SENG8060 21W – Project Part 03

Due August 14, 2021, 11:00 pm

SENG8060

Introduction

This is the third part of three-part project **to be completed in pairs**. You will remain in the groups assigned for Assignment 1. In this project assignment, you are asked to complete a series of challenges around a vulnerable web application. The vulnerable web application is called OWASP Juice Shop. Each part of the project will ask you to solve different sets of challenges.

This project will introduce many new concepts to you. You are not expected to know how to immediately solve each challenge on your own. Below is a table of the concepts you will learn. This table is gathered from here: https://pwning.owasp-juice.shop/part1/categories.html

Category	OWASP	CWE	WASC
Broken Access Control	A5:2017, API1:2019, API5:2019	CWE-22, CWE-285, CWE-639	WASC-02, WASC-09, WASC-16
Broken Anti-Automation	OWASP-AT-004, API4:2019, OWASP-AT-010, OAT-009, OAT-015, OAT-008	CWE-362	WASC-11, WASC-21
Broken Authentication	A2:2017, API2:2019	CWE-287, CWE-352	WASC-01, WASC-49
Cross Site Scripting (XSS)	A7:2017	CWE-79	WASC-8
Cryptographic Issues	A3:2017	CWE-326, CWE-327, CWE-328, CWE-950	-
Improper Input Validation	ASVS V5, API6:2019	CWE-20	WASC-20
Injection	A1:2017, API8:2019	CWE-74, CWE-89	WASC-19, WASC-28, WASC-31
Insecure Deserialization	A8:2017	CWE-502	-
Security Misconfiguration	A6:2017, A10:2017, API7:2019, API9:2019, API10:2019	CWE-209	WASC-14, WASC-15
Security through Obscurity	-	CWE-656	-
Sensitive Data Exposure	A3:2017, API3:2019, OTG-CONFIG-004	CWE-200, CWE-530, CWE-548	WASC-13
Unvalidated Redirects	A10:2013	CWE-601	WASC-38
Vulnerable Components	A9:2017	CWE-829, CWE-506, CWE-1104	-
XML External Entities (XXE)	A4:2017	CWE-611	WASC-43

Project Summary

You will **research** each subject, understand and solve challenges. You may use the *hint* or *show answer* feature, but you will need to explain what you did for marks. Furthermore, the grading is based on your explanation of the problem, your solution and a walkthrough for proof for each challenge. Google is your friend, if you don't understand something, research it.

For this project you will need a working virtual machine of **Kali Linux** with the **OWASP Juice Shop version 12.6.1** installed and running on it. The instructions for how to setup a Kali Linux virtual machine, how to install the OWASP Juice Shop, and how to run the OWASP Juice shop have been discussed in class and the labs, and there are videos provided on eConestoga to walk you through the process. If you have issues with getting Kali Linux or OWASP Juice Shop to work, please contact your professor as soon as possible.

This project has been divided into 3 parts to allow you to gain feedback and experience as you progress. Each project part will increase in complexity and difficulty. **Part 03 is worth 40% of your total project mark**.

Be sure you have completed the Initial Reading section in Project Part 01.

Project Part 03 Requirements

For Part 03, you are required to complete the above reading, as well as 4 tasks. The complete list of challenges, along with their hints and solutions can be found here:

Link to Challenge List

Task 1

Complete the following challenges:

1. Post some feedback in another users name

Hint: For this challenge, you may find the Inspector tool in Firefox useful. It can be found in the menu (The "hamburger button", three horizontal lines button), under Web Developer > Web Developer Tools, and then the Inspector tab in the bottom left corner. You are able to change the html page you are viewing by right clicking the html code and selecting "Edit as HTML".

Task 2

Complete the following challenges:

2. Access a confidential document

3. Gain access to any access log file of the server

Hint: For this challenge, you may find a tool like ZAP useful. It has a feature called Forced Browse which we discussed in class that can be of assistance. More information on Forced Browse can be found at this link.

Task 3

Complete the following challenge:

1. Dumpster dive the Internet for a leaked password and log in to the original user account it belongs to

Hint: The challenge **Access the administration section of the store** from Project Part 01 may assist in this challenge.

Task 4

Complete the following challenge:

1. Unlock Premium Challenge to access exclusive content

Project Part 03 Submission Requirements

For Part 03, you should submit a .doc or .docx file on eConestoga which contains a link to a video recorded by the team. In this video, you will be graded on:

a) Your demonstration of the challenges being completed.

b) An explanation of what vulnerability is being exploited by the challenge.

c) An explanation of how the vulnerability could be fixed or addressed.

d) A brief discussion of how the issue presented in the challenge might occur in a real-world scenario.

The video should be done in your own words. Each group member should present some information. There is no minimum time length requirement, just as long as it takes you to adequately explain each challenge. You may use Zoom to record your video (be sure you make any Zoom recordings public), or you may record a video using any application (OBS [Link to OBS], etc.) and upload the video to any streaming service (YouTube, Google Drive, etc.). Please contact me if you are having any issues recording or uploading your video.

A full rubric is available on eConestoga in the Rubric section.