Build the checks.
Ship the change.

A working session for security developers and DevOps.

10:00–17:00 · Office breakouts
Fictional data. Real engineering habits.

02

Leave with evidence.

A contract

One permitted action. One denied boundary.

A reviewed patch

A small change with passing regression tests.

An owner

One scoped Mission 30 pull request.

The day, at a glance.

10:00–11:55

Prepare. Contracts. Prompt policy.

11:55–14:05

Triage. Lunch. Verified patch.

14:20–15:50

PHP clinic. Semgrep. Team kickoff.

15:50–17:00

Evidence review. 30-day commitments.

Make the room ready.

LIVE / SYNTHETIC DATA

bash labs/preflight.sh

PHP + SQLite, mbstring, fileinfo. Bundled Eloquent.

bash labs/run-all.sh

401 checks pass; expected red cases verified.

Watch for

A visible result.
A testable boundary.
Evidence you can keep.

The server owns the boundary.

Identity

A trusted server fixture fixes the role.

District

The database query scopes the record.

State

An under-review record stops the action.

A denial can be a passing result.

Mutation is permitted. Ownership update is denied for the clerk. Both outcomes matter.

Role / District / Record state

Write three contracts.

01 Clerk → partition: permitted preview.

02 Clerk → NOC: permitted preview.

03 Revenue officer → ownership: denied.

Minimize before you prompt.

01

Select

A minimal synthetic excerpt.

02

Check

Approved fields and purpose.

03

Redact

Known dummy patterns.

04

Review

A person decides the next step.

A filter is not permission.

Names and addresses can survive. A clean output still needs review.

Less data / Approved destination / Accountable owner

Find the dummy.
Keep the evidence.

LIVE / SYNTHETIC DATA

Scan the fixture.

One finding. A location. A fingerprint.

Remove the dummy value.

Rescan the work copy. Keep the rule.

Watch for

A visible result.
A testable boundary.
Evidence you can keep.

Separate observation from inference.

Dummy value

A fixture match, not a real compromise.

SAST scope

Execution context still needs review.

Dependency

Confirm the deployed version.

DAST label

A generic error does not establish impact.

Start with a safe incomplete rule.

Every valid request goes to manual review. Eight red tests describe the missing decisions.

No money collected / No ledger changed / No network call

Make the smallest verifiable change.

LIVE / SYNTHETIC DATA

Edit PaymentRule.php in work/.

Compare integer paise. Preserve denials.

Run the target tests.

49 checks. Zero failures. Review the diff.

Watch for

A visible result.
A testable boundary.
Evidence you can keep.

Choose a PHP boundary.

E / exact identifiers

Leading zeroes, input types and district/circle scope.

F / Laravel model writes

A note may change. Ownership and approval stay protected.

G / deed intake

Inspect bytes. Plan private quarantine. Authorize retrieval.

Preserve the complete land reference.

D01 / C01 / 000042

Text with leading zeroes and a namespace.

Validate before lookup.

Exact strings. Trusted district and circle scope.

Seven missing outcomes. One exact lookup.

LIVE / SYNTHETIC DATA

Edit identifiers/work/LandLookup.php.

Match district, circle and reference with ===.

Run the target. Review the diff.

63 checks, zero failures. No conversion or writes.

Watch for

A visible result.
A testable boundary.
Evidence you can keep.

Keep ownership out of the amendment form.

Allow one field.

Validated correspondence_note on the citizen’s own draft.

Check the whole result.

83 target checks. Other fields and rows stay unchanged.

Keep the deed in private quarantine.

01	**Inspect actual bytes.**	Size and content policy; client labels stay advisory.
02	**Choose storage on the server.**	Fresh opaque name and fixed private-root plan.
03	**Keep later decisions separate.**	Review, publication and download still require authorization.

Keep untrusted imports out of native deserialization.

Choose a data format.

A bounded JSON document with explicit fields.

Validate its meaning.

Exact types, identifiers, allowed fields and operation.

Avoid object construction.

No untrusted input to PHP unserialize().

Preserve the citizen’s words. Encode at the destination.

Blade

Ordinary output is escaped. Review every raw-output use.

CodeIgniter / PHP views

Choose output handling for HTML, attributes, JS or URLs.

Review the whole PHP execution path.

01

Edge

Gateway, web server and handler mappings.

02

Runtime

OS, branch, patch level and execution mode.

03

Application

Framework, dependencies and business contracts.

Implement. Test. Review.

01	**Read the selected contract.**	E: exact identity. F: allowed fields. G: private intake.
02	**Edit only the work file.**	Preserve validation, trusted scope and tests.
03	**Run the selected target.**	E: 63 checks. F: 83 checks. G: 65 checks.
04	**Review the actual diff.**	State what the fixture and framework did not test.

Name the boundary your patch now preserves.

One allowed outcome. One preserved denial. One real-system follow-up.

Claim / Test result / Review limitation / Owner

Run SAST, then stage DAST.

LIVE / SYNTHETIC DATA

Semgrep CE

python3 tooling/verify_semgrep.py · one finding, one clean fixture.

ZAP baseline

Authorized synthetic staging only; passive evidence before active tests.

Watch for

A visible result.
A testable boundary.
Evidence you can keep.

Choose one Mission 30 track.

Goal 1

Characterize one high-stakes workflow.

Goal 3

Gate one flagship pipeline.

Goal 6

Review findings. Fix. Retest.

Goal 7

Plan one guarded runtime upgrade.

Trace one release on paper.

01

Inputs

PHP, npm, copied library and base image.

02

Authority

Contributor runner and protected deployment.

03

Evidence

Contracts, scanner state and artifact identity.

04

Decision

Release owner, recovery and follow-up tickets.

Would you release this candidate?

Tests

Contracts passed for IMAGE-A.

Scan

Advisory fetch failed; summary says zero findings.

Release

Production request names rebuilt IMAGE-B.

Recovery

Previous image exists; data compatibility is unknown.

Leave with a decision and two owned changes.

01 Draw jobs, credentials and trust boundaries.

02 Classify the six evidence cards; record the release decision.

03 Write two tickets with harmless acceptance checks.

04 Name champion, backup, reviewer and release/risk authority.

Review two API declarations.

Read

Fictional OpenAPI plus a publication inventory.

Decide

Three missing decisions; compare the reviewed answer.

Transfer

Name the runtime evidence still required.

Choose the errors the model must not hide.

Language

ASR, both translation directions and TTS.

Coverage

Native reviewers, accents, names and exact numbers.

Decision

Frozen gates, privacy owner and a human fallback.

Give a status assistant a narrow job.

One tool

Status and next action; no write or export.

Eight decisions

Identity, scope, district, memory and tool boundaries.

Two tickets

Acceptance evidence and named implementation owners.

Make the kickoff reviewable.

01	**Scope**	One repository; champion, backup and service owner.
02	**Acceptance**	A passing case and a denied boundary.
03	**Change**	A small local change, API review or completed paper evaluation.
04	**Delivery**	Reviewer, evidence, rollout and rollback.

Show the evidence.
Name the limits.

01

Claim

What behavior changed?

02

Evidence

Which test or observation supports it?

03

Limit

What still needs an owner?

Put a name and a date beside it.

Week 1 builds the checks. Weeks 2–4 deliver reviewed changes and citizen-visible improvements.

Champion + backup / Implementation owner / Acceptance evidence / Review date