Intigriti Bug Bytes #236 - May 2026

BY AYOUB • MAY 30, 2026

Hi hackers,

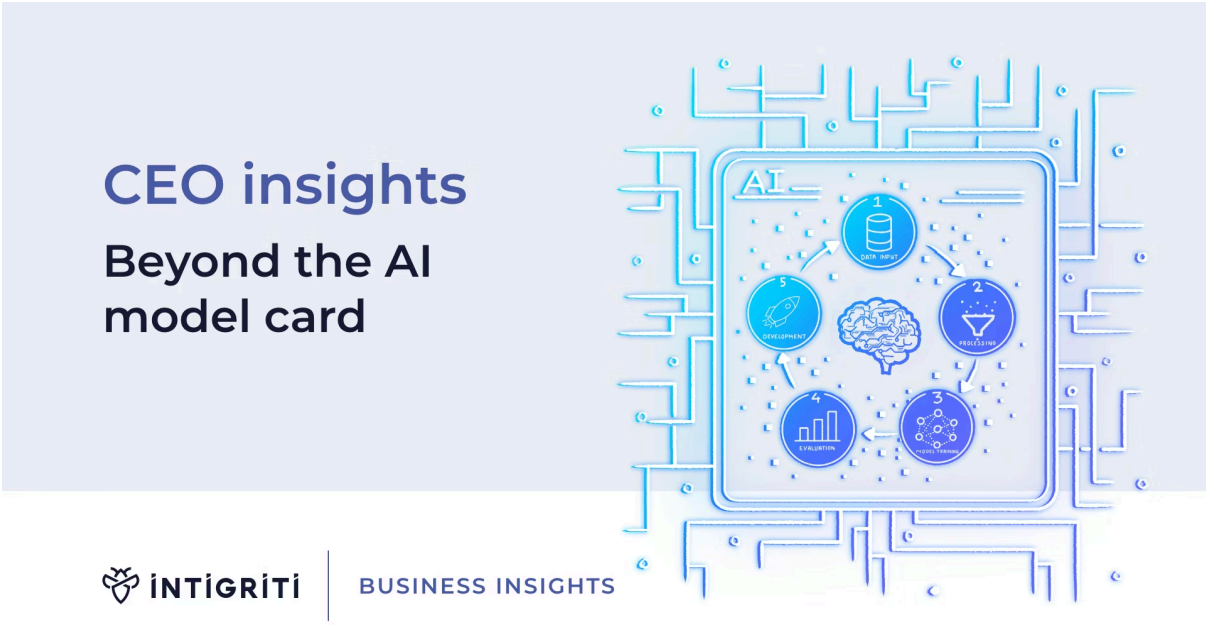
Welcome to the latest edition of Bug Bytes! In this month's issue, we'll be featuring:

- Earning $148K via RCE in Google Cloud
- How public Google API keys became Gemini credentials
- Our first official Burp Suite extension
- Two new bypasses for Chrome's Sanitizer API
- One-click account takeover from a sanitized name field

And so much more! Let's dive in!

CEO insights: beyond the AI model card

AI model cards have become a standard part of how organizations document their AI systems. Our CEO argues that truly managing AI risk goes well beyond what a model card covers. In this post, he shares his perspective on the steps security teams should take to address the gaps that documentation alone cannot fill.



CEO insights: Beyond the AI model card

NIS2 compliance beyond the April 2026 deadline

With the April 2026 NIS2 deadline now passed, the focus shifts from initial compliance to building sustainable security practices. This article looks at what organizations in scope for NIS2 compliance should be prioritizing now, from incident reporting obligations to supply chain risk management.

NIS2 compliance beyond the April 2026 deadline

Upcoming: Intigriti Bug Bounty Meetup in Austin, TX

Come join us in Austin, Texas, on June 20th! Our Hacker Ambassador Ryan (roll4combatus) is hosting a full day of talks, bug bounty hunting, and networking.

Event details:

Saturday, June 20, 2026

Hotel Van Zandt, Austin, Texas

10AM - 5PM (CDT)

To participate: Please send a message to our Hacker Ambassador via LinkedIn or X/Twitter.

