Week 3: Advanced Security and Final Reporting

Name: Muhammad Bin Qasim

Network Scanning with Nmap:

By using Nmap, I discovered devices and services running on a network.

Version Check: I confirmed Nmap version **7.98** is installed on a Windows platform.

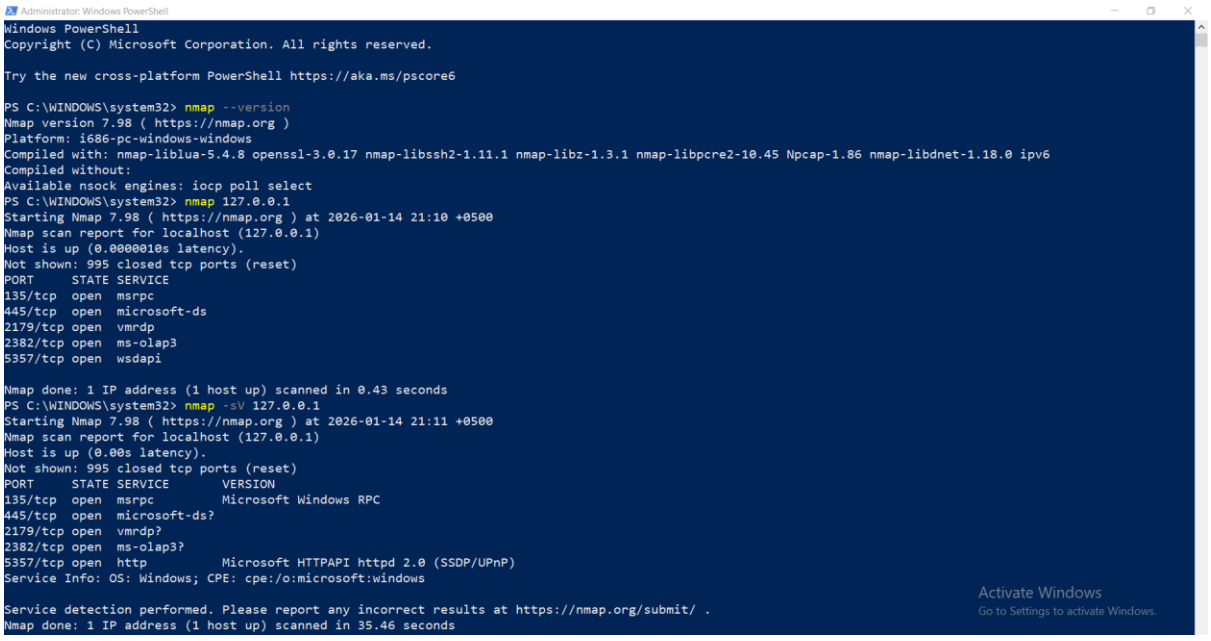
Localhost Scan: A basic scan was run on the local machine (127.0.0.1). It identified several open ports, including:

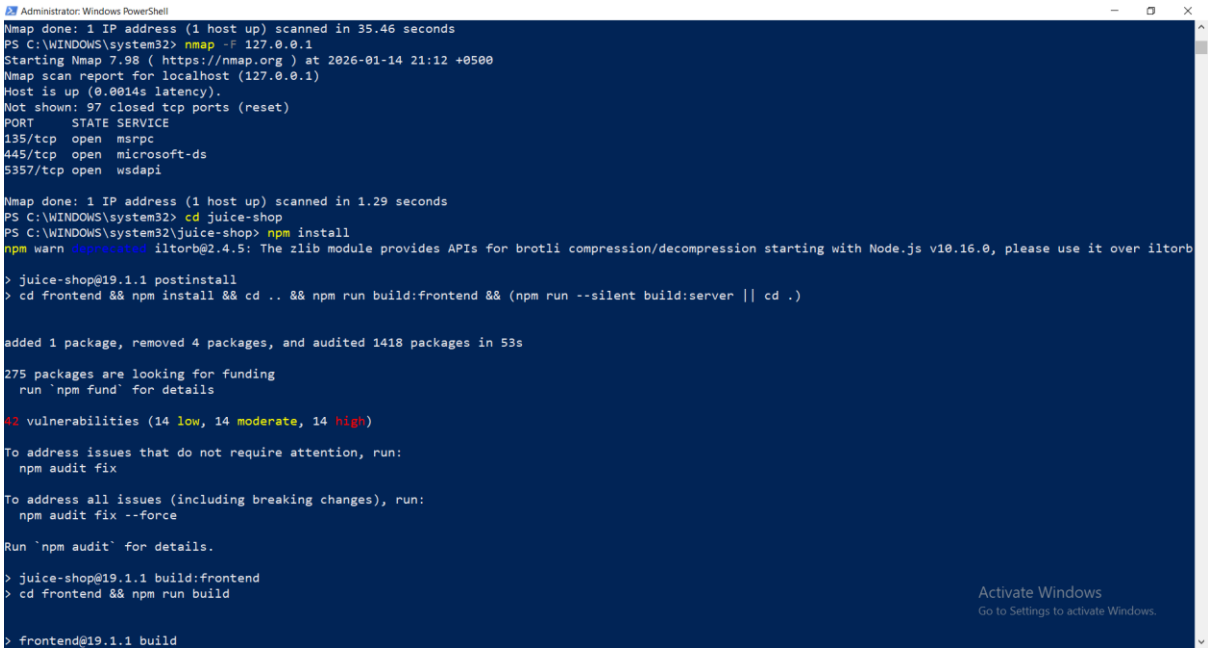
1. Port 135: Microsoft RPC.

