Intigriti Bug Bytes #222 - March 2025

BY INTIGRITI · MARCH 14, 2025 · LAST UPDATED ON JULY 30, 2025

Hey hackers,

Each month, we team up with bug bounty experts to bring you insights, platform updates, new programs, and upcoming community events—all to help you find more bugs!

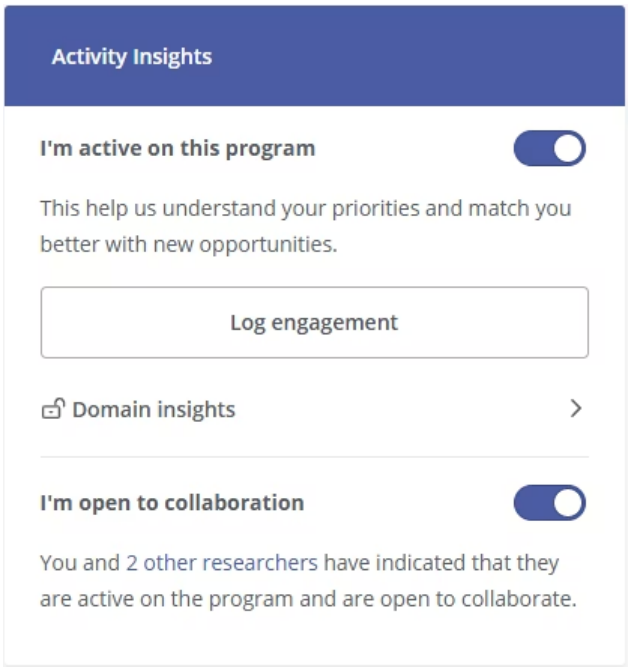
Product updates

New Feature: Gain Deeper Insights into Researcher Activity

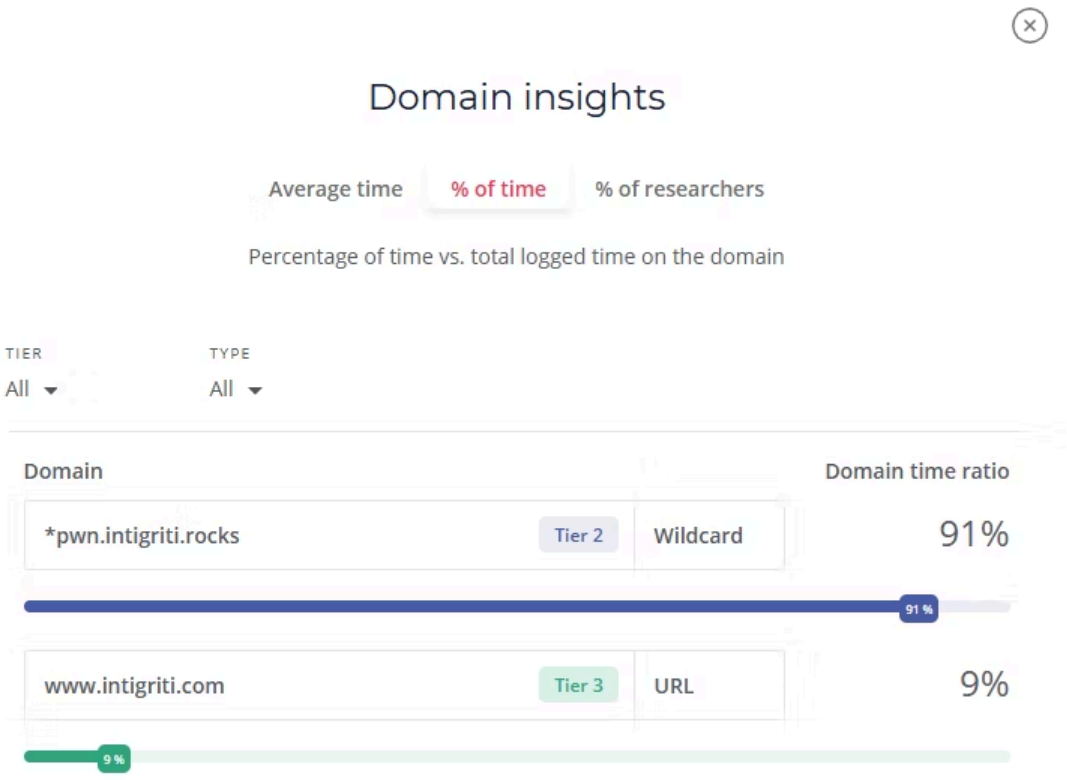
We're excited to introduce a new way for researchers to **gain valuable insights** into their time allocation across different domains within a program.

By sharing how they distribute their efforts, *researchers unlock access to* Domain Insights—a comprehensive dashboard that reveals aggregated statistics on how other active researchers in the program are spending their time.

This feature helps researchers benchmark their focus, identify trends, and make more informed decisions about their work.



Intigriti's New Activity Insights



Intigriti's New Domain Insights

Hacking Time: Can you spot the XSS vulnerability?

XSS might be easy to find or not.... Can you seem to spot the cross-site scripting (XSS) vulnerability in this code snippet?