Intigriti Bug Bounty Meetup in Austin, TX

Intigriti 0526 CTF results are in

May's Pixel Pioneers Intigriti challenge featured a DOM-clobbering vulnerability that allowed for DOM-based cross-site scripting. 178 hackers reported the correct solution, some even finding other unintended bugs.

Quick recap:

- 178 hackers reported the correct solution
- First blood went to oxship (@oxxxssh)
- And 33 hackers wrote a nice write-up

If you want to put your hacking skills to the test, be sure to give the Pixel Pioneers 0526 CTF a go before heading over to Bugology, where you can find all the researchers' submitted solutions.

Intigriti 0526 Challenge

Blogs & videos

Exploiting SQL injection vulnerabilities

Exploiting SQL injection vulnerabilities Cover Image

Despite what most bug bounty hunters think, **SQL injections are far from dead.** You just need to know where and how to test for them. In our latest article, we explored how SQL injection vulnerabilities arise, how to test and exploit them to leak secrets, bypass authentication, and even achieve RCE.

- **As vulnerability submissions continue to grow, coordinating triage at scale has become one of the bigger challenges in crowd-sourced security.** Our latest product update introduces AI Triage Assist,

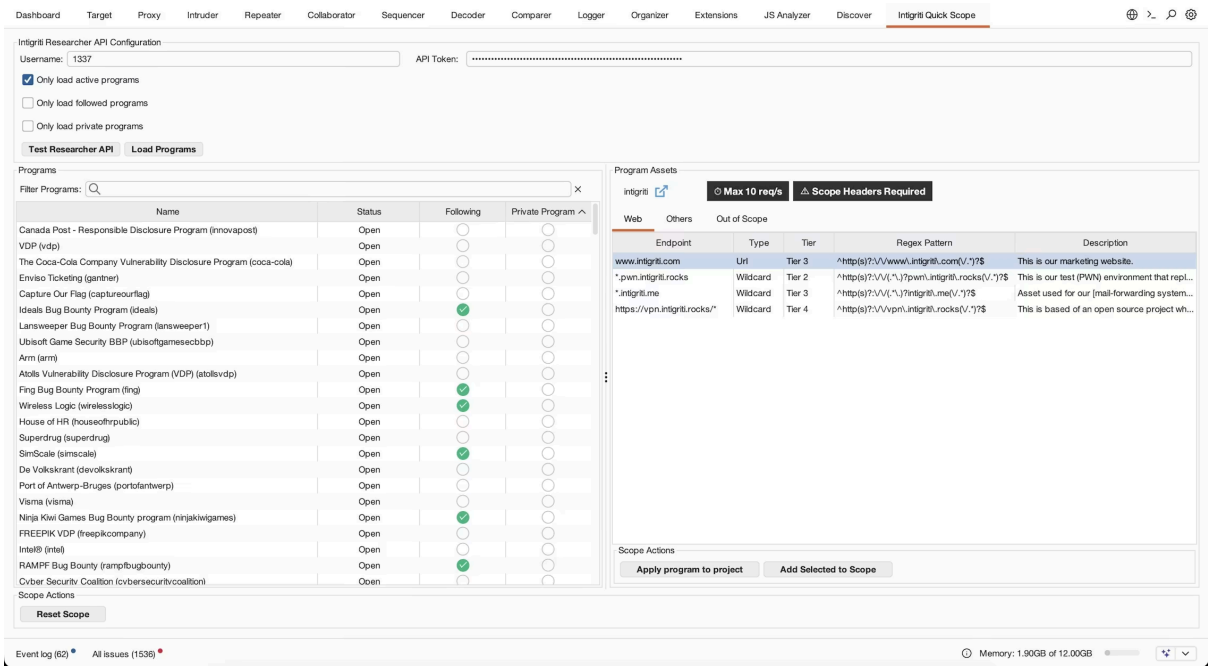
a new feature designed to help security teams handle increasing volumes of reports more efficiently. If you are curious about how AI is changing the triage workflow, this article is certainly worth reading.

- **We've noticed a spike in AI-generated vulnerability reports.** Some are great, others sadly never meet the bar. In this re-post, we revisit how to use AI effectively for vulnerability report writing and what makes a report worth submitting.