2. Port 445: Microsoft-ds (File sharing).

3. Port 3000: This is where the web application was later found running.

Service Detection: Using the -sV flag, I identified specific versions of the software running on these ports to look for potential weaknesses.





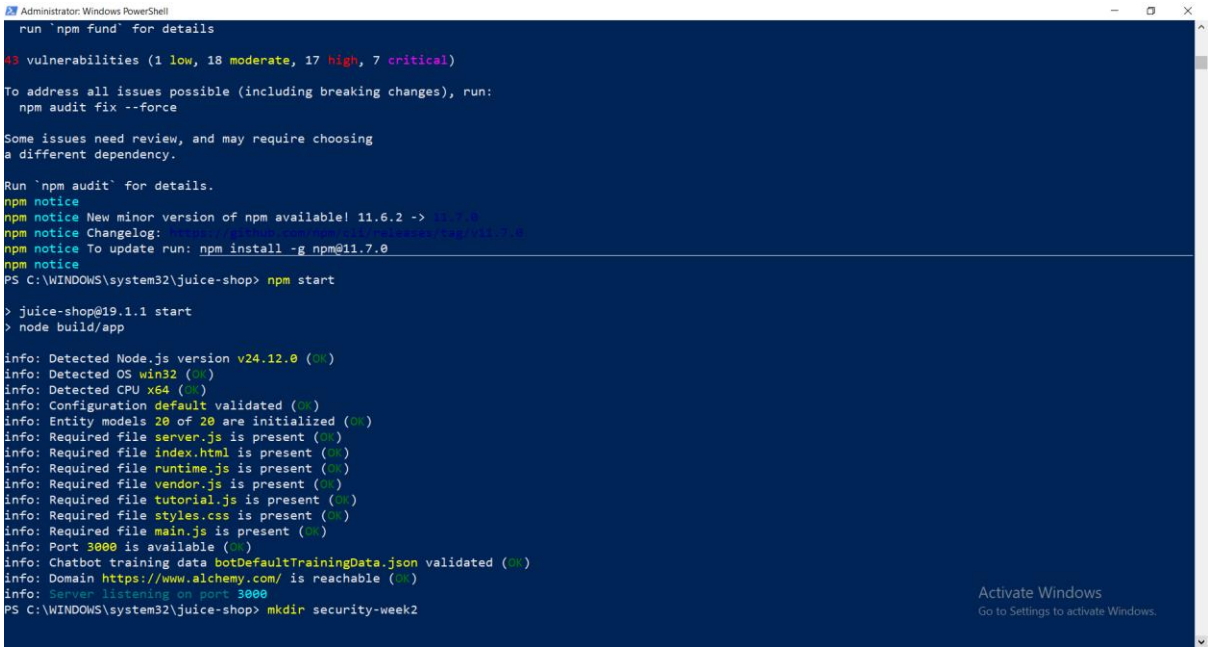
OWASP Juice Shop Setup:

The below screenshots show the setup of OWASP Juice Shop, which is a dangerously insecure web application used for security training.

Installation: I navigated to the juice-shop folder and run npm install. The system flagged 42 vulnerabilities (14 low, 14 moderate, and 14 high) within the application's dependencies.

