Intigriti Bug Bytes #232 - January 2026

BY AYOUB · JANUARY 16, 2026

Hi hackers,

Welcome to the latest edition of Bug Bytes (and the first of 2026)! In this month's issue, we'll be featuring:

- Hijacking official AWS GitHub repositories
- New anonymous bug bounty forum
- Finding more IDORs & SSRFs using a unique methodology
- New JavaScript file scanner to find hidden endpoints

And so much more! Let's dive in!

Intigriti SantaCloud CTF results are in

December 2025 was a blast! Thanks to our highly engaged community members, we successfully hosted 2 CTF challenges in one month. SantaCloud CTF was special as we switched up the rewards pool. Instead of the usual swag vouchers, the winners took home a limited-edition t-shirt.

Quick recap:

- 84 hackers reported the correct flag
- 6 winners received a cool t-shirt
- And 20 hackers wrote a nice write-up

This CTF challenge represented an administrative cloud portal that enabled the management and distribution of all packages santa had to deliver. Researchers were tasked with gaining initial access (without bruteforcing) and capturing the flag by exploiting two separate vulnerabilities.

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

Intigriti SantaCloud CTF

[Read the write-ups]

Official write-up for 1225 Thanos CTF

Intigriti 1225 Thanos-themed CTF by [Renwa] featured 6 different client-side security vulnerabilities, which, when chained, allowed for XSS on the root domain. Only 6 hackers managed to solve this CTF.

If you wish to read in-depth about what it took to solve Intigriti 1225, be sure to take a look at our technical article, reviewed by the challenge author.

December CTF Challenge: Chaining XS leaks and postMessage XSS Cover Image

[Read the official write-up]

New: Hacker Spotlight Series

We launched a new monthly hacker spotlights series to share how researchers break into bug bounty, with the occasional practical tips for beginners and intermediate hunters.

Our first hacker spotlight guest is Isira Adithya. We chatted with him to learn how he went from starting at 16 to achieving financial independence and building a thriving security career by 21, including:

- How he kicked off his bug bounty journey
- How dedication and curiosity unlocked incredible opportunities
- What the "hacker mindset" means to him
- Practical tips for anyone considering bug hunting as a path into cybersecurity

From the first bug to financial independence. How bug bounty hunting shaped Isiras path

[Dive deeper into his story]

New podcast series: Office Hours

Yesterday was the first episode of Office Hours. In this new podcast series, we'll sit together with bug bounty hunters & security researchers to answer YOUR bug bounty & web security-related questions on Discord & Twitter/X Spaces!

Yesterday's episode featured Émile, the co-founder of Caido. We talked all about using proxy intercepting to find bugs, the future of Caido, and how it'll empower bug bounty hunters & security researchers like you during security testing.

Recordings will be published soon. Be sure to keep an eye out for our socials to be notified.

Intigriti Office Hours

[Join our Discord community]

Reflecting on 2025, shaping 2026

We sat down with our C-suite to talk about 2025 wins, lessons learned, and what's coming for Intigriti in 2026.

In our conversation, we discussed:

- Biggest milestones from 2025
- Strategic priorities for this year
- New partnerships and platform innovations
- How we're empowering bug bounty researchers in 2026

Reflecting on 2025, shaping 2026. What Intigriti leadership has to say.

[Dive into the full interview]

2026 Security forecast report

A lot happened in 2025, and we've worked hard to distill the most important key elements that will shape the future of cybersecurity in 2026 into a single unified report.

Cut through the noise with real data on:

- Navigating AI hallucination
- Supply chain threats
- What actually matters in 2026

2026 Security forecast report

Download your copy

Latest platform updates

New researcher earnings API

We're excited to announce a new API endpoint specifically designed to give security researchers a comprehensive overview of their payout details. This endpoint allows you to retrieve comprehensive details for all your bounties, bonuses, and pentest payouts. Enabling you to track your earnings and integrating payout data into your personal workflows.

Learn more

New: Improved hacker profiles

We introduced a new profile enhancement that allows ethical hackers to display their reputation points from other major bug bounty platforms alongside their Intigriti achievements. This optional feature gives hackers full control to showcase a more complete view of their experience and expertise, while ensuring Intigriti's built reputation remains clearly represented. By unifying fragmented reputation data, we're helping hackers present a complete professional profile that strengthens trust and recognition across the researcher community.

