# Intigriti Bug Bytes #237 - June 2026

BY AYOUB · JUNE 26, 2026

## Hi hackers,

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

- A 10-year-old pre-auth RCE in phpBB
- Earning $500K hacking Google with AI
- Reading any Salesforce Marketing Cloud account's emails
- New DOMPurify sanitizer bypass
- Mapping abandoned S3 buckets to redo SolarWinds at scale

And so much more! Let's dive in!

## Using AI the smart way: interview with Cristian Zot (CristiVlad25)

Cristian Zot, better known as @CristiVlad25, needs little introduction. An active researcher, experienced pentester, and Intigriti Hacker Ambassador, he is a familiar voice on our Intigriti Office Hours podcast, a regular at platform meetups, and most recently took the stage at our Bounty Sync in London to lead a discussion on AI in security.

In this interview, we continue that conversation, with a refreshingly grounded take on using AI the smart way in offensive security workflows.

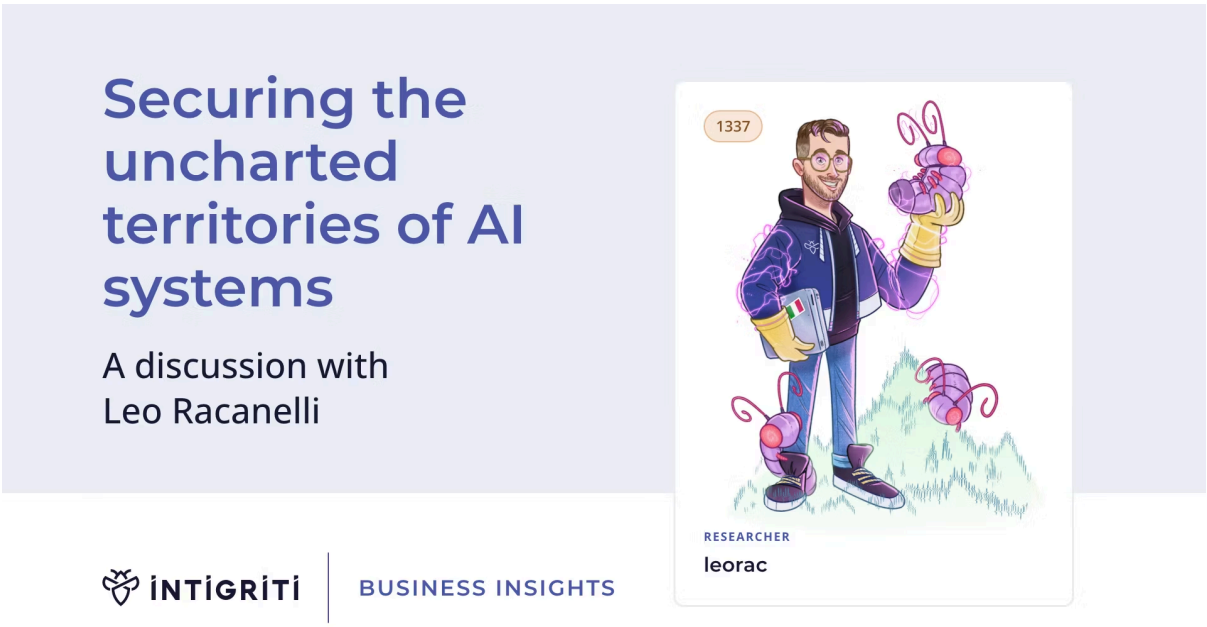

Using AI the smart way. Interview with Cristian Zot (CristiVlad25)

# Securing the uncharted territories of AI systems: a discussion with Leo Racanelli

In our latest blog, we speak with Leo Racanelli, bug bounty hunter and Intigriti Ambassador, about what AI means for the people working closest to the edge of security. The discussion covers why AI applications introduce a new breed of vulnerabilities, how AI is becoming a teammate in bug bounty workflows, why human creativity remains essential when testing AI systems, and the value of building playbooks and libraries of AI findings.

As AI adoption accelerates, securing these systems takes more than traditional approaches. It takes curiosity, collaboration, and a deeper understanding of how AI can be manipulated in the real world.

