Intigriti Bug Bytes #233 - February 2026

BY AYOUB · FEBRUARY 20, 2026 · LAST UPDATED ON FEBRUARY 23, 2026

Hi hackers,

Welcome to the latest edition of Bug Bytes! In this month's issue, we'll be featuring:

- How a read-only Kubernetes permission turned into full cluster takeover
- AI agent autonomously finds a 1-click RCE
- Race condition in blockchain infrastructure worth billions
- Finding over 500 high-severity vulnerabilities with AI
- Analyzing static code false-positive free

And so much more! Let's dive in!

Intigriti 0126 CTF results are in

January's CTF revealed to be a tough one! Cryptigriti was presented as a deliberately vulnerable crypto exchange platform. The goal was to capture the flag by exploiting a client-side vulnerability that allowed transferring funds from the platform administrator account!

Quick recap:

- 7 hackers reported the correct flag
- First blood went to nandayo
- And 2 hackers wrote a nice write-up

If you want to put your hacking skills to the test, be sure to give Cryptigriti CTF a go before heading over to the Bugology, where you can find all the researchers' submitted solutions.

Intigriti 0126 CTF

[Read the write-ups]

Official write-up for INTIGRITI 0126 CTF

January's CTF challenge featured a crypto-themed CTF vulnerable to a postMessage vulnerability, which allowed for unauthorized fund transfers. Only 7 hackers managed to solve this CTF.

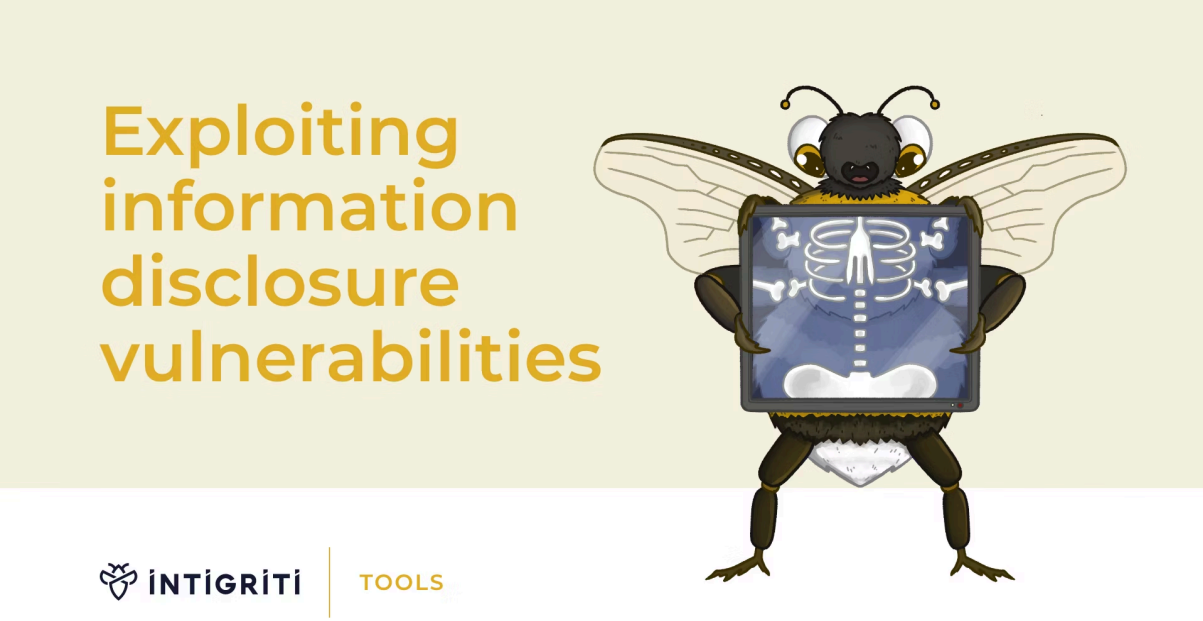
If you wish to read in-depth about what it took to solve Intigriti 0126, be sure to have a look at our official write-up for this challenge.

Intigriti 0126 CTF Challenge: Exploiting insecure postMessage handlers Cover Image

[Read the official write-up]

Blogs & videos

Exploiting information disclosure vulnerabilities



Exploiting information disclosure vulnerabilities Cover Image

Information disclosure vulnerabilities may seem easy to exploit... But they're surprisingly complex to find, making it difficult for us to score critical findings. In our latest article, we've lined up several ways to test and exploit information disclosure vulnerabilities, including practical examples to help you distinguish sensitive info disclosures from non-confidential strings.

