# Intigriti Bug Bytes #228 - September 2025

BY INTIGRITI · SEPTEMBER 12, 2025 · LAST UPDATED ON SEPTEMBER 19, 2025

## Hi hackers,

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

- A common (yet unknown) SSRF attack vector in Next.js Middleware
- Exploiting PDF processors by generating and uploading malicious PDF payload files
- A full reconnaissance breakdown on how to approach any target

And so much more! Let's dive in!

## INTIGRITI 0825 results are in

This month's challenge by @0xblackbird featured a unique misconfiguration in Next.js Middleware that introduced a server-side request forgery (SSRF) vulnerability. With only 7 solves, it joins the top of the toughest challenges ever to be featured on Intigriti.

Quick recap:

- 7 hackers reported the correct flag
- First blood went to @J0R1AN
- And 2 hackers wrote a nice write-up


INTIGRITI Challenge 0825

[Read all write-ups]

# INTIGRITI 0825 official write-up

Our latest community challenge featured a unique SSRF pattern in NextJS Middleware that many developers (& security researchers) don't know about. That's why we decided to publish an official write-up to help raise awareness.

If you wish to learn how it was possible to escalate this simple SSRF and leverage an internal Jenkins instance to achieve RCE, make sure you read our technical guide.


August CTF challenge: Exploiting SSRF via NextJS Middleware Cover Image

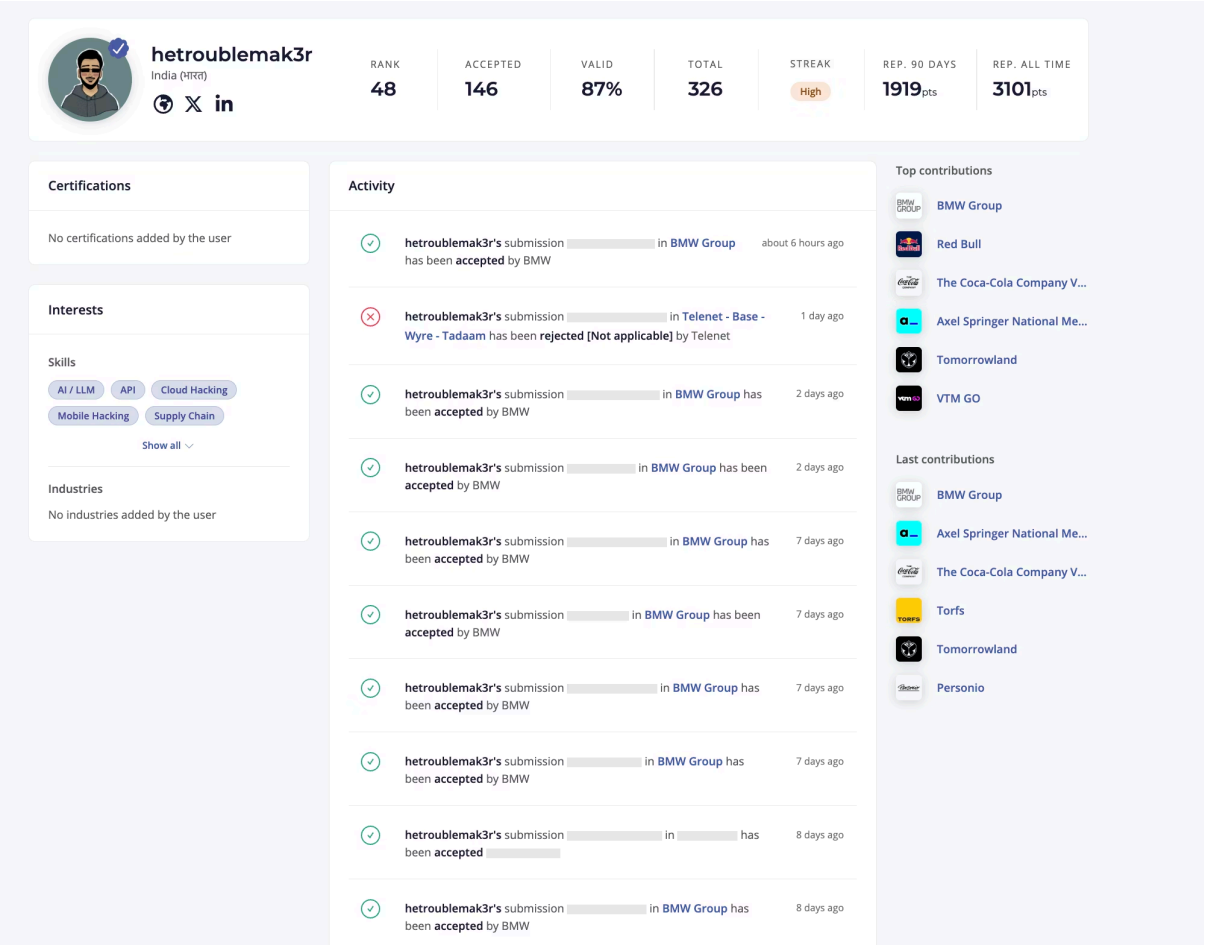
[Read the write-up]

# Platform updates

## New centralized researcher profile

This new centralized researcher profile helps researchers like you by providing a convenient, unified hub to manage your information and track your performance.