Tools & resources

Tools

Intigriti Quick Scope (IQS)



Intigriti Quick Scope (IQS)

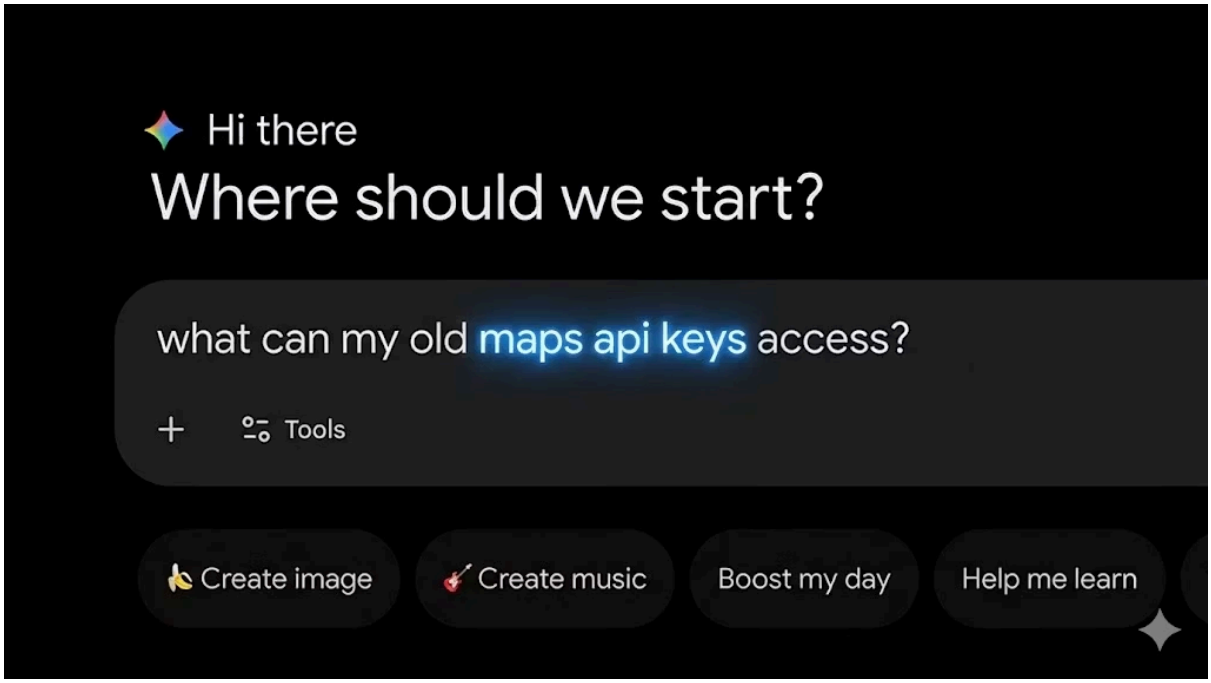
Our first official Burp Suite extension is now live in the BApp Store. Intigriti Quick Scope (IQS) fetches all your public and private programs directly from the Researcher API and auto-configures your Burp Suite project scope and mandatory request headers with a single click. If you are regularly switching between Intigriti programs in Burp Suite, be sure to give it a try.

- **Manually filtering through Burp Suite request history for possible vulnerabilities you might have missed can be tedious.** Burp AI Agent by @six2dez1 brings AI-powered passive and active scanning to Burp Suite, covering 62 vulnerability classes with 10 backend options, including fully local models via Ollama.

- **Stripped Rust binaries are notoriously difficult to reverse engineer.** Oxidizer is a new Rust-specific decompiler built on Angr that recovers enums, pattern matching, operators, and macros from stripped binaries and outputs them as readable Rust pseudocode.

Resources

Google API Keys Weren't Secrets. But then Gemini Changed the Rules.



Google API Keys Weren't Secrets. But then Gemini Changed the Rules.

