



Gaurav Sood





Agenda

1. Brief Overview of Hacking
2. OWASP Top 10
3. Toolbox
4. OWASP Juice Box
5. Live Hack



Hacking

- Unauthorized access to digital assets
- Individuals and Organizations
- Exploit chinks in system
- Types:
 - White Hat (Ethical)
 - Black Hat (Malicious)
 - Gray Hat



Steps Involved in Hacking

- Reconnaissance
- Enumeration
- Exploitation
- Persistence
- Lateral Movement
- Hiding Tracks



Reconnaissance





Reconnaissance

- **Information about Target**
- **OSINT**
- **Search Engines**
- **Dorking**



Enumeration





Enumeration

- **Hosts**
- **Networks**
- **Endpoints**
- **Files**
- **Devices**



Exploitation

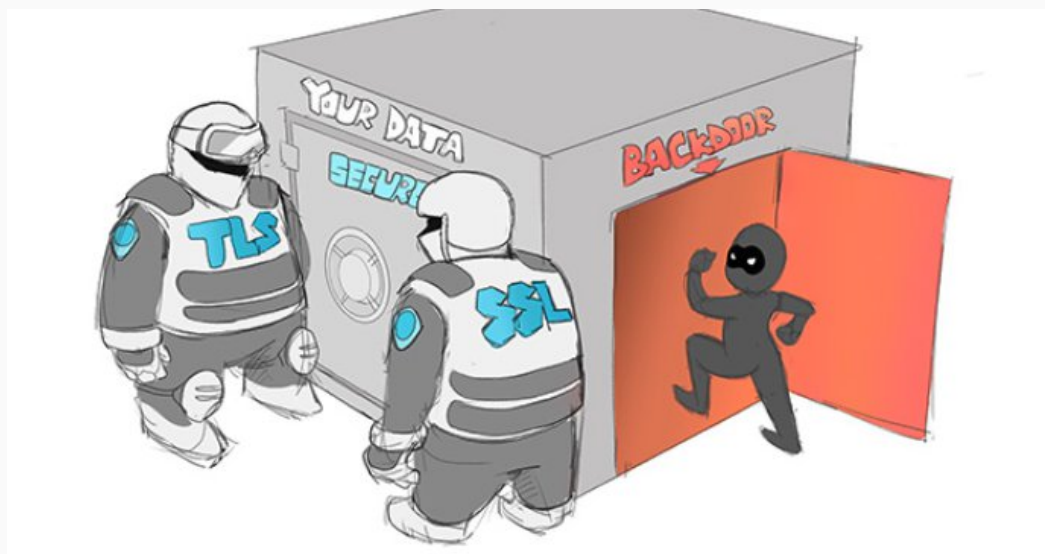
- **Gain Access**
- **Privilege Escalation**
- **Information Disclosure**
- **RCE**





Persistence

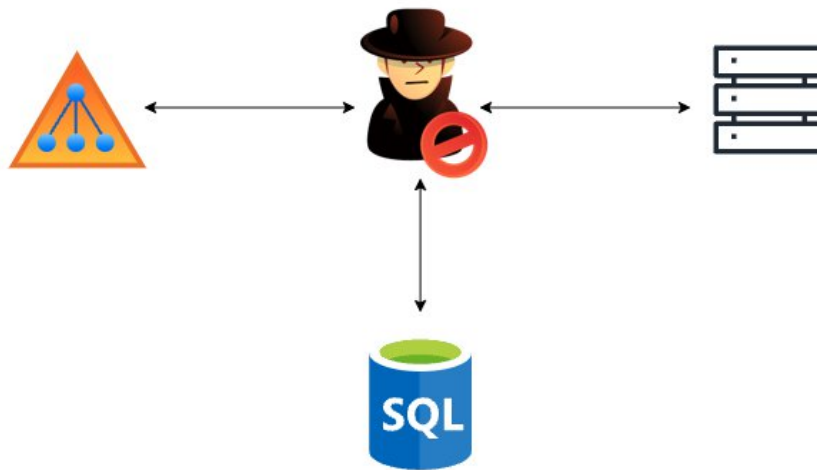
- Maintain Access
- Backdoors
- Account creation





Lateral Movement

- Active Directory
- Databases
- Servers





Hiding Tracks

- Audits
- Filesystem changes
- Obfuscate file locations





Web Application Hacking

- Exploiting vulnerabilities in web apps
- Motives
 - Getting privileged information
 - Financial gain



OWASP Top 10

- OWASP -> Open Worldwide Application Security Project
- Top 10 -> list of most critical security risks to web applications
- Current List:
 - Broken Access Control
 - Cryptographic Failure
 - Injection
 - Insecure Design
 - Security Misconfiguration
 - Vulnerable Libraries
 - Server Side Request Forgery (SSRF)
 - Data Integrity Failures
 - Authentication Failures
 - Monitoring Failures



