Project

Hands-on Exploration of Web Application Vulnerabilities through Seed Labs

Information Security

Fall 2024

Submission Guidelines:

PLEASE READ THE FOLLOWING GUIDELINES VERY CAREFULLY.

- This is a Group based activity. Minimum group members should be **two** and maximum group members allowed are **three**.
- Your lab report should be well documented with every step of the lab clearly explained along with the relevant screenshots.
- You are to clearly label all screenshots/figures properly with short description to what the screenshot is representing. Marks will be deducted in case the screenshots are blur, not placed properly or not labelled properly
- Submitting a report with only screenshots and no description will receive zero credit
- You can use CHATGPT or any other AI tools for ideas or research but refrain from using the exact content. Include screenshots of the prompts you give to CHATGPT while doing research as part of the Appendix
- The **font size for the headings** of your report is **16** with the default font type. The **font size** to be used is **12 for the report body** and the font type to be used is **Times New Roman** with **1.5 line spacing**
- Submit your report in a digital format on GCR link. Assignments handed over email or on WhatsApp will not be accepted
- Submit your report on Google Classroom as a PDF document using the following naming format: **IS_Project_<section>_<RollNo>>_<RollNo>>_<RollNo>**
  E.g.**, IS_Project_B_20i1234_20i1235_20i1236**
- Make sure to include the Turnitin report of your submitted project. You can reach out to the library representative to submit your report along with your code to obtain the Turnitin report. Make sure you complete the assignment at least 2 days before the deadline so that you may get the Turnitin reports timely
- **Cases of plagiarism and copying will be taken very seriously and could lead to severe consequences as per the university policy**
- NO PROJECT will be accepted after the deadline.

Objective:
The objective of this project is to equip students with practical experience in identifying, exploiting, and mitigating common web application vulnerabilities using the Seed Labs platform. Through this project, students will gain a deeper understanding of SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).

Project Details:

1. **Lab 1:** SQL Injection Attack
   Students will explore how SQL injection attacks can exploit web applications and learn techniques to secure applications against such attacks.
2. **Lab 2:** Cross-Site Scripting Attack Lab
   This lab focuses on identifying and exploiting XSS vulnerabilities and understanding their impact on web application security.
3. **Lab 3:** Cross-Site Request Forgery Attack Lab
   Students will understand how CSRF attacks occur and learn defense mechanisms to prevent them.

Group Size:

- **For groups with two members**:
  - All group members must complete **Lab 1 (SQL Injection)**.
  - Additionally, the group must choose and complete **one of Lab 2 (XSS)** or **Lab 3 (CSRF)**.
- **For groups with three members**:
  - The group is required to complete all three labs: **SQL Injection**, **XSS**, and **CSRF**.

Deliverables:

A detailed report for each completed lab, including the following:

1. Lab setup and execution process.
2. Observations and findings.
3. Explanation of exploited vulnerabilities.
4. Mitigation techniques and recommendations.
5. Screenshots as per the guidelines given in instructions above.

Evaluation Criteria:

- Completeness and accuracy of lab execution.
- Depth of analysis and quality of the lab reports.
- Adherence to project requirements based on group size.
- Clarity of the demonstration.

Deadline:

- The completed project, including all deliverables, is due on **as per the deadline available on GCR**.