



# Intigriti Bug Bytes #219 - December 2024

BY BLACKBIRD-EU · DECEMBER 13, 2024 · LAST UPDATED ON MARCH 6, 2025

**Bug Bytes is finally back!** Each month we sit down with experienced bug bounty community members to deliver this new insightful newsletter to help you find more bugs, keep you updated with the latest platform updates and programs on Intigriti and share upcoming community events!

If you haven't subscribed yet, click on the link below to receive your copy of the monthly newsletter filled with exclusive bug bounty tips, infosec news and much more!

<https://newsletter.intigriti.com/>

## Latest Platform Updates

We're pleased to announce we have switched our ID checks provider to ensure the crucial step of validating your ID is as seamless as possible.

If you haven't already, be sure to validate your researcher profile (this will boost your chances of being invited to private programs!).

[Get Verified!](#)

# 1337UP LIVE CTF 24 – Video Walkthrough's



Intigriti 1337UP Live CTF Event 2024

Missed our annual CTF event? We've got you covered! Check out CryptoCat's video walkthrough's covering each of this year's challenges via our [YouTube Channel](#).

# Yahoo moves its Bug Bounty Program exclusively to Intigrity!

**yahoo!**

📢 Special announcement

## Now exclusively on Intigrity

 INTIGRITI



Yahoo! Bug Bounty Program

Start [submitting reports today](#) and be in with the chance of earning some exclusive swag.

[Hack on Yahoo!](#)

# Blogs and Videos

## Hacking With Shodan & Censys!

### Complete guide to finding more vulnerabilities with Shodan and Censys



Complete guide to finding more vulnerabilities with Shodan and Censys Cover Image

Have you ever wondered how pro bug bounty hunters keep finding interesting assets that lead to critical bugs via Shodan or Censys? We've published an entire article for you that dives deep into [finding valuable assets to find more vulnerabilities with internet search engines!](#)

- Testing a target that makes use of a NoSQL database (such as MongoDB)? NoSQLMap by [@codingo](#) is your best friend! [It's an extensive tool to help you detect potential NoSQL injection vulnerabilities](#), a non-commonly tested bug type!
- What if we told you there's a tool to help you find interesting assets and hosts related to your target without having to check Shodan, Censys, ZoomEye and tons of other services? [Meet Uncover by @pdiscoveryio! It's simple and it allows you to combine several external sources and get a summarized \(and easy-to-parse\) output!](#)
- [Shodan for AWS: AWSEye.com is an interesting tool](#) that can be deployed to enumerate all AWS services used by your target! Just enter an AWS account ID and watch for interesting results to come your way!

## Tools and Resources

### Tools

Misconfig Mapper

A banner for Misconfig Mapper. On the left, a dark blue background contains the text 'Misconfig Mapper' in white. To the right, a light blue world map is shown with several circular markers in blue, red, and green. A magnifying glass is positioned over the map, focusing on a specific area.

# Misconfig Mapper



Misconfig Mapper

[You're missing out on critical misconfigurations if you aren't using Misconfig Mapper!](#) A simple tool that can help you automate security misconfiguration detection on your list of targets!

- Your bug bounty methodology is everything! It can help you find more unique bugs! [Learn how to craft your own unique methodology to find more vulnerabilities!](#)
- Authentication vulnerabilities are hard to spot! [This new article covers everything from simple authentication bypasses to more advanced cases!](#)
- Want to dive even deeper into authentication vulnerabilities? [We've also covered 7 advanced ways to bypass multi-factor authentication implementations!](#) This article is a must to add to your current checklist!
- New Hackademy Videos have been published! [This series of new videos will guide you through exploiting LLMs](#), an increasingly new feature you'll come across in new bug bounty targets!

## Resources

Finding SQL Injections Like a PRO!

## A Advanced SQL Injection Techniques

# Advanced SQL Injection Techniques by nav1n0x

Here are some Advanced SQL Injection Techniques I commonly use. Happy hunting! 👍

Advanced SQL Injection Techniques by nav1n0x

[@nav1n0x](#)—a talented hacker on Intigriti—[shares his entire methodology and approach to hunting for advanced SQL injection vulnerabilities, including interesting WAF bypasses!](#)

- In case you aren't aware yet, [@zseano](#) has shared [his methodology for hacking web applications and bug bounty programs into a single PDF file!](#)
- Are you already [following us on X/Twitter?](#) If not, you're missing out on (almost) daily tips to help you find more vulnerabilities! [Here's our recent post to help you find more vulnerabilities with BurpSuite match & replace rules!](#)
- Found an SQL Injection? [Try to escalate it to an RCE! Here are 5 ways to do so!](#)
- [Portswigger Labs introduced new interactive testing labs for Web Cache Deception vulnerabilities!](#) These bugs can help you trick a caching service to serve your poisoned cache to achieve stored XSS for example!