Read the full discussion




Securing the uncharted territories of AI systems. A discussion with Leo Racanelli

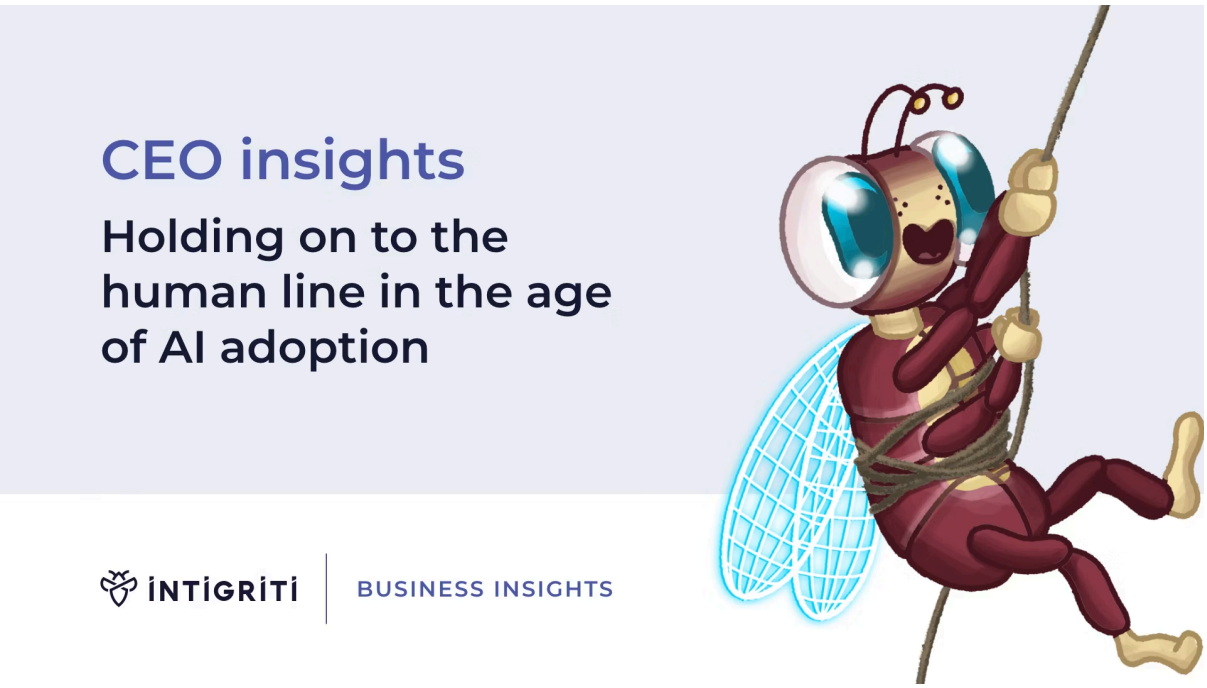
## Marketer by day, bug hunter by night: interview with Stefan Goossens (G0053)

We sat down with Stefan Goossens, better known as G0053 (@g0053me), to talk about his journey into bug hunting, balancing hacking with a full-time career, and what keeps him motivated in the cybersecurity community. Stefan's story is a good reminder that you do not need a traditional path to get into security. Curiosity, consistency, and a willingness to learn can take you a very long way.


Marketer by day, bug hunter by night. Interview with Stefan Goossens (G0053)

# CEO insights: holding on to the human line in the age of AI adoption

In his latest post, our CEO shares his perspective on what AI adoption means for security teams, and why keeping people in the loop matters more than ever as automation expands. If you are thinking about how to balance AI tooling with human judgment in your own program, this one is worth a read.




CEO insights: holding on to the human line in the age of AI adoption

# Intigriti named Best Security Company at the 2026 SC Awards Europe

We are thrilled to share that Intigriti has won Best Security Company (under 250 employees) at the 2026 SC Awards Europe! Judged by an independent panel of Europe's leading cybersecurity experts, this award highlights our commitment to setting the benchmark for innovation, resilience, and crowdsourced security leadership.

