Intigriti Bug Bytes #226 - July 2025

BY INTIGRITI · JULY 18, 2025 · LAST UPDATED ON JULY 19, 2025

Hi hackers,

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

- Exploiting Log4Shell (Log4J) in 2025
- An indispensable GitHub recon tool (not the one you have in mind)
- A repository full of bug bounty tips, resources and tools
- One of the most comprehensive guides on finding exposed S3 buckets

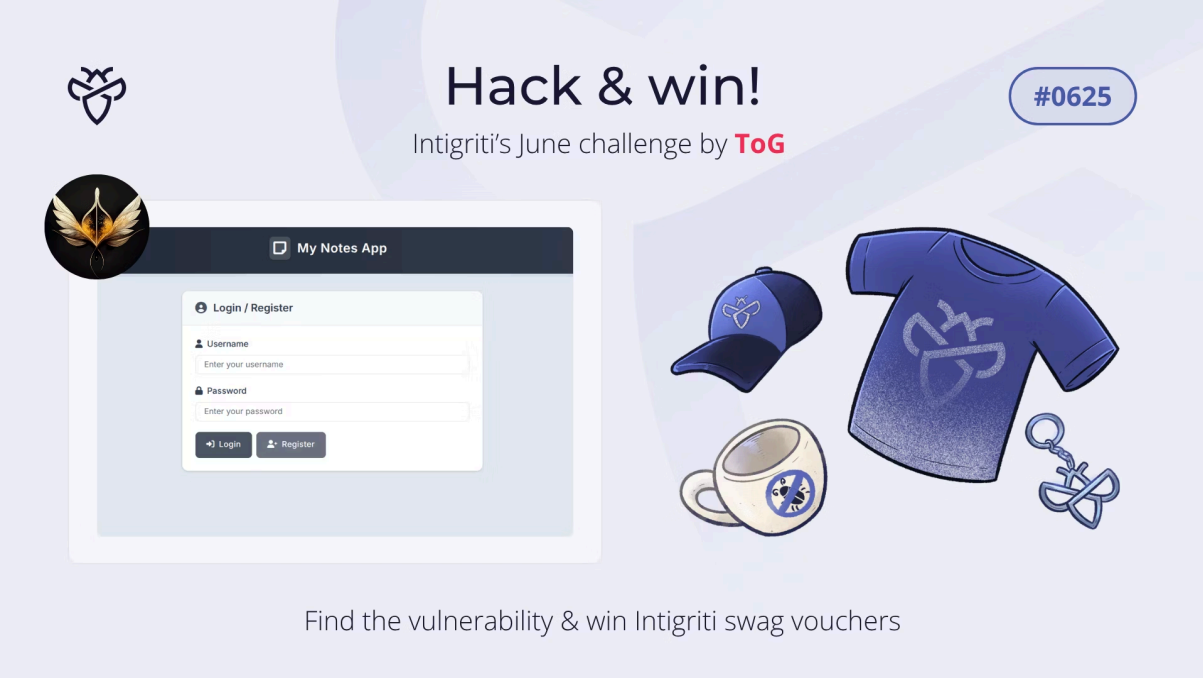
And so much more... Let's dive in!

INTIGRITI 0625 results are in!

Tougher than ever before: only 13 researchers found their way in and captured the flags. This latest challenge by @Toogidog featured a cache poisoning vulnerability and a remote code execution using Chromium.