- Many researchers overlook postMessage vulnerabilities, but when correctly chained, they can be deceptively powerful. January 0126 CTF featured a vulnerable DeFi platform that leveraged an unrestricted postMessage XSS to achieve full admin account compromise, ultimately allowing unauthorized fund transfers. If you're looking to level up your client-side hacking skills, this detailed walkthrough breaks down the exact steps to solve Intigriti 0126 CRYPTIGRITI CTF challenge.

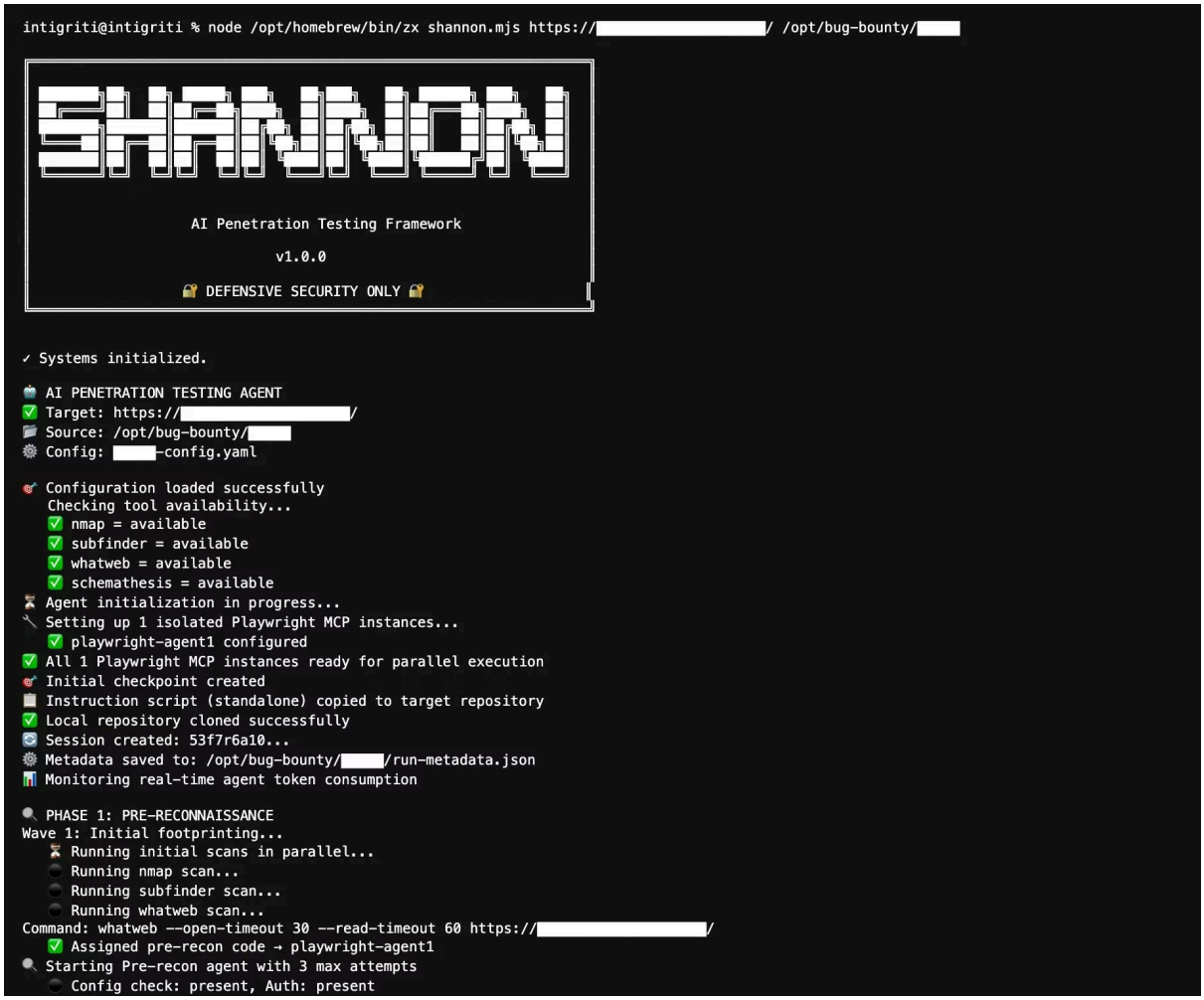
- During the month of December, we shared 31 bug bounty tips with the aim of helping (new) bug bounty hunters to find their first bug in 2026. In case you missed it, we've condensed all 31 tips into a single, comprehensive article.

