Intigriti Bug Bytes #224 - May 2025

BY INTIGRITI · MAY 23, 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 results are in!

An easier-than-usual challenge featuring the dangers of vibe-coded applications! Thank you to everyone who has participated! Some key takeaways:

- 94 hackers reported the flag!
- First blood went to @s3bsrt!
- And 21 hackers wrote a nice write-up, and @_CryptoCat made a detailed walkthrough video!

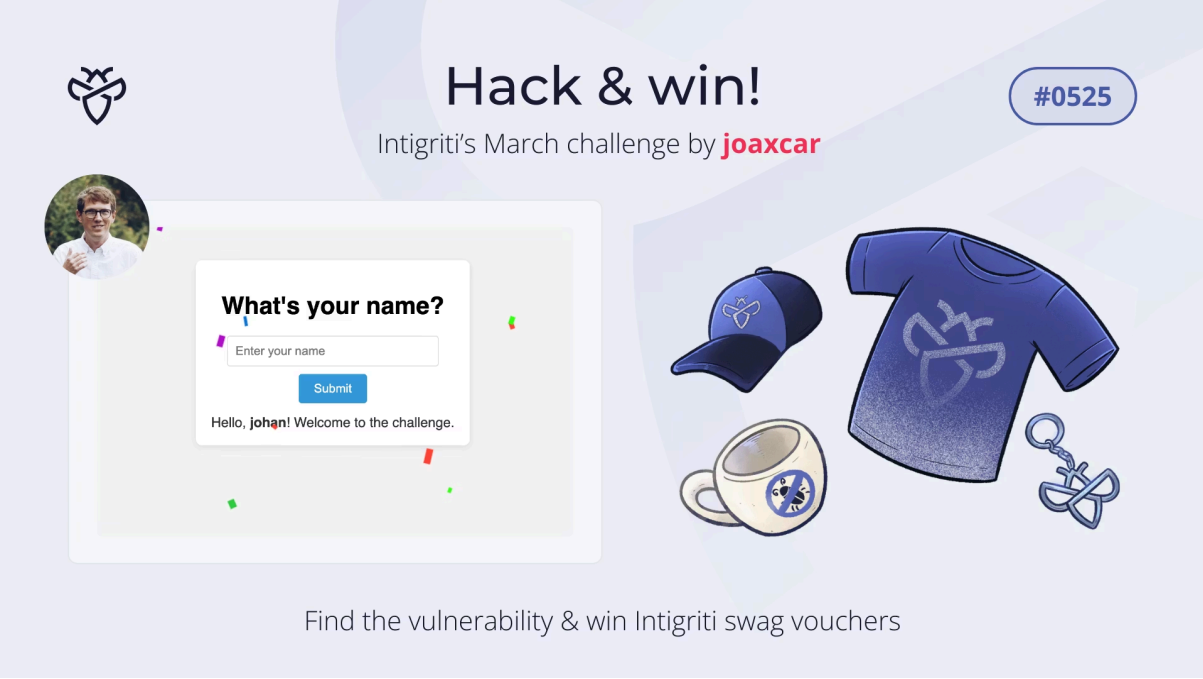
HackDonalds Challenge

Read Community Write-Ups!

Monthly Hacking Challenge: Confetti

This month Intigriti hosted a new XSS challenge made by joaxcar . This challenge featured some ReDoS, DOM clobbering and a URL sanitization bypass. We got a lot of submissions again with some very well-made reports. Some stats about the challenge:

- 13 hackers found the correct solution
- 7 hackers wrote a cool writeup
- First blood went to @salvatoreabello!



Intigriti Challenge 0525

[Read Community Write-Ups!](#)

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!

Spring Heist 2025

Do you have what it takes to...

- Participate in a virtual hacking event
- Earn bounties of up to **€10,000**
- Hack interesting banking targets that challenge your creativity
- And for 2 weeks non-stop?

Buckle up! Spring Heist 2025 is finally here! Apply now and have a chance to win a private invitation to a Live Hacking Event in Belgium!

[Apply Today](#)

Latest Platform Updates

New features have arrived to help you discover the most relevant programs and tailored to 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.

Bug Bounty Talks Tool Is Live!

Bug Bounty Talks Tool

We're thrilled to launch our brand-new Bug Bounty Talks page, a space where companies and event organizers can discover and request talks from top ethical hackers in our community.

