

SECURITY INCIDENT REPORT

CASE FILE: OPERATION SCHOLARSHIP NOW

CHED Scholarship Now Portal — Simulated Cyber Incident Investigation

Group Name / Number	[Enter group name or assigned group number]
Lead Submitter	[Full name of the ONE member who will submit]
Course / Program	Introduction to Proactive and Reactive Internet Investigation
Case	Operation Scholarship Now
Report Classification	TRAINING EXERCISE — SIMULATED INCIDENT
Date of Submission	[DD Month YYYY]
Final Filename	Group##_OperationScholarshipNow_IncidentReport.pdf

IMPORTANT: Only one member submits the final PDF on behalf of the entire group.

Submission Instructions

1. Complete this report as a group using only evidence that can be reasonably supported by the case materials, simulated tools, logs, screenshots, and observations.
2. List the FULL NAME and EMAIL ADDRESS of every participant in the Group Membership section. Verify spelling before submission.
3. Only ONE designated group member must submit the final report for the entire group. Duplicate submissions are not required.
4. Before submission, remove instructional placeholder text, check formatting, and ensure all figures/screenshots are readable.
5. Save/export the completed report as PDF. Submit the FINAL PDF report to justinpineda.com using the designated submission channel/page provided by the instructor.
6. Recommended filename: Group##_OperationScholarshipNow_IncidentReport.pdf.
7. Do not include real passwords, personal credentials, unrelated personal data, or live malicious code in the report.

Evidence standard: Separate OBSERVATION from INTERPRETATION. A scanner finding may establish exposure or vulnerability, but it does not by itself prove successful exploitation. Correlate multiple sources before stating a conclusion.

Group Membership and Submission Accountability

Every person who participated in the investigation must appear below. Add rows if necessary.

#	Full Name	Email Address	Role / Contribution	Present?
1	[Name]	[Email]	[e.g., Log analysis / IOC / Report writing]	☐ Yes
2	[Name]	[Email]	[e.g., Log analysis / IOC / Report writing]	☐ Yes
3	[Name]	[Email]	[e.g., Log analysis / IOC / Report writing]	☐ Yes
4	[Name]	[Email]	[e.g., Log analysis / IOC / Report writing]	☐ Yes
5	[Name]	[Email]	[e.g., Log analysis / IOC / Report writing]	☐ Yes
6	[Name]	[Email]	[e.g., Log analysis / IOC / Report writing]	☐ Yes
7	[Name]	[Email]	[e.g., Log analysis / IOC / Report writing]	☐ Yes

#	Full Name	Email Address	Role / Contribution	Present?
8	[Name]	[Email]	[e.g., Log analysis / IOC / Report writing]	☐ Yes

Designated Submitter

[Full name]

Submitter Email

[Email address]

Group Confirmation☐ We confirm that only the designated submitter will send the final PDF.

1. Executive Summary

Write this section last. In approximately 250–400 words, summarize the incident, major findings, business/user impact, confidence level, and the most important immediate actions.

2. Incident Background and Initial Situation

Describe what CHED Scholarship Now is, what was initially reported, what information was available at the start, and why an investigation was initiated. Do not state later discoveries as if they were initially known.

3. Scope and Investigation Objectives

Define what your group examined and what questions you attempted to answer.

Systems / Assets Examined

[Portal, application form, logs, simulated endpoints, etc.]

Time Period Examined	[Relevant incident window]
Primary Investigation Questions	[What happened? How? What was affected?]
Tools / Evidence Sources	[DirBuster-style, WAF, server logs, app logs, IOC, etc.]
Out of Scope / Limitations	[What could not be established from the available evidence?]
Assumptions	[State only necessary assumptions; avoid unsupported speculation.]

4. Incident Timeline

Reconstruct the sequence of events. Use timestamps where available. Distinguish confirmed events from inferred sequence.

Date/Time	Event	Evidence Source	Observation	Interpretation	Confidence
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low
[Time]	[Event]	[Log/tool]	[What was observed]	[What it may mean]	High / Med / Low

5. Findings and Evidence

Document each significant finding separately. A finding should answer an investigative question and cite the evidence that supports it.

Finding 1: [Short descriptive title]

Finding Statement

[What can you reasonably conclude?]

Evidence / Artifact

[Log entry, URL, hash, screenshot, scanner result, etc.]

Source / Tool

[Where was it obtained?]

Technical Analysis

[Explain what the evidence indicates.]