- A single low-severity bug rarely makes a report stand out, but chain it with another, and you might land a critical. In our latest article, we break down how exploit chaining works in practice, covering pivoting, lateral movement, and privilege escalation, with input from our Hacker Community Lead and Pentest Delivery Manager. If you're looking for ways to turn informational findings into high-impact submissions, this one's for you.

Tools & resources

Tools

Shannon



Shannon

Have access to the source code? Be sure to try out Shannon, a fully autonomous, open-source AI static code analyzer that examines your source code to find vulnerabilities, then actually exploits them in the web browser to prove they're valid.

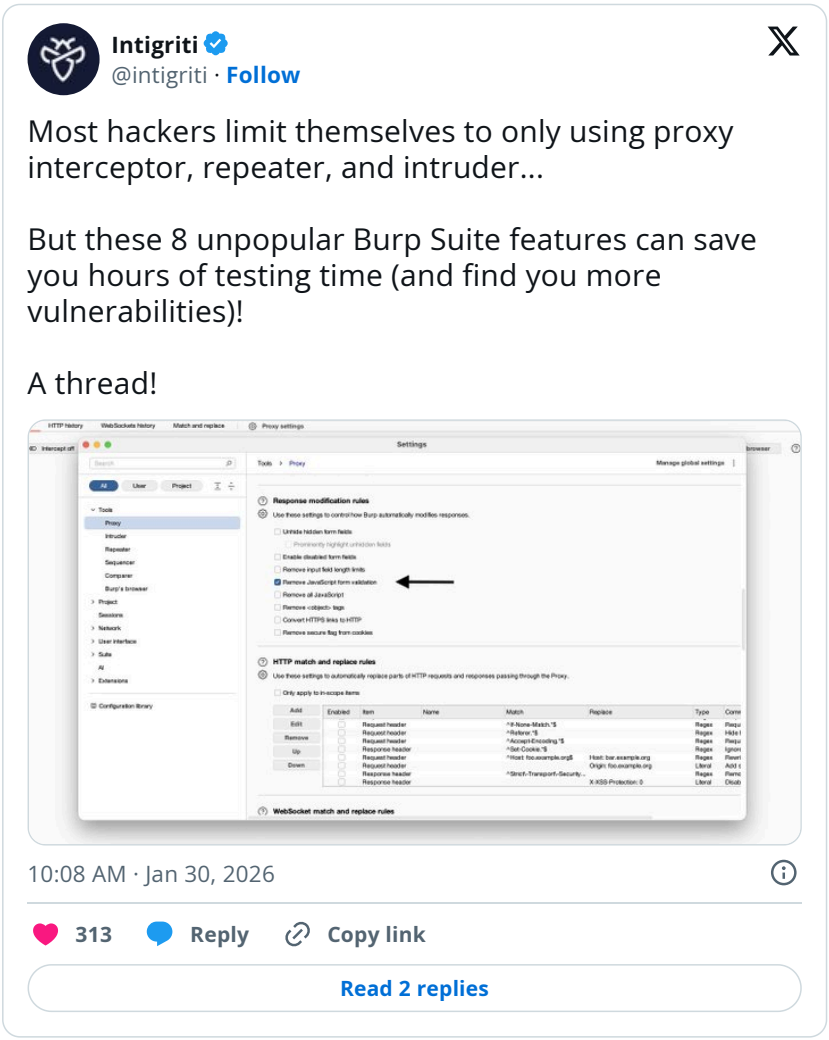
- Recon can be a tedious process... Bugbounty_tools by @thedawgyg is a repository containing simple bug bounty tools to help you speed up the reconnaissance process & find more vulnerabilities such as XSS, SSRF and much more.
- Finding an XSS vulnerability only to be held back by CSP can be frustrating... Luckily, using a tool like CSPBypass.com can help us bypass content security policies by searching for any documented JSONP endpoints. Wish to learn more about CSP bypassing? Be sure to read our comprehensive article on this topic.
- Rep+ by @BourAbdelhadi is a lightweight, AI-powered proxy interceptor that comes as a Chrome extension. Allowing you to easily intercept, modify, and replay requests without having to leave your

web browser. It's a useful tool if you want to limit the need to constantly switch between your browser and proxy interceptor for simple tasks.

- Caido has recently announced its new, official web extension that helps you easily proxy traffic from your web browser to Caido. It also includes a useful feature which auto-detects proxy listeners to prevent any manual setup.

Resources

Mastering Burp Suite for more vulnerabilities



Want to master Burp Suite? This thread is your key. We shared 8 underrated Burp Suite tricks that allow you to test web applications faster and more efficiently, plus to help you discover more bugs.

