# Intigriti Bug Bytes #229 - October 2025

BY BLACKBIRD-EU · OCTOBER 31, 2025

## Hi hackers,

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

- Cool trick to find disclosed secrets in internal web extensions
- A repository full of WAF bypasses
- Hacking Intercom misconfigurations
- Wayback Machine for hackers

And so much more! Let's dive in!

## INTIGRITI 1025 results are in

October's Intigriti challenge (by @chux13786509) brought hundreds of hackers together to hack a vulnerable web shop for a week! With over +100 solves, it easily joins the list of the most solved and most popular challenges ever to be featured on Intigriti.

Quick recap:

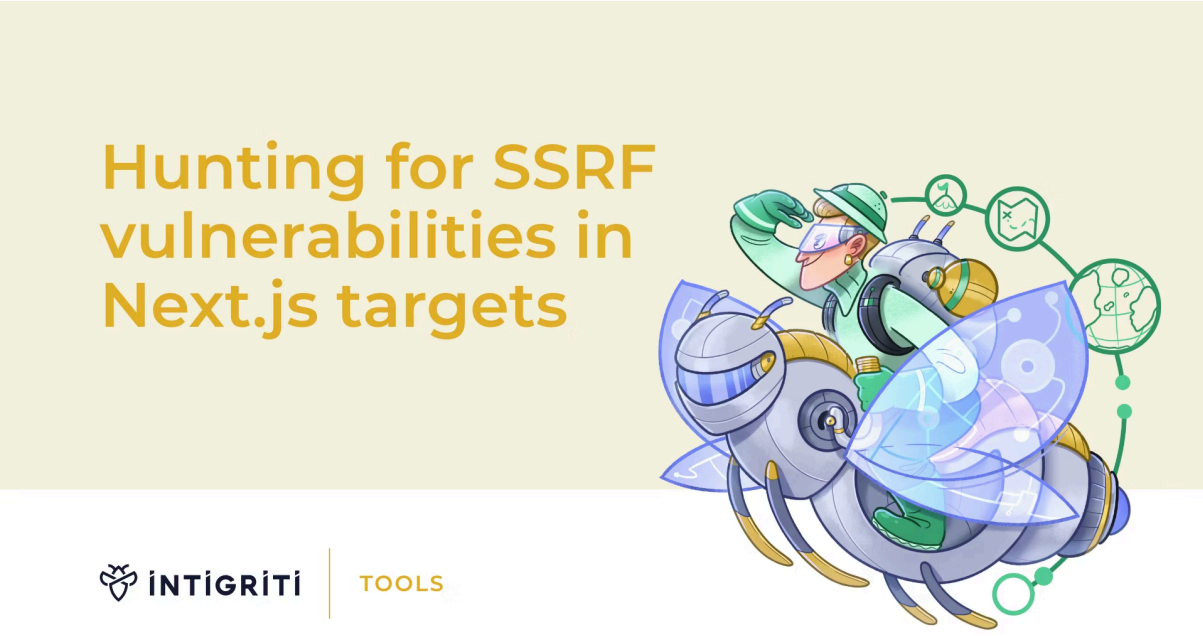
- 103 hackers reported the correct flag
- First blood went to luryus
- And 35 hackers wrote a nice write-up


Intigriti Challenge 1025

[Read all write-ups]

## Blogs & videos

### Hacking Next.js targets




Hunting for SSRF vulnerabilities in Next.js targets Cover Image

Next.js powers millions of web applications... yet its complexity creates the perfect environment for SSRF vulnerabilities to arise. Developers often expose new endpoints that enable arbitrary HTTP requests. In

our technical article, we documented 3 SSRF [attack vectors in Next.js targets] and how you can exploit them.