Corroborating Evidence

[What other source supports this?]

Confidence

☐ High ☐ Medium ☐ Low

Limitations / Alternative Explanation

[What remains uncertain?]

Insert supporting screenshot(s) immediately below this finding if useful. Add a caption and redact irrelevant personal information.

[Insert screenshot / evidence image here]

Finding 2: [Short descriptive title]**Finding Statement**

[What can you reasonably conclude?]

Evidence / Artifact

[Log entry, URL, hash, screenshot, scanner result, etc.]

Source / Tool

[Where was it obtained?]

Technical Analysis

[Explain what the evidence indicates.]

Corroborating Evidence

[What other source supports this?]

Confidence☐ High ☐ Medium ☐ Low**Limitations / Alternative Explanation**

[What remains uncertain?]

Insert supporting screenshot(s) immediately below this finding if useful. Add a caption and redact irrelevant personal information.

[Insert screenshot / evidence image here]

Finding 3: [Short descriptive title]**Finding Statement**

[What can you reasonably conclude?]

Evidence / Artifact

[Log entry, URL, hash, screenshot, scanner result, etc.]

Source / Tool

[Where was it obtained?]

Technical Analysis

[Explain what the evidence indicates.]

Corroborating Evidence

[What other source supports this?]

Confidence☐ High ☐ Medium ☐ Low**Limitations / Alternative Explanation**

[What remains uncertain?]

Insert supporting screenshot(s) immediately below this finding if useful. Add a caption and redact irrelevant personal information.

[Insert screenshot / evidence image here]

Finding 4: [Short descriptive title]**Finding Statement**

[What can you reasonably conclude?]

Evidence / Artifact

[Log entry, URL, hash, screenshot, scanner result, etc.]

Source / Tool

[Where was it obtained?]

Technical Analysis

[Explain what the evidence indicates.]

Corroborating Evidence

[What other source supports this?]

Confidence☐ High ☐ Medium ☐ Low

Limitations / Alternative Explanation

[What remains uncertain?]

Insert supporting screenshot(s) immediately below this finding if useful. Add a caption and redact irrelevant personal information.

[Insert screenshot / evidence image here]

Finding 5: [Short descriptive title]**Finding Statement**

[What can you reasonably conclude?]

Evidence / Artifact

[Log entry, URL, hash, screenshot, scanner result, etc.]

Source / Tool

[Where was it obtained?]

Technical Analysis

[Explain what the evidence indicates.]

Corroborating Evidence

[What other source supports this?]

Confidence☐ High ☐ Medium ☐ Low**Limitations / Alternative Explanation**

[What remains uncertain?]

Insert supporting screenshot(s) immediately below this finding if useful. Add a caption and redact irrelevant personal information.

[Insert screenshot / evidence image here]

6. Indicator of Compromise (IOC) Register

Record relevant indicators discovered during the exercise. Do not invent IOCs that were not observed.

IOC Type	Value	Where Found	Context	Assessment	Confidence
[IP/hash/domain/file]	[Value]	[Source]	[Context]	[Malicious/Suspicious/Unknown]	[H/M/L]
[IP/hash/domain/file]	[Value]	[Source]	[Context]	[Malicious/Suspicious/Unknown]	[H/M/L]
[IP/hash/domain/file]	[Value]	[Source]	[Context]	[Malicious/Suspicious/Unknown]	[H/M/L]
[IP/hash/domain/file]	[Value]	[Source]	[Context]	[Malicious/Suspicious/Unknown]	[H/M/L]
[IP/hash/domain/file]	[Value]	[Source]	[Context]	[Malicious/Suspicious/Unknown]	[H/M/L]
[IP/hash/domain/file]	[Value]	[Source]	[Context]	[Malicious/Suspicious/Unknown]	[H/M/L]
[IP/hash/domain/file]	[Value]	[Source]	[Context]	[Malicious/Suspicious/Unknown]	[H/M/L]
[IP/hash/domain/file]	[Value]	[Source]	[Context]	[Malicious/Suspicious/Unknown]	[H/M/L]

7. Attack Sequence / Incident Reconstruction

Explain the most defensible sequence of activity. Address the relationship, if any, between service disruption, reconnaissance, exploitation, persistence, defacement, malicious file replacement, endpoint impact, and simulated social propagation.

8. Root Cause and Contributing Factors

Identify the technical root cause(s) and the security/control weaknesses that allowed the incident to occur or persist. Separate root cause from symptoms.

