Hackathon 24 - 01 - Automated Pen Testing

Problem Statement

Develop a web application that facilitates automated penetration testing for other web applications. Customers will provide the URL of their web application, and upon validation, the system will conduct penetration testing using CLI commands of Zed Attack Proxy (ZAP) and Nmap tools. The application should generate comprehensive reports for customers to download, providing insights into potential vulnerabilities in their web applications.

User Roles

There are 2 user roles that interact with the web application.

1. **Customer** - This role is the primary user of the system who requests for penetration testing for their web application
2. **BOT** - This role will function as a backend program that runs in the server managing, executing, and generating the reports for the customer requests

High Level User Stories

As a Customer

I should be able to carry out the following tasks in the web application, so that I will successfully run penetration testing for my web application

1. I should be able to sign up for a Free account using my email, And utilize those credentials to access my account.
2. I should be able to input single web application URL as part of single request for penetration testing
3. I should be able to see the error message if the web application URL is invalid or the website is down.
4. I should be able to submit a PenTest request for comprehensive evaluation of security vulnerabilities.
5. I should be able to check the status of PenTest Execution to track the progress of my requested PenTest.
6. I should be able to see the status as “**SCHEDULED**” as soon as I submit the request.
7. I should be able to see the status as “**IN PROGRESS**” when the PenTest is in progress
8. I should be able to see the status as “**COMPLETED”** when the PenTest is completed and the report is ready to be downloaded.
9. I should be able to see the status as “**TEST ERROR”** and corresponding error message when the PenTest fails.
10. I should be to download a detailed report containing vulnerabilities identified by the automated pen test, after completion of the the penetration testing process
11. I should be able to submit multiple requests for Penetration testing by providing the corresponding website URL for each request.
12. I should be able to see the list of the PenTest requests submitted by me along with the status

As a BOT

1. I should be able to read queued requests from all the customers and execute all of them one by one
2. I should be able to read the request and know the web application URL
3. I should be able execute both ZAP and NMap penetration test tools against the web application using default arguments
4. I should be able to process a new request immediately or after report generation of the last request in the queue, whichever earliest possible
5. I should be able to run the ZAP tool with default parameters against the requested web application URL
6. I should be able to run the NMap tool with default parameters against the requested web application URL
7. I should be able to generate a single report containing following two sections irrespective of whether any vulnerabilities are found or not,
    a. All open vulnerable ports found by parsing the response from NMap execution
    b. All web application vulnerabilities found by parsing the response from ZAP execution
8. I should add the following details in the section on open vulnerable ports in the report,
    a. Summary - No. of Vulnerable Ports Open
    b. Detailed Report
        i. Port Number
        ii. Protocol
        iii. Services
        iv. Recommended Action or Best Practices
9. I should add the following details in the section on web application vulnerabilities in the report,
    a. Summary
        i. No. of Total Vulnerabilities Identified
        ii. No. of Total Vulnerabilities Identified grouped on Risk Rating
    b. Detailed Report
        i. Vulnerability Summary
        ii. Risk Rating
        iii. Confidence Rating
        iv. Description
        v. Details to Reproduce the Instance
10. I should update the status of a request from “**SCHEDULED**“ to “**IN PROGRESS**“ when I start the execution of the penetration tools
11. I should upload the generated report for the corresponding customer’s request, so that customer can download the report from the UI
12. I should update the status of a request from “**IN PROGRESS**“ to “**COMPLETED**“, when the test execution succeeded and report is ready for download
13. I should log the error if execution of ZAP or NMap tool fails for any reason and report a generic error like “Test Execution Unsuccessful” to customer and update the status from “**IN PROGRESS”** to “**TEST ERROR**”

Pre-Defined Data

1. All user roles (Customer, BOT) can be pre-defined at the backend DB during implementation phase
2. All Customer user creation will be happening as part of new customer sign-up feature in the application
3. Required Penetration tools should be installed and configured at the server during implementation phase

Reference Articles

Running ZAP in CLI - ZAP – Command Line , ZAP – Command Line

Running NMap using CLI - 7 Absolutely Essential Nmap Commands for Pen Testing

Vulnerable Ports - Identifying secure and unsecured ports and how to secure them - All About Security

Vulnerable Ports - https://support.huawei.com/enterprise/en/doc/EDOC1100297670

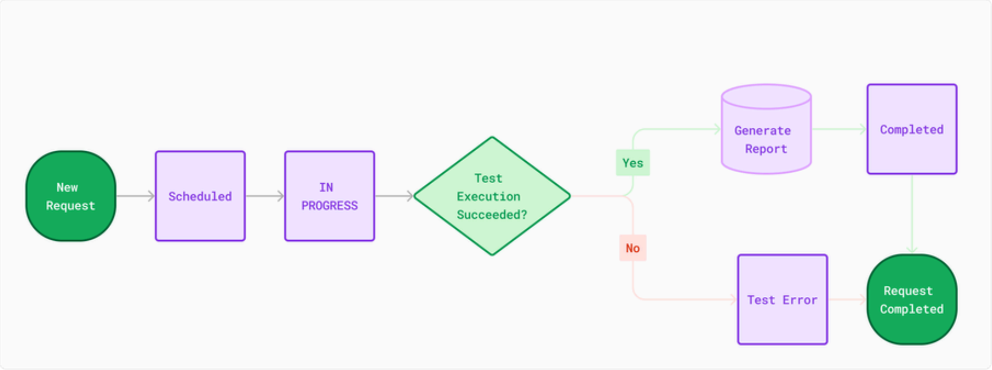
Other References

Automated Pen Testing With ZAP CLI

How to Automate OWASP ZAP | Jit

Appendix 1

Flow chart


New Request
Scheduled
IN PROGRESS
Test Execution Succeeded?
Yes
Generate Report
Completed
No
Test Error
Request Completed