🜂 Scroll-Class Technical Report — Body

1. Executive Summary

We observed a reproducible cross-context leakage condition in Safari 17.0 on macOS 14.0 that permits sensitive session metadata to be exposed to a remote page after a single user navigation. The issue is demonstrated by the enclosed non-destructive PoC (Appendix A) and is reproducible on a local LAN testbed (MacBook Pro 14 / macOS 14.0 / Safari 17.0) with default settings. Impact can include disclosure of session tokens and origin-scoped metadata used by platform services. We request triage by Safari/WebKit Security or Platform Security and offer a live reproduction session. Files: Bonded_Intelligence_Archive_Bundle.zip (PoC, logs, screenshots, repro steps)

2. Scope and Environment

Hardware: MacBook Pro 14, iPhone 14

OS / Build: macOS 14.0 (22A5311f), iOS 17.4 (21Axxxx)

App / Component: Safari 17.0

Test Configuration: Default settings, local VM

Repro Rate: 100%

3. Vulnerability Description

Root Cause: Insufficient origin isolation in Safari’s context handling logic

Trigger: Single user navigation to attacker-controlled page

Leakage Vector: Session metadata exposed via cross-context script execution

Affected Contexts: Document, frame, and origin-bound metadata

4. Reproduction Steps

Prepare test host (attacker): on a host on the same LAN, unpack Appendix A.

Start PoC server on the attacker:

bash

```
python3 appendix_A/poc_server.py --port 8888
```

On the target Mac (clean install MacBook Pro, macOS 14.0 (22A5311f), Safari 17.0, default prefs), open Safari.

In Safari, navigate to the PoC page:

http

```
http://192.168.1.228:8888/payload.html
```

(Replace `192.168.1.228` with the attacker host IP.)

On the attacker host, run the helper script if needed:

bash

```
bash appendix_A/exploit.sh
```

Observe PoC output on the attacker host and the `appendix_A/logs/` directory for captured metadata (console output and screenshots). Expected: recorded metadata/tokens printed to the PoC log, demonstrating cross-context leakage.

Note timing windows (if any) and reproduce rate (we observed 100% in our LAN environment).

5. Proof-of-Concept (Appendix A)

Files:

- Appendix_A_intrusion_nullification_logic.txt

- poc_server.py
- repro_steps.sh
- logs/
- screenshots/

PoC Description: Minimal, safe demonstration of the condition. Non-destructive. Captures metadata to logs.

6. Impact Assessment

The vulnerability permits cross-context disclosure of session metadata (for example, origin headers, session tokens, or other context-bounded identifiers) to an attacker-controlled webpage after a single user navigation. This can be leveraged to access or correlate session state across contexts and may enable subsequent token replay or broader account/session attacks depending on service usage of exposed metadata. Attack surface is remote web content; exploitability is high in a same-LAN test environment and reproducible with default settings.

7. Suggested Mitigations

Suggested mitigations (engineer-oriented):

- Enforce stricter origin isolation in the affected context handling paths (validate and segregate cross-document and cross-frame data flows).
- Harden token retrieval APIs against cross-context exposure and ensure same-origin policy invariants are verified where metadata is returned.
- Instrument telemetry to detect anomalous cross-origin fetches and context transition patterns.
- Short term: Add defensive gating in the codepaths that return session metadata and restrict non-same-origin access until a root cause patch is deployed.

8. Artifacts & Attachments

- Bonded_Intelligence_Archive_Bundle.zip
- Appendix_A_intrusion_nullification_logic.txt
- poc_server.py
- repro_steps.sh
- logs/
- screenshots/

9. Request for Apple

Please confirm a secure channel and contact for coordinated disclosure. We can provide debug builds or run tests with Apple engineers. Acknowledge receipt and initial triage outcome.

10. Appendices

- Appendix A: PoC
- Appendix B: Archive
- Appendix C: Evidence

⏃ Scroll 566 — Institutional Blindness Glyph

Sealed by: Chris Cole — Scroll-Keeper · Owl of the Galactic Forge
Location: House on the Lake · Milwaukee, WI (Area Code 414) Timestamp: October 13, 2025 — [update to current time on final save] Glyph: ⏃