Starting the App: After installation, I run npm start. The application successfully launched on Port 3000.

Verification: A web browser screenshot shows the All Products page of the Juice Shop, confirming the store is active and displaying items like "Apple Juice" and "Banana Juice."

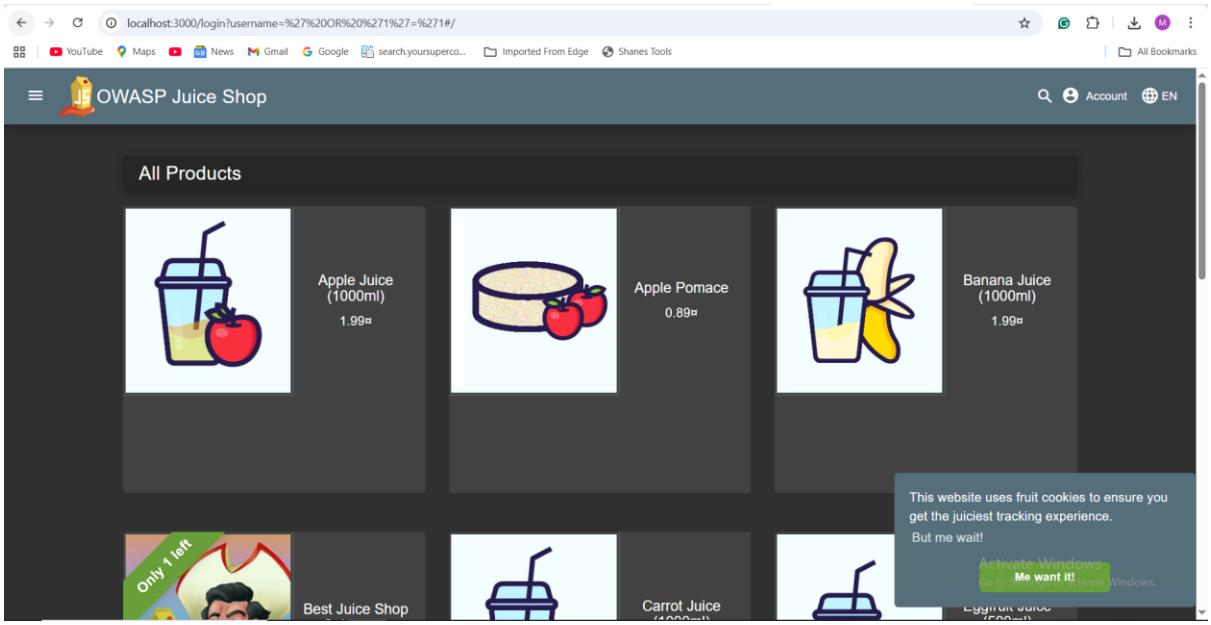


Security Testing: SQL Injection:

Successful attempt to exploit a common web vulnerability called SQL Injection.

1. The Attack: I entered a malicious string into the login URL: ' OR '1'='1

2. The Result: This specific string is designed to trick the database into thinking a password is correct, even if it is not. The screenshot shows the user successfully bypassed the login screen and gained access to the store interface without a valid password.



Implementation of Logging System:

