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.

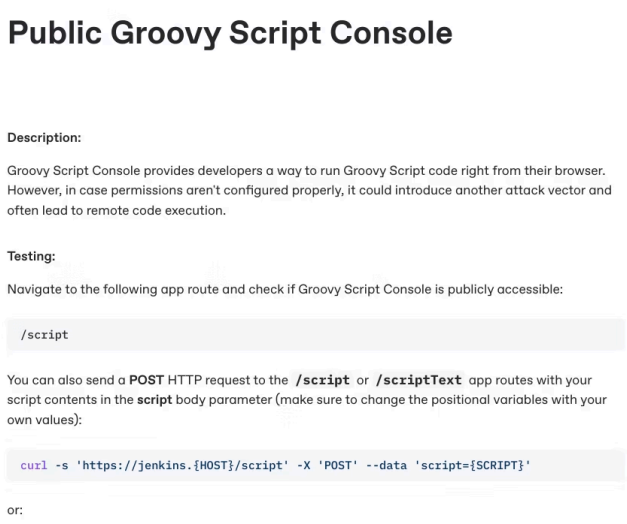
It serves as a valuable resource for both attackers and defenders to map out and understand the common misconfigurations that can lead to security vulnerabilities in these services.

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).

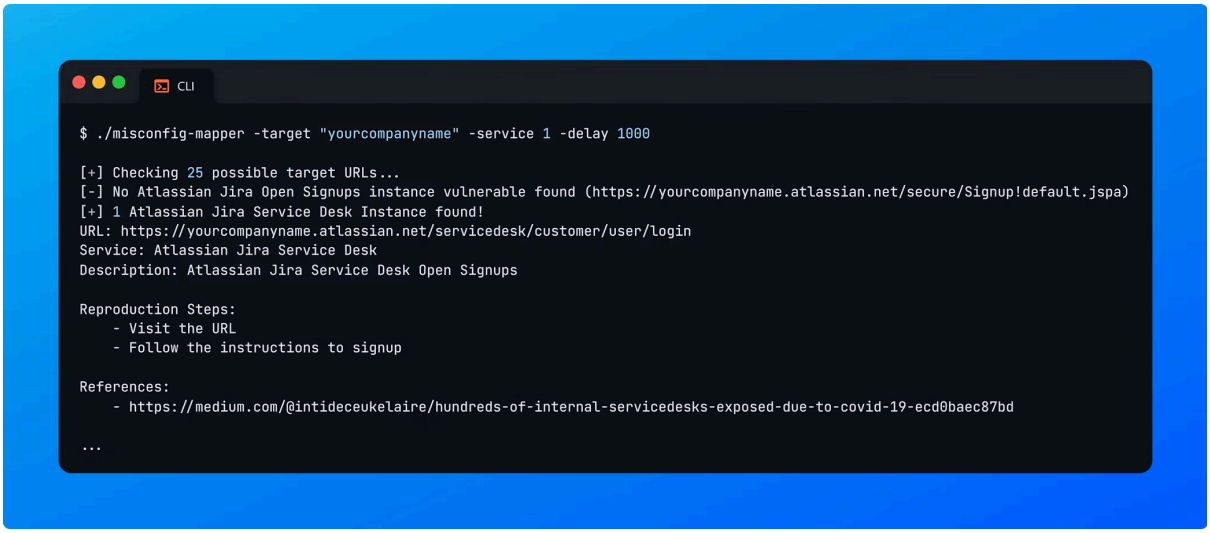


Example of a Public Groovy Script Console accessible on a misconfigured Jenkins instance.

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!



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!

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!