- Hacktron's research team discovered an RCE in Google's Antigravity IDE by exploiting the browser extension's overly permissive settings. The action allowed arbitrary file writes via path traversal, enabling code execution by placing files in the user's Startup folder.

- Hetmehta breaks down CVE-2026-25049, a critical type confusion RCE in n8n. Apparently, by sending non-string data types to the expression evaluator, an attacker can bypass TypeScript-based sanitization entirely, achieving command execution on the server.

- Some targets may look protected from the outside, while you're actually only 1 step removed from an RCE. In this post, @0xacb shares a breakdown of an interesting vulnerability chain that enabled @spaceraccoonsec to leverage a target returning a 404 page to full RCE via directory traversal and exposed JBoss console.

- @Rhynorater shares a quick tip on bypassing Chrome's auto URL decoding by tossing in %ff to keep your payloads intact.

- In this thread, we documented various ways to leverage your browser developer tools to find more vulnerabilities, such as CSP bypasses, DOM-based XSS, postMessage flaws, etc.

- In this article series, @thedawgyg shares how he uses fuzzing to discover new vulnerabilities. Part 1 and part 2 are now available.

- Anthropic (the team behind Claude AI) used their Opus 4.6 to find over 500 high-severity 0-day vulnerabilities in well-tested open-source codebases. Unlike fuzzers, the model reasoned about code, read git commit history to identify incomplete patches, and crafted targeted proofs-of-concept.

- @spaceraccoonsec built a GitHub Action-based threat intelligence workflow using LLMs to detect security patches in open-source repos before a CVE is published. His tool caught a command injection "never-day" in a Next.js canary release, highlighting the shrinking window between patch and exploit.

- Focal Security researchers discovered a cross-tenant vulnerability in Google Cloud's Apigee (CVE-2025-13292). By pointing Apigee at the GKE metadata endpoint to fetch a service account token, then escalating through Dataflow, they gained read/write access to verbose access logs and analytics data belonging to thousands of other organizations, including plaintext JWT tokens that could be used to impersonate end users.

- Ethiack's autonomous hacking agent, Hackian, discovered a 1-click RCE in OpenClaw (issued as CVE-2026-25253) in under 2 hours. By exploiting a WebSocket gateway URL override and missing origin validation, an attacker could potentially leak auth tokens and execute arbitrary commands on the victim's machine (even on local instances).

- @ozgur_bbh discusses bug hunting strategies in the age of AI, including some helpful tips.

- @3nc0d3dGuY shares a practical guide on how to fuzz and hack APIs, covering how to understand API structures, identify authorization mechanisms, and effectively utilize tools like ffuf and Burp Suite for fuzzing across various parameters.

- @mavlevin reveals a race condition in Flashbots' MEV relay that could have allowed traders to win Ethereum block auctions without paying their bids. The bait and switch exploited a non-atomic check-then-act (or TOCTOU) pattern in Redis, enabling a swap of the winning payload between database reads.

- @grahamhelton3 documents how a commonly granted Kubernetes nodes/proxy GET permission enables full RCE in any pod across a cluster.

- @castilho101 demonstrates how to steal Salesforce OAuth tokens by abusing the WAF layer.

- @mokhansec demonstrates how a simple IDOR in a crypto platform's CSV export feature exposed the full trading histories.

- @j_zere chains a cache deception vulnerability with a client-side path traversal (CSPT) to achieve account takeover. Neither bug was exploitable alone, but combined, the CSPT forced an authenticated request to a cacheable endpoint, letting the attacker retrieve the victim's token from the CDN.
- @samm0uda found multiple XSS vulnerabilities in Meta's Conversion API Gateway ($312.5K total bounty). A stored JavaScript injection in the backend allowed attacker-controlled code to execute on www.meta.com and millions of third-party sites that loaded the shared analytics script.
- @JatinBanga18 discovered a bug that exposed private Instagram posts to anyone.
- FearsOff disclosed a Cloudflare zero-day that enables access to any host globally via ACME exploitation.

Company news

2026 Kickoff Event: Intigriti turns 10

We're officially entering our 10th year, and we kicked things off with our annual company kickoff, bringing together the full team to reflect, celebrate, and plan for what's next.

