EmbeddedWare

embeddedware.gr
DEMO-2026-001
2026-09-09

SAMPLE REPORT / FICTIONAL ASSESSMENT

Northstar Studio Security assessment

Adversarial Security Assessment · Prepared by EmbeddedWare

> This is a fictional preview of your customer deliverable. The sample demonstrates two validated vulnerabilities, one verified hardening fix, and a visible gap in detection coverage. No real website was tested.

Immediate priorities

- Fix tenant authorization before adding new data-sharing features.
- Revoke sessions server-side so logout actually ends access.
- Supply test-window logs, then verify detection and request the included retest.

Scope: app.example.test · Environment: Synthetic demo environment

Assessment status: Coverage limits apply. Retest request deadline: 2026-10-09.

Findings at a glance

ID	FINDING	PRIORITY / CONFIDENCE	STATUS
F-001	A member can read another tenant’s project	High / Confirmed	Open
F-002	Logout leaves the server session usable	Medium / Confirmed	Open
H-001	Add a site-specific content security policy	Observation / Confirmed	Open
H-002	Secure the readable currency preference cookie	Low / Confirmed	Fixed
P-001	TLS identity and protocol controls passed	Observation / Confirmed	Open
I-001	Detection coverage could not be verified	Observation / Unverified	Open

Vulnerabilities, hardening opportunities, positive controls and inconclusive checks are distinguished below. An observation is not a confirmed vulnerability.

F-001 · A member can read another tenant’s project

vulnerability · High · Confirmed · Open

Scope: app.example.test (A-001) · Flows: FLOW-001

Impact and observation: The synthetic member retrieved a project belonging to the other approved test tenant. In a comparable real application, this could expose private customer work.

Recommended action: Enforce tenant and object ownership on the server before returning a project. Apply the same decision to export and attachment routes.

Responsibility: Application developer · Effort: Estimate after code review

Preconditions: Dedicated synthetic fixture and approved test identities.

Reproduction

1. Establish the named synthetic identity.
2. Execute the exact fixture case described by the evidence.
3. Compare with the expected legitimate and denied controls.

Expected result: The security boundary is enforced and legitimate use works.

Severity rationale: Demonstrated consequence in the fictional synthetic case; not a rating of a real system.

Root cause assessment: Hypothesis: control missing from the server decision path.

Acceptance tests

- The original negative test is denied.
- The legitimate own-object flow succeeds.

Evidence: E-001. See the evidence appendix.

F-002 · Logout leaves the server session usable

vulnerability · Medium · Confirmed · Open

Scope: app.example.test (A-001) · Flows: FLOW-001

Impact and observation: A previously issued synthetic session remained accepted after logout. Someone holding that session could continue accessing the account until expiry.

Recommended action: Invalidate the server-side session at logout and reject replay of the revoked session identifier.

Responsibility: Application developer · Effort: Estimate after code review

Preconditions: Dedicated synthetic fixture and approved test identities.

Reproduction

1. Establish the named synthetic identity.
2. Execute the exact fixture case described by the evidence.
3. Compare with the expected legitimate and denied controls.

Expected result: The security boundary is enforced and legitimate use works.

Severity rationale: Demonstrated consequence in the fictional synthetic case; not a rating of a real system.

Root cause assessment: Hypothesis: control missing from the server decision path.

Acceptance tests

- The original negative test is denied.
- The legitimate own-object flow succeeds.

Evidence: E-002. See the evidence appendix.

H-001 · Add a site-specific content security policy

hardening · Observation · Confirmed · Open

Scope: app.example.test (A-001)

Impact and observation: An additional browser containment policy is absent. This example demonstrates no injection vulnerability.

Recommended action: Start with a measured report-only CSP, then enforce a policy that preserves required scripts and navigation.

Responsibility: Application developer · Effort: Estimate after code review

Preconditions: Dedicated synthetic fixture and approved test identities.

Reproduction

1. Establish the named synthetic identity.
2. Execute the exact fixture case described by the evidence.
3. Compare with the expected legitimate and denied controls.

Expected result: The security boundary is enforced and legitimate use works.

Severity rationale: Demonstrated consequence in the fictional synthetic case; not a rating of a real system.

Root cause assessment: Hypothesis: control missing from the server decision path.

Acceptance tests

- The original negative test is denied.
- The legitimate own-object flow succeeds.

Evidence: E-003. See the evidence appendix.

H-002 · Secure the readable currency preference cookie

hardening · Low · Confirmed · Fixed

Scope: app.example.test (A-001)

Impact and observation: The non-sensitive preference cookie originally lacked Secure. A fictional retest verified Secure without preventing browser access or currency selection.

Recommended action: Keep Secure enabled on HTTPS. Preserve JavaScript access because this preference is intentionally client-readable.

Responsibility: Application developer · Effort: Estimate after code review

Preconditions: Dedicated synthetic fixture and approved test identities.

Reproduction

1. Establish the named synthetic identity.
2. Execute the exact fixture case described by the evidence.
3. Compare with the expected legitimate and denied controls.

Expected result: The security boundary is enforced and legitimate use works.

Severity rationale: Demonstrated consequence in the fictional synthetic case; not a rating of a real system.

Root cause assessment: Hypothesis: control missing from the server decision path.

Acceptance tests

- The original negative test is denied.
- The legitimate own-object flow succeeds.