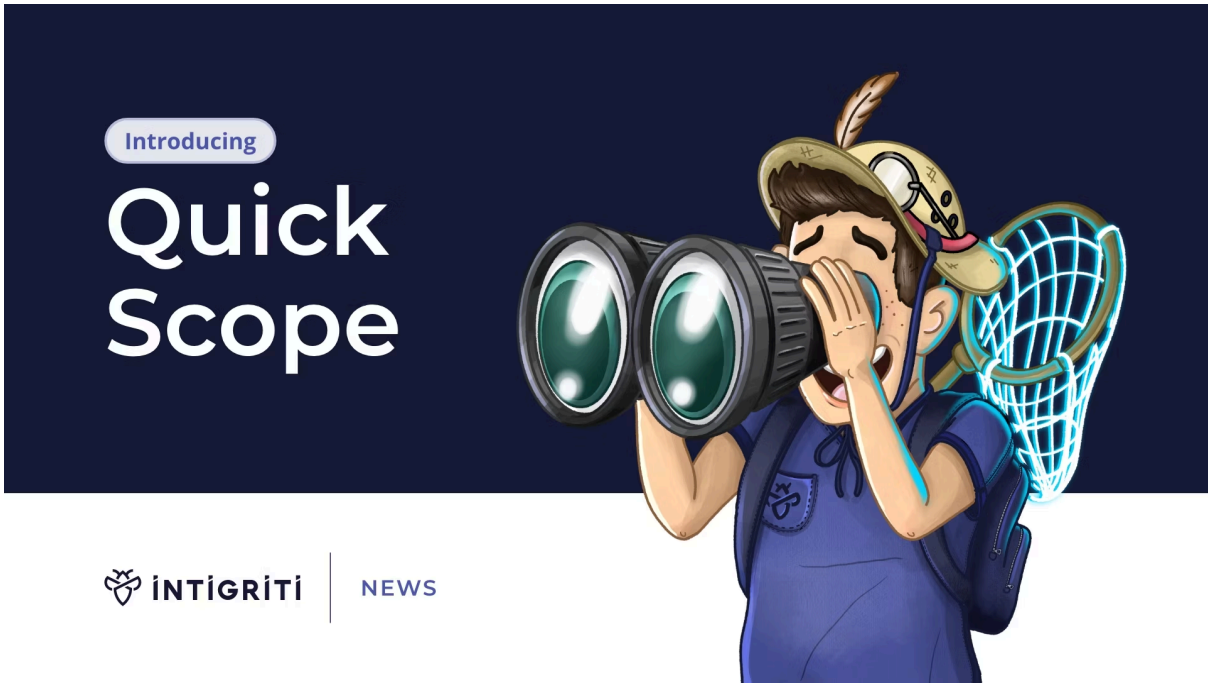
A sincere thank you to our researcher community, our customers, and our internal team for making this recognition possible.


Intigriti Wins Best Security Company of the Year, 2026, SC Awards Europe

# Intigriti Quick Scope (IQS) wins PortSwigger's 2026 Burp Suite Extension Award

It is now official: Intigriti Quick Scope (IQS), our first official Burp Suite extension, has won first place in the 'Best API & Specialist Testing' category in PortSwigger's 2026 Burp Suite Extension Awards.

PortSwigger runs an annual community-voted competition recognizing the best Burp Suite extensions of the year. Our category featured 16 nominated extensions, and the result came down to a community vote. A huge thank you to everyone who voted for us.




Introducing Intigriti Quick Scope Cover Image

# Intigriti recognised in the Deloitte EMEA Technology Fast 500 2025

We are proud to share that Intigriti has been recognized in the Deloitte EMEA Technology Fast 500 2025, the ranking of the 500 fastest-growing technology companies across Europe, the Middle East, and Africa. Recognition here reflects our growth and ambition to scale with consistency and impact.


