



# Intigriti Bug Bytes #223 - April 2025

BY INTIGRITI · APRIL 11, 2025 · LAST UPDATED ON JUNE 13, 2025

Hello Hackers

Spring is in the air, and so is the sweet scent of freshly reported bugs. Intigriti's blooming too—each month, we squad up with elite hackers to drop hot tips, platform news, shiny new programs, and community events you won't want to miss. Let's make this bug season one for the bounty books.

## Hackdonalds Challenge!

Want a bonus challenge? Quick, the game is still on! Find and [submit your flag](#) before Tuesday, 15 April!

In this bonus challenge—which is much easier than usual—we highlight the true dangers of vibe coding and using AI without precautions for web development!

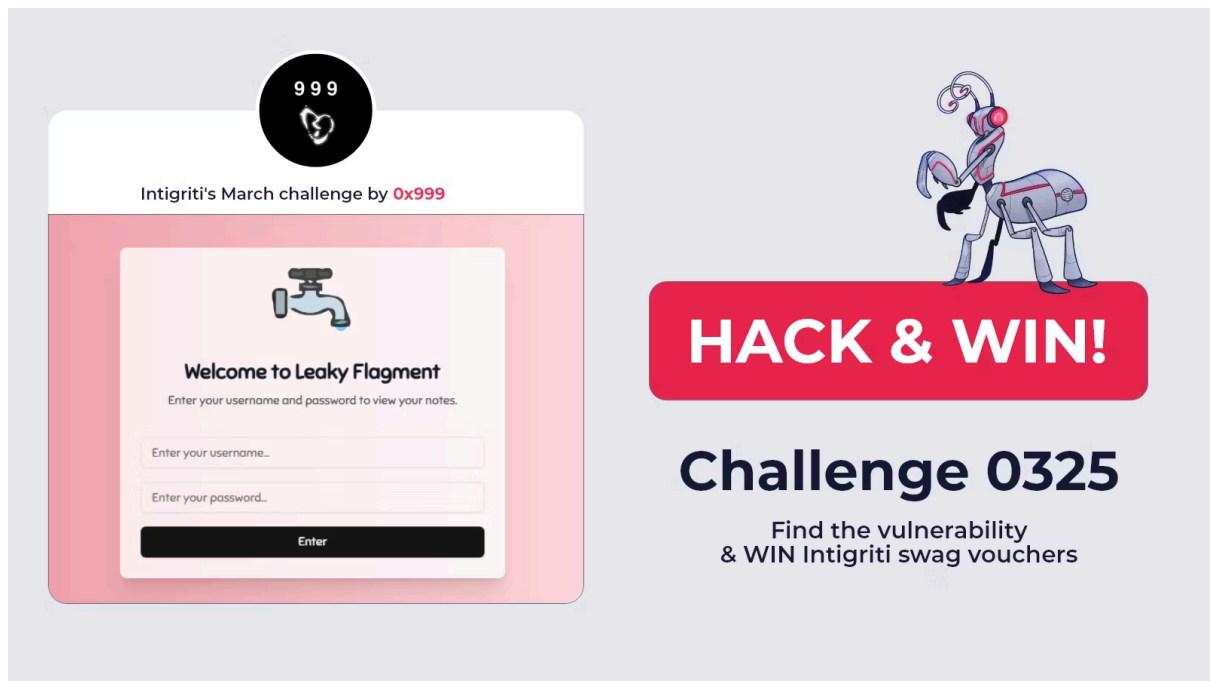


HackDonalds Challenge

## Intigriti's March 2025 Challenge

Intigriti's March challenge proved to be harder than usual with only 16 solves (congratulations to @J0R1AN for getting first blood)! This month's challenge (0325) featured an XSS vulnerability that you could've exploited only by combining multiple other client-side vulnerabilities!

We highly recommend you read the 10 coolest [community write-ups](#) available for this challenge on our Bugology!

