Intigriti Bug Bytes #227 - August 2025

BY INTIGRITI · AUGUST 15, 2025

Hi hackers,

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

- Evading WAFs like Cloudflare, Akamai & AWS Cloudfront
- Creating your complete bug bounty automation system
- A powerful, targeted backup file scanner
- Bypassing CSP to achieve XSS via a cool trick with PDF files

And so much more! Let's dive in!

INTIGRITI 0725 results are in

With only 7 confirmed solves, our latest XSS challenge by @J0R1AN proved to be one of the toughest challenges ever to be featured on Intigriti.

Quick recap:

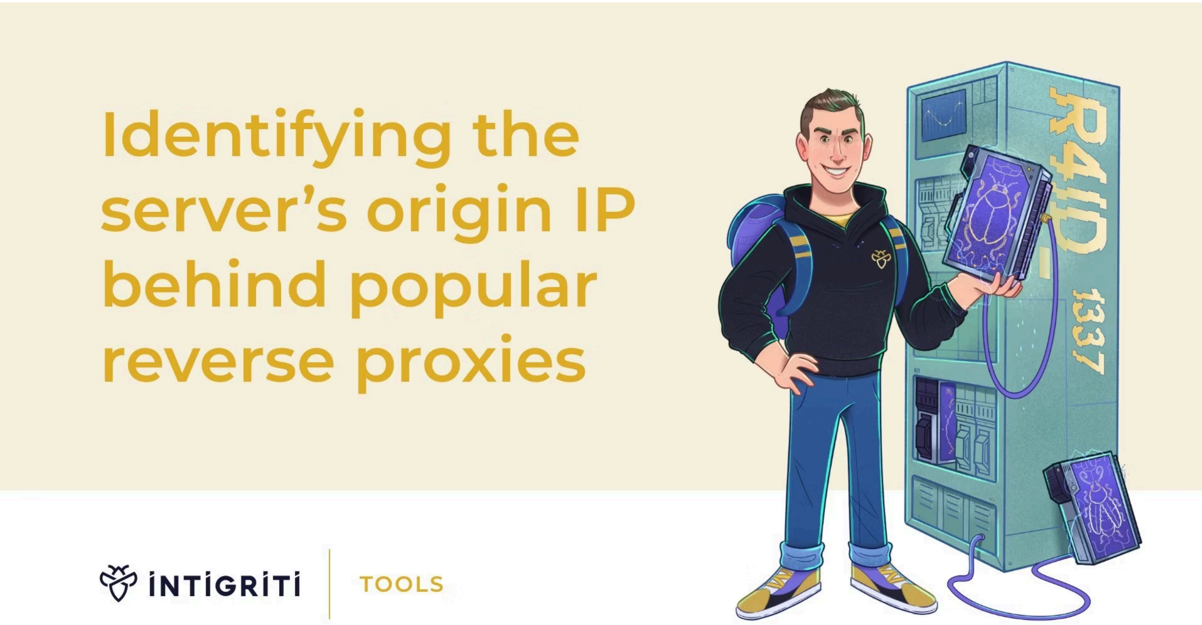
- 7 hackers reported the correct flag
- First blood went to @dr_brix
- And 3 hackers wrote a nice writeup

INTIGRITI 0725 Challenge

[View all write-ups]

Blogs & videos

[Identifying the server's origin IP]



Identifying the server's origin IP behind popular reverse proxies Cover Image

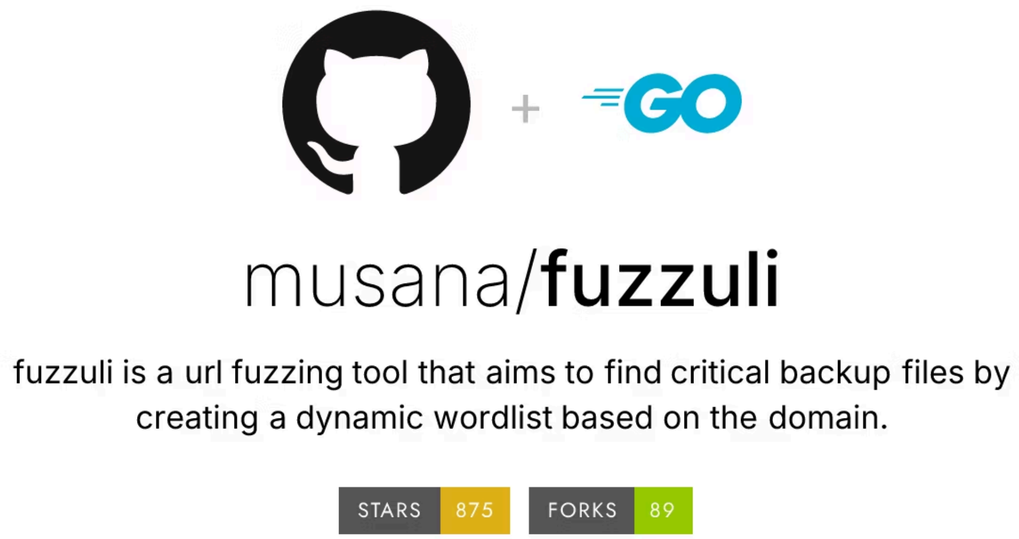
Finding a possible SQL injection point only to be stopped by a WAF can feel daunting... But what if you could bypass this same WAF and still achieve SQLi? In our technical article, we covered multiple ways to [identify the origin IP] of your target behind CDNs & WAFs.

- **GitHub dorking is mostly overlooked...** Yet, it is the place where developers accidentally commit API keys, database credentials, and other secrets (almost every single day). In our detailed article, we've documented how you can use GitHub dorking to find more vulnerabilities.
- **Throwback to our previous article: File uploads are everywhere...** Sometimes, a simple validation mistake can result in a high-severity finding (such as RCEs). In our technical article, we documented a few cool tricks you could try next time you're testing a file upload feature.

