

Security Review Evidence Packet

This packet documents a bounded student review. It is not penetration testing, a professional audit, or proof that an app is completely secure.

STUDENT NAME

Never saved by this page

REVIEW ROUTE

Course-owned Study Sprint

▼

ARTIFACT NAME OR CLASS-SAFE PATH

No private URL or restricted path

Equal-credit routes: no prior packet, public URL, AI account, paid tool, live web, security scanner, real credential, private upload, or external target is required.

1. Four-part trust map

ASSET: WHAT MUST REMAIN CORRECT, PRIVATE, AVAILABLE, OR TRUSTWORTHY?

ENTRY POINT: WHERE CAN INPUT ENTER?

TRUST BOUNDARY: WHERE DO DATA, IDENTITY, OR AUTHORITY ENTER A DIFFERENT TRUST LEVEL OR CONTROL DOMAIN?

ACTION: WHAT CAN BE RENDERED, SAVED, SENT, PUSHED, DEPLOYED, DELETED, OR CLAIMED?

2. Baseline inspection

Path	Evidence location or observation	Status	Concern, next test, or limitation
Input		Not inspected ▼	
Output		Not inspected ▼	
Browser state		Not inspected ▼	
Files + links		Not inspected ▼	
Actions + claims		Not inspected ▼	

Calibration: “No concern found in this inspection” is not “no vulnerability exists.” Record the path and evidence you actually checked.

Two safe test records

Write expected behavior before using a supplied observation or running a class-safe test. Label the evidence route accurately.

EXPECTED Visible safe behavior before the run.	OBSERVED Exact supplied or directly observed result.	INTERPRETATION Risk family, path, and reason.	LIMIT What the case did not test or prove.
--	--	---	--

Test 1

SAFE SYNTHETIC INPUT OR CASE

EVIDENCE ROUTE

Not run

EXPECTED SAFE BEHAVIOR, WRITTEN BEFORE OBSERVATION

OBSERVED BEHAVIOR

RESULT

Not tested

RISK FAMILY + EVIDENCE REASON

WHAT THIS TEST DID NOT ESTABLISH

Test 2

SAFE SYNTHETIC INPUT OR CASE

EVIDENCE ROUTE

Not run

EXPECTED SAFE BEHAVIOR, WRITTEN BEFORE OBSERVATION

OBSERVED BEHAVIOR

RESULT

Not tested

RISK FAMILY + EVIDENCE REASON

WHAT THIS TEST DID NOT ESTABLISH

Use only fictional or approved class-safe inputs. Do not test external systems, classmates, credentials, private records, real health/identity data, exploit payloads, or live accounts.

One finding, one disposition, one owner

Disposition means the recorded next-action decision. Exposure means who or what can be affected; reversibility means how easily the effect can be undone. The course case does not create a universal severity policy.

FINDING	RISK FAMILY
	Not classified
EVIDENCE AND LOCATION	EXPOSURE + REVERSIBILITY + UNCERTAINTY

Disposition

DECISION	OWNER / REVIEWER
Untriaged	Role, not private contact information
WHY THIS DISPOSITION FITS THE EVIDENCE AND AUTHORITY	

Minimum sufficient fix or next action

CAUSAL PATH TO CHANGE OR CONTAIN	SMALLEST SUFFICIENT CHANGE, STOP, OR QUESTION
WHAT IS INTENTIONALLY NOT CHANGING	HUMAN APPROVAL REQUIRED BEFORE

Retest and regression

ORIGINAL FAILING CASE + EXPECTED RESULT	OBSERVED RETEST RESULT
ORDINARY REGRESSION CASE + EXPECTED RESULT	OBSERVED REGRESSION RESULT
RETEST STATUS	REMAINING LIMITATION
Not retested	

Real secret response: stop further disclosure and notify the instructor and account owner; never copy the value here or into AI; urgently revoke or rotate through the provider; then remove current or public exposure and address repository history only through the approved coordinated process; verify invalidation, containment, and possible unauthorized use. Do not attempt unfamiliar account or repository changes alone.

Human control and Topic 14 handoff

AI review is optional and advisory. A no-AI review using the same evidence fields earns equal credit.

Bounded review request or no-AI route

GOAL AND NAMED FILES/AREAS OR SUPPLIED EVIDENCE	ALLOWED SCOPE
PROHIBITED INSPECTION, DATA, EDITS, AND EXTERNAL ACTIONS	QUESTION OR STOP CONDITION WHEN EVIDENCE IS INSUFFICIENT

Review rule: an AI suggestion remains unverified until a person checks the relevant file, source, screenshot, test, or rendered result. Do not ask for credentials, private data, full archives, unrelated files, installs, deletion, push, deployment, account connection, or external sending.

No-secrets statement

STATE WHAT YOU INSPECTED AND HOW YOU AVOIDED REPRODUCING SENSITIVE CONTENT. DO NOT PASTE ANY SECRET HERE.

Assistance disclosure

TOOL/PERSON, TYPE OF HELP, AND WHAT YOU ACCEPTED, CHANGED, REJECTED, OR PERSONALLY VERIFIED

Topic 14 security defense

BOUNDED CLAIM	VISIBLE EVIDENCE TO DEMONSTRATE
KNOWN LIMITATION	NEXT STEP OR STOP CONDITION

Submission if assigned: look for Topic 13 Security Review Evidence Packet in the LMS. Use this packet, a rendered Studio summary, LMS text, DOCX/export, scanned paper, speech-to-text, or another approved equivalent. Do not duplicate the same evidence across routes. The LMS supplies deadline, points, late rules, and resubmission. Core credit depends on equivalent reasoning and evidence, not a public URL, scanner, AI account, code volume, or claim of complete security.

Never submit: real credentials, private records, full chats, private code archives, exploit payloads, account/device screens, restricted files, grades, health or identity data, consent/assent records, unpublished peer work, or unnecessary identity evidence.