The exploitation method showcased in this example is **commonly overseen** by most bug bounty hunters, as they're not aware of the possibility to pass your malicious XSS payload in this different format!

Vulnerable Code Snippet

We highly recommend try to solve this and THEN and only then head out to the solution here in our X post.

Blogs and Videos

Here is the selection of Intigriti blogs and articles around the internet of the past month we suggest you to read.

Hacking WordPress Targets!

5 Ways to hack WordPress targets Featured Image

Over 500 million websites are powered by WordPress, but not every instance receives the same security attention, especially if it's a self-hosted WordPress version! In our most recent article, we've featured 5 ways to hack WordPress targets!

- Checkout systems are prominent to price manipulation vulnerabilities! In our recently rewritten article, we've documented 6 ways to bypass payment gateways and place orders for free!
- The "Top 10 Web Hacking Techniques of 2024" by PortSwigger is an essential read for penetration testers, security researchers, and developers looking to stay ahead of the latest attack methodologies. This report showcases the most innovative web security vulnerabilities discovered in the past year, providing technical insights into advanced exploitation techniques.
  Key takeaways include:
  - **OAuth** Flow Hijacking via Cookie Tossing – Exploiting inconsistencies in how browsers handle cookies to hijack OAuth authentication flows, leading to account takeovers.
  - **Wildcard Web Cache** Deception – Using path traversal techniques to bypass caching rules, allowing attackers to poison web caches and leak sensitive user data.
  - **Same-Site Scripting on Mobile Browsers** – Leveraging quirks in SameSite cookie handling to escalate session hijacking attacks across subdomains.
  - **Advanced Cross-**Origin Attacks – New techniques to bypass CORS protections, leading to unauthorized access to restricted web resources.
  - **Server-Side Prototype** Pollution in Modern JavaScript Frameworks – Exploiting object prototype manipulation to trigger remote code execution (RCE) in Node.js applications.

  It is a **crucial** resource for those working in offensive security, bug bounty programs, and secure application development who want to deepen their understanding of modern web exploitation

techniques.

Tools and Resources

Tools

Misconfig Mapper

Misconfig Mapper

Misconfig Mapper: This is an automated tool to help you detect security misconfigurations in popular third-party services—got featured in Help Net Security Magazine and crossed 650 GitHub stars! Try it out and give us your feedback or commit!

- Found a target using GraphQL? We have a whole video series to take you step by step into all related attacks. Find the first video of the series here. Insider Tip: Try sending the introspection query to map out all mutations and queries and explore them in GraphQL Voyager!

- Hacking WordPress targets? Well, there are many out there! Look at WPScan's complete list of vulnerable WordPress plugins. We all know as a hacker you want to automate the entire process of finding security vulnerabilities in WordPress CMS, therefore we suggest WPScan. This is an easy-to-use tool to help you automate from backup file scanning to detecting and exploiting vulnerable WordPress plugins!

- The h4cker repository is a well-structured cybersecurity resource hub, aggregating tools, documentation, and references across domains like reverse engineering, OSINT, penetration testing, and cloud security. Its organized taxonomy ensures efficient access for both novice and expert security professionals.

Resources

NoSQL Injections by @CryptoCat

@CryptoCat's most recent video explains NoSQL injections in database operators to help bypass authentication!

- @coffinxp7 shares his methodology on finding information disclosure vulnerabilities using the Internet Archive (Wayback Machine)!
- @bxmbn documents a bypass of one of his recent IDOR reports that resulted in a $10,000 bounty!
- Vitor shares how he hacked high-profile bug bounty targets and earned over $30,000 in bounties!
- VHost fuzzing is a must nowadays! Discover how you can perform virtual host fuzzing using Ffuf with this one simple command!
- Are you aware of these common vulnerabilities in e-commerce targets? @irsdl has shared a complete guide featuring several attack vectors in financially oriented web applications!
- Ever wondered how most experienced hackers find interesting parameters? We've documented 6 methods to enumerate hidden parameters in API endpoints and application routes!
- Are you fuzzing with multiple HTTP methods? If not, you should! We've featured a simple way to bruteforce content using Ffuf with multiple different HTTP methods! And while you're there, drop us a follow!
- This oldie but goodie video series for reverse engineering has been brought up by one of our employees, and we do see why! It is a very detailed and step by step guide that everyone can follow. If you are new or struggling with reversing, we highly recommend this series to help you to dive into this challenging but interesting topic of hacking.

Behind the screens

Grafana Open Port Event

Recently, 10 epic researchers teamed up at our Open Port event to hack Grafana Labs—a public program on Intigriti! If you want to get involved in the next one, make sure to submit lots of bugs and your effort will be rewarded with bonuses and cool events like this!

Grafana Open Port Event

Events

Intigriti @ Vulncon 2025

Next month, Intigriti will be sponsoring CVE/FIRST VulnCon 2025 for the second year, and we'd love to connect with you! We will be there from April 7-10, 2025, so be sure to stop by and say hello to claim your swag and meet the team! We're also thrilled to announce that our very own Niels Hofmans will be taking the stage to present:

: - ' -

How can it get any better than this?

Feedback and Suggestions

If you have feedback or suggestions to help us build and grow, we want to hear from you! Pop a note over to support@intigriti.com and we'll take it from there!

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