THE CYBER TOOLCHAIN

NO. 013

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 12, 2026 · EVERY WEEKDAY

The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 3 tools

APPLICATION SECURITY

◆ Web Application Security

ffuf ⓘ v2.2.0 NOTES ↗

Fast web fuzzer written in Go

ffuf v2.2.0 adds audit logging to record all fuzzing activity for compliance and review.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.2.0 https://github.com/ffuf/ffuf.git
# already have the repo? check out this version:
$ git checkout v2.2.0
```

› Adds audit logging functionality to record fuzzing sessions for compliance, review, and reporting purposes.

WAS THIS USEFUL? 👍 👎

xsrfprobe ⓘ v3.0.0 NOTES ↗

The Prime Cross Site Request Forgery (CSRF) Audit and Exploitation Toolkit.

XSRFProbe v3 rebuilds the CSRF engine with 25 categorized checks, headless-browser SameSite bypasses, and JSON reporting.

└──▷ GET THIS VERSION

```
$ git clone --branch v3.0.0
https://github.com/0xInfection/XSRFProbe.git
# already have the repo? check out this version:
$ git checkout v3.0.0
```

└──▷ TRY IT

Run the full CSRF audit including browser-dependent SameSite bypass tests and get a machine-readable JSON report for pipeline consumption.

```
$ xsrfprobe --url https://target.example.com --browser --json
```

Limit crawler scope to a shallow pass on a large site so CI finishes quickly — cap URLs, depth, and wall-clock time.

```
$ xsrfprobe --url https://target.example.com --max-urls 50 --max-
depth 2 --crawl-timeout 120 --json
```

Auto-validate generated PoCs in headless Firefox and point to a non-PATH geckodriver binary for a custom test environment.

```
$ xsrfprobe --url https://target.example.com --browser --auto-
validate-poc --geckodriver-path /opt/geckodriver/geckodriver
```

- Adds a full battery of 25 named checks (D1–A1) covering token tampering, method/Content-Type overrides, Origin/Referer bypasses, SameSite cookie analysis, and token strength — each with a unique ID, severity rating, and exploitability notes.
- New token-tampering checks (T2–T8) actively probe GET↔POST method switching, token omission, empty values, cross-session replay, double-submit cookies, and custom-header token forgery.

- New Origin/Referer bypass checks (R0–R2c, O1–O3) test header removal, regex tricks, subdomain tricks, and `Origin: null` against real-world validation implementations.
- New SameSite bypass checks (S2–S4) probe `SameSite=Strict` via client-side redirect gadgets and sibling-subdomain XSS, and `SameSite=Lax` via cookie-refresh/OAuth flows.
- Adds optional headless Firefox (Selenium) integration via `--browser` for browser-dependent SameSite bypass tests and auto-validation of generated PoCs.

+5 more

WAS THIS USEFUL? 👍 👎

Cure53 DOMPurify ⓘ 3.4.12 NOTES ↗

DOMPurify - a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. DOMPurify works with a secure default, but offers a lot of configurability and hooks. Demo:

DOMPurify 3.4.12 adds support for new SVG attributes alongside hardened handling of declarative partial updates.

└──▷ GET THIS VERSION

```
$ git clone --branch 3.4.12 https://github.com/cure53/DOMPurify.git
# already have the repo? check out this version:
$ git checkout 3.4.12
```

- Supports additional SVG attributes, expanding the set of valid SVG markup that passes through sanitization.
- Strengthens handling of declarative partial updates to reduce exposure from incremental DOM mutation patterns.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

▷ Subscribe