

# Security Testing Best Practices

---

RUSEC Spring General Meeting #02

# Agenda

- What is security testing and why do organizations utilize it?
- What are the different types of security testing
- Ethical and legal nuances
- How to get started and where to learn
- Bug Bounty Hunting



# Why do organizations test their controls?

Examples of controls: MFA on all logins, security guards at entrances, VPNs, Active network monitoring

## Protection

- Regular testing finds security weaknesses **before** attackers can exploit them
- Just like checking your locks at home

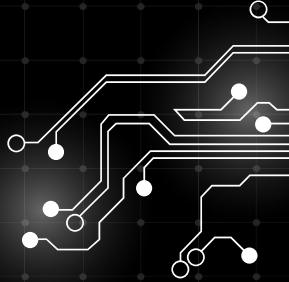
## Compliance

- Many industries require security testing by law
- Shows proof of working security to regulators

## Cost Prevention

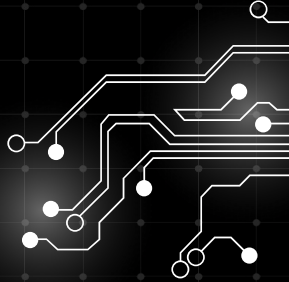
- Finding issues early prevents expensive security incidents
- Avoids system downtime and data loss

## Risk Management

- New cyber threats emerge daily
  - Testing ensures defenses stay current
- 



# Main Types of Security Testing

- Vulnerability Scanning
  - Penetration Testing
  - Application Security Testing
  - Web App Security Testing
  - API Testing
  - Security Auditing
  - Risk Assessments
  - Security Posture Assessments
- 

# Vulnerability Scanning

- Vulnerability scanning is the process of using automatic tools to scan for vulnerabilities (either in software, hardware, networks, or systems)
- Types of vulnerability scanning:
  - Application
    - Dynamically scans (DAST) applications for common security flaws found in the OWASP T10
    - Common Tools: BurpSuite, Rapid7
  - Network
    - Checks infrastructure (firewalls, switches, routers, and servers) for vulnerabilities
    - Common tools used: Nessus, Tenable, nmap
  - Cloud
    - Helps to identify vulnerabilities common to AWS, Azure, etc.
    - Common tools: QualysGuard, Wiz
- Helps to identify threats, but not assess which ones are valid!

# Security Auditing

---

- Is an evaluation of an organization's security posture to identify vulnerabilities, threats and compliance gaps
  - *Compliance audit* ensures regulatory compliance
    - HIPAA, ISO/IEC 27001, NIST CSF,
- **Security posture** is an organization's overall cybersecurity strength and its ability to identify, prevent, respond to and recover from security threats and risks
- Depth vs Breadth
  1. Read the news and constant updates on new CVEs
  2. If a vendor you work with is compromised, you may be exposed as well.
  3. Do an audit at least twice a year, either internally or externally - hiring a VAPT (Vulnerability Assessment & Pen Testing) service company.

# Risk Assessments

	Negligible	Minor	Moderate	Significant	Severe
Very likely	Low - Medium	Medium	Medium - High	High	High
Likely	Low	Low - Medium	Medium	Medium - High	High
Possible	Low	Low - Medium	Medium	Medium - High	Medium - High
Unlikely	Low	Low - Medium	Low - Medium	Medium	Medium - High
Very unlikely	Low	Low	Low - Medium	Medium	Medium

- helps organizations identify, analyze, and prioritize cybersecurity risks to mitigate threats effectively.
  - **Risk** measures how likely a potential threat is to affect an organization and how much damage that threat would do
1. Identify assets, threats and vulnerabilities
  2. Evaluate risk impact to company
  3. Prioritize risk based on potential damage
  4. Develop strategies to mitigate risk

# Web Application Security Testing

- Testing web applications for vulnerabilities in the system to prevent hackers from exploiting those vulnerabilities and stealing sensitive information.
- Testing Techniques
  - **Static Application Security Testing (SAST):** tests applications prior to deployment
    - Common tests: Buffer Overflows, hardcoded secrets
  - **Dynamic Application Security Testing (DAST):** tests applications after deployment
    - Common tests: insecure HTTP, SQL injections, Cross Site Scripting (XSS)
  - **Software Composition Analysis (SCA):** tests vulnerabilities commonly found in libraries and packages
- Why test?
  - It's important to make sure that applications are protected from attackers attempting to gain access to information
  - Practicing due diligence in ensuring that you protected your application to the best of your ability



# Application Security Testing

A comprehensive process of evaluating software application security to identify and mitigate potential vulnerabilities. Typically focused on internally developed and used software such as custom enterprise applications or other software you are responsible for maintaining whether as a client or customer.