Sign in to your account

New: Notification upon mitigated vulnerability

We deployed a new notification system that alerts researchers when their duplicate submission has been resolved, inviting you to test the fix and search for potential bypasses.

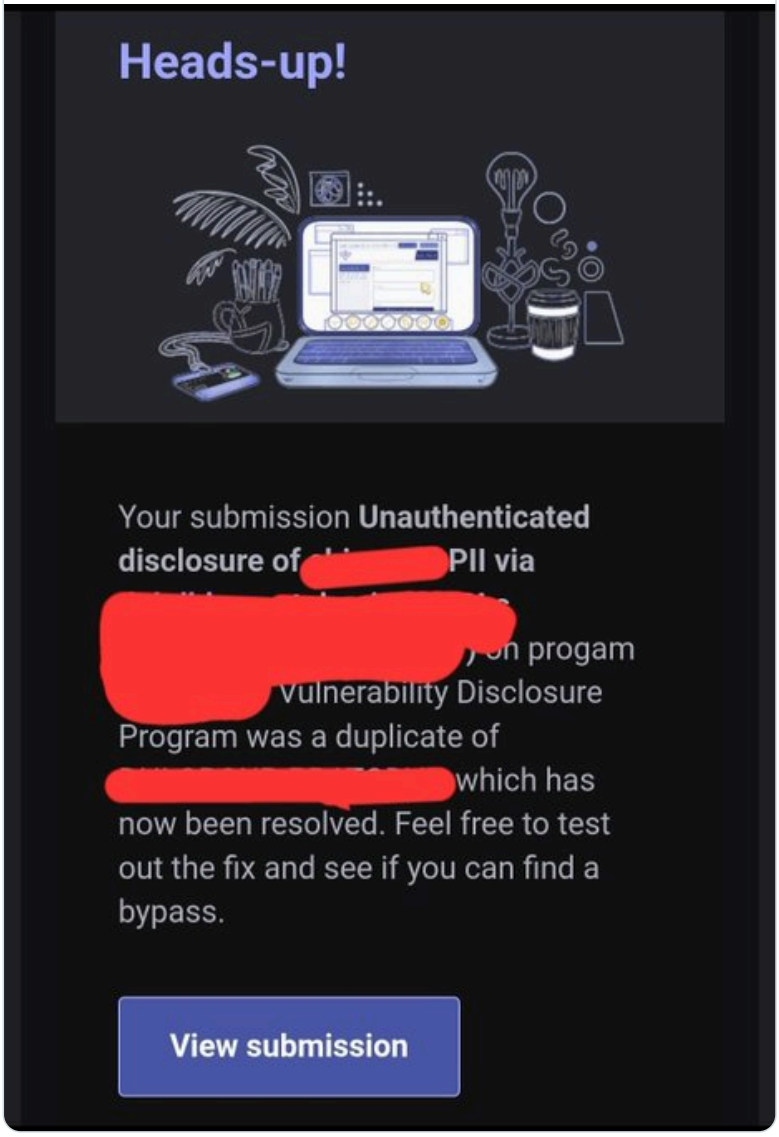
This feature ensures that hackers stay informed about resolution status and creates opportunities to earn additional bounties by identifying new bypasses to the initial remediation.

Intigriti
@intigriti · **Follow**

This is a new feature we deployed!

Whenever your duplicate submission gets resolved, we'll notify you and invite you to find bypasses!

> **n3dir** @n3dir_
> I received a retest email for a duplicate for the first time. I reported this one a month ago. @intigriti
>
> I still haven't found a valid report, but I will not stop grinding.



