COMP307

Lab Assignment 8

Web Application Test Plan

- Work in groups of at most 4 students.
- Read the material from 'OWASP Testing Guide' the "Principles of Testing" section and "How to Write the Report of Testing" section. https://www.owasp.org/index.php/Reporting
- Create a word document named "Web Application Test Plan" that includes the following elements (you'll be responsible to determine what to document in this report based on what you learned in your research):
    - Executive Summary
    - Table of Contents
    - Overview of the tests you would perform and your reasons for including each test.

For this test scenario, assume that you are the network admin for "Online Appliance Parts", an internet-based company that provides appliance parts, such as accessories for washer, dryers, ranges, stoves, ovens, refrigerators, etc., to residential and corporate customers. This e-commerce site receives most of its income from online credit card purchases. Repeat customers receive discounts based on the amount of their total

1. Executive Summary

The executive summary sums up the overall findings of the assessment and gives business managers and system owners a high level view of the vulnerabilities discovered. The language used should be more suited to people who are not technically aware and should include graphs or other charts which show the risk level. Keep in mind that executives will likely only have time to read this summary and will want two questions answered in plain language: 1) *What's wrong?* 2) *How do I fix it?* You have one page to answer these questions.

The executive summary should plainly state that the vulnerabilities and their severity is an **input** to their organizational risk management process, not an outcome or remediation. It is safest to explain that tester does not understand the threats faced by the organization or business consequences if the vulnerabilities are exploited. This is the job of the risk professional who calculates risk levels based on this and other information. Risk management will typically be part of the organization's IT Security Governance, Risk and Compliance (GRC) regime and this report will simply provide an input to that process.

2. Test Parameters

The Introduction should outline the parameters of the security testing, the findings and remediation. Some suggested section headings include:

2.1 Project Objective: This section outlines the project objectives and the expected outcome of the assessment.

2.2 Project Scope: This section outlines the agreed scope.

2.3 Project Schedule: This section outlines when the testing commenced and when it was completed.

2.4 Targets: This section lists the number of applications or targeted systems.

2.5 Limitations: This section outlines every limitation which was faced throughout the assessment. For example, limitations of project-focused tests, limitation in the security testing methods, performance or technical issues that the tester come across during the course of assessment, etc.

2.6 Findings Summary: This section outlines the vulnerabilities that were discovered during testing.

2.7 Remediation Summary: This section outlines the action plan for fixing the vulnerabilities that were discovered during testing.

And then have something like the Findings section, except this will have table with TestID, headings, and Test Description. No Findings/severity/recommendation columns