CSC 4620 – Web Site Security Review using OWASP Tools
Spring 2020

Introduction

As described by its authors at https://www.owasp.org/index.php/OWASP_Juice_Shop_Project, "OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!" This flawed web application will be the focus of your security review.

In this exercise, you will use the OWASP Zed Attack Proxy (ZAP) tool to evaluate the Juice Shop's website and develop a report of your security issue findings. Below are some resources which can provide more information about the website and the tool.

Video

- OWASP ZAP Tutorial Videos
  This video group contains videos about different tools and uses of the OWASP ZAP tool portfolio.

Web

- OWASP ZAP project - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- OWASP Juice Shop – https://github.com/bkimminich/juice-shop

Implementation

You will first download the OVA file from https://www.dropbox.com/s/j9xma4s5waznlf4/OWASP-v2.ova?dl=0. This Ubuntu desktop was created within VirtualBox 6.0.16 with guest extensions. The user name is *owasp-user,* and the password is *owasp-pass*.

We will be running the Juice Shop web application as a docker app. To start the application, open the Terminal app. At the prompt, type "sudo docker run –rm -p 3000:3000 bkimminich/juice-shop". In a **separate** Terminal window, start the OWASP-ZAP tool by typing "sudo ./ZAP_2.9.0/zap.sh". This will start a Java-based GUI. Ignore the warnings about the certificates being out of date.

To run the security scan, select the Automated Scan option on the right side of the screen. Next, type http://localhost:3000 in the URL textbox and then click the Attack button. The scan will take a few minutes to complete.

Deliverables

Based upon the output from the ZAP tool, provide a summary of issues discovered and suggest mitigations for these issues. Remember, this site was created to intentionally contain security flaws. While you are only required to use the ZAP tool for this assignment, suggest some other tools that could provide additional site analysis.

Submit a Word document with all of your findings.