Project 3: Nmap Enumeration and Vulnerability Analysis Report:

Name: Prabhat Solanki

Date: 29th November 2024

Target: http://zero.webappsecurity.com

1. Objective

The objective of this report is to document the results of enumeration and vulnerability scanning performed on the target URL using Nmap. The tasks include identifying open ports, enumerating HTTP services, and detecting potential vulnerabilities.

2. Tools Used

Tool: Nmap (Version 7.94SVN)
Platform: Parrot OS

3. Enumeration Findings

3.1 Open Ports

1. Port 80 (HTTP): Open
2. Port 443 (HTTPS): Open

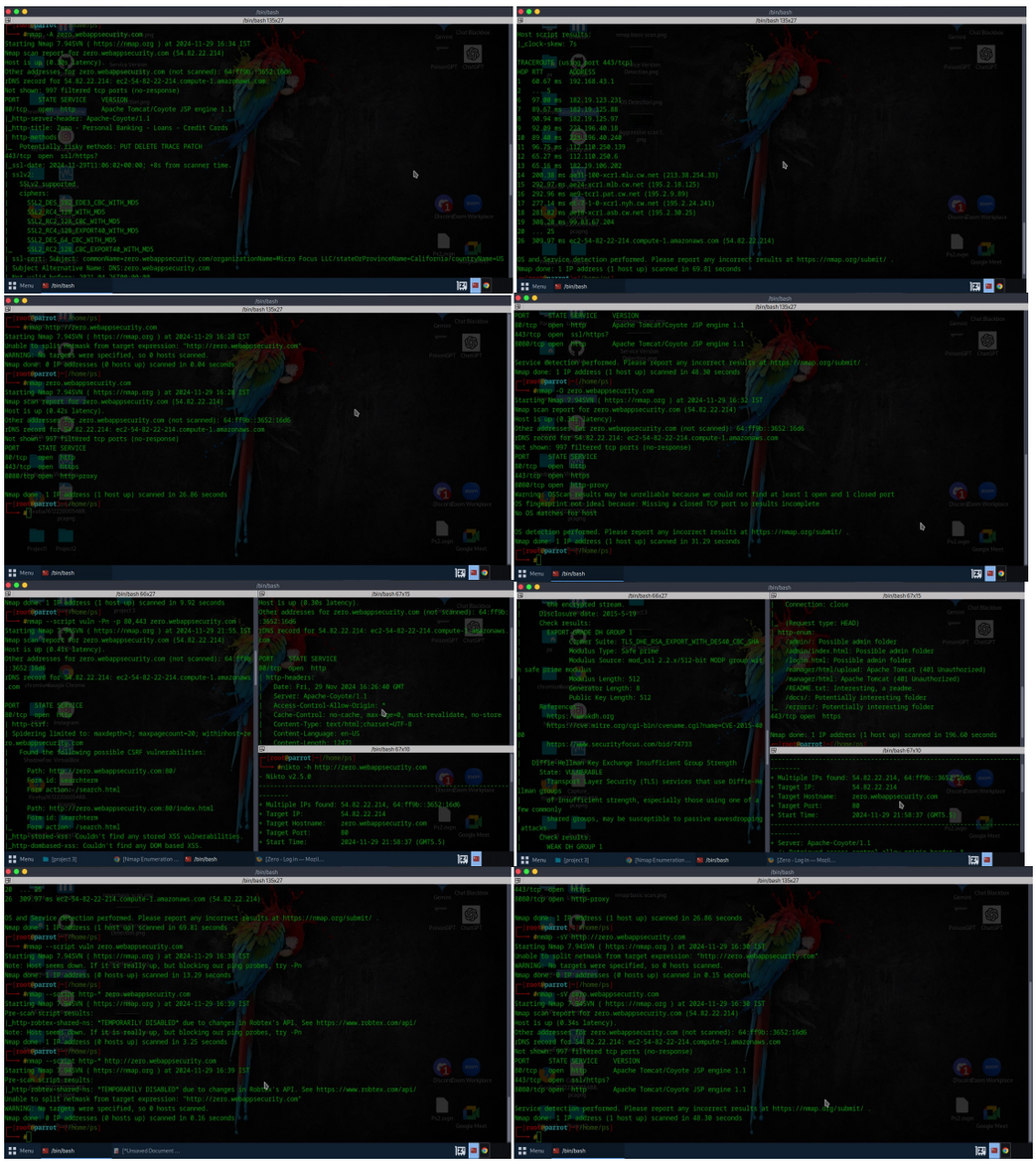
3.2 HTTP Enumeration

1. HTTP Title: Zero - Personal Banking - Loans - Credit Cards
2. HTTP Methods Supported: GET, HEAD, POST, OPTIONS
3. Interesting Directories Identified:
   - /admin/
   - /admin/index.html
   - /login.html
   - /manager/html (401 Unauthorized)
   - /README.txt
   - /docs/
   - /errors/

4. Vulnerability Findings

1. CSRF Vulnerabilities:
   - Found in search forms at / and /index.html
2. TLS Vulnerabilities:
   - Logjam: Weak Diffie-Hellman Key Exchange (CVE-2015-4000)
   - POODLE (CVE-2014-3566)
   - SSL/TLS CCS Injection (CVE-2014-0224)

5. Screenshots



6. Conclusion

The Nmap enumeration and vulnerability analysis of zero.webappsecurity.com revealed several interesting findings, including open HTTP and HTTPS ports, administrative directories, and vulnerabilities related to TLS configurations. Recommendations include upgrading to secure TLS configurations, restricting unauthorized directory access, and implementing proper CSRF protections.