The image is a promotional graphic for an Intigriti challenge. On the left, there is a screenshot of a web application titled "Welcome to Leaky Flagment". The page has a pink background and a white header with a black circle containing the number "999" and a heart icon. Below the header, it says "Intigriti's March challenge by 0x999". The main content area features a faucet icon, the title "Welcome to Leaky Flagment", and a subtitle "Enter your username and password to view your notes." There are two input fields: "Enter your username..." and "Enter your password...", followed by a black "Enter" button. On the right side of the graphic, there is a red rounded rectangle with the text "HACK & WIN!" in white. Below this, the text "Challenge 0325" is displayed in a large, bold, black font. Underneath, it says "Find the vulnerability & WIN Intigriti swag vouchers". At the top right, there is a cartoon illustration of a robot with a red head and a backpack. The background of the entire graphic is a light gray gradient.

Intigriti Challenge 0325

Missed the challenge? Buckle up as we organize these challenges every month! Just make sure to [follow us](#) on Twitter/X to stay updated when do!

## Program Updates

[Arm](#) has just launched its new bug bounty platform with rewards of up to €15,000! Do you have what it takes to hack Arm's firmware and hardware devices? Read all about it [here](#).

## Platform Updates

It took us some time, but we delivered BIG! So, the product team has been busy and has exciting things to share!

### New Releases:

- **Researcher Onboarding Questionnaire** (Only for new accounts) - Moving forward all researchers joining intigriti will have the opportunity to select their interests and skill level to enable them to find the best programs fitting their skills and get their first bounty faster!
- **Markdown editor Enhancements:** Enjoy an improved full-screen mode with a fully functional toolbar and a refined preview mode for accurate content rendering. These updates are designed to help you focus on what matters most — clear, seamless collaboration and reporting.

### Coming Soon — April 30th:

We're launching new features to help you discover the most relevant programs and tailor your experience:

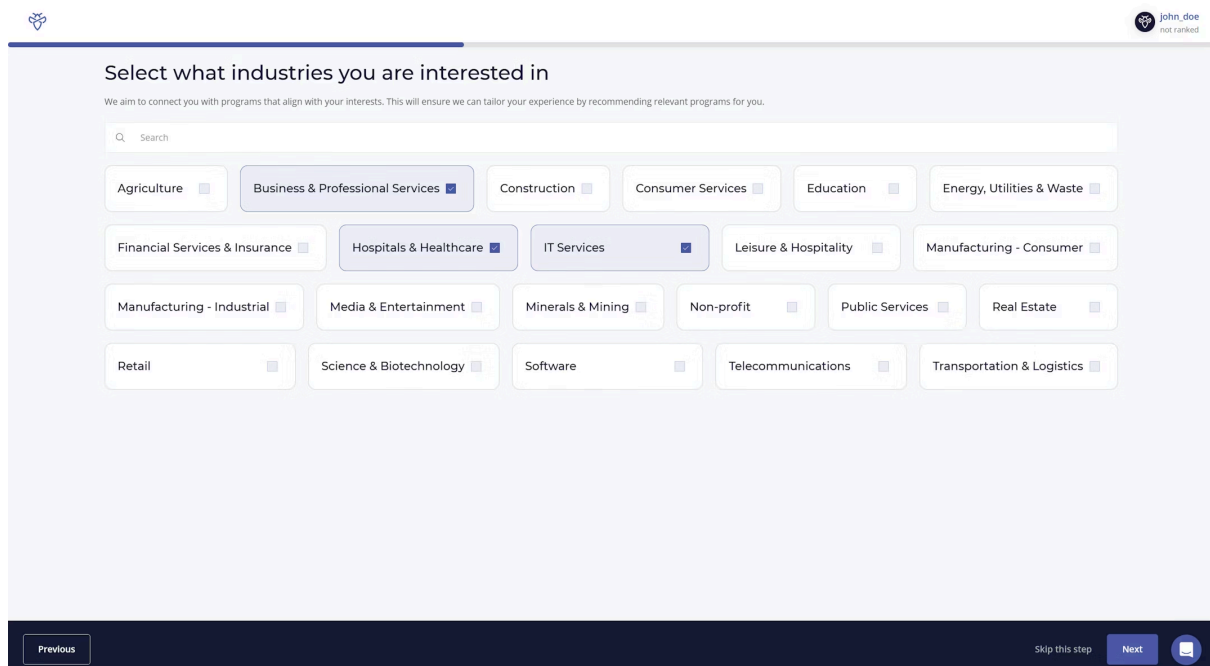
- **Industry Filters** — Easily filter programs by industry to focus on what matters most to you.