Intigriti recognised in the Deloitte EMEA Technology Fast 500 2025

# Intigriti 0626 Inside Job CTF results are in

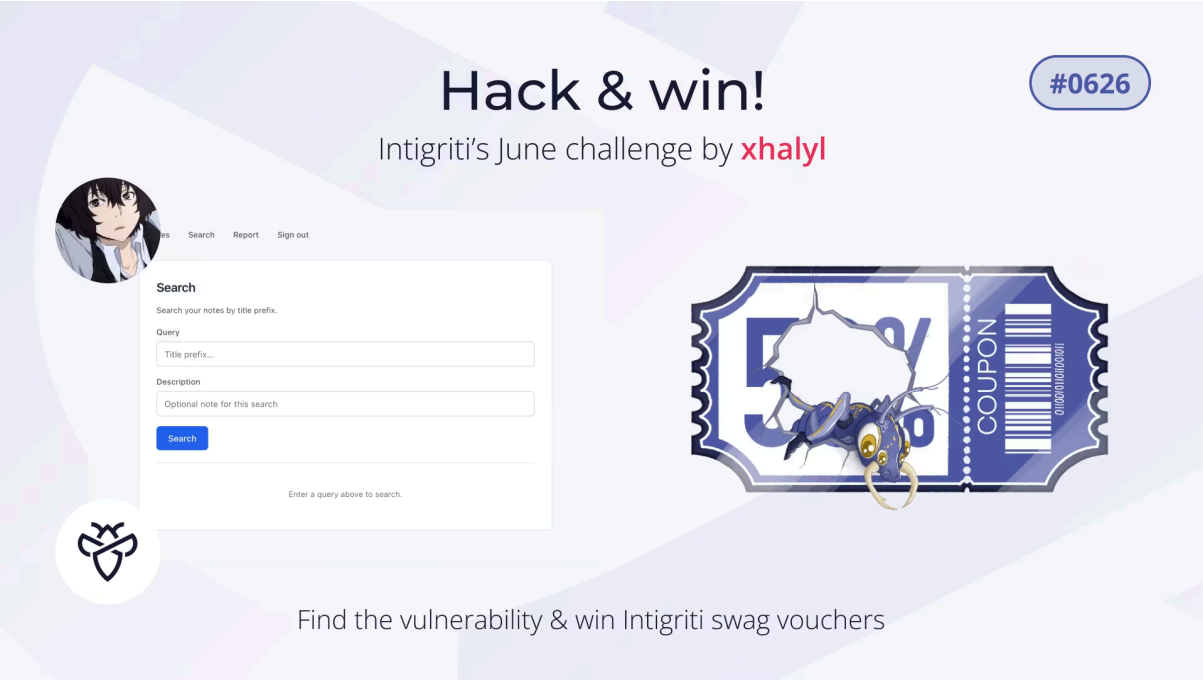
June's Inside Job CTF challenge featured a dangling markup vulnerability that allowed you to exfiltrate the flag by exploiting insecure CSP rules. Some hackers even uncovered other unintended bugs along the way.

Quick recap:

- 43 hackers reported the correct solution
- First blood went to bhavya32 (@bh4vy4x07)

- And 10 hackers wrote a nice [write-up]