## Testing Techniques

- Automated Code Analysis
- Penetration Testing Techniques and Automated Security Scanning
- Utilizing previously mentioned tools for static and dynamic testing as well as Software Composition Analysis Tools (SCA) which automatically scan an application's codebase.

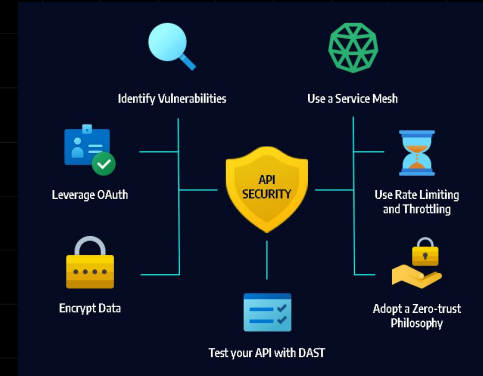
## Why test an application's code base?

- **Memory Management Issues** - Bugs like buffer overflows and use-after-free occur due to improper memory handling.
- **Race Conditions & Concurrency Bugs** - Poor synchronization in multi-threaded applications can lead to privilege escalation or data corruption.
- **Insecure Object Deserialization** - Maliciously crafted objects can execute arbitrary code when deserialized.
- **Hardcoded Secrets & Insecure Cryptography** - Exposed API keys, credentials, or weak cryptographic implementations can lead to direct compromise.

# API Security Testing

Application Programming Interface (API) - Connect apps and services together, typically from a third party.

- API Security testing revolves around two primary components of using an API
  - Evaluate the risk and security of an API, often seeing how it responds to malicious requests
  - Monitoring for exposed API keys
- Attacks can intercept the communication between an API and an app to steal information, create MiTM (man-in-the-middle) and DDoS attacks
- In 2023 84% of security professionals experienced an API related incident.
- The average cost to remediate an API incident was \$591,000.
- API Examples: Logins with existing accounts, Google Maps Platform, Pay with PayPal, Spotify Web API





# Penetration Testing

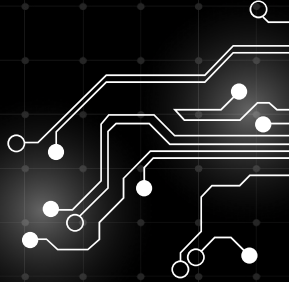
## Penetration Testing (Pen Testing) Overview

- **Definition:** Simulated cyber attack on a system, network, or application to identify vulnerabilities before malicious actors exploit them.
- **Goal:** Improve security by uncovering weaknesses and providing remediation strategies.

## Types of Pen Tests

- **Black Box** – Tester has no prior knowledge of the system; simulates an external attacker.
- **White Box** – Full access to internal system details; tests from an insider perspective.
- **Gray Box** – Partial knowledge of the system; simulates an attacker with some internal access.

## Common Testing Phases

1. **Planning & Reconnaissance** – Define scope, gather intelligence on the target.
  2. **Scanning & Enumeration** – Identify open ports, services, and vulnerabilities.
  3. **Exploitation** – Attempt to gain access using known vulnerabilities.
  4. **Post-Exploitation & Privilege Escalation** – Assess impact by gaining higher privileges.
  5. **Reporting & Remediation** – Document findings and suggest fixes.
- 

# Red Teaming

- Simulation of a cyber attack on a network to determine its security.

- Done with special permission (RoE)
- Requires A LOT of paperwork to show what was done and often
- Can take anywhere from a couple weeks to a year to complete an engagement

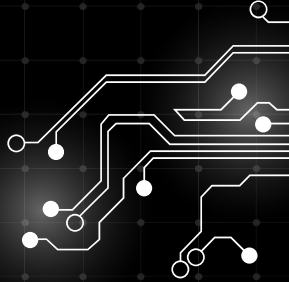


A decorative graphic on the left side of the slide, featuring a stylized circuit board with glowing nodes and lines.

