

# AlAhliyya Amman University

# Security Assessment Finding Report

Bussiness Confidential

Scope (tick or list): Web App ☐ API ☐ Cloud Storage ☐ OAuth ☐ Mobile Simulator ☐

Prepared by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: 2025-10-11

Table of Contents

[AlAhliyya Amman University 1](#_Toc211103686)

[Security Assessment Finding Report 1](#_Toc211103687)

[1. Executive Summary 2](#_Toc211103688)

[2. Rules of Engagement (RoE) and Assumptions 2](#_Toc211103689)

[3. Scenario Background & Narrative 2](#_Toc211103690)

[4. Scope & Architecture (Technical) 2](#_Toc211103691)

[5. Seeded Vulnerabilities & Flags 2](#_Toc211103692)

[6. Scoring Rubric and Flag Submission 3](#_Toc211103693)

[7. Detailed Findings Template (for red teams) 3](#_Toc211103694)

[8. Blue Team / Incident Response Playbook 3](#_Toc211103695)

[9. Evidence & Artifacts (Appendix) 3](#_Toc211103696)

[10. Forensic Timeline Template 4](#_Toc211103697)

[11. Remediation Roadmap & Risk Prioritization 4](#_Toc211103698)

[12. Scenarios Mapping Guide 4](#_Toc211103699)

[13. Judge’s Checklist & Evaluation Form 4](#_Toc211103700)

[14. Appendix: Templates 4](#_Toc211103701)

[15. How to Use This Document (Logistics) 4](#_Toc211103702)

## 1. Executive Summary

Provide a brief (one-page) non-technical summary of the scenario, objectives, and high-level findings. Suggested fields to fill:

- Short description of the exercise (2–3 lines).

- Number of seeded issues by severity (Critical / High / Medium / Low).

- Overall simulated risk posture and top 3 recommendations.

## 2. Rules of Engagement (RoE) and Assumptions

List authorized targets, prohibited actions, testing windows, data handling rules, and stakeholder contact information.

Fields:

- Testing Window: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Authorized IPs / Hostnames: \_\_\_\_\_\_\_\_\_\_\_\_

- Prohibited Actions: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Contact / Emergency: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 3. Scenario Background & Narrative

Provide the fictional organization description, recent events (realistic hooks), and public-facing artifacts for OSINT. Attach sample press release or social posts if applicable.

Narrative:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 4. Scope & Architecture (Technical)

Include architecture diagram (attach separately), list of services, auth flows, and external integrations.

In-scope hosts/services:

- Service: \_\_\_\_\_\_\_\_\_\_ Hostname/IP: \_\_\_\_\_\_\_\_\_\_ Notes: \_\_\_\_\_\_\_\_\_\_

- Service: \_\_\_\_\_\_\_\_\_\_ Hostname/IP: \_\_\_\_\_\_\_\_\_\_ Notes: \_\_\_\_\_\_\_\_\_\_

## 5. Seeded Vulnerabilities & Flags

Use the table below to list each seeded vulnerability, its difficulty, and the flag string. Duplicate the table as needed.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Flag ID | Vulnerability | Location (URL/API) | Difficulty | Points | Notes / Repro Steps |
| CPTC{CHTR}-XSS-001 | Stored XSS | /posts/create | Low | 10 | Payload in post content renders JS executing FLAG string. |

Guidance: include learning objectives and expected evidence for each flag.

## 6. Scoring Rubric and Flag Submission

Specify flag format, points per difficulty, submission requirements, and any penalties. Example: Low=10, Medium=25, High=50.

## 7. Detailed Findings Template (for red teams)

Provide a template for findings that teams should submit. Include the following fields (copy per finding):

- Title:

- Flag:

- Severity:

- Affected component(s):

- Summary:

- Reproduction steps:

- Evidence (screenshots/HTTP requests):

- Root cause:

- Mitigation:

## 8. Blue Team / Incident Response Playbook

Include detection rules, hunt queries, containment, forensic artifacts, and communication templates. Examples:

- Detection rule: multiple password resets from same IP within X minutes => alert

- Forensic artifacts: web server logs, object storage access logs, DB logs

## 9. Evidence & Artifacts (Appendix)

Attach seeded accounts, sample logs, and sample payloads. Use synthetic data only.

Seeded accounts table:

|  |  |  |  |
| --- | --- | --- | --- |
| Username | Email | Role | Password |
| student1 | student1@example.local | user | Passw0rd! |

## 11. Remediation Roadmap & Risk Prioritization

Short-term (hours/days):  
- Revoke exposed tokens  
- Patch config  
Medium-term (weeks):  
- Hardening, secure CI/CD  
Long-term (months):  
- Threat model and bug bounty

## 12. Scenarios Mapping Guide

Mapping guidance for the five flavor scenarios (ChatterNet, InfluenceMe, CampusConnect, NewsLink, PhotoSphere). Fill which flags belong to which flavor.

## 13. Judge’s Checklist & Evaluation Form

Include a table or form for judges. Example fields:  
- Technical correctness (0-5)  
- Reproducibility (0-5)  
- Impact assessment (0-5)  
- Creativity (0-5)  
- Adherence to RoE (Pass/Fail)

## 14. Appendix: Templates

Include sample notification emails, flag submission web form sample, and sanitization checklist.

## 15. How to Use This Document (Logistics)

Step-by-step instructions for organizers to deploy and validate the scenario, run the competition, and debrief.