## Recent Events

**CTF 24':** A massive thanks to all who took part in helping us build our biggest CTF event yet – check out the final scores [here](#).

**OpenPort Germany:** Back in November, members of the community gathered in-person for a weekend of live hacking on [Allegro](#).



OpenPort Germany Participants

## Behind The Screens

Hackers Team leveled up with Burp Suite training



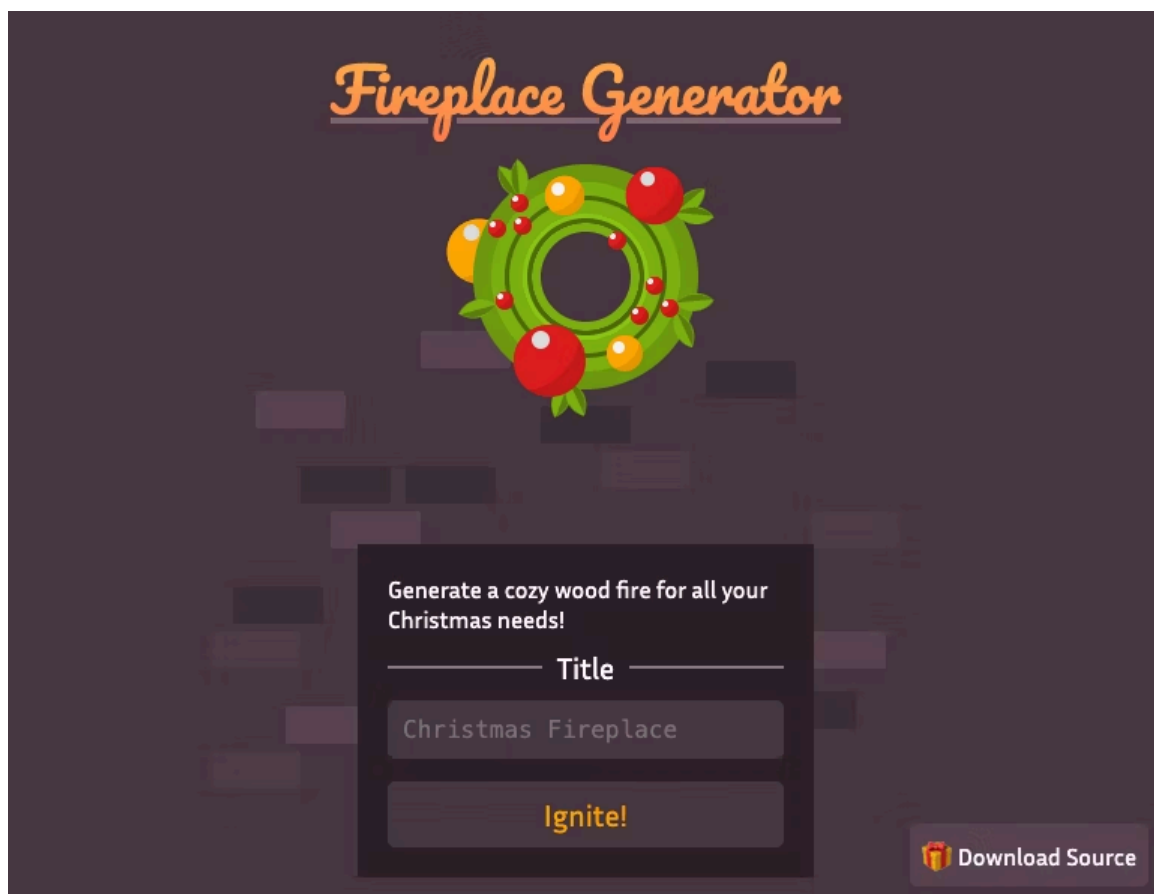
Hackers Team leveled up with Burp Suite training

Our Hacker Ops Team (Triage and Community) just leveled up with an insightful Burp Suite training session!

The training, 'Mastering Burp Suite Pro - 100% Hands-On', equipped our team with the latest techniques in web security testing, ensuring we stay ahead of the curve in protecting our clients.

This hands-on education not only strengthens our team's expertise but also reinforces our dedication to providing top-notch security services.

## Monthly Challenge



Intigriti's December Challenge

Intigriti's December Challenge by Jorian is here. Pop an alert here, <https://challenge-1224.intigriti.io/> and hack to get amazing swag! The list of prizes are:

- First blood: €100 swag
- 5 random [correct] submissions: €50 swag
- 5 best writeups/videos: €50 swag

Make sure to solve and submit your writeups by Thursday 19th of December.

# Feedback and Suggestions

Our researchers are at the core of everything we do. 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!

As 2024 draws to a close we want to take a moment to reflect on a truly remarkable year here at Intigriti.

Each member of our community makes us who we are, and we couldn't be prouder of what we have achieved together – thank you!

Wishing you a restful holiday season, see you in 2025...

Team Intigriti

**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)