Intigriti Bug Bytes #235 - April 2026

BY AYOUB • APRIL 24, 2026 • LAST UPDATED ON APRIL 25, 2026

Hi hackers,

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

- Compromising an NPM package with 40M weekly downloads
- Bypassing Cloudflare WAF for a full ATO
- 20-part series on exploiting JWT vulnerabilities
- First Intigriti Bug Bounty Meetup

And so much more! Let's dive in!

Common misconceptions about bug bounty, debugged

Bug bounty still gets misunderstood by security teams, execs, and even hackers themselves. We've compiled the most common misconceptions we hear, from "it's just pentesting with a different name" to "only big companies can run a program", and broke down what's actually true.

The A(I) future of bug bounty

AI is reshaping how researchers hunt, how triagers review, and how programs scale. In this article, we examine where AI is already making a real difference in bug bounty, where it's falling short, and what the next few years might look like for the researchers adapting alongside it.

Vulnpocalypse Now? How AI is changing vulnerability discovery

Are we in a "vulnpocalypse", a world where vulnerabilities are discovered and exploited faster than they can be patched? In our latest article, Intigriti's COO Ed Parsons takes a grounded look at what AI is actually doing to vulnerability research right now: the rise in AI-assisted submissions we're seeing on the platform, where the hype around Claude Mythos and Project Glasswing starts to break down, and why human researchers aren't going anywhere despite the noise.

Vulnpocalypse now? How AI is changing vulnerability discovery

Upcoming: Intigriti Bug Bounty Meetup in Brasov

Our Hacker Ambassador Cristian (@CristiVlad25), together with the Brașov Cybersecurity Community, is hosting the next Intigriti Bug Bounty Meetup in Romania! Whether bug bounty is something you're looking to get into, or you're already a seasoned hunter, come talk bounties and meet others doing the same.

Event details:

May 14, 2026

Hotel Ambient (Sala Millenia), Brașov, Romania

18:00 – Open End

Reminder: Spots are limited & registration is required.

Intigriti Bug Bounty Meetup in Brasov

Save my spot

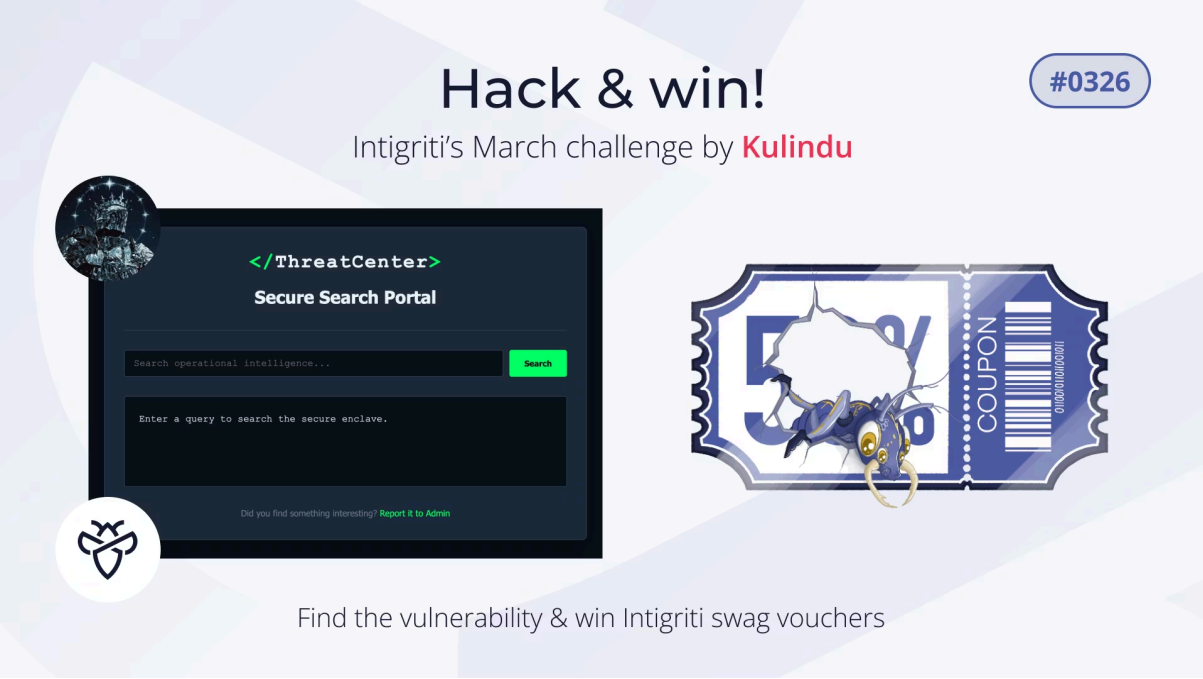
Intigriti 0326 CTF results are in

March's CTF challenge featured another deliberately vulnerable target, with the goal of capturing the flag using an XSS. A strict CSP and a restricted DOMPurify implementation stood in the way, so the trick was to chain DOM clobbering with a CSP bypass to ultimately read the admin's flag.

