|  |  |
| --- | --- |
| **Web Application Pen-Testing (WAPT)**  Diploma in CSF  Year 2 (Oct 2022) Semester 4 | Week 7 -17 |
| Assignment |
| **Assignment Write-up** | |
| **Assignment Weightage: 40%** | |

## 

**1.0 OBJECTIVES**

This assignment allows students to practice web app pen-testing methodology and skills. It aims to make students apply what they have learned in the course, and to acquire further knowledge and skills in web-application pen-testing through experiential learning.

At the end of this pen-test assignment and in accordance to the type of assignment, students are expected to be able to accomplish most of the following:

* To establish a Scope and Rules of Engagement Document for the project;
* To sign a pen-test contract and non-disclosure with the client;
* To carry out information gathering/reconnaissance to gather and document information needed for the project;
* To carry out scanning and mapping to map out the target web application system;
* To scan/detect vulnerabilities in the target web application;
* **To design proof of concept case(s) for exploitation and post-exploitation**;
* To exploit the vulnerabilities found in accordance to endorsed proof of case for exploitation;
* To document the findings and present the findings and recommendations;
* To write a web application **pen-test report for the client (Volume 1) and tutor (Volume 2)** in accordance to the template provided; and
* **To create a video presentation for the client on the vulnerabilities found, finding from exploitation and post-exploitation and recommendations;**
* **To create a video presentation for the tutor on your contributions, learnings, individual reflections and team reflections.**

**2.0 ASSIGNMENT DETAILS**

* The web sites submitted for pen-testing are owned by the industry or ICT. The ICT owned website is either in-housed or developed by vendor from the industry.
* It is envisaged that all these web sites have some form of vulnerabilities. Your first task is to speak to the owner of the selected site and construct a **scope document** and a **rule of engagement.**

* Your team will then proceed to **sign a contract** and **non-disclosure documents** with the client using the template provided by the school.
* Your team members will proceed to establish the web application system architecture through scanning or information obtained from the client/developer. The activities and evidences must be captured and presented in Volume 1 of the report.
  + **Each member must use a different scanning tool to scan to obtain the necessary information needed.**
* Scan for vulnerabilities and establish first cut Vulnerability Severity Findings Table and decide on a number of severe cases. To design at least **ONE** Proof of Concept (PoC) use case for Exploitation and Post Exploitation.
* Present your **PoC** to you client and seek his/her’s permission to proceed. **The PoC must be officially signed-off before your team proceeds with the exploitation and post-exploitation.**
  + **Each member must show evidence of 1 post-exploitation activity.**
* Complete the exploitation and post exploitation activities, compile your report and create a video findings for the client.
* Create a separate video for your tutor to share your contributions to the project, learning points and implications. There is a need for a team reflections and individual’s reflection in this exercise.
* The above serves as a guide base on our methodology (See extra slides on Pen-Test Methodology). In practise, you may adjust to suit your team’s strength and experiences. Remember to get involve in the assignment so that you can construct your knowledge, skills and confidence over time.

**3.0 OTHER IMPORTANT DETAILS**

The following needs to be accomplished by each member of the team:

* Information gathering/Reconnaissance: each team member must take up one unique and appropriate reconnaissance tool to gather **meaningful and purposeful information** about the web-application system.
* Scan and Test Vulnerabilities: each team member needs to discover as many different types of vulnerabilities (OWASP Top 10) as possible. It is important to describe the tools and steps taken on how he/she discovered the vulnerabilities.
* Exploitation and Post Exploitation: team members must work together to establish severity table for the vulnerabilities found (See extra slides on Severity Table), **select most severe vulnerabilities and design proof of concept case for exploitation & post-exploitation (see extra slides)**, only exploit the vulnerabilities after obtaining written permission from the client.
* Students are reminded that all samples (if any) are provided as a guide and they are not perfect in nature. You are to consult the tutor and enhance them where appropriate.

**4.0 MAIN DELIVERABLES**

**4.1** **Signed-Off Contract (10 marks) comprise of**

- Contract & Schedule Document

- Signed-off Document

- Scope Document

- Rules of Engagement Document

- Non-Disclosure Document

- See templates and samples given in Team

**4.2** **Pen-Test Report – 50 marks**

Note - Number of pages of report must not be more than 60 pages (excluding Appendices).

**Report Template for Client Report (Volume 1-20 marks) – To Submit to Team’s Channel**

Cover Page with Title  
Sign-off Page by Team Members

Executive Summary (2 pages)

Contents Outline

1.0 Introduction

2.0 Client Information

3.0 Pen-Test Schedule

4.0 Information Gathering Summary Findings

5.0 Vulnerabilities Summary Findings

6.0 Exploitation & Post-Exploitation Summary Findings

7.0 Recommendations

8.0 Summary

9.0 Appendices

1. Signed-off Proof of Concept Exploitation Use Cases

\*The above are the minimum contents. Team may enhance the template in accordance to the project. Please discuss with tutor in-charge.

**Report Template for Tutor Report (Volume 2–30 marks) – Not to Be Given to Client**

Cover Page with Title  
Sign-off Page by Team Members

Contents Outline

1.0 Detailed Evidences of Information Findings

2.0 Detailed Evidences of Vulnerability Scanning

3.0 Detailed Evidences of Proof-of-Concept Exploitation

4.0 Contributions

Contributions of each team member must be clearly tabulated, containing the tools he/she used, for the reconnaissance, scanning of vulnerabilities and exploitation activities he/she conducted.

5.0 Team Reflection

6.0 Individual Reflection

7.0 Summary

\* Section: 1-3 must include screenshots and procedures, and **name of pen-tester** who contributed to the activities.

**4.4** **Pen-test Video Presentation for Client (To be recorded and to submit to Team’s Channel) – 20 Marks**

Cover Page with Title

Overview of Project

Table of Vulnerabilities Found and Severity

Proof of Concept Cases Designed for Exploitation

Results of Exploitation and Recommendation

Summary

\* The above are the minimum contents. Team may enhance the template in accordance to the project. Please discuss with tutor in-charge.

**4.5 Contributions and Reflections Video Presentation for Tutor and LIVE Q&A (if needed) – 20%**

Contributions

Contributions of each team member must be clearly tabulated, containing the tools he/she used, for the reconnaissance, scanning of vulnerabilities and exploitation and post-exploitation activities he/she conducted.

Team Reflection

Individual Reflection

\* The above are the minimum contents. Team may enhance the template in accordance to the project. Please discuss with tutor in-charge.

**5. DEADLINES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Deliverables | % | **Deadlines** | Where to Submit |
| 1. | Signed-Off Contract | 10 | Sunday, 2359, end of Week 12 | Final Version to Team Channel  - Team Leader to Submit |
| 2. | Report for Client (Volume 1) | 25 | Sunday, 2359, end of Week 15 | Final Version to Team Channel  - Team Leader to Submit |
| 4. | Report for Tutor (Volume 2) | 25 | Sunday, 2359, end of Week 15 | Final Version to Team Channel  Team Leader to Submit |
| 5. | Video Presentation for Client | 20 | Sunday, 2359, end of Week 16 | MP4 Final Video to Team’s Channel  Team Leader to Submit |
| 6. | Contributions and Reflections Video Plus Q&A if needed | 20 | Sunday, 2359, end of Week 16 | MP4 Final Video to Team’s Channel  Team Leader to Submit |
| 7. | Showing Video & Q&A in Class |  | Week 17 in Class |  |

**6.0** **WARNINGS**

6.1 DO NOT plagiarize in this assignment, any such attempt would have serious consequences.