Tools & resources

Tools

Fuzzuli



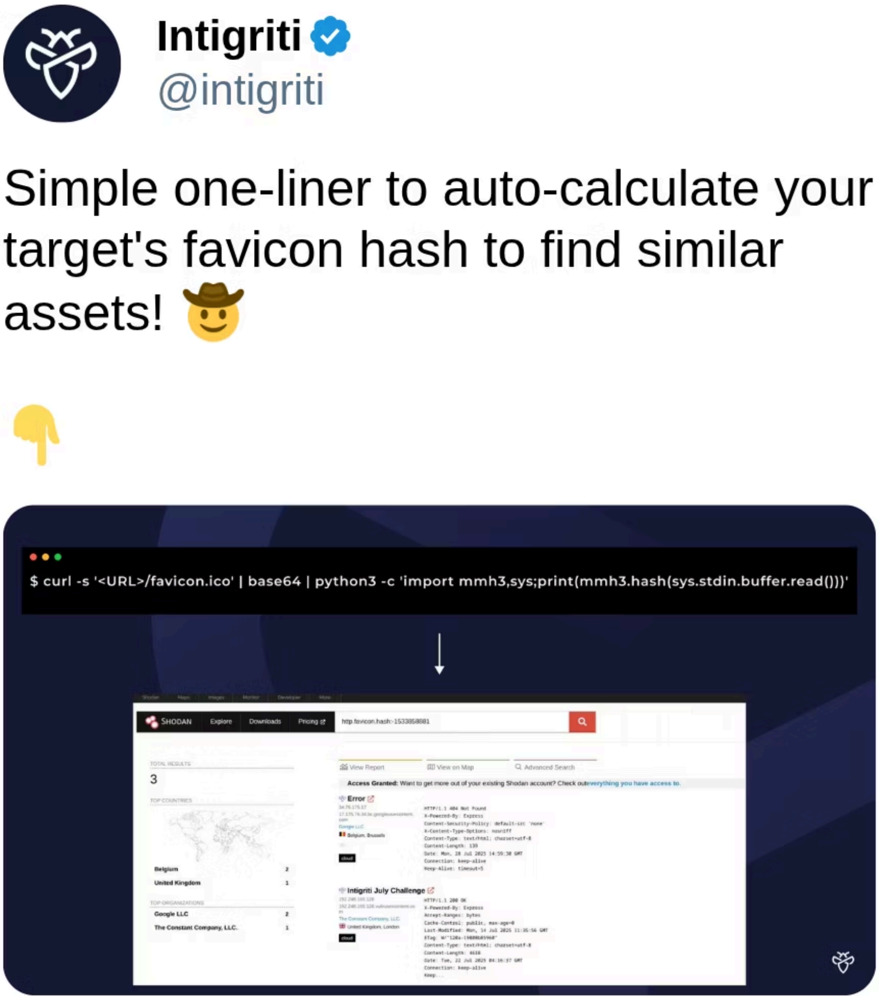
Fuzzuli backup file scanner

In need of a quick way to check for accidentally uploaded backup files on your target? Fuzzuli by @musana is a blazing-fast backup file scanner. It also includes features like dynamic wordlist generation for generating more accurate results. Learn more about using targeted wordlists to find more vulnerabilities in our technical article.

- **DOM-based XSS vulnerabilities are one of the most overlooked XSS types.** Domloggerpp by @kevin_mizu is a simple web extension to help you trace JavaScript DOM sinks leading to DOM-based vulnerabilities (such as XSS).
- **WAFs (such as Cloudflare, Akamai, and AWS Cloudfront) are tough to bypass.** Luckily, we have tools like Hackoriginfinder by @hakluke, a simple tool to help identify the server origin IP behind reverse proxies. If you require a more in-depth view on how to identify the server origin IP behind popular reverse proxies, give our detailed article a read.

Resources

Find more vulnerabilities with favicon hashes



One-liner to calculate favicon hash

Favicon hashes can help expand your attack surface by finding similar in-scope targets. Check out our recent post where we shared a simple, one-liner to calculate the favicon hash and use it in Shodan. Let us know if you found it helpful by following us @INTIGRITI!

- Looking to level up your bug bounty automation? Rs0n shares in this video his methodology and approach to automating bug bounty hunting.
- Log4Shell (Log4J) is still present in 2025, while most researchers have moved on, some are still scoring critical bugs with it. In our technical thread, we share how you can identify and exploit Log4Shell in 2025.
- Bypassing WAFs can be a tricky, time-consuming task. @coffinxp7 shares how to find the server's origin IP of any target.
- This researcher scored a nice bounty on Intigriti by submitting a bug in GraphQL. If you want to learn more about hacking GraphQL targets and also start to hunt for critical GraphQL bugs, we've prepared a short thread for you with all the resources you need to get started.

- Blocked by CSP? @xssdoctor shares a cool trick in his thread to bypass CSP using PDF files.

Intigriti at DEF CON

DEF CON 33 was incredible! The energy, the brilliant minds, and the conversations with our community made it unforgettable.

Quick recap:

- Our Chief Hacker Officer, Inti De Ceukelaire, presented the Magical Hacks show, packed with both mind-blowing hacking and magic tricks.
- We hosted a Friday morning meet-up with coffee and fresh food to kick off the second day of DEF CON.
- Our private suite provided a relaxed space for in-depth conversations with our CEO and team throughout the event.

Don't miss our next hacker gathering, follow us on LinkedIn and Twitter/X for upcoming event announcements.

DEF CON 33 - Magical Hacks show by Inti

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!