Quick recap:

- 71 hackers reported the correct flag
- First blood went to infernosalex
- And 19 hackers wrote a nice write-up

If you want to put your hacking skills to the test, be sure to give the 0326 CTF a go before heading over to the Bugology, where you can find all the researchers' submitted solutions.



Intigriti 0326 CTF

Blogs & videos

BugQuest 2026: 31 Days of Broken Access Control

BugQuest 2026: 31 Days of Broken Access Control Cover Image

Broken access control has held the top OWASP Top 10 spot for a reason, they're everywhere, and most researchers still only scratch the surface of what's possible. BugQuest 2026 was our 31-day campaign built to help researchers land their first BAC bug, with a new challenge, tip, or walkthrough every single day of the month. If you missed it live, the full series is still available to work through at your own pace,

and it's one of the best on-ramps we've published for anyone trying to get serious about access control testing.

- **AI-generated vulnerability reports are on the rise,** but the bar for what constitutes a valid report is only getting higher. Our in-depth article covers a complete guide on how you can use AI for report writing, including how to get real value out of LLMs without falling into the usual traps, like submitting hallucinated payloads, unvalidated PoCs, or generic AI-worded replies to triager feedback. Worth a re-read, especially if you've been leaning on AI in your workflow.
- **Curious how the CTF 0326 challenge was meant to be solved?** Our official write-up walks you through the entire exploitation chain, from the initial DOM clobbering to CSP bypass and final flag capture. A great read, whether you solved it or got stuck halfway.

Tools & resources

Tools

XNLDorker

XNLDorker

Google dorking is essential for recon, but having to do it manually can become tedious. Xnldorker by @xnl_h4ck3r simultaneously pulls search results from Google, Bing, DuckDuckGo, and more with concurrent anti-bot detection and automatic result deduplication built in. If you rely on dorking as part of your recon pipeline, this one will save you a lot of manual hassle.

- **Testing for XXE via file uploads can become complex and time-consuming.** OXML_XXE by @willvandevanter embeds XXE and XML exploits into a wide range of file

formats, such as DOCX, XLSX, PPTX, ODT, SVG, and more, so you can spray payloads across any upload endpoint without having to hand-craft each format yourself.

- **Digging through URL shortener archives by hand takes forever.** URLHunter by @utkusen_en searches exposed URLs from Bitly, Google, and other shortener services using URLTeam's archives, making it a quick way to surface forgotten or leaked links tied to your target.

- **Struggling to enumerate more subdomains using traditional wordlists?** CewlAI by @rez0__ leverages AI to analyze patterns in your seed domain list and generate new domain variations based on your target's naming conventions.

Resources

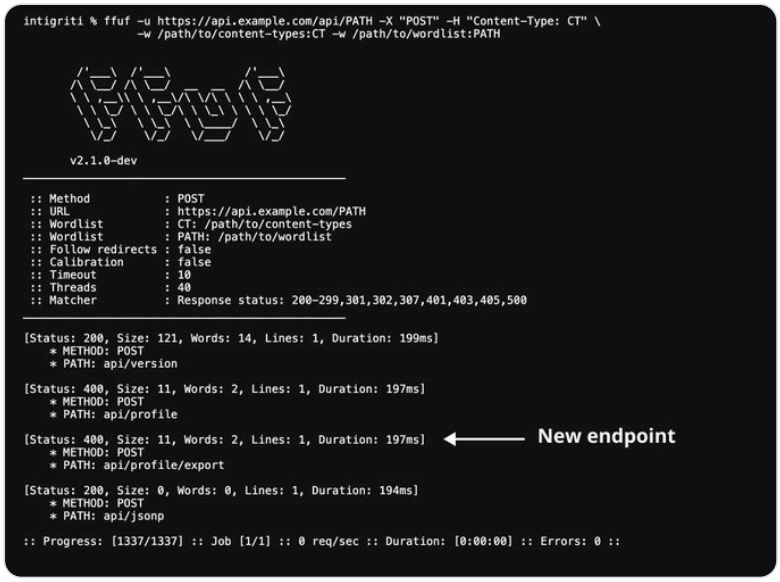
Fuzzing with multiple content types

Intigriti
@intigriti · **Follow**

Fuzzing with no content-type set
Fuzzing with multiple content-types (application/json, application/xml, application/x-www-form-urlencoded)

Quick tip! Always fuzz with multiple content-types! Some app routes and API endpoints only accept specific content-types!

