hackerone

Web Hacking Methodology

Welcome to the world of ethical hacking! In this document, we'll explore the fundamental steps of web hacking methodology, which will serve as your roadmap to finding vulnerabilities in web applications. Remember, the goal here is to enhance security, not exploit it.

1. Information Gathering

Understanding your target is crucial. Gather information about the web application, including:

- Domain and Subdomains: Identify all associated domains and subdomains.
- Technologies Used: Determine the web server, programming languages, and frameworks in use.
- Publicly Available Information: Search for information on social media, forums, and search engines.

2. Reconnaissance

Dig deeper into your target:

- Whois Lookup: Discover domain ownership information.
- DNS Enumeration: Find additional subdomains and their IP addresses.
- Port Scanning: Identify open ports for potential entry points.

3. Scanning

Now it's time to scan for vulnerabilities:

- Vulnerability Scanners: Use tools like Nessus, OpenVAS, or Nikto to identify common vulnerabilities.
- Web Application Scanners: Tools like Burp Suite, OWASP ZAP, or Acunetix can help find web-specific flaws.
- Manual Testing: Perform manual tests for more advanced vulnerabilities.

4. Enumeration

Enumerate and gather detailed information about the application's structure:

- Directory and File Enumeration: Identify hidden directories and files.
- User Enumeration: Check for user accounts and roles.
- API Endpoints: Discover and test API endpoints.

5. Vulnerability Analysis

Examine the data collected for vulnerabilities:

- OWASP Top Ten: Check for common web vulnerabilities like SQL injection, XSS, and CSRF.
- Authentication and Authorization Flaws: Test for weaknesses in authentication and authorization mechanisms.
- Input Validation Issues: Probe for issues related to input validation such as XSS

6. Exploitation

This is where you prove the existence of vulnerabilities:

- Exploit Development: If necessary, develop or use exploits for discovered vulnerabilities.
- Post-Exploitation: Gain deeper access to the system and extract valuable data.

7. Post-Exploitation

Maintain access, pivot, and gather more data:

- Privilege Escalation: Look for ways to escalate your privileges.
- Data Extraction: Gather sensitive data without leaving traces.
- Cover Your Tracks: Remove evidence of your presence.

8. Reporting

Ethical hacking is only valuable if you share your findings:

- Report Writing: Create a detailed report outlining vulnerabilities and their potential business impact.
- Recommendations: Suggest mitigation steps for each issue.
- Clear Communication: Ensure your findings are well-documented and understandable. Include video and images whenever possible in your POC.

9. Retesting

Work with the organization to fix the vulnerabilities:

- Collaboration: Engage with developers and system administrators.
- Testing Fixes: Verify that vulnerabilities are adequately patched.
- Education: Offer training to prevent future issues.

10. Continuous Learning

Security is an ever-evolving field:

- Stay Updated: Follow security blogs, attend conferences, and join forums.
- Practice: Continue honing your skills through ethical hacking labs and challenges.

Remember, ethical hacking requires consent and adherence to legal and ethical guidelines. Always obtain proper authorization before testing any web application. Happy hacking, and may you contribute to a safer online world!