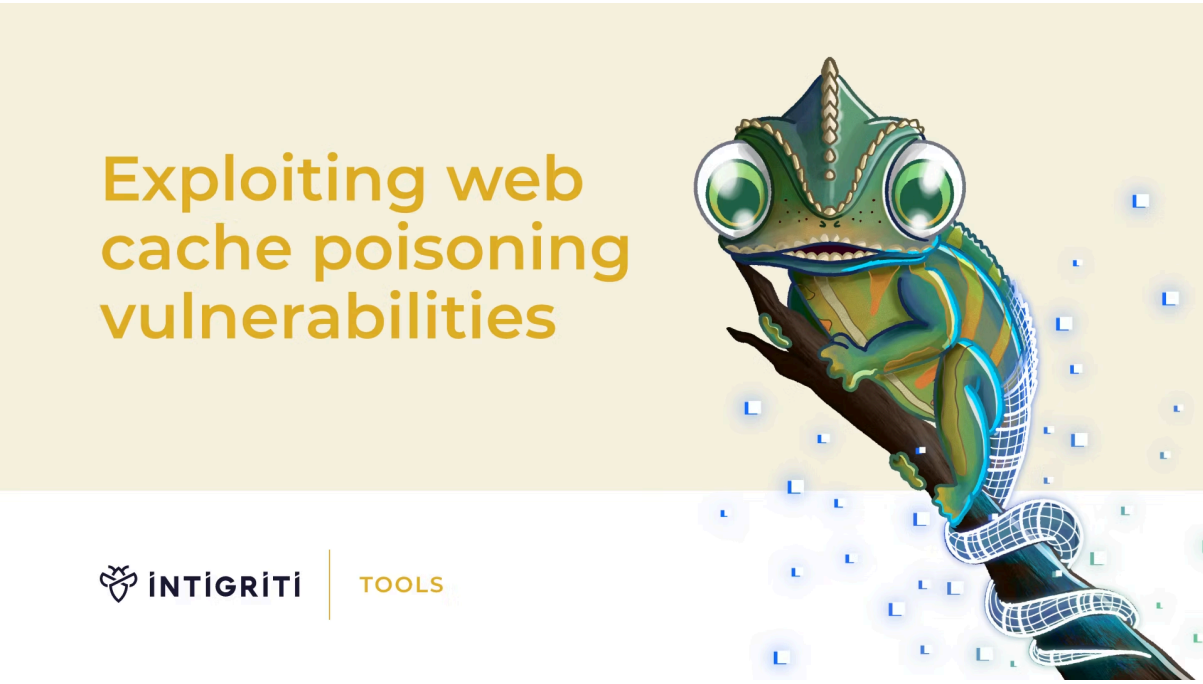
If you want to put your hacking skills to the test, be sure to give the Inside Job 0626 CTF a go before heading over to [Bugology], where you can find all the researchers' submitted solutions.




Intigriti 0626 Inside Job CTF results are in

## Blogs & videos

### [Exploiting web cache poisoning vulnerabilities]




Exploiting web cache poisoning vulnerabilities Cover Image

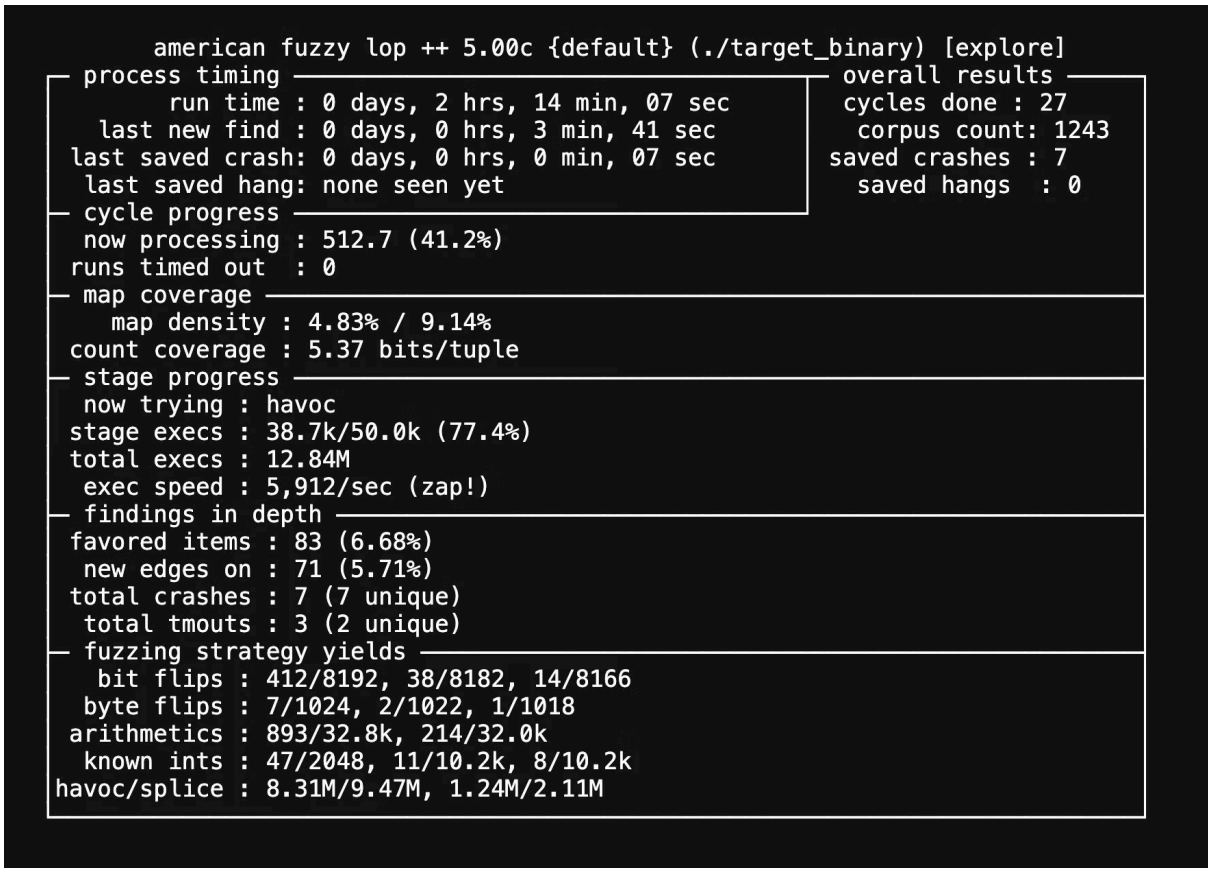
Most hunters skip web cache poisoning because it looks intimidating, but a single misconfigured cache layer can regularly turn into critical findings, even on heavily tested targets. In our latest article we walk you through identifying cache layers, spotting unkeyed inputs, and chaining them into real impact. This time, we teamed up with Zhero, who is well-known for his research around cache poisoning vulnerabilities. Read the article.