Example Show more



9:03 AM · Mar 30, 2026

359 Reply Copy link

Read 4 replies

Some APIs and application endpoints are configured to only **respond when a certain content type is supplied within your request.** Next time, when fuzzing, always try to fuzz with multiple Content-Type headers. Here's a simple trick to do so with Ffuf!

- **CSPT is quietly baked into almost every major frontend framework.** @xssdoctor breaks down how client-side path traversal appears across React, Angular, Vue, and others, with concrete examples of how framework defaults hand you the dot-dot-slash for free. Read the full piece on CTBB Labs.

- **Finding an XSS only to have Cloudflare's WAF stand in your way can be quite frustrating.** @YourFinalSin shared a payload using the oncontentvisibilityautostatechange event handler that slips past Cloudflare's filter, and then escalated the bypass all the way to a full account takeover.

- **Some cloud infrastructure bugs are impactful enough to help you gain access to other tenants.** @omer_asfu at Focal Security published Kicking the Bucket, a deep dive into critical RCE and cross-tenant exploits across three different GCP products.

- **Supply chain attacks are increasingly becoming more impactful.** @0xLupin compromised an NPM package with 40 million weekly downloads in his first week on the job, a great read on how quickly a small oversight in package maintenance can blow up.

- **Every JWT write-up online covers the same two or three attacks and then stops.** @pingiskok got tired of jumping between 40 blog posts and wrote a 20-part series covering JWT exploitation, all in one place.

- **Pre-auth RCE chains don't come around often.** WatchTowr Labs published a full breakdown of their Progress ShareFile pre-auth RCE chain (CVE-2026-2699 and CVE-2026-2701), walking through every step from initial access to code execution.

- **iText's PDF parser has been a recurring source of XXEs, and it still continues to cause issues.** @saur1n shares From PDF to Pwn, detailing an out-of-band XXE found through a PDF upload on a real target.

- **Bypassing SSRF protections becomes significantly more complex when the fix covers IPv6 and TOCTOU attacks.** @red_darkin shares A Real SSRF Story, walking through a bypass that used IPv6 and redirect handling to defeat the filter.

- **Is AI killing bug bounty?** @NahamSec tackles the question head-on in his latest video, with his usual mix of practical perspective and community context.

- **Some internal networks are one non-resolvable hostname away from being wide open.** @damian_89_ shares how he gained access to Starbucks' internal network using a non-resolvable hostname, a solid reminder that unusual DNS configurations can help with exploitation.

- **Proving a blind SQLi is significantly more challenging when a WAF rate limit is standing in your way.** @0xabfe walks through bypassing WAF rate limiting to get a clean, demonstrable PoC for a blind SQL injection.

- **A full-read SSRF is one of those primitives that almost never shows up cleanly anymore.** @eib____ shares how he chained OAuth Dynamic Client Registration, open URL redirects, and path normalization quirks into a full-read SSRF.

- **Cookie injection is an underappreciated XSS sink.** @RenwaX23 shows how a same-site DOM XSS can be triggered through cookie injection, with a side note on how fast AI-assisted hackers are closing in on this bug class.
- **Clickjacking isn't dead, it's just moved to the middle mouse button.** This researcher introduces an auxclick-based variant that sidesteps several of the classic defenses.
- **Five chained XSS turned into €5,000.** @shivangmauryaa shares how he chained 5 XSS at xyz.com into a 5000€ payout, with a breakdown of each finding and how they stacked.
- **$2M in bounties later, some lessons are worth sitting down for.** @NahamSec looks back on a decade in bug bounty in 'I Earned $2M Hacking. Here's Everything I Know', equal parts retrospective and practical advice.
- **An XSS can sometimes be escalated into an ATO.** @medusa_0xf shares a video walkthrough of a bug chain that ran XSS WAF bypass OAuth code theft full account takeover, with the chain getting out of hand in the best possible way.

Company news

Intigriti's first Ambassador Bug Bounty meetup in Stuttgart

Our first German meetup took place in Stuttgart, and the turnout was incredible! Everyone, from complete beginners to seasoned hackers, showed up. Huge thanks to our new Hacker Ambassador, Marc-Oliver (@marcolivermunz), for organizing, Alex Olsen (@appSecExp) for flying out from the UK to provide on-site support, and Valeriy Shevchenko (@Krevetk0Valeriy) for an awesome talk.

A few takeaways from the day worth carrying home:

- Understanding beats tools every time
- Always question your assumptions
- And consistency beats perfection

This definitely won't be our last German meetup.

Intigriti's first Ambassador Bug Bounty meetup in Stuttgart

Feedback

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 community@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