# How do I study Security Testing?

The best way, is to do it. Pentesting and other forms of security testing are skills that have so many variables. It's almost impossible to learn from books due to so many variables and outcomes being possible. So the best way is to get hands on experience and understand what to do in certain scenarios.

Vulnerabilities change and rarely to two networks, two applications, and two organizations look the same.

A decorative graphic on the right side of the slide, featuring a stylized circuit board with glowing nodes and lines.

# BE CAREFUL!!!!

Please don't nmap or ping random IPs. You will get a visit from the FBI



# What do you need

- Virtual Machine (VM)
  - VMWare
  - Virtualbox
- HackTheBox (HTB) account
- TryHackMe (THM) account
- Working computer
- Awareness





**BUG**



**BOUNTY**





# Bug Bounty Hunting

Competitive freelance programs that pay security researchers of all skill levels and backgrounds to identify and report vulnerabilities for a “bounty” (typically money)

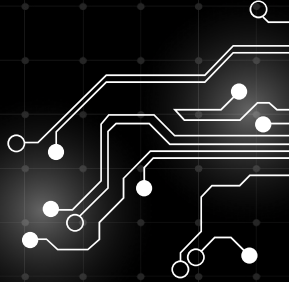
## Why Do Companies Offer Bug Bounties?

- Identify security flaws before attackers exploit them.
- Leverage a diverse group of ethical hackers with different perspectives.
- Cost-effective alternative to traditional security assessments.

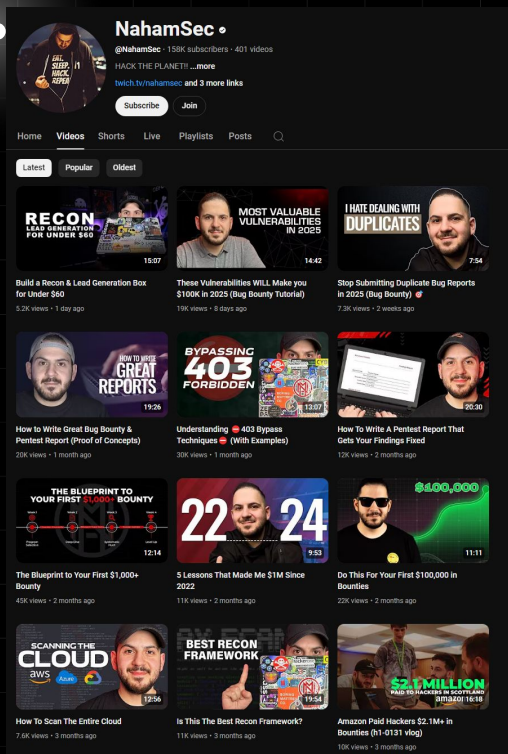
## How Do They Work?

- Researchers test an application within a defined **scope** and **set of rules**.
- Vulnerabilities are reported through a responsible disclosure process.
- Companies verify and reward valid findings based on severity.

## Platforms for pursuing and learning Bug Bounty Hunting

- HackerOne
  - Bugcrowd
  - Synack
- 

# Resources and Pitfalls



How cinzinga got into Bug Bounties as a college sophomore

Google Bug Hunters

HACKER101

## Learn how to hack.

Explore dozens of free capture the flag challenges to build and test your skills while accessing hundreds of hours of video lessons. Meet other learners and get mentored by experienced hackers in the Hacker101 Community Discord channel.

Get Started

# If Bug Bounty Programs Won't Buy Someone Will

ZERODIUM Payouts for Mobiles\*

FCP: Full Chain with Persistence  
RCE: Remote Code Execution  
LPE: Local Privilege Escalation  
SBX: Sandbox Escape or Bypass

■ iOS  
■ Android  
■ Any OS

Up to \$2,500,000											1.001 Android FCP Zero Click Android
Up to \$2,000,000											1.002 iOS FCP Zero Click iOS
Up to \$1,500,000											2.001 WhatsApp RCE+LPE Zero Click iOS/Android
Up to \$1,000,000											2.002 iMessage RCE+LPE Zero Click iOS
Up to \$500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android		
Up to \$200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS		
Up to \$100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	9.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS		