SESSION 2: WEB EXPLOITATION

By: J0eHarr7

whoami

id

>> uid=1000(j0eharr7) gid=1002(j0eharr7) groups=1002(j0eharr7)

whoami

>> 5th Fifth Year Student ENSA Marrakech, Cybersecurity Consultant

and DevSecOps Engineer

python chihaja.py

>> Part Time CTF Player 5T4F1T, Fulltime Debugger at 5AM with Cup of Coffee & OumKhaltoum

DISCLAIMER !!!!!!!!!!!

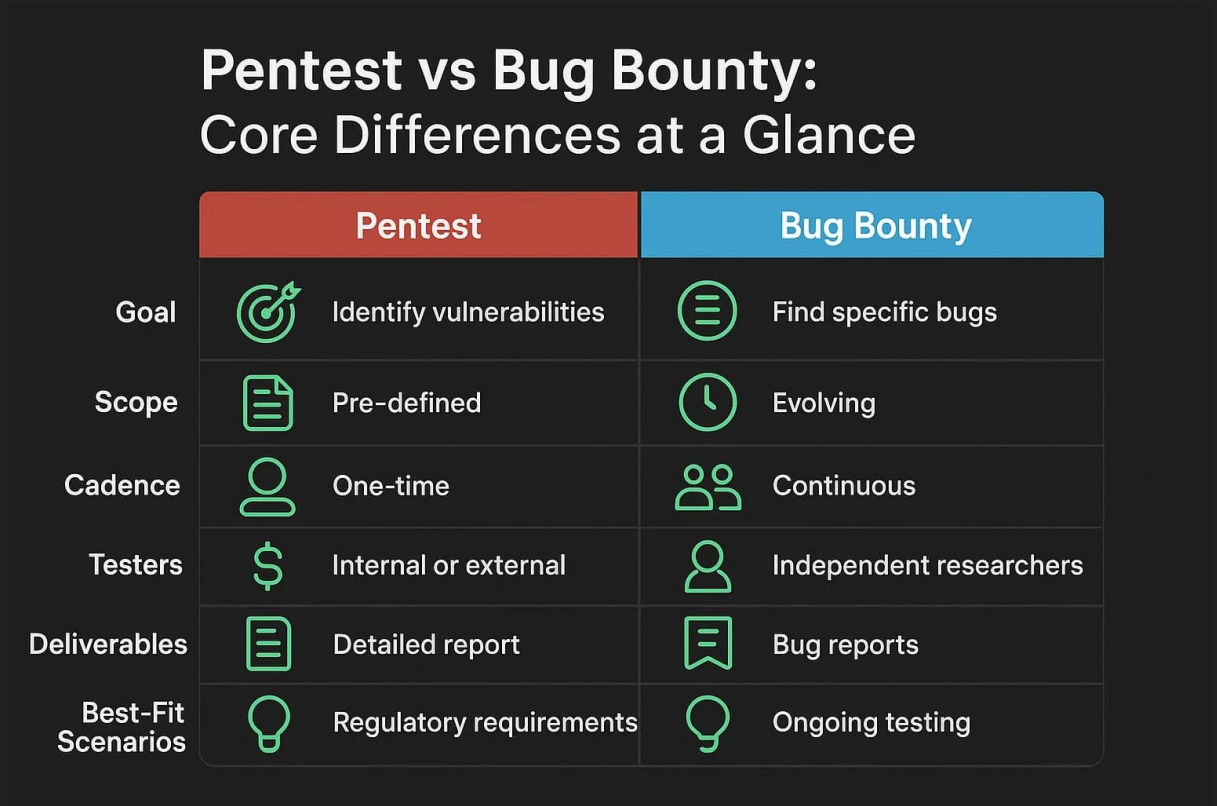
THE CONTENT IN THIS SESSION IS FOR EDUCATIONAL PURPOSES ONLY AND I’M NOT RESPONSIBLE FOR ANY ILLEGAL ACTIONS.

BrainRot

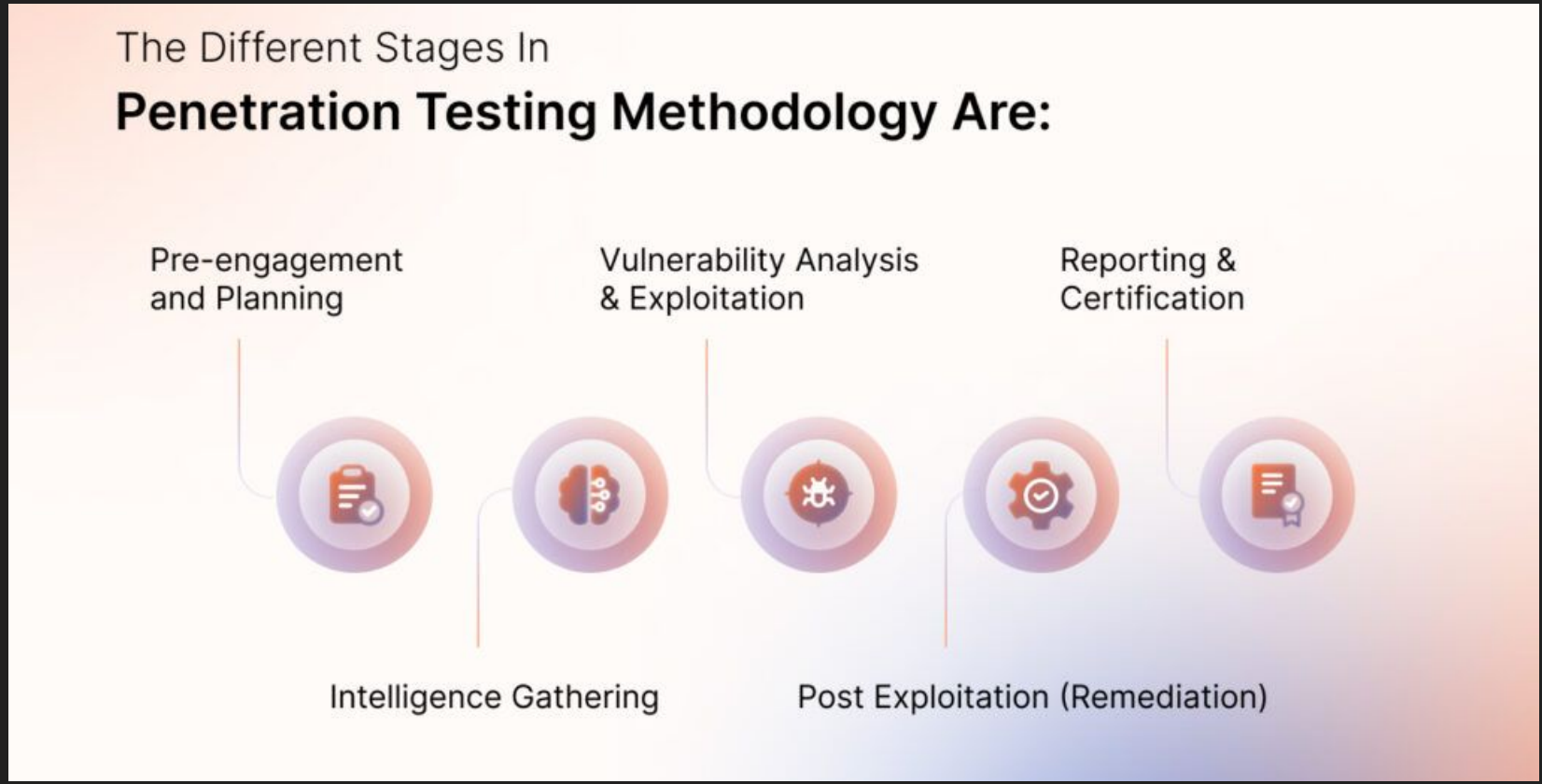
- How to approach a web application like a true Hacker ?!
- Pentester vs Bug Bounty Methodology

Let THE FUN BEGIN

Pentest VS Bug Bounty



Penetration Testing Methodology



Bug Bounty Program

1. Reconnaissance and Subdomain Enumeration

1.1 Subdomain Enumeration

- subfinder -d target.com -silent -all -recursive -o subfinder_subs.txt
- amass enum -passive -d target.com -o amass_passive_subs.txt
- ffuf -u https://FUZZ.target.com -w wordlist.txt -t 50 -mc 200,403 -o ffuf_subs.txt

1.2 Google Dorks

- filetype:xls inurl: email.xls carte bancaire
- site:*.target.com inurl:"*admin | login" | inurl:.php | .asp

1.3 Content Discovery

- feroxbuster -u https://target.com -w /usr/share/wordlists/common.txt -r -t 20 -o recursive_results.txt
- dirsearch -u https://target.com -w /usr/share/wordlists/content_discovery.txt -e php,html,js,json -x 404 -o dirsearch_results.txt
- ffuf -u https://target.com/FUZZ -w /usr/share/wordlists/content_discovery.txt -mc 200,403 -recursion -recursion-depth 3 -o ffuf_results.txt

2. Vulnerability Assessment

2.1 Automation Tools:

- nikto
- owasp zap
- open vas
- nmap -sC
- skipfish
- nessus
- wpscan

2.2 CVE Databases

- Exploit-DB
- NVD (National Vulnerability Database)
- Vendor Advidories
- Github Advisory Database

NDKHLO CHWIYA FL M39OL DB

OWASP TOP 10:2025

- A01:2025 Broken Access Control
  - Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification or destruction of all data, or performing a business function outside the user's limits.
  - (kadir chi action critique nta ma3ndkch l79 fiha)
- A02:2025 Security Misconfiguration
  - Security misconfiguration is when a system, application, or cloud service is set up incorrectly from a security perspective, creating vulnerabilities.
  - (dev team is low on security mesures)
- A03:2025 Software Supply Chain Failures
  - Software supply chain failures are breakdowns or other compromises in the process of building, distributing, or updating software. They are often caused by vulnerabilities or malicious changes in third-party code, tools, or other dependencies that the system relies on.
- A04:2025 Cryptographic Failures
- A05:2025 Injection
  - An injection vulnerability is an application flaw that allows untrusted user input to be sent to an interpreter (e.g. a browser, database, the command line) and causes the interpreter to execute parts of that input as commands.
- A06:2025 Insecure Design
  - This category focuses on risks related to design and architectural flaws, with a call for more use of threat modeling, secure design patterns, and reference architectures.
- A07:2025 Authentication Failures
  - When an attacker is able to trick a system into recognizing an invalid or incorrect user as legitimate, this vulnerability is present.
- A08:2025 Software or Data Integrity Failures
- A09:2025 Security Logging & Alerting Failures
- A10:2025 Mishandling of Exceptional Conditions

Arsenal

- https://github.com/amrelsagaei/Bug-Bounty-Hunting-Methodology-2025?tab=readme-ov-file#3-advanced-enumeration-techniques
- https://owasp.org/Top10/2025/