Week 1: Learning Tasks

Pre-Technical Learning:

Read Articles:

- Overview of XSS:https://owasp.org/www-community/attacks/xss/
- Basics of web application security: https://martinfowler.com/articles/web-security-basics.html

Watch Videos:

- Cross-Site Scripting (XSS) Explained: https://www.youtube.com/watch?v=EoaDgUgS6QA
- Burp Suite Tutorial for Beginners: https://www.youtube.com/watch?v=G3hpAeoZ4ek

Participate in Discussions:

- Join and read discussions in cybersecurity forums such as: Reddit's r/netsec

This should provide a solid foundation and enhance understanding before tackling the technical tasks.

Week 1 Tasks: XSS Focus on testphp.vulnweb.com

1. Initial Reconnaissance:

- Scan the application ports using a tool like Nmap to identify open ports.
- Determine the versions of web server, database, and other technologies used by the site.
- Identify the web technologies/frameworks (e.g., PHP, Apache) using tools like Wappalyzer or BuiltWith.
- Make sure to store all the findings because we are gonna use this target throughout the internship!

2. Testing for XSS:

- Use OWASP ZAP or Burp Suite to test various input fields for XSS vulnerabilities.
- Attempt to insert harmless test scripts (e.g., `<script>alert('test');</script>`) in search bars, comment sections, and other input fields.
- Note where the script executes and whether it is reflected back to the user, stored, or affects the DOM.

3. Exploiting the XSS Vulnerability:

- Once an XSS vulnerability is identified, perform a controlled exploit. Inject scripts to see how they affect the application.
- Document the process and the impact of the exploit (e.g., stealing cookies, defacing the page).

4. Understanding the Security Issue:

- Analyze why the XSS vulnerability is occurring. Look at the source code (if accessible) or infer from the application behavior.

- Determine if the issue is due to lack of input validation, improper output encoding, or other security misconfigurations.

5. Recommended Actions:

- Research and document recommended actions to mitigate the identified XSS vulnerability.
- Suggested actions could include proper input validation, output encoding, using Content Security Policy (CSP), and setting secure attributes for cookies.

6. Documentation and Submission:

- Document your learning process and progress.
- Compile all findings with screenshots, including steps taken, test results, exploit details, root cause analysis, and recommended actions into a detailed report.

Reporting Instructions:

1. **Format:**
   - Compile your documentation in PDF format.
   - Rename your file using the format: (referenceID_name).
2. **Submission:**
   - Submit your reports to web-tasks@offensiox.com.
   - Email subject: “Week 1 Task (*ReferenceID*)”
3. **Platform:**
   - Once your reports have been submitted, you will receive **Secret Key** for Week 1 on your email. Submit it at OffensioX Internship Platform.

4. **Deadline:**
    - Last day to submit the report is at midnight, 01st of August, 2024.
5. **Help:**
    - Incase of any inquire related to task write at internships@offensiox.com or create ticket at Discord