SIL765: Networks and System Security

Semester II, 2023-2024

Assignment-4

April 1, 2024

Problem: Website Security Analysis

A website is a crucial component of any digital e-commerce business. It can also be simply used as a digital representation of an organization, and a platform where visitors can obtain information about the organization. However, with increasing technology usage, websites have become vulnerable to various cyber threats. In this assignment, you will learn to use penetration testing tools to find vulnerabilities in websites of your choice.
Note - Please do not perform penetration testing on any security-sensitive website as the source of the test can be traced back to you.

Testing Tools

You can choose any tool that is available online. A few examples of the tool are given below.

- **Metasploit** - `https://www.metasploit.com`
- **Nmap** - `https://nmap.org/`
- **Burp Suite** - `https://portswigger.net/burp`
- **OpenVAS** - `https://www.openvas.org/`

Exploring tools other than these is highly encouraged.

Security Evaluation and Report Submission

In this assignment, you need to analyze any two popular websites for security vulnerabilities using any two testing tools. For each of the two selected websites, try finding vulnerabilities by using each of the two tools and submit a detailed report containing the following.

1. Explain at least four vulnerabilities you tried to find using the tool. Explain the functionality of the tool, i.e., how the tool tested the vulnerabilities. ($2 \times 2 \times 5 = 20$ Marks)
2. For at least two critical vulnerabilities tested by the tool, but not found on the website, explain the security measures deployed on the website which mitigate those vulnerabilities. ($2 \times 2 \times 5 = 20$ Marks)
3. For at least two critical vulnerabilities found by the tool on the website, explain how those vulnerabilities can be used to launch attacks and validate that the vulnerabilities can be practically exploited. ($2 \times 2 \times 10 = 40$ Marks)
4. For the discovered vulnerabilities, suggest mitigation techniques that could be deployed by the website ($2 \times 2 \times 5 = 20$ Marks).