CSE 543: Computer Security

Fall 2022
Project 2: Web Security
Due: 11:59 pm (eastern time), December 8 , 2022

November 15, 2022

1 Instructions

- We have built a web application for students to perform constrained attacks on it. You can access this application using your browser - `https://cse543-web-security.aplayerscreed.com/react/`
- Every student will be given a unique username and password by the TA (through canvas message). If you have not received this by the project release date, please reach out to the TA asap.
- You will have to attempt and perform all the tasks in the project ONLY using your credentials given by the TA. This is very crucial to successfully verify if you have completed all tasks.
- There are four sections of tasks –
  - SQL Injection
  - Sensitive Data Exposure
  - XSS Cross Site Scripting tasks
  - CSRF Request forgery tasks
- Here is the list of files that need to be submitted in .zip or .tar.gz format –
  - Report containing clear explanation and screenshots of successful attempts on each task.
  - An index.html file for Task 4.1
  - An index.html file for Task 4.2
- All the tasks are self-explanatory and have enough details that help you complete them on the website itself.
- You need to do some level of online reading about different kinds of attacks that are expected in this project. The class lectures should also give a very good introduction to these concepts. Some tasks also have external links to good documentation that help understand the web vulnerabilities.
- If you find any issue with the website or if you believe some service is down, please contact the TA through mail or Canvas as soon as possible.
- NOTE: Do not collaborate with anyone for solving the tasks. Work individually and reach out to course staff for help if you're really stuck with something.

- NOTE: All the attacks that you perform in this Lab are only for educational purposes. You are not encouraged to try similar attacks on any other website. It might be a punishable offense if you're caught.

2 Report Instructions

- The report HAS to be in (.doc, .docx) formats only. Avoid PDF format.
- Every task would have a certain input required from the students that basically achieves the task intent. Clearly specify that text you use in your report. The TA should be able to copy it from your report to easily reproduce the same for grading.
- Every successful attempt for the task should be recorded using screenshots in your report.
- By default, for every task, you have to give a short write-up on how you actually completed it.
- There are some tasks which also ask you to answer some questions. Accordingly write the answers in your report task-wise.

3 Grading

- Correct format and clean report submission – 30 points
- SQL Injection – 170 points
  - Task 1.1 = 20 pts
  - Task 1.2 = 30 pts
  - Task 1.3 = 50 pts
  - Task 1.4 = 70 pts
- Sensitive Data Exposure – 20 points
  - Task 2.1 = 20 pts
- XSS Cross Site Scripting Tasks – 90 points
  - Task 3.1 = 30 pts
  - Task 3.2 = 60 pts
- CSRF Request Forgery Tasks – 90 points
  - Task 4.1 = 30 pts
  - Task 4.2 = 60 pts
- So, in total the project is worth 400 Points. Happy Hacking!!!