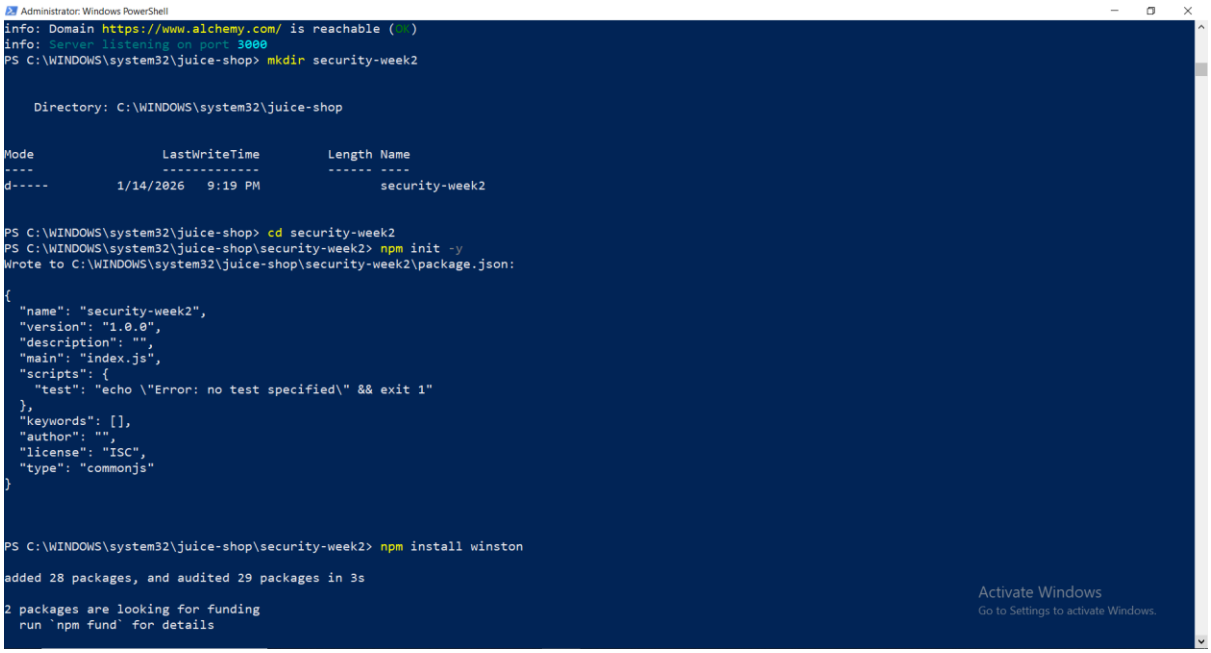
Finally, I created a custom security logging tool to track activities within the environment.

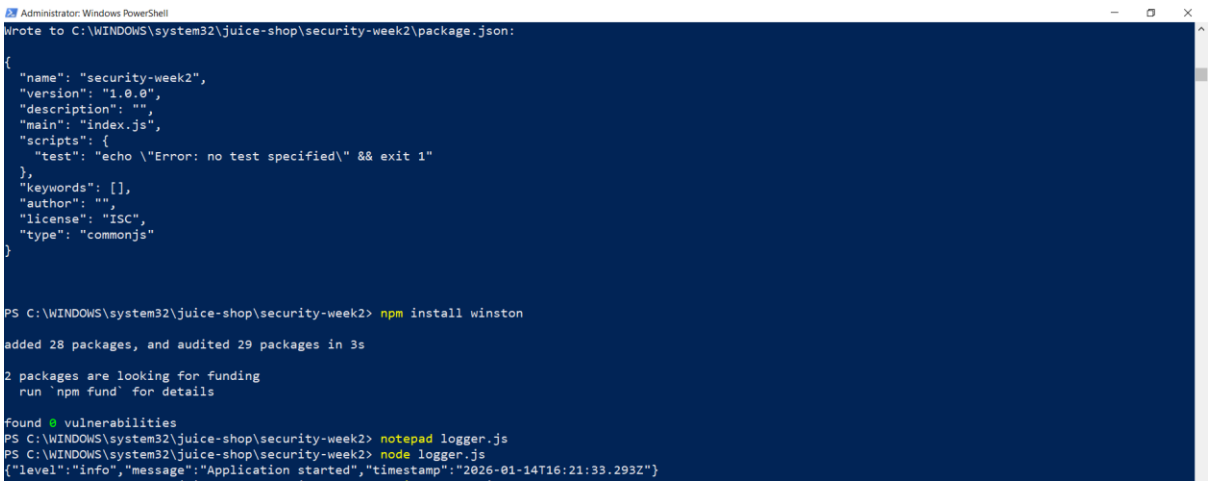
Project Initialization: A new directory named security-week2 was created, and a new Node.js project was started using npm init -y.

Winston Library: Installed **Winston**, a popular logging library for Node.js.

Coding the Logger: A file named logger.js was created.

Testing: I run node logger.js, and the terminal showed a successful log entry: {"level":"info","message":"Application started",...}.





Logger.js File:

At Last:

Through this task, I learned how to use Nmap for network reconnaissance to identify open ports like 135, 445, and 3000 on a local system. I gained hands-on experience in web security by successfully using a SQL injection payload, ' OR '1'='1, to bypass the authentication of an OWASP Juice Shop application. Additionally, I developed a functional logging system using the Winston library in Node.js to record security events into a persistent security.log file.

GitHub Repository Link:

https://github.com/MBQ17/Week-3---Advanced-Security