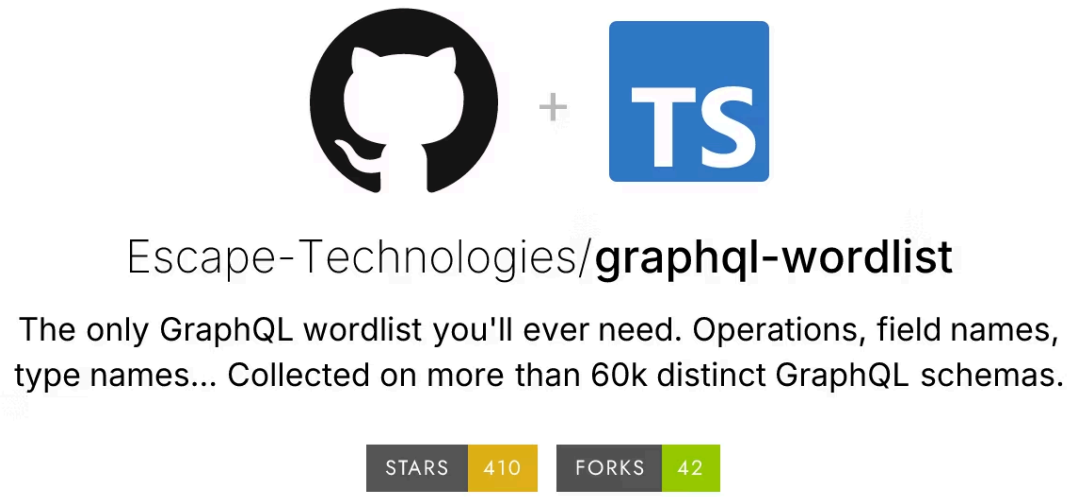
- **We all know that the efforts of performing reconnaissance pay off.** Yet, hard-coded API keys and exposed credentials remain one of the most overlooked attack vectors. Sometimes, they're even hidden in plain sight. In our comprehensive guide, we've outlined multiple proven methods to [discover and validate secrets] across your bug bounty targets.

- **Finding a possible SQL injection point only to be stopped by a WAF can feel daunting...** But what if you could bypass this same WAF and still achieve SQLi? In our technical article, we covered multiple ways to [identify the origin IP] of your target behind CDNs & WAFs.

# Tools & resources

## Tools

### [GraphQL Wordlist]




GraphQL Wordlist

**Testing GraphQL targets & struggling to effectively enumerate more operations and queries?**

This comprehensive [GraphQL wordlist], built from 60k+ real GraphQL schemas, contains the most common field names, operations, and arguments to help you discover hidden attack surfaces.

- **Manually running Google dorks is time-consuming and often gets your IP blocked...** [Pagodo] is a simple, open-source tool that automates the entire Google Hacking Database (GHDB) scraping process, letting you systematically test thousands of dorks against your target while rotating through proxies to avoid detection.