Quick recap:

- 13 hackers reported the correct flag
- First blood went to @dimariasimone
- And 4 hackers wrote a nice writeup (including some interesting unintended solutions you can learn a thing or two from)



INTIGRITI 0625 Challenge

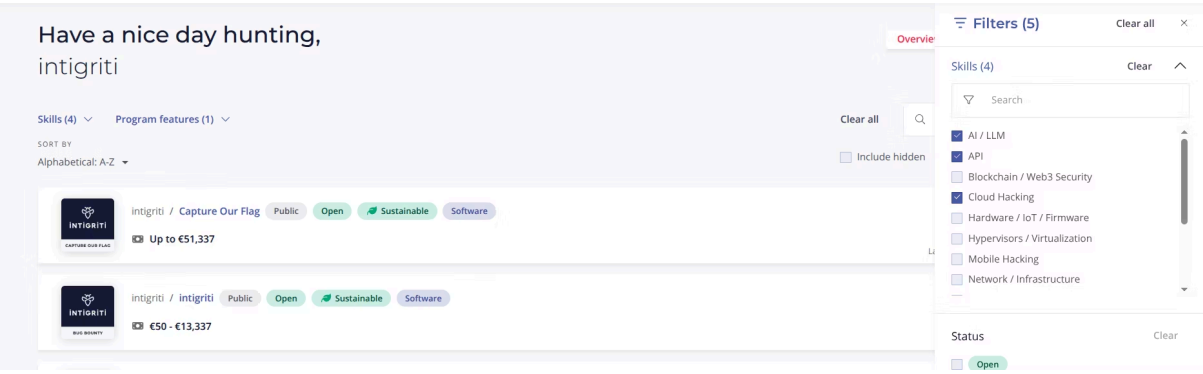
[View all write-ups]

Latest platform updates

New: Skillset matching

We've recently introduced a 'Required Skills' feature for program assets. Companies can now tag their assets with a matching skillset that's required to test the asset type.

It has never been easier for researchers like you to easily find programs and assets that match your specific hacking skills and receive accurate new program recommendations.

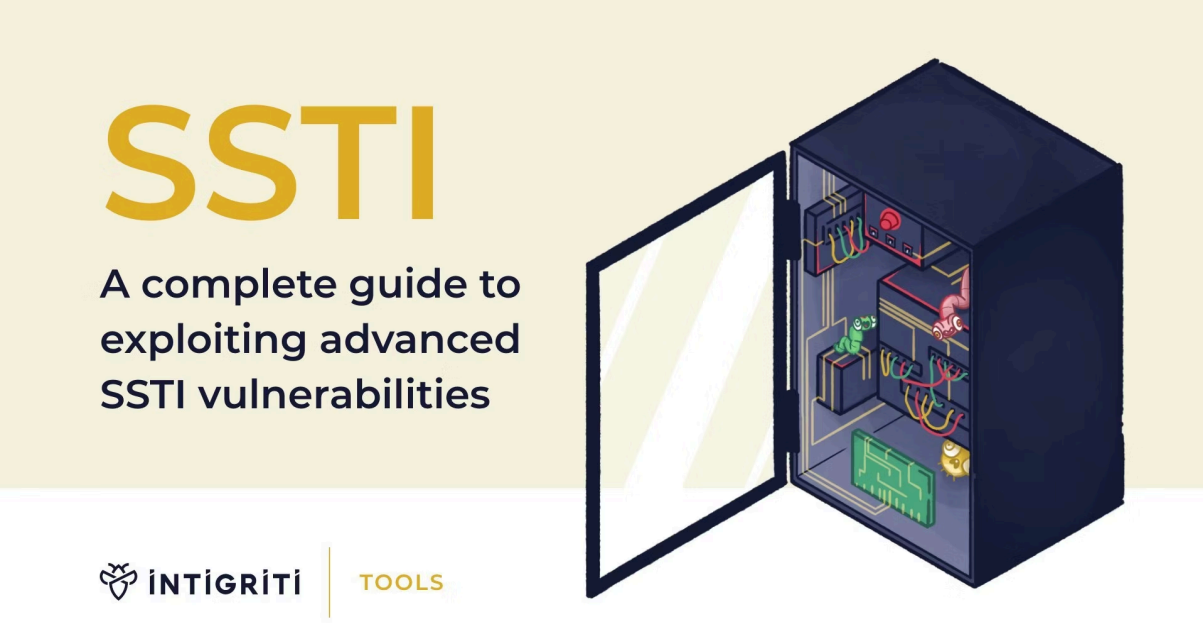


Intigriti skillset matching

[Sign in to your account]

