Intigriti Bug Bytes #225 - June 2025

BY INTIGRITI · JUNE 13, 2025

Hello hackers,

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

- Becoming an Intigriti Pentester
- Exploiting CORS in 2025 (even when SameSite is set to 'Strict')
- A forgotten tool to quickly score new hidden endpoints (right before you close Burp Suite)
- 12 API hacking techniques
- Common ways to find RCEs in your bug bounty target

And so much more! Let's dive in!

Become an Intigriti Pentester

Are you ready to take your cybersecurity expertise to the next level? Intigriti's Penetration Testing as a Service (PTaaS) program offers experienced security researchers an exclusive opportunity to conduct comprehensive security assessments for enterprise clients.

Check if you meet the criteria to become an Intigriti Pentester.

Learn more

Latest Platform Updates

New update to submission statuses

We've made a minor improvement as to how we handle submission evaluations. We updated the classification system for 'Informative' submissions by changing their status from 'positive' to 'neutral.'

This means that when security researchers submit findings that provide valuable information but don't constitute actionable vulnerabilities, these submissions will no longer artificially inflate or deflate their performance metrics and validity ratios.

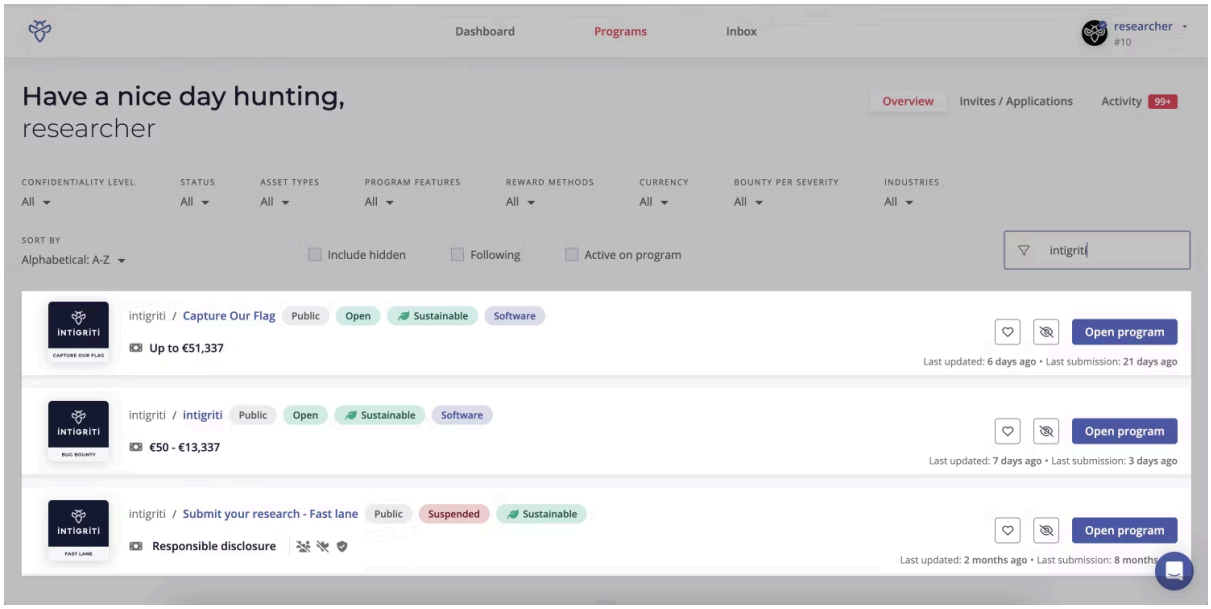
This change ensures that researcher validity ratios accurately reflect impactful contributions, enhancing the fairness of evaluations.

Learn more

Help us make Intigriti better!

We're working on a better browsing experience for bug bounty programs on Intigriti, starting with the program cards you see across the platform.

These cards are your first look at a program, and we want to make sure they highlight the info that matters most to you. What helps you decide whether to click into a program? What's missing?



Intigriti bug bounty program cards

Take our short survey (it only takes a few minutes) and help shape what comes next. Your input directly influences how we design, prioritize, and display program info, making it easier for you to find the right targets faster.

Thanks for helping make Intigriti better, one card at a time.

Take the survey now

Blogs and Videos

Here is a selection of Intigriti blogs and articles from the past month to support your reading:

Exploiting CORS in 2025

CORS: A complete guide to exploiting advanced CORS misconfiguration vulnerabilities Featured Image

CORS misconfigurations can pose significant risks in the right conditions, even in 2025. From extracting sensitive data to fetching internal-only resources! Read our detailed article on our blog to learn how to exploit CORS misconfigurations.

- Forget bruteforcing parameters... There are several other ways to enumerate hidden parameters. The same parameters that lead to all sorts of vulnerabilities, including XSS, SQLi, and potentially even command injections! Learn in our most recent article how you can discover almost all potential parameters on any endpoint or application route.
- Throwback to our previous article: File upload features are quite common in applications. When implemented incorrectly, they can open up a way for you to gain remote code execution! We've outlined several ways to exploit insecure file uploads in bug bounty targets.

Tools and Resources

Tools

JSON2Paths

JSON2Paths by s0md3v

Want to quickly score new endpoints? Before you wrap up and close Burp Suite, try to run JSON2Paths, a simple tool that helps you find new API endpoints and app routes by fetching Burp Suite's history.