- **Going from zero to your first valid bug report?** We just launched the Bug Bounty Starter Kit, a free guide covering recon and tooling, the exploitation of SQLi, XSS, and BAC vulnerabilities, and how to write a report that gets triaged faster. Get yours now.

# Tools & resources

## Tools

### AFL++




AFL++

Manually testing native code and binaries for memory corruption bugs is nearly impossible without automation. AFL++ is an open-source, high-performance fuzzer that automatically discovers crashes and vulnerabilities by intelligently mutating inputs and tracking code coverage. If you are getting into binary research or low-level vulnerability hunting, this one is a solid place to start.

- **Want LLM-powered code review against your bug bounty targets?** Metis by @arm is an open-source tool that uses LLMs to perform deep security code reviews, catching complex vulnerabilities such as logic and design flaws that traditional SAST tools typically miss. In a new internal benchmark, Metis now flags nearly all vulnerabilities that traditional SAST tools fail to catch. It can be pointed at open-source bug bounty targets or even TypeScript source code recovered from JS sourcemaps.

- Tired of manually scanning Burp traffic for sensitive data? HaE by @VulkeyChen is a Burp Suite extension that automatically highlights and extracts sensitive data patterns across your HTTP traffic using customizable regex rules.

## Resources

[8 Million Requests Later, We Made The SolarWinds Supply Chain Attack Look Amateur]


8 Million Requests Later, We Made The SolarWinds Supply Chain Attack Look Amateur

@watchtowrcyber spent two months claiming around 150 abandoned S3 buckets and quietly served the resulting 8 million-plus requests for software updates, binaries, virtual machines, and more. The research demonstrates exactly how unmaintained S3 namespaces can be turned into a supply chain attack rivalling SolarWinds, and AWS responded by rolling out namespaces for new S3 buckets shortly after publication. If you are interested in offensive research that advances the industry, this one is a must-read.

- Earning $500,000 hacking Google with AI. @brutecat details how AI-assisted methodology led to a $500K bounty on Google, and shares the workflow behind it.

- A 10-year-old critical vulnerability in phpBB is affecting tens of millions of users. @pilvar222 at Aikido publishes an account takeover chain leading to unauthenticated RCE on the latest version. The bug went unnoticed for more than a decade and is reportedly priced at around $50K in public 0-day brokers.