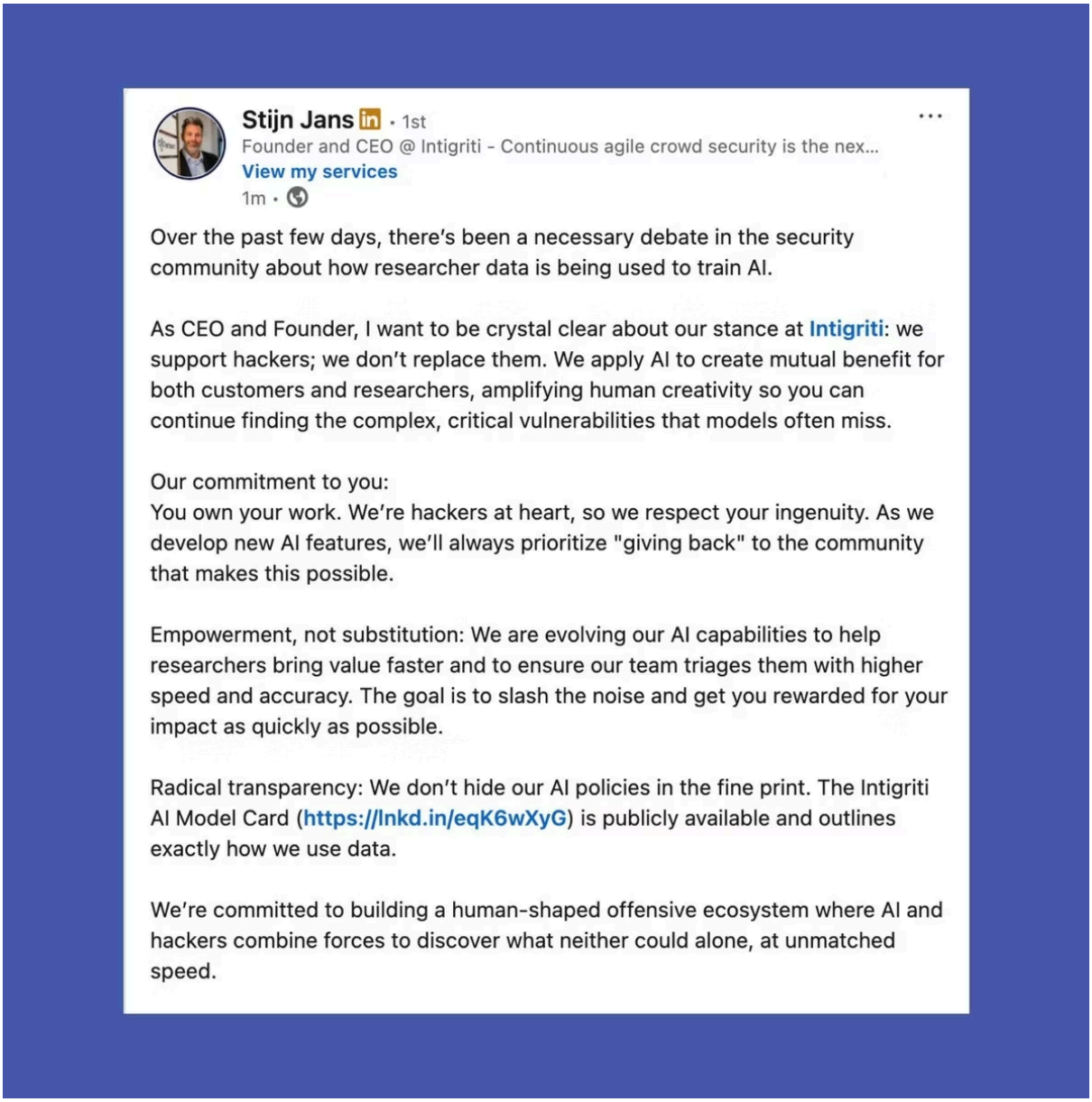
The highlight was a customer and hacker panel featuring Norberts Dulbinskis (Red Bull), Chris Lakin (Dropbox), and our very own Flo van der Vlist, who's closing in on 1,000 vulnerabilities found on our platform. Key takeaways:

- Speed matters. Dropbox's public program went live in just 2–3 weeks.
- Community scales security. Red Bull engages researchers through local hubs and recognition.
- AI is a tool, not a replacement for human expertise when it comes to complex vulnerabilities.

View LinkedIn post

Statement on AI & researcher IP

Our CEO, Stijn Jans, shared Intigriti's stance on AI and researcher IP. Read the full statement on LinkedIn.



Intigriti's statement on AI & researcher IP

[Read the full statement]

Feedback & suggestions

Before you click away: Do you have feedback, or would you like your technical content to get featured in the next Bug Bytes issue? We want to hear from you. Feel free to send us an email at support@intigriti.com or DM us on X/Twitter, and we'll take it from there.

Did you like this Bug Bytes issue? Consider sharing it with your friends and tagging us along on X/Twitter, Instagram, or LinkedIn.

Wishing you a bountiful month ahead,

Keep on rocking!

AUTHOR

Ayoub

Senior security content developer

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com