- Preferred Industries in Profile — Set your industry preferences in your profile for a more personalized program feed.

## Further in the future:

- Recommended programs (based on chosen industries)
- Neutral informative submissions

More details for the upcoming launches will come SOON! Stay tuned to Intigriti to be always informed and up to date!



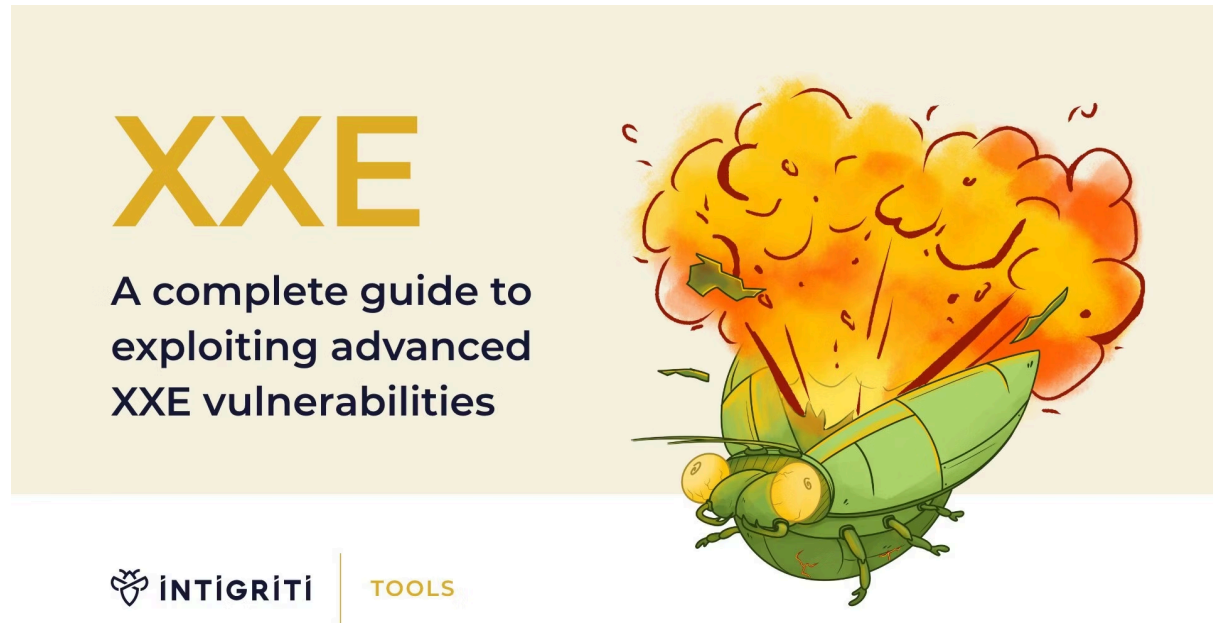
The screenshot displays the 'Select what industries you are interested in' step of the onboarding process. At the top right, the user's name 'John, doe' and status 'not ranked' are visible. Below the title, a search bar is present. The main area contains a grid of 24 industry categories, each with a checkbox. The following industries are selected: Business & Professional Services, Hospitals & Healthcare, and IT Services. The other 21 industries (Agriculture, Construction, Consumer Services, Education, Energy, Utilities & Waste, Financial Services & Insurance, Leisure & Hospitality, Manufacturing - Consumer, Manufacturing - Industrial, Media & Entertainment, Minerals & Mining, Non-profit, Public Services, Real Estate, Retail, Science & Biotechnology, Software, Telecommunications, and Transportation & Logistics) are not selected. At the bottom, there are 'Previous' and 'Next' buttons, along with a 'Skip this step' link and a help icon.

Intigriti Researcher Onboarding

## Blogs and Videos

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

## Exploiting XXE vulnerabilities



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

Have you ever wondered how some hunters are still finding XXE vulnerabilities today? Even though they're seemingly harder to detect, they still remain an impactful vulnerability class worth testing for! Read one of our most recent articles where we document 8 different [XXE exploitation cases](#) for you to test on your targets!

