CPTC Homework #6

Resources

1. **Use the Kali on elsa.sdc.cpp to interact with the "SuperSecretWebApp" box for this assignment.**
2. **You can attempt to stylize your report and finding blocks based off of prior CPTC ones**
    a. **https://github.com/globalcptc/report_examples/tree/master/2020**

Questions

1. Explain what a web framework is. (5 points)
2. Give a possible use-case for the tool Burp Suite. (5 points)

Labs

1. OWASP TOP 10 TryHackMe Room: https://tryhackme.com/room/owasptop10 (30 points)
2. Perform an assessment on the web application running on 192.168.1.2:5000. Note as many technical findings as you can, but at least 3. The goal is not necessarily to obtain a shell, but to note the ***web*** vulnerabilities that you find.
    a. There is a SSTI (Server side template injection) vulnerability located somewhere within this webapp. Find it, exploit it, and describe how your exploit works. Use a finding block to format your response.
    b. There is a SQL Injection vulnerability located somewhere within this webapp. Find it, exploit it, and describe how your exploit works. Use a finding block to format your response.
    c. There is an IDOR (Insecure direct object reference) vulnerability located somewhere within this webapp. Find it, exploit it, and describe how your exploit works. Use a finding block to format your response.
    d. There is a XSS (Cross site scripting) vulnerability located somewhere within this webapp. Find it, exploit it, and describe how your exploit works. Use a finding block to format your response.
    e. There is a LFI (Local file inclusion) vulnerability located somewhere within this webapp. Find it, exploit it, and describe how your exploit works. Use a finding block to format your response.

f. There is a RFI (Remote file inclusion) vulnerability located somewhere within this webapp. Find it, exploit it, and describe how your exploit works. Use a finding block to format your response.
g. There is a SSRF (Server side request forgery) vulnerability located somewhere within this webapp. Find it, exploit it, and describe how your exploit works. Use a finding block to format your response.

*There may be multiple instances of the same type of vulnerability. As a pentester, it is good practice to try to find as much as you can and report about it.

**This is not an exhaustive list; there may be more vulnerabilities. It is good practice to note these findings and mention them in the report.

Deliverables

1. **Submit a PDF with all of the following:**
    a. **answers to all the questions**
    b. **a screenshot showing completion of the TryHackMe room**
    c. **in the same document, a stylized report (see above for examples) containing a title page, table of contents, and technical findings section that contains:**
        i. **a finding block for each web technical finding you identify**
        ii. **each finding block, at minimum, must contain:**
            1. **Impact**
            2. **Likelihood**
            3. **Reproduction steps**
            4. **Remediation recommendations**
2. **Make sure all sections and images are readable and labeled.**
3. **Name the file with the following format: FirstLast_CPTCHomework6.pdf**

If you are trying out for the team, make sure you submit your PDF in Canvas.

Otherwise, please use this form if you want to be graded: https://forms.gle/gfQtfmxnve6z6ojD9.