For years, **Google API keys used for services like Maps and Firebase were considered non-sensitive**, and developers deployed them publicly without concern. **That changed with Gemini.** Researchers at @trufflesec scanned millions of websites and found nearly 3,000 Google API keys, originally intended for public-facing services, that now also authenticate to Gemini. Anyone who finds these keys can access uploaded files, cached data, and charge LLM usage to the account holder's bill, affecting even Google's own public API keys.

- **Earning $148,337 via remote code execution in Google Cloud Production Environment.** @brutecat shares the full story of StubZero and the steps that led to one of the larger cloud bounty payouts in recent memory.
- **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 article on CTBB Labs.
- **Pre-auth SQL injection in Drupal Core, no authentication required.** Researchers at @SLCyberSec published a technical analysis of CVE-2026-9082, an anonymous SQL injection in Drupal Core affecting installations running a PostgreSQL backend.
- **Interested in what Chrome's Sanitizer API lets through?** @hash_kitten documents two bypasses for Chrome's built-in Sanitizer API and the edge-case behavior that makes them possible.
- **What started as a self-XSS in a sanitized name field ended in a one-click account takeover.** @j_zere details the full chain of bypasses that turned an initially unexploitable finding into a critical vulnerability.

- **XSS usually ends when the server patches the issue.** @amrelsagaei explains in Client Side 02: ServiceWorker Bugs how an injected Service Worker can keep running in a victim's browser long after the original vulnerability is patched.
- **An interesting look at automating Entra ID tenant lockouts using AI and browser automation.** @DebugPrivilege demonstrates how JavaScript automation and Microsoft Graph API calls can be combined to simulate ransomware-style cloud attacks against Azure environments.
- **Testing modern microservices architectures requires a different approach.** @mustafabilgicii covers three real-world vulnerabilities from banking and fintech microservices, including a full SSRF via internal subdomain fuzzing, a JWT scope flaw leading to account takeover, and proxy routing parameter pivoting into internal networks.
- **Two zero-day vulnerabilities found in cPanel.** @Yshahinzadeh from the Voorivex team documents a reflected XSS affecting every Mailman page and a stored XSS in the Moderation Queue.
- **Authentication bypass and privilege escalation through Supabase misconfigurations.** This writeup covers how chained access control weaknesses in misconfigured Supabase instances led to a $1,800 bounty.
- **Gathering information during a red team engagement without triggering detection is harder than it sounds.** @HackingLZ shares practical techniques for maximizing information gathering while staying under the radar during red team operations.
- **An honest look at where AI-assisted bug hunting helps and where it does not.** @aituglo shares his experience with AI-assisted vs fully autonomous bug hunting, including a memorable story of Claude making an unexpected purchase while testing access controls.
- **A hacker made $40,000 using Claude Code for bug bounty.** @nahamsec breaks down the methodology and workflow behind this Claude Code-powered bounty run in this YouTube video.
- **Looking to create Nuclei templates for recently disclosed CVEs?** @pdiscoveryio shares a quick trick using CVEmap to find CISA-marked, remotely exploitable CVEs that have a public POC but no Nuclei template yet.
- **New to SQL injection?** We published a beginner-friendly SQLi exploitation thread covering the fundamentals of finding and exploiting SQL injection vulnerabilities.
- **A quick Burp Suite tip for crawling dynamically loaded JavaScript.** @the_IDORminator shares a useful technique for adding hundreds of undiscovered JavaScript chunk files to the Burp Suite Sitemap using Intruder, making them much easier to parse and review.

Company news

BountySync+Social London

Our BountySync+Social event at our new London office was a great success. Researchers and security teams came together for a day of conversations, cocktails, and ice cream. A big thank you to our host @appSecExp, hacker ambassador @CristiVlad25, and our very own Chris Holt and Greg Jenkins for leading a great multi-perspective discussion on AI and bug bounty. See you at the next one!

BountySync+Social London

Hacker Hideout in Utrecht, NL

22 hackers from multiple countries gathered in Utrecht for Hacker Hideout, hunting on Intigriti programs and sharing tips and tricks throughout the day. Discussions also touched on the future of AI-assisted hacking and autonomous agents. Big shoutout to René de Sain and Stefan Goossens for organizing the event!

Hacker Hideout in Utrecht, NL

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