



Introducing Misconfig Mapper: The ultimate security misconfiguration tool

BY INTIGRITI · APRIL 29, 2024 · LAST UPDATED ON MARCH 6, 2025

In case you missed it on our Twitter channel, we've recently launched [Misconfigurations Mapper](#) (or MisconfigMapper for short)! Misconfig Mapper is a new project designed by Intigriti Hackers Team to help you find security misconfigurations in popular services used at your bug bounty/penetration testing targets (such as Atlassian, Jenkins, etc.)

Additionally it can help you find several security system flaws. From basic access control misconfigurations to code injections & remote code execution vulnerabilities.

Misconfig Mapper

Misconfig Mapper is a new project developed by Intigriti to help bug bounty hunters, and security researchers map out common security misconfigurations in well-known software services and products like Atlassian, Jenkins, and GitLab but also popular frameworks like PHP Laravel.

It serves as a valuable resource for both attackers and defenders to map out and understand the common misconfigurations that can lead to security vulnerabilities in these services.

In this blog post, we will cover the main benefits and features of Misconfig Mapper and also show you how to use the automated tool that comes with it. In case you prefer a non-written guide, check out the video we prepared for you.

Documentation

The documentation is the main resource, and we included all the information you will need to understand, detect, and mitigate the security misconfiguration.

Each section or security misconfiguration is divided into 6 separate categories, description, proof of concept URL, steps to reproduce, potential impact, mitigation steps, and also resources (if available).

Public Groovy Script Console

Description:

Groovy Script Console provides developers a way to run Groovy Script code right from their browser. However, in case permissions aren't configured properly, it could introduce another attack vector and often lead to remote code execution.

Testing:

Navigate to the following app route and check if Groovy Script Console is publicly accessible:

```
/script
```

You can also send a **POST** HTTP request to the `/script` or `/scriptText` app routes with your script contents in the `script` body parameter (make sure to change the positional variables with your own values):

```
curl -s 'https://jenkins.{HOST}/script' -X 'POST' --data 'script={SCRIPT}'
```

or:

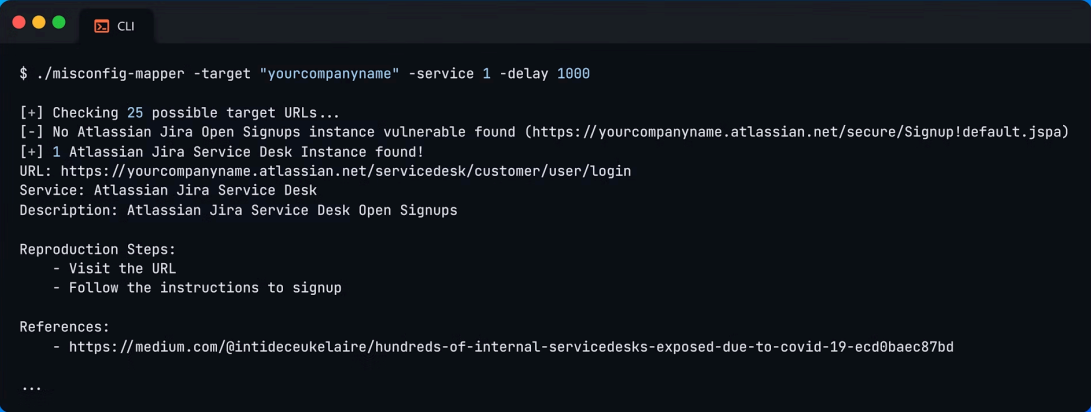
Example of a Public Groovy Script Console accessible on a misconfigured Jenkins instance.

The documentation is available [here](#).

Batteries Included!

Misconfig Mapper also comes with its own dedicated automated scanner to help you test these security misconfigurations at scale!

The scanner is written in Golang and is also aimed at helping you automate and find these issues quickly!



```
CLI
$ ./misconfig-mapper -target "yourcompanyname" -service 1 -delay 1000

[+] Checking 25 possible target URLs...
[-] No Atlassian Jira Open Signups instance vulnerable found (https://yourcompanyname.atlassian.net/secure/Signup!default.jspa)
[+] 1 Atlassian Jira Service Desk Instance found!
URL: https://yourcompanyname.atlassian.net/servicedesk/customer/user/Login
Service: Atlassian Jira Service Desk
Description: Atlassian Jira Service Desk Open Signups

Reproduction Steps:
- Visit the URL
- Follow the instructions to signup

References:
- https://medium.com/@intideceukelaire/hundreds-of-internal-servicedesks-exposed-due-to-covid-19-ecd0baec87bd
...
```

Example of a misconfigured "Atlassian Jira Service Desk" finding using Misconfig Mapper.

It is also similar to Nuclei's template-based scanner, as it too uses templates to guide the scanner in reproducing the detection phase and identifying potential findings! Moreover, adding new templates for new security misconfigurations is straightforward & simple thanks to the available type definitions and documentation!

The scanner also features several options, including a wildcard and permutation flag to further expand your testing coverage!

Supported Services

As of now, there are over 15 services documented and over 10 misconfigurations automated! We are planning to gradually add support for more services and misconfigurations over time!

We welcome and appreciate contributions a lot as well! If you'd like to help with documenting and/or creating new templates, please feel free to [check out the Contributions guide](#) that can be found on the official GitHub repository!



```
$ ./misconfig-mapper -list-services

| ID | Service
|----|-----
| 0  | Atlassian Jira Open Signups
| 1  | Atlassian Jira Service Desk
| 2  | Slack
| 3  | Google Groups Misconfigured Read Permissions
| 4  | Google CloudStorage Bucket Misconfigured Read Permissions
| 5  | Jenkins Open Signups
| 6  | Jenkins Public Groovy Script Console
| 7  | Gitlab Private Source Code Snippets Exposed
| 8  | Drupal Nodes with Misconfigured Access Controls
| 9  | Laravel Debug Mode Enabled
| 10 | Laravel Telescope enabled in production
| 11 | GraphQL Introspection Query Enabled
```

A list of automated misconfigurations.

Try it out

All-in-all, you should give it a go on your current or next bug bounty target!
Check out the scanner on [our official GitHub account!](#)

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com