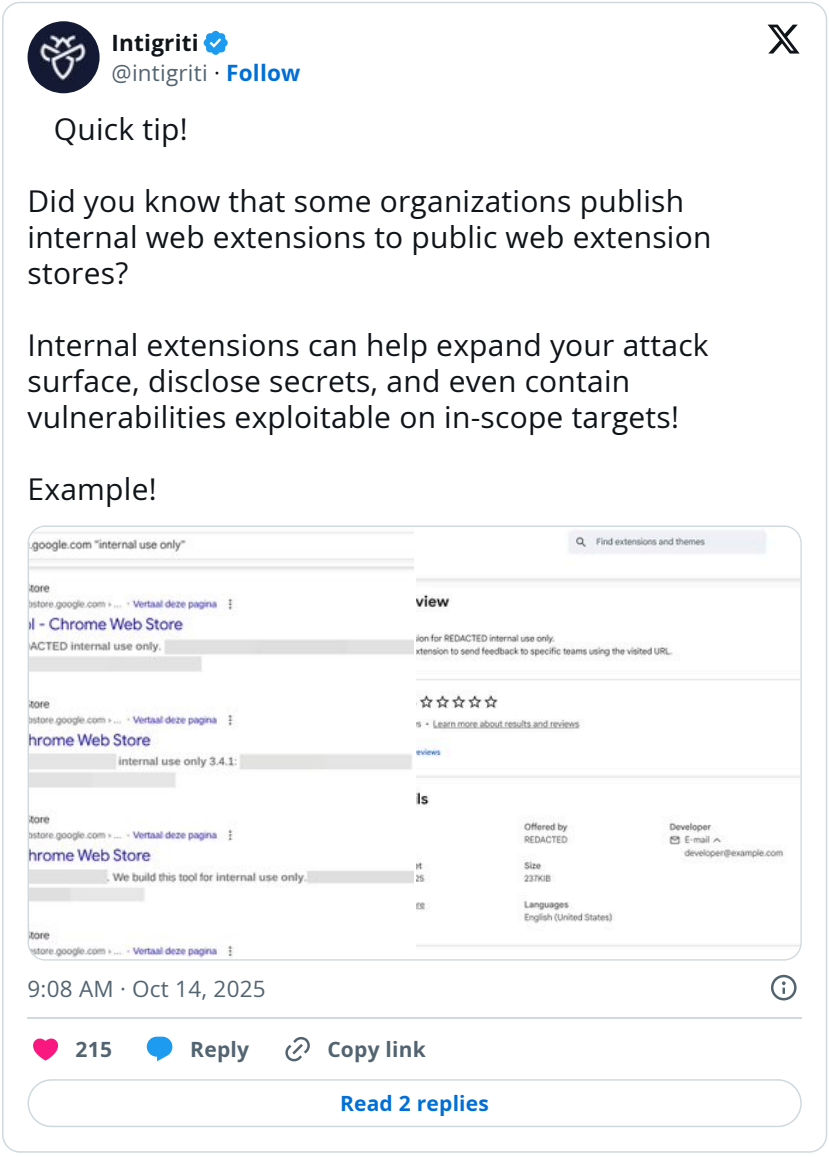
- **Ever wanted to automate your entire recon process for your target?** Check out [Frogy 2.0], an open-source tool that automates your entire recon workflow. It also helps you prioritize assets based on several factors.

- **WAFs don't have to block your payloads...** This comprehensive repository documents WAF fingerprinting techniques, evasion methods, and known bypasses for dozens of popular firewalls, helping you understand and test WAF protection mechanisms effectively. Even though the content is from a while ago, some techniques are still relevant today.

- **Heads up mobile hackers! Frida just launched Simmy,** a new backend for Apple's Simulators on macOS that helps you simulate iOS processes just like on physical devices. Check out the announcement post on Twitter/X.

# Resources

## Hacking internal web extensions




**Did you know that some organizations publish internal web extensions to public web extension stores?**

Some of them contain secrets and even exploitable vulnerabilities on in-scope targets! In our post, we show you exactly how to enumerate possible plugins published by your target.

- Intercom chat widgets may seem harmless... yet many organizations fail to enforce identity verification, allowing attackers to impersonate any user and access their entire support chat history. This write-up documents 3 critical misconfigurations that expose sensitive customer conversations, including session leakage and persistent sessions after logout.

- This cool research article documents how you can further leverage a simple CRLF vulnerability into an XSS, even when CSP script-src is set to self.

- Server-side cookie overwrites typically prevent cookie-based DOM XSS... yet this article demonstrates 3 clever bypasses: exploiting scope mismatches between endpoints, leveraging Chrome's innerHTML quirk with img tags, and abusing JSON injection to overwrite window.location for XSS execution.

- Wayback Machine can be used in a variety of ways... for us hackers, it can help us expand our attack surface and score more bounties. This article documents how you can discover hidden pages, links, and parameters with the Wayback Machine.

- CSPT (Client-Side Path Traversal) attacks are often seen as low-severity vulnerabilities, yet when further leveraged with services like Cloudflare's Image Proxy, they can be weaponized to leak sensitive cross-origin data. This well-written article demonstrates how you can exploit scenarios like these.

- A good wordlist only helps increase your chances of discovering hidden assets and possibly scoring more bounties. In our thread, we shared 5 wordlists that can help you expand your attack surface.

- Just getting started with bug bounty? We've shared a small thread with links to 4 videos to learn 4 vulnerability types in 400 seconds. Check out this thread, and while you're at it, make sure to leave a follow if you want us to post more related web hacking content.

## 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!