- Report writing is integral in bug bounty! But do you also know how to make your reports stand out so much that you get invited to more private programs, experience faster triage, and even earn a bonus on top of your bounty? We've lined up 8 actionable guidelines for you to follow in our most recent article to help you [write more effective reports](#)!
- Salesforce Experience CRM is complex, and security misconfigurations are easy to arise! Enterprises using custom Apex components can quickly (and unintentionally) open up new security gaps! In our [detailed article](#), we documented some of the most commonly occurring security issues in Salesforce Lightning apps!

## Tools and Resources

### Tools

[Misconfig Mapper](#)

The banner features a dark blue background on the left with the text 'Misconfig Mapper' in white. To the right, a light blue world map is overlaid with several circular heatmaps in blue, red, and green. A magnifying glass with a grey handle is positioned over the map, focusing on a specific area.

# Misconfig Mapper



Misconfig Mapper

[Misconfig Mapper](#) just received an update and almost reaches 700 GitHub project stars (can you help us reach it?!). This tool runs on your valuable feedback and contributions! Feel free to open a GitHub issue or pull request with your input!

- Meet [FfufAI](#): a wrapper that combines the power of Ffuf and OpenAI/Antrophic's models to help you generate interesting files and extensions on the go and detect more hidden content!
- Want to bypass weak validations through unusual normalizations in web apps? [REcollapse](#) is a black-box regex fuzzer that can help you discover payload normalization issues that result in validation bypass!
- Found a potentially vulnerable WordPress plugin? Make sure to head over to [WPScan's Vulnerable Plugins](#) directory! This vulnerability definition database documents almost all vulnerable versions of WordPress plugins!
- [Gohacks](#) is a repository with a collection of all @TomNomNom's bug bounty tools for performing recon and discovering vulnerabilities such as SQLi, XSS, SSRF, etc.!

## Resources

### [NoSQL Injections by @CryptoCat](#)

New video's published! @\_CryptoCat explains [NoSQL injections](#) and how they can be exploited to bypass authentication! We've also restructured our channel and categorized video topics in each playlist! Have a look, and while you're there, [subscribe](#) to our channel to never miss out on new content!

- @zhero\_\_\_ and his teammate @inzo\_ document their recently discovered [authentication bypass in Next.js](#) middleware (CVE-[2025-29927](#))!
- Price manipulation issues are still present in targets like yours! We've curated a small but actionable [thread](#) for you to find these types of vulnerabilities (with images)!

- Do you have an XSS that's held back by CSP? Maybe [this thread](#) can help you finally display the popup!
- @J0R1AN documents how he's found a [cache deception vulnerability](#) in his own website, a vulnerability type that could've resulted in sensitive information disclosure!
- @Ali\_4fg documents a typical [CSRF vulnerability](#) in a GraphQL target and earns a \$2,500 bounty! If you want to dive deeper into GraphQL hacking, make sure you read our [detailed article](#) on our blog!
- Auth bypasses, Google VRP write-ups, CVEs, and more! The [latest CTBB podcast](#) features several of the latest hacking techniques published by community members!

## Behind the screens

### Intigriti at VulnCon!

Intigriti attended VulnCon, a security conference where our head of security & IT delivered an engaging presentation about effective strategies for scaling vulnerability management programs in enterprises!



Intigriti at VulnCon 2025

### Insomni'Hack 2025

Our Intigriti team recently traveled to Lausanne, Switzerland, for the Insomni'Hack 2025 conference! Lenneart, our Head of Triage, represented the company with enthusiasm, connecting with security researchers from around the globe and distributing our exclusive collection of cool stickers!



Intigriti at Insomni'Hack 2025

## 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](mailto:support@intigriti.com) and we'll take it from there!

Wishing you a bountiful month ahead,

Keep on rocking!

**REQUEST A DEMO**

[intigriti.com/demo](https://intigriti.com/demo)

**VISIT THE WEBSITE**

[intigriti.com](https://intigriti.com)

**GET IN TOUCH**

[hello@intigriti.com](mailto:hello@intigriti.com)