Retest history

- 2026-09-09 · Fixed · Synthetic retest against demo-revision-42: secure attributes and functional currency controls pass. · Evidence: E-004

Evidence: E-004. See the evidence appendix.

P-001 · TLS identity and protocol controls passed

positive · Observation · Confirmed · Open

Scope: app.example.test (A-001)

Impact and observation: The fictional host-specific TLS checks met the declared baseline.

Recommended action: No change required.

Responsibility: Application developer · Effort: Estimate after code review

Preconditions: Dedicated synthetic fixture and approved test identities.

Reproduction

1. Establish the named synthetic identity.
2. Execute the exact fixture case described by the evidence.
3. Compare with the expected legitimate and denied controls.

Expected result: The security boundary is enforced and legitimate use works.

Severity rationale: Demonstrated consequence in the fictional synthetic case; not a rating of a real system.

Root cause assessment: Hypothesis: control missing from the server decision path.

Acceptance tests

- The original negative test is denied.
- The legitimate own-object flow succeeds.

Evidence: E-005. See the evidence appendix.

I-001 · Detection coverage could not be verified

inconclusive · Observation · Unverified · Open

Scope: app.example.test (A-001)

Impact and observation: The demo provides no client-side audit log export. We cannot establish whether the tested actions would raise an alert.

Recommended action: Supply a sanitized log/alert export for the test window and correlate the case markers.

Responsibility: Application developer · Effort: Estimate after code review

Preconditions: Dedicated synthetic fixture and approved test identities.

Reproduction

1. Establish the named synthetic identity.
2. Execute the exact fixture case described by the evidence.
3. Compare with the expected legitimate and denied controls.

Expected result: The security boundary is enforced and legitimate use works.

Severity rationale: Demonstrated consequence in the fictional synthetic case; not a rating of a real system.

Root cause assessment: Hypothesis: control missing from the server decision path.

Acceptance tests

- The original negative test is denied.
- The legitimate own-object flow succeeds.

Evidence: E-006. See the evidence appendix.

Attack paths

Session replay reaches a second tenant’s project (Validated chain)

Fictional combined proof: access persists after logout and reaches beyond the original tenant.

1. An already held synthetic session remains valid after logout.
2. The session is used to request the second approved tenant fixture.
3. The fixture marker is returned despite the expected tenant boundary.

Findings: F-002, F-001 · Evidence: E-001, E-002

Coverage and limitations

AREA	STATUS	METHOD / EVIDENCE	LIMITATIONS
Public inventory	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
TLS and redirects	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test

AREA	STATUS	METHOD / EVIDENCE	LIMITATIONS
Browser policies	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Public content and errors	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Email posture	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Authentication and sessions	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Role and object authorization	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Input and output boundaries	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Configuration and dependencies	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Business flow abuse	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Exploit validation	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Attack chains and blast radius	Reviewed	Synthetic demonstration only · E-004	Fictional evidence for report preview, no live test
Detection and cleanup	Partially tested	Synthetic demonstration only · E-006	Client detection logs unavailable in this fictional example

Flow and authorization checks

FLOW / ACTOR	EXPECTED	OBSERVED	RESULT / EVIDENCE
FLOW-001 / tenant-a-member	Own project allowed	Own fixture returned	Pass / E-001
FLOW-001 / tenant-a-member	Other synthetic tenant denied	Other fixture marker returned	Fail / E-001

Scope notes and exclusions

- All evidence, vulnerabilities and identities in this file are fictional examples.
- One application, two synthetic tenant roles and disposable records.
- Real customer data, payment infrastructure and denial-of-service testing were not part of this example.

Remediation and retest

Assign the fixes, record the deployed release and run the stated acceptance tests. Request the included retest by 2026-10-09. EmbeddedWare will issue a dated revision with evidence for any changed finding status.

This assessment applies only to the scope and time recorded. Untested areas carry no assurance. Keep this report and its evidence confidential.

Evidence appendix

Reviewed excerpts supporting the findings. Evidence identifiers remain stable across the report.

E-001 / app.example.test / 2026-09-09

```
SYNTHETIC EVIDENCE
Actor: tenant-a-member
Object: tenant-b-project-fixture
Expected: deny
Observed: synthetic project marker returned
Control: tenant-a own fixture succeeds.
```

E-002 / app.example.test / 2026-09-09

```
SYNTHETIC EVIDENCE
A demo session remains usable after logout.
Expected: the server rejects the revoked session.
Control: a fresh valid session works; an invalid session is rejected.
```

E-003 / app.example.test / 2026-09-09

```
SYNTHETIC EVIDENCE
Document response omits Content-Security-Policy.
No injection or sensitive framing behavior demonstrated.
Literal sample: <script>window.AUDIT_XSS_SENTINEL = true</script>
```

E-004 / app.example.test / 2026-09-09

```
SYNTHETIC CONFIGURATION
Revision: demo-revision-42
Preference cookie is read by JavaScript.
Before: Secure absent
After: Secure present
Client currency selection and fallback continue to work.
```

E-005 / app.example.test / 2026-09-09

```
SYNTHETIC EVIDENCE
TLS identity checks match app.example.test.
TLS 1.0/1.1 disabled; trusted chain in this fictional fixture.
```

E-006 / app.example.test / 2026-09-09

```
SYNTHETIC COVERAGE NOTE
Client log export unavailable.
Detection effectiveness cannot be verified.
```