Making it easier for you to keep your public-facing profile up-to-date to build credibility and showcase your expertise.

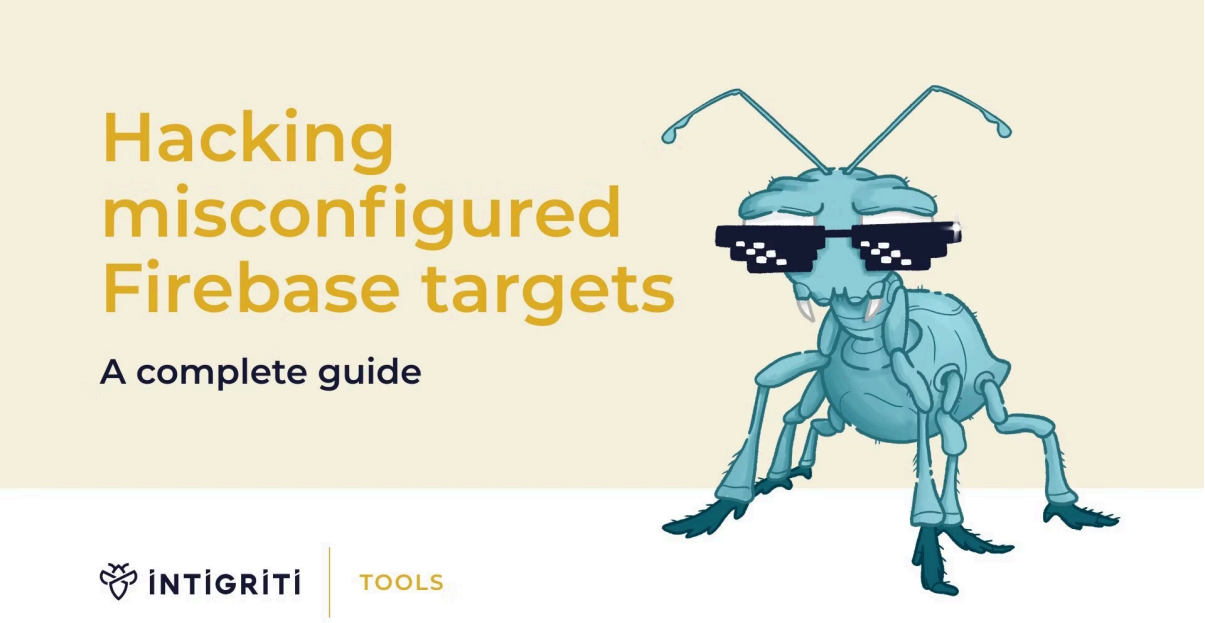



New centralized researcher profile on intigriti.com

[Sign in to your account]

# Blogs & videos

## Hacking Firebase targets




Hacking misconfigured Firebase targets: A complete guide Cover Image

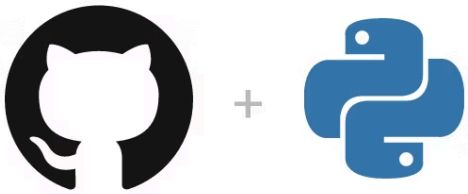
Firebase targets make use of custom security rules that are much more complex to get right... causing security misconfigurations to stay undiscovered for months. In our technical article, we dove deeper into understanding and exploiting vulnerable Firebase targets to leverage misconfigurations into data leaks.

- **You've probably come across a target that featured a (web-based) plugin ecosystem...** often seen as an undiscovered, new attack surface for us to explore. As developers fail to draw the correct line between security and extensibility, security issues will keep arising. In our detailed guide, we've outlined 4 common security issues to test for when approaching a target featuring a web-based plugin/add-on marketplace.
- **The invisible injection point and delayed execution make them an easily overlooked vulnerability...** yet they can still form a severe impact on any organization out there. In our technical guide, we documented our methodology for finding blind XSS vulnerabilities, including a few cool payloads you could try next time you're testing a target for blind XSS.