7:52 PM · Dec 22, 2025

91 Reply Copy link

Read 6 replies

[Start hunting on Intigriti]

Blogs & videos

Chaining XS leaks and postMessage XSS

December CTF Challenge: Chaining XS leaks and postMessage XSS Cover Image

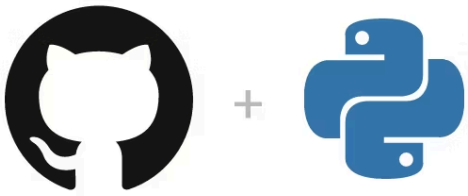
XS-Leaks and postMessage vulnerabilities are deceptively powerful when chained together, yet many researchers overlook them in favor of more obvious attack vectors. This December's CTF challenge features a multi-stage exploitation technique combining client-side timing attacks, CSP bypasses, and DOM manipulation to achieve XSS on the main domain. If you're looking to level up your client-side hacking skills, this detailed walkthrough breaks down the exact steps to solve Intigriti 1225 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're planning to publish a resource that consolidates all 31 tips into a single document. Be sure to follow us across our socials to be notified.
- Next.js is a popular and widely used React framework, its complexity can introduce critical security flaws like Server-Side Request Forgery (SSRF). This article dives into advanced SSRF exploitation techniques targeting Next.js applications.

Tools & resources

Tools

JSAnalayzer



jenish-sojitra/**JSAnalyzer**

JSAnalyzer

Do you find analyzing JavaScript files too hard? JSAnalyzer is a new Burp Suite extension by @_jensec that auto-extracts API endpoints, URLs, and sensitive links from JS. It also performs smart noise filtering to minimize false positives and prevent reporting of random, verbose strings.

- We know some targets introduce hardened measures against XSS attacks, including restricting input lengths. Tiny XSS Payloads is a cheat sheet by @terjanq featuring all types of short payloads, with the shortest payload counting only 17 characters!

- BugBounty.Forum is a newly launched, independent community forum where researchers share knowledge, ask questions related to bug bounty, and help each other out. It's the place to learn from others' experiences and engage in discussions with credible community members.

- SSRFs are fun to find, but it's always nice to escalate them to RCEs. Surf by @assetnote helps you discover hidden SSRF targets in cloud environments. It works by scanning a list of hosts to identify domains that are configured to only accept traffic from internal sources, perfect candidates for SSRF exploitation that bypass traditional IP-based filters.

Resources

Finding more IDORs

In some cases, user sessions can be overwritten through trivial means, allowing for easy authorization bypasses, such as IDORs. @the_IDORminator explains how abusing certain in-app components can lead to session stuffing and help with identifying more IDORs.

- IDORs are simple to exploit but quite complex to find. This researcher failed to enumerate valid password hashes required for the vulnerable request, but learned that this parameter wasn't validated for SSO-connected accounts, allowing for unauthorized account deletion.
- SSRFs are cool bugs and pay out a lot. @thedawgyg shares his story of earning over $1M by only reporting SSRF vulnerabilities.
- @sl4x0 shows how a chain of public CMS misconfigurations can lead to full remote admin access. This article is a clear example of understanding how smaller issues can be further leveraged into much more critical vulnerabilities.

- @_bergee_ shares a fascinating story of finding two critical vulnerabilities, including an RCE via command injection, within a single .zip file. Your reminder to always test file uploads thoroughly for various vulnerabilities.
- @H4cktus explores how even a seemingly innocent /health endpoint can be weaponized to compromise a multi-billion-dollar company.
- We all had to start somewhere. @jugnupanchal2812 documents their journey from beginner to earning their first badge by effectively hunting for leaked secrets. If you're planning to start bug bounty in 2026, you may learn a thing or two from this article.
- @BourAbdelhadi showcases how using Rep+ (a lightweight Chrome DevTools extension to intercept requests) led to identifying a critical Supabase JWT exposure, enabling the enumeration of tables and sensitive data.
- @zhero__ shares invaluable insights into the mindset, strategies, and the alchemy behind successful bug bounty hunting, while highlighting the importance of continuous learning and iteration to light. Although this is a non-technical article, it remains a highly insightful read for anyone trying to improve their bug bounty skills.
- @iamgk808 shares an incredible story of his bug bounty journey, detailing how persistence through failures ultimately led to significant earnings. The article includes several tips you can apply to become better at hunting for bugs.
- Wiz uncovered a critical vulnerability in AWS CodeBuild, allowing attackers to hijack the official AWS GitHub repositories and leak secrets in build logs.
- If you followed us on Twitter in 2025, you may recall us from numerous bug bounty tips and web hacking tricks we shared. We've scoured our timeline and listed the 20 most helpful bug bounty tips we shared in 2025 in a single thread. If you enjoy our content, be sure to follow.

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