Whether you're looking to book a speaker for your next security meetup or want to learn from the best, this is the place to start.

How it works:

- Browse talks from talented researchers
- Submit a request via the form
- We'll review and forward valid requests directly to the speaker

Are you a hacker with a story to tell? Submit your own talk and join the lineup, it's quick and easy!

Visit the Bug Bounty Talks Page

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 NoSQLi injection vulnerabilities]

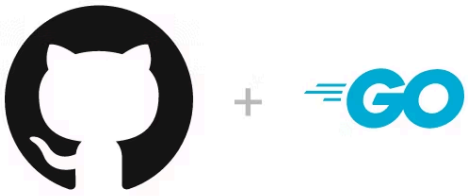
NoSQL injections are quite easy to exploit compared to classic SQL injections... But they're seemingly so much harder to spot! In our most recent [article], we documented how you can identify, exploit, and escalate this notorious SQL injection type!

- Want to start finding more subdomain takeover vulnerabilities? Without catching duplicates? Read our [detailed article] on how you can start finding subdomain takeovers that most other hunters miss out on!
- Vibe coding is one of the latest trends that is taking over the web development space! We curated an [in-depth guide] for you to follow to spot more vulnerabilities in AI-generated code!

Tools and Resources

Tools

[SQLTimer]



c1phy/sqltimer

A fast, minimalistic scanner for time-based SQL injection (SQLi) detection – built in Go.

SQLTimer

Want to quickly scan for time-based SQL injections? Make sure you give SQLTimer a try! It's a simple, blazing-fast tool (written in Golang) and available on GitHub!

- @albinowax from PortSwigger shared a quick and simple script to help you test for race condition vulnerabilities! A bug type that can lead to all sorts of unexpected outcomes!
- Looking for mobile pentesting tools? Check out Medusa by Ch0pin, a framework to help you test Android & iOS mobile apps!
- Fuzzing with weird characters can introduce interesting responses. Recollapse is a simple fuzzing tool to help you fuzz for unusual normalizations in web apps and generate payloads to bypass weak validations!
- Want to transform your payload into obscure characters? Unicode Text Converter is a simple tool that lets you easily convert your payloads into weird characters to bypass weak filters!

Resources

Investigating an in-the-wild campaign using RCE in CraftCMS

Investigating an in-the-wild campaign using RCE in CraftCMS

RCE in CraftCMS! This technical investigation report by Orange Cyberdefense goes in-depth on how a server was compromised through 2 CVEs in CraftCMS!

- When testing for 2FA bypasses, always examine your requests! @tabaahi_ shares in his latest article how he could bypass 2FA through a quite simple trick! If you want to dive deeper into 2FA hacking, make sure you also give this article a read!
- Account takeover vulnerabilities can be achieved in various ways! @sec_0xbro documents how he could take over any account through 2 different password reset vulnerabilities!
- Are client-side bugs hard to spot for you? Not anymore after you've gone through the following extensive list of resources for client-side vulnerabilities!
- Developers still push unwanted code to production! Nocley and his teammate Fatman shared how they'd discovered an ENV file via GitHub Dorking!
- We all know SSRF vulnerabilities can turn into impactful vulnerabilities. Skyer documents his way of finding an SSRF vulnerability to gain access to internal panels and millions of user records!

Behind The Screens

Intigriti at CyberSec Europe!

Intigriti attended CyberSec Europe! Our team delivered 3 exceptional talks ending with our Chief Hacker Officer (CHO), @intidc, bringing magic to the main stage!

Quick Recap!

- "Unmasking the Hacker" (May 21, 16:00-16:30) featuring a fireside chat with a top ethical hacker.
- "Scaling Vulnerability Management" (May 22, 10:00-10:30) with our Head of Security & IT Niels H. sharing practical advice for organizations with limited resources.
- And "The Grand Finale," where our Chief Hacker Officer Inti De Ceukelaire will present his "magical hacks" show as the closing presentation.

Intigriti at CyberSec Europe

Intigriti is now CREST Accredited!

Intigriti is now officially CREST accredited! A prestigious recognition that validates our robust methodologies and commitment to delivering top-tier security pentesting services!

Read all about it in our latest **article**!

CREST Accreditation Reinforces Intigriti's Pentesting Excellence

Read the full article

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
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com