Blogs & videos

Exploiting SSTI vulnerabilities



SSTI: A complete guide to exploiting advanced SSTI vulnerabilities Cover Image

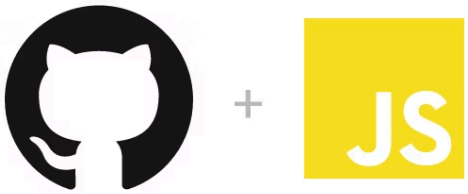
Server-side template injections (SSTIs) are still common and can often be escalated to RCE... yet most bug bounty hunters still struggle to spot them. In our article, we've outlined several SSTI exploitation techniques, including advanced filter and sandbox bypasses.

- **While most moved on, some bug bounty hunters are still hunting for Log4Shell even to this day.** In our most recent article, we show you exactly how to uncover Log4Shell vulnerabilities that others are missing in 2025.
- **Throwback to our previous article: Prepping for an upcoming CTF competition?** No stress, we've got your back. Read our beginner-friendly guide where we share 10 practical tips to help you solve your first CTF challenge.

Tools & resources

Tools

MapperPlus



midoxnet/**mapperplus**

MapperPlus facilitates the extraction of source code from a collection of targets that have publicly exposed .js.map files.

MapperPlus JavaScript sourcemap unpacker

Found a JavaScript source map file but failed to read it? Check out MapperPlus, a simple tool to unpack JavaScript source map files using a headless web browser.

If you'd like to learn more about the significance of JavaScript files for bug bounty hunters and how properly examining these files can land you more bounties, check out this article.

- Just starting in bug bounty, or are you looking to learn about more attack vectors? KingOfBugBountyTips is a collection of bug bounty tips, resources, tools, and so much more to help you land your first or next bounty.
- We all understand the importance of performing GitHub reconnaissance. GitHub Dork Helper is a simple tool that auto-prefills possible keywords you can search for on your target's repositories.

Resources

Find more vulnerabilities with reconnaissance

Find more vulnerabilities with reconnaissance

Want to learn how to start finding more vulnerabilities... with reconnaissance? Our recent in-depth thread provides a step-by-step guide to help you spot more vulnerabilities by leveraging information that's already out there.

- **Need to quickly figure out the origin IP of your target server?** Check out this simple checklist that outlines 5 different ways to determine the origin IP of targets behind Cloudflare, Akamai, etc. And let us know if you found it helpful by following us @INTIGRITI!
- **S3 buckets** are everywhere. But that doesn't mean they are all properly configured. This article by @coffinxp outlines an interesting way to find exposed S3 buckets like a pro.
- **Looking for a full guide on GitHub recon from a pro hacker?** Check out this detailed article by @GodfatherOrwa covering common GitHub reconnaissance techniques to discover secrets and other leaked data.
- **Still haven't found your first server-side request forgery vulnerability?** This detailed walkthrough, curated by 2 talented hackers, share their story of finding SSRFs in the wild.

- **Need some resources to learn more about server-side template injections?** We got you covered. This thread features 5 videos, all teaching the concept of SSTI identification and exploitation.
- **JavaScript files are goldmines for bug bounty hunters.** This deep dive by kpwn goes through common ways to manually analyze JavaScript files.
- **Web application firewalls (WAFs) can be frustrating and tricky to evade.** This article by Isec goes in-depth on common evasion techniques to bypass WAFs altogether.

Behind the screens

Meet Intigriti at DEF CON 33

Are you ready for DEFCON33? The Intigriti team is!

Come join us on August 7-10 at the Bug Bounty Village and let's make this DECON unforgettable!

We love to connect with valuable researchers like you!

Meet Intigriti at DEF CON 33

Learn more

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!

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com