# Tools & resources

## Tools

### Malicious PDF Generator



# jonaslejon/malicious-pdf

💀 Generate a bunch of malicious pdf files with phone-home functionality. Can be used with Burp Collaborator or Interact.sh

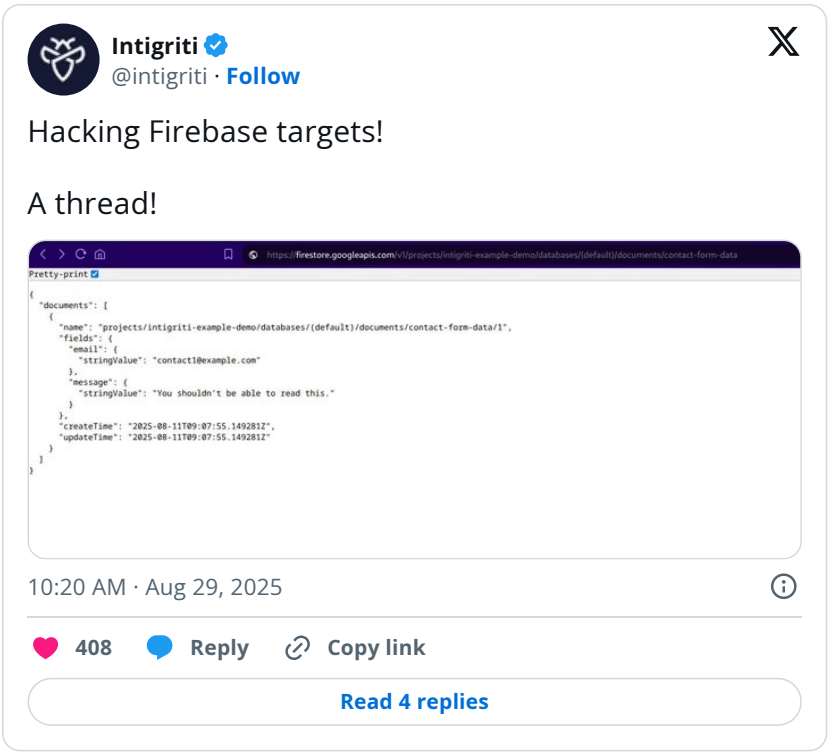

Malicious PDF Generator

**Testing for file upload vulnerabilities?** Make sure to give Malicious PDF Generator a try. It's an open-source toolkit to quickly generate tens of malicious PDF files designed to help exploit various vulnerabilities and insecure features found in PDF readers.

- **Targeting Firebase applications?** Try out Insecure Firebase Exploit, a simple Python-based tool to quickly test for missing access controls and validation checks.
- **Looking for a unified resource to read write-ups, bug bounty articles, and other hacking material?** Make sure you check out BugBountyHunting.com, a simple search engine by @payloadartist to help you discover new, valuable web hacking resources.
- **If you're neglecting security misconfigurations,** you're possibly leaving lots of bugs on the table… Try out Misconfig Mapper, a simple, template-based tool that can help you easily check your list of targets for possible third-party security misconfigurations.

## Resources

### Hacking Firebase targets




**Targeting Firebase applications?** Make sure to go through this thread to learn more about exploiting common vulnerabilities and security misconfigurations in Firebase targets.

- Dzmitry explains how he found remote code execution in Facebook, resulting in a +$100K bounty.
- Server-side request forgery (SSRF) can be escalated. Skyer shares how he exploited an SSRF vulnerability to access millions of PII records.
- Difficulties with reading and understanding regex patterns? @nahamsec explains how regexp can be weaponized in his latest video.
- Never estimate CTFs as they can teach valuable bug bounty lessons. @renwa shares his story of finding a critical UXSS through a CTF.
- Did you know that you could exploit an XSS by pasting your payload? @coffinxp documents how to exploit and weaponize copy-paste XSS.
- HTTP request smuggling vulnerabilities are still present. This most recent article from Portswigger shows how HTTP/1.1 can still benefit bug bounty hunters who search for request smuggling vulnerabilities.
- Targeting a bug bounty program that uses Firebase? Make sure you read @_m1tZ's article on approaching Firebase targets to map out common security misconfigurations.
- Account takeovers are critical by nature. @medusa_0xf shares her story of finding and exploiting an account takeover vulnerability in the forgotten password authentication flow.
- Hesar101 shares his story of chaining an SSO misconfiguration, self-XSS, and cache poisoning into a 0-click account takeover.
- Reconnaissance can help you uncover several critical vulnerabilities. @coffinxp breaks down his entire methodology for performing reconnaissance on your bug bounty target (including a checklist).

- Looking for a quick way to enumerate cloud buckets utilized by your target? Check out this post documenting how you can enable Google dorking to enumerate cloud buckets!

## Feedback & suggestions

**Before you click away!** Do you have feedback, or would you like 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 tagging us along on X/Twitter, Instagram, or LinkedIn!

Wishing you a bountiful month ahead,

Keep on rocking!