|  |  |
| --- | --- |
| **Web Application Pen-Testing (WAPT)**  Diploma in CSF  Year 2 (Oct 2021) Semester 4 | Week 5 -17 |
| Assignment |
| **Assignment Write-up** | |
| **Assignment weightage: 40%** | |

## 

**1.0 OBJECTIVES**

This assignment allows students to practice web app pen-testing methodology. 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 devise a pen-test plan for the project;
* To carry out 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 prove of concept case(s) for exploitation**;
* T**o brief client on the vulnerabilities found, proof of concept case for exploitation and discuss next phase of action;**
* 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 the client; and
* To write a web application **pen-test report for the client and tutor** in accordance to the template provided.

**2.0 ASSIGNMENT DETAILS**

* The web sites submitted for pen-testing are owned by the industry except one is own by ICT. The ICT owned website is also 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 come up with 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 2 of the report.
  + **Each member must use a different scanning tool to scan to obtain the necessary information needed.**
* Establish first cut Vulnerability Severity Findings Table and decide on a number of severe cases. To design at least **THREE** Proof of Concept (PoC) use cases 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.**
* Complete the exploitation and post exploitation activities, compile your report and present your findings to the client. These needs to be video recorded as evidence.
* Create a separate video 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. In practise, you may adjust to suit your team’s strength and experiences. Remember to involve constructing your knowledge, skills and confidence over time.

**3.0 OTHER IMPORTANT DETAILS**

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

* Passive and Active Reconnaissance: each team member must take up one unique and appropriate passive (1) and active reconnaissance (1) tool to gather **meaningful and purposeful information** for the project**.**
* 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, **select most severe vulnerabilities and design prove of concept case for exploitation**, exploit the vulnerabilities after obtaining written permission from the client.
* Students are reminded that all samples are provided as a guide and they are not perfect in nature. You are to enhance them where appropriate.

**4.0 MAIN DELIVERABLES**

**4.1** **Signed-Off Scope and Rules of Engagement Documents (To submit to Team’s Channel) – 20 marks**

- See samples given

**4.2** **Signed-Off Contract and Non-Disclosure Documents (To submit to Team’s Channel) – 10 marks**

- See templates given in Team

**4.3** **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 Scope Document
2. Signed-Off Rules of Engagement Document
3. Signed-Off Agreement/Contract
4. Signed-Off Non-Disclosure Document
5. 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  
wSign-off Page by Team Members

Contents Outline

1.0 Evidences of Information Findings

2.0 Evidences of Vulnerability Scanning

3.0 Evidences of Proof-of-Concept Exploitation

4.0 Contributions

Contribut

ions 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

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

**4.4** **Pen-test LIVE Presentation for Client (To be recorded and to submit to Team’s Channel) – 10 Marks**

Cover Page with Title

Overview of Project

Contents Outline

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 Video (To be recorded and to submit to Team’s Channel) and LIVE Q&A (if needed) – 10%**

**5. DEADLINES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Deliverables | % | **Deadlines** | Where to Submit |
| 1. | Signed-Off Scope and Rules of Engagement Documents | 20 | 2359, 26th December 2021  (end of Week 10) | Final Version to MeL, Team Leader to Submit |
| 2. | Signed-Off Contract and Non-Disclosure Documents | 10 | 2359, 2nd January 2022  (end of Week 11) | Final Version to MeL, Team Leader to Submit |
| **3.** | **Report for Client** | **25** | **2359, 30th January 2022**  **(end of Week 15)** | **Final Version to MeL, Team Leader to Submit** |
| **4.** | **Report for Tutor** | **25** | **2359, 30th, January 2022**  **(end of Week 15)** | **Final Version to MeL, Team Leader to Submit** |
| 5. | Pen-test LIVE Presentation for Client | 10 | **2359, 20th February 2022**  (end of Week 18) | MP4 Final Video to Team’s Channel, Team Leader to Submit |
| 6. | Contributions and Reflections Video Plus Q&A if needed | 10 | 2359, 6th, February 2022  (end of Week 16) | MP4 Final Video to Team’s Channel. Team Leader to Submit |

**6.0** **WARNINGS**

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