Category	Issue	Evidence	Contribution to Incident
Root Cause	[Issue]	[Evidence]	[How it contributed]
Vulnerability / Patch Mgmt	[Issue]	[Evidence]	[How it contributed]
Monitoring / Detection	[Issue]	[Evidence]	[How it contributed]
Access Control	[Issue]	[Evidence]	[How it contributed]
File Integrity / Change Mgmt	[Issue]	[Evidence]	[How it contributed]
Incident Response	[Issue]	[Evidence]	[How it contributed]

9. Impact Assessment

Assess observed and plausible impact without overstating what the evidence proves.

Impact Area	Observed Impact	Potential Impact	Severity	Evidence
Availability	[Observed]	[Potential]	[Critical/High/Med/Low]	[Evidence]
Integrity	[Observed]	[Potential]	[Critical/High/Med/Low]	[Evidence]
Confidentiality	[Observed]	[Potential]	[Critical/High/Med/Low]	[Evidence]
Students / End Users	[Observed]	[Potential]	[Critical/High/Med/Low]	[Evidence]
CHED Operations	[Observed]	[Potential]	[Critical/High/Med/Low]	[Evidence]
Reputation / Trust	[Observed]	[Potential]	[Critical/High/Med/Low]	[Evidence]

10. Containment, Eradication, and Recovery Recommendations

Recommend practical actions in priority order. Tie each recommendation to a finding or risk.

Priority	Action	Purpose	Owner	Timing	Related Finding	Success Measure
Immediate	[Action]	[Why]	[Owner]	[When]	[F#]	[Measure]
Immediate	[Action]	[Why]	[Owner]	[When]	[F#]	[Measure]
Short-term	[Action]	[Why]	[Owner]	[When]	[F#]	[Measure]
Short-term	[Action]	[Why]	[Owner]	[When]	[F#]	[Measure]
Medium-term	[Action]	[Why]	[Owner]	[When]	[F#]	[Measure]
Medium-term	[Action]	[Why]	[Owner]	[When]	[F#]	[Measure]

11. Detection and Prevention Improvements

Describe improvements that would reduce recurrence or improve detection. Consider WAF/rate limiting, patching, secure configuration, authentication, file integrity monitoring, EDR, logging/SIEM, backups, awareness, and incident-response procedures where supported by the case.

12. Conclusions

State only conclusions that are supported by the evidence. Identify what is confirmed, what is likely, and what remains unknown.

Confirmed

[Facts directly supported by evidence]

Likely / Assessed

[Reasonable interpretation supported by correlation]

Unknown / Not Established

[Questions the available evidence cannot answer]

Appendix A — Evidence Index

List screenshots, log excerpts, scanner outputs, and other artifacts included with the report.

Evidence ID	Description	Source	Date/Time	Related Finding	Page / Appendix
E-01	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-02	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-03	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-04	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-05	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-06	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-07	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-08	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-09	[Description]	[Source]	[Timestamp]	[F#]	[Page]
E-10	[Description]	[Source]	[Timestamp]	[F#]	[Page]

Appendix B — Screenshots / Supporting Artifacts

Paste only relevant screenshots. Every image should have a short caption explaining what it shows and why it matters.

Figure B-1: [Caption]

[Insert screenshot here]

Relevance: [Explain how this supports a finding.]

Figure B-2: [Caption]

[Insert screenshot here]

Relevance: [Explain how this supports a finding.]

Figure B-3: [Caption]

[Insert screenshot here]

Relevance: [Explain how this supports a finding.]

Figure B-4: [Caption]

[Insert screenshot here]

Relevance: [Explain how this supports a finding.]

Appendix C — Final Quality and Submission Checklist

Complete this checklist before the designated submitter sends the report.

- ☐ All participant names and email addresses are complete and correct.
- ☐ One designated submitter is identified.
- ☐ Findings are supported by evidence and do not rely on unsupported speculation.
- ☐ Scanner results are not presented as proof of exploitation unless corroborated.
- ☐ Timeline is internally consistent.
- ☐ Screenshots are readable and appropriately captioned.
- ☐ Recommendations map to identified findings/risks.
- ☐ Instructional placeholders have been removed or completed.
- ☐ The document has been proofread.
- ☐ The final document has been exported/saved as PDF.
- ☐ Filename follows the required naming convention.
- ☐ Only one person will submit the final PDF for the group.
- ☐ Final PDF will be sent to justinpineda.com through the designated submission channel/page.

END OF TEMPLATE