Broken Access Control

- Users can do stuff outside of their permission set
- Violation of Least Privilege
- Missing access control policies



Broken Access Control

Impact

- accessing and modifying data of other users
- elevation of privilege
- accessing unauthorized pages or resources



Injection

- Untrusted user data sent to application that can lead an attacker to run commands or access unauthorized data
- Common Types:
 - SQL Injection (SQLi)
 - Cross Site Scripting (XSS)
 - Command Injection



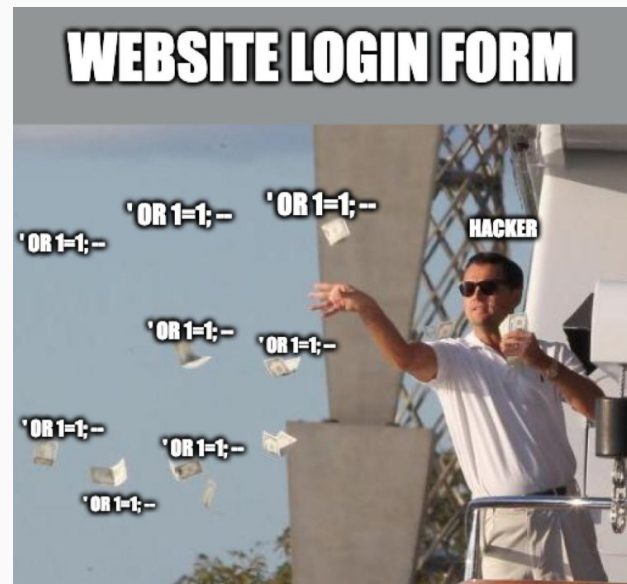
Injection

- **Impact**
 - **leaking privileged information**
 - **remote code execution**



SQLi

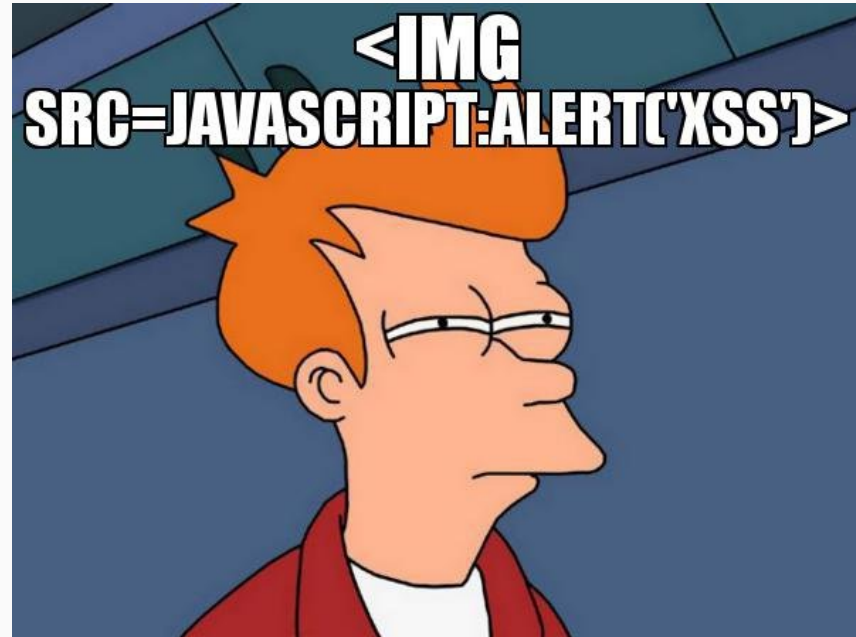
- Payloads for params that directly deal with the database
- Impact
 - Information disclosure
 - Tamper with existing information





XSS

- Malicious scripts injected into websites
- Impact
 - Session Hijacking
 - Data theft / disclosure
 - Phishing





Command Injection

- OS commands executed through payloads
- Impact
 - System compromise
 - RCE
 - Privilege Escalation





Cryptographic Failures

- Failures / lack of cryptographic controls
- Common Failures:
 - Weak cryptographic ciphers
 - Lack of TLS
 - Unsalted password hashes