- A Client-Side Path Traversal chain with serious impact. @mugh33ra walks through a CSPT exploitation chain that escalated into wiping an entire organisation's data.

- Reading any Salesforce Marketing Cloud account's emails without authentication. @SLCyberSec disclosed a vulnerability in Salesforce Marketing Cloud that allowed them to leak PII and emails from any customer instance, no authentication required.

- A new DOMPurify XSS bypass. @cure53berlin publishes an advisory for a DOMPurify bypass using the selectedcontent element and a re-clone trick.

- **Looking for a fresh PostgreSQL SQL injection trick?** Jerry Luong shares a blind SQLi technique that uses dollar-quoting to slip past regex sanitizers, injecting scalar subqueries through unquoted column-name positions in dynamic PL/pgSQL and extracting data through a boolean oracle with zero schema knowledge.

- **A hidden HTTP/2 attack revisited 14 years after HPACK.** @calif_io describes a new attack against HTTP/2 header compression that Codex helped uncover during a code audit, with a candid look at how the issue was missed in the original protocol review.

- **A Universal XSS in Firefox Focus and Klar for iOS.** @RenwaX23 shares a write-up for CVE-2026-11799, a race condition in the WebKit navigation flow that bypasses redirect-scheme validation in Mozilla's privacy-focused mobile browsers.

- **A 1-click GitHub token theft through a VSCode bug.** This write-up details how a single click could lead to GitHub token exfiltration due to a quirk in VSCode's URI handling.

- **Earning $7,000 by hacking AI with a single email.** @NahamSec walks through the methodology behind a $7K AI vulnerability discovered via a crafted email.

- **Auth bugs pay the most in bug bounty, but most hunters never touch them.** @amrelsagaei breaks down web auth the way the developer who built it sees it, covering sessions, JWTs, OAuth 2.0, the Authorisation Code Flow, PKCE, and OpenID Connect.

- **Broken authentication leading to chat impersonation.** @kullai12 shares how trusting too much in an API design allowed an attacker to impersonate a victim and chat as them directly.

- **Another XSS in Craft CMS, this time with some pretty annoying requirements.** @_CryptoCat shares the full analysis of CVE-2026-55793, including the requirements that make it exploitable in practice.

- **Targeting invitation-based workflows?** @awais0x1 published a practical checklist for testing invite flows, built from real-world HackerOne reports research.

- **From failure to $32,000.** @Justsvampire shares the bug bounty journey that led to a $32K payout, with the lessons learned along the way.

- **Bypassing a 403 to access an internal intranet portal.** @termireum details how a few targeted bypasses turned a 403 Forbidden into a €1,500 bounty on a real-world program.

- **A tiny URL parameter that broke an entire web store's pricing logic.** @0xraselrana shares the $2K bug that came from spotting an overlooked parameter in a checkout flow.

- **New to bug bounty?** @saqibarif98 writes about his first $1,000 bug bounty journey and the practical lessons that helped him get there, a useful read for anyone starting out.

# Company news

## Bug Bounty Meetup Austin, TX

Our Hacker Ambassador Ryan Bonner (@BadAt_Computers) hosted a packed Bug Bounty meetup in Austin, Texas, on June 20. The room was full, the finds were great, and many new hacker friendships were made over the day. Thanks to everyone who came out and to Intigriti for sponsoring the event.


Bug Bounty Meetup Austin, TX

## BSides Leeds, UK

BSides Leeds was a blast! We brought some prompt-injection challenges to the booth, and the community's response was fantastic. A huge thanks to everyone who stopped by, and a shoutout to the PortSwigger team for partnering up with us on the day. Great conversations, great community, and a great day all round. See you next time!


BSides Leeds, UK

## Bug Bounty Village at OrangeCON 2026

We hosted our Bug Bounty Village at OrangeCON on June 4 at Meervaart Theatre in Amsterdam. Attendees joined us for a live CTF, talks on breaking into bug bounty and the life of a triager, space to connect with the community, and some cool swag. Thanks to everyone who came by to say hi.

Bug Bounty Village at OrangeCON 2026

# 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