- Struggling with bypassing Cloudflare for that one SQLi or XSS? What if we told you you could bypass CF altogether? Check out CF-Hero, a simple wrapper tool to find the origin IP of targets behind Cloudflare.
- Found a potential target vulnerable to a CVE but can't find a working proof of concept? Check out Shodan Exploits, a simple tool that maps out several third-party vulnerability databases to help you query CVE proof of concepts.

Resources

12 API Hacking Techniques

12 API hacking techniques by Intigriti

Have you tried these 12 API hacking techniques on your target? From finding blind XSS vulnerabilities to helpful tips to catch blind XXEs hidden in plain sight!

Check out this extensive thread and let us know if you found it helpful by following us @INTIGRITI.

- Do you hunt for authenticated dashboards on your bug bounty targets? @impratikdabhi found an unauthenticated Kibana dashboard, resulting in a $$$ bounty! Read all about it in his article.
- JavaScript files are always interesting to analyze as they contain references to new endpoints, parameters and sometimes even secrets! @kpwn shares an in-depth article on JS file analysis for web application pentesting.
- Whenever testing bug bounty targets, always pay close attention to session tokens. @moblig documents how he exposed personal identifiable information (PII, including SSNs) through leaked session tokens without an expiry date, resulting in a $15,000 bounty.
- Who said you can't find bugs on public programs? @tabaahi_ shares how he bypassed an incorrect 2-FA implementation in a public bug bounty program, resulting in a $6,000 bounty.

- Throwback: Ever wondered where all the RCEs are? @gregxsunday from Bug Bounty Reports Explained curated a list of the most common ways to achieve remote code execution on one of your bug bounty targets! Watch the video on YouTube.

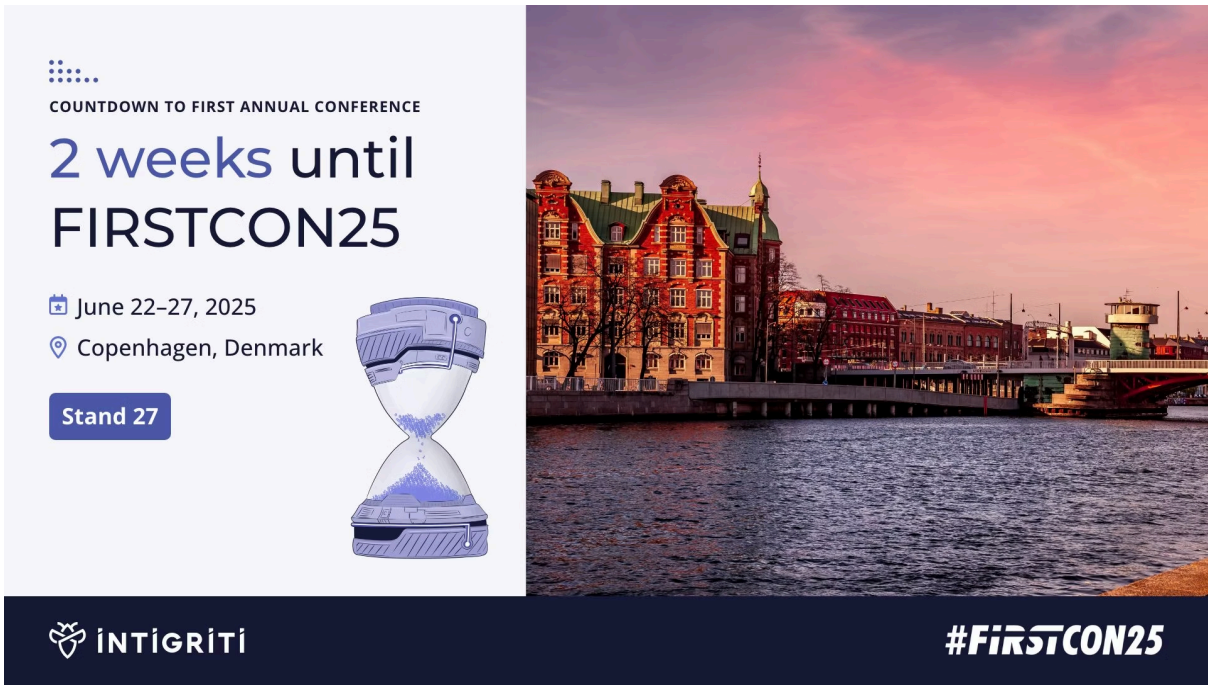
- Vulnerability chaining is still one of the best ways to leverage lower-severity bugs and escalate them to high-severity findings! Learn how this researcher escalated a simple XSS and CORS misconfiguration (with SameSite set to 'Strict') into a 1-click account takeover.

Behind The Screens

Intigriti at FIRSTCON25

Intigriti will be attending FIRSTCON25, an annual gathering for cyber security professionals in Copenhagen, Denmark from June 22 to 27.

If you're there, come and meet the Intigriti team! We will be at stand 27.



Intigriti at FIRSTCON25

Feedback and Suggestions

Before you click away: Do you have feedback or want 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 tag us along on X/Twitter, Instagram or LinkedIn!

Wishing you a bountiful month ahead,

Keep on rocking!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com