Impact

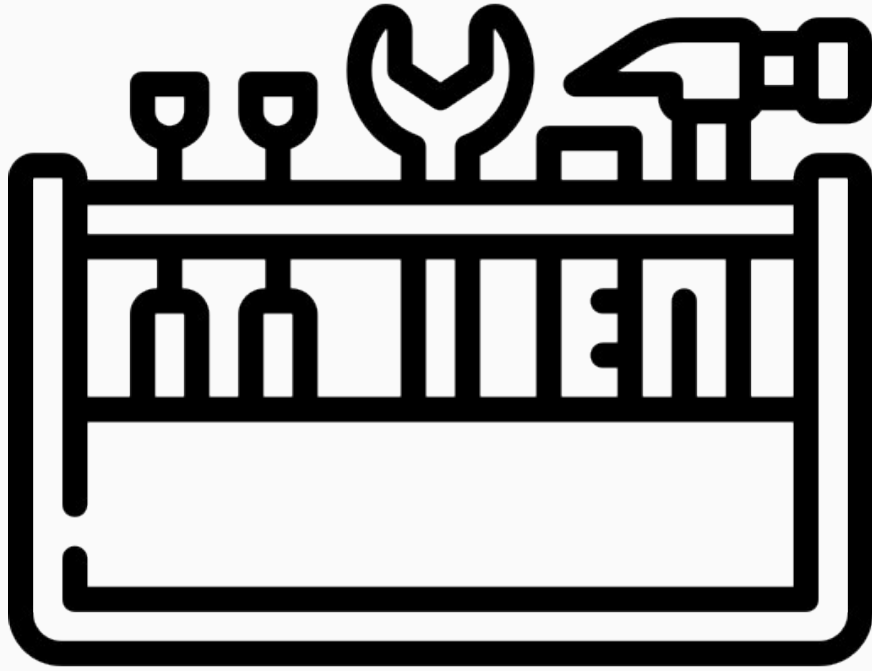
- cracking password hashes through Rainbow Tables
- spying on network traffic





Toolbox

- BurpSuite
- FoxyProxy
- Kali Linux tools





BurpSuite

- Security application for penetration testing of web applications
- Features:
 - Proxy
 - Intruder
 - Repeater
 - Collaborator





BurpSuite

Installation

<https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install>



Kali Linux

- Linux distribution based on Debian for penetration testing and digital forensics
- Tools:
 - nmap
 - Metasploit
 - Burpsuite
 - John the Ripper
 - sqlmap
 - Wireshark





Kali Linux

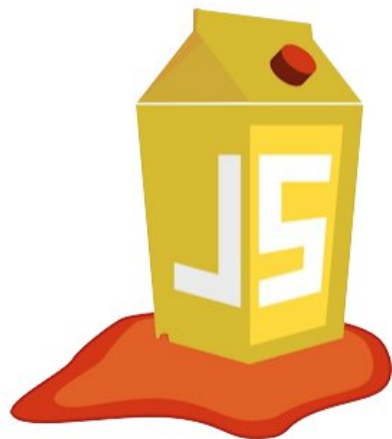
- Install on Virtualbox
- <https://www.kali.org/get-kali/>

Kali Linux



OWASP JuiceShop

- Deliberately insecure web application for security trainings and CTFs





OWASP JuiceShop

- <https://pwning.owasp-juice.shop/companion-guide/latest/part1/running.html>
- Docker

```
docker pull bkimminich/juice-shop
```

```
docker run -d -p 3000:3000 bkimminich/juice-shop
```


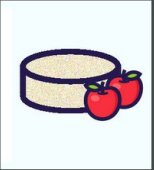





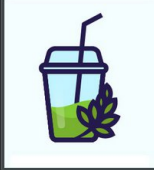


OWASP JuiceShop

OWASP Juice Shop

Account Your Basket 0 EN

All Products

 <p>Apple Juice (1000ml) 4.99 0.99=</p> <p>Add to Basket</p>	 <p>Apple Pomace 0.89=</p> <p>Add to Basket</p>	 <p>Banana Juice (1000ml) 1.99=</p> <p>Add to Basket</p>	 <p>Best Juice Shop Salesman Artwork 5000=</p> <p>Add to Basket</p>
 <p>Carrot Juice (1000ml) 2.99=</p> <p>Add to Basket</p>	 <p>Eggfruit Juice (500ml) 8.99=</p> <p>Add to Basket</p>	 <p>Fruit Press 89.99=</p> <p>Add to Basket</p>	 <p>Green Smoothie 1.99=</p> <p>Add to Basket</p>



Live Hack!

- Environment setup
- Let's go!



Learn Hacking

- JuiceShop
- VulnHub
- TryHackMe
- HackTheBox
- Ethically try a live program!



Takeaways

- General steps in Hacking Web Applications
- OWASP Top 10
- Basic use of Burpsuite
- Intro into Kali Linux
- Hacking a vulnerable web application



References

1. OWASP Top 10 - <https://owasp.org/www-project-top-ten/>
2. OWASP Juice Shop - <https://owasp.org/www-project-juice-shop/>
3. PortSwigger Labs - <https://portswigger.net/web-security/all-labs>
4. John Hash Formats - <https://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats>



Questions?





Feedback



