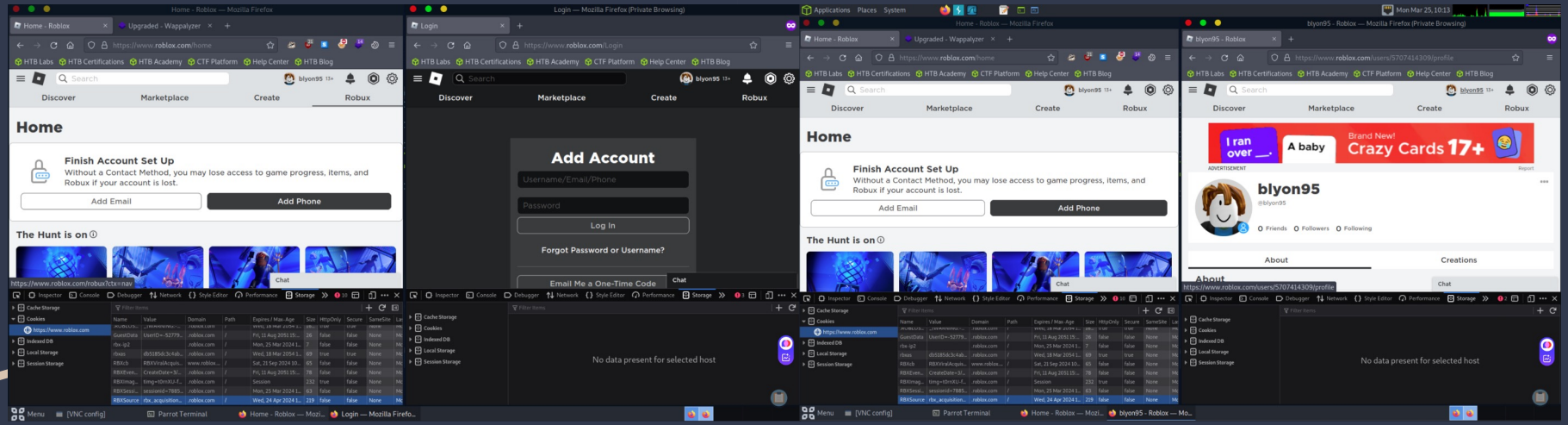
Even though no vulnerabilities were found during this assessment, the following practices are recommended to maintain a robust security posture:

1. Continue regular security audits and penetration testing to detect and mitigate potential vulnerabilities.
2. Stay updated with the latest security patches for the web application framework and third-party libraries.
3. Monitor security advisories and apply updates as soon as they become available.

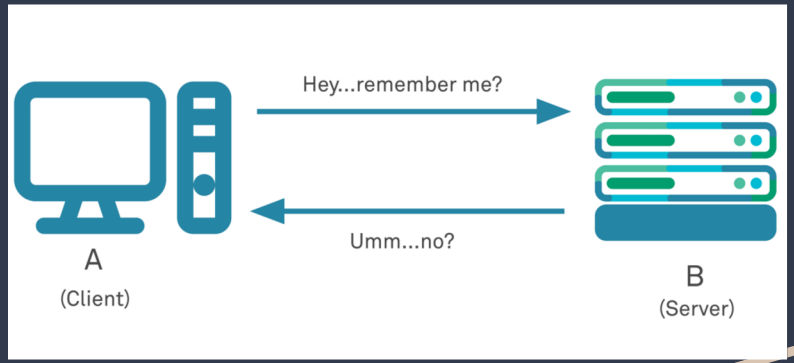
Session Attack Findings - Session Hijacking

Successful Demonstration

- **Successfully replicated the session environment on Roblox**
- **Gained control of the user session without authentication**



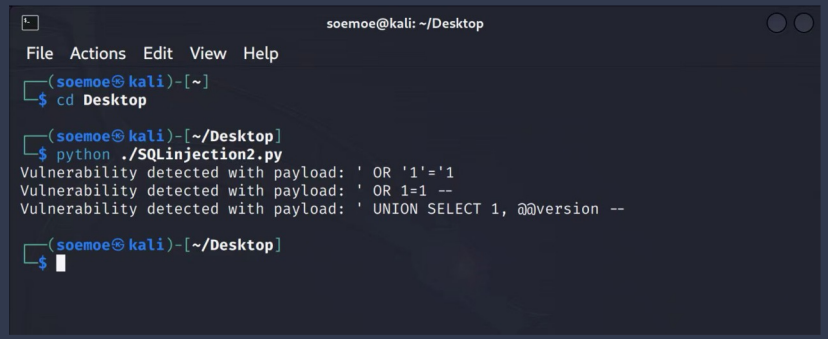
Session Attack Findings - Session Hijacking



Recommendations for Enhancing Web Security

- Enforce the use of HTTPS to ensure all data is encrypted during transmission.
- Implement HSTS to eliminate the risk of HTTPS downgrade attacks.
- Secure cookies by setting the ‘HttpOnly’, ‘Secure’, and ‘SameSite’ attributes.
- Regularly change session identifiers and establish session timeouts to reduce risk.
- Strengthen account security with multi-factor authentication.

Database Attack Findings

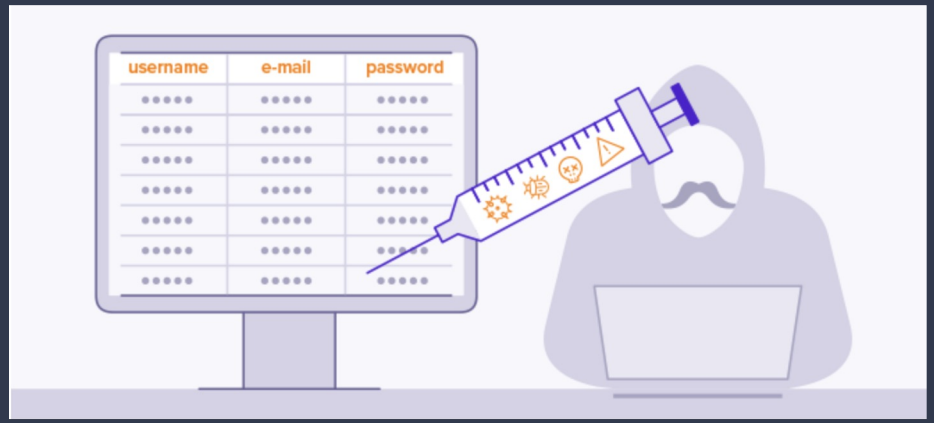


- **SQL Map Wizard: A guided setup for SQL injection testing using SQLMap, though it faced challenges due to incorrect URL formatting which ended the test prematurely.**

- **Python Script: A script that sends SQL payloads via HTTP POST requests to detect vulnerabilities, successfully identifying multiple SQL injection .**

Database Attack Recommendation

- Use of Prepared Statement and ORM tools
- Comprehensive Input Validation
- Error Handling
- Least Privileged Access
- Web Application Firewalls (WAFs)
- Regular Security Testing and Audits



Part 3

Conclusion

Conclusion

Robust and Reliable

Thank You