 **s0md3v** / **Corsy**

[Watch](#) 12 [Star](#) 434 [Fork](#) 39

[Code](#) [Issues 1](#) [Pull requests 3](#) [Projects 0](#) [Security](#) [Insights](#)

Join GitHub today

Dismiss

GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.









[Sign up](#)


CORS Misconfiguration Scanner


[20 commits](#) [1 branch](#) [0 packages](#) [2 releases](#) [2 contributors](#) [GPL-3.0](#)

[Branch: master ▾](#) [New pull request](#)

[Find file](#) [Clone or download ▾](#)

 s0md3v Merge pull request #8 from afranche/master ...	Latest commit d1da167 9 days ago
 core	should resolve #7 10 days ago
 db	Update details.json 9 days ago
 CHANGELOG.md	changelog for 0.2-beta 12 days ago
 LICENSE	Initial commit 12 days ago
 README.md	updated donation link 10 days ago
 corsy.py	bumped version 12 days ago
 requirements.txt	Create requirements.txt 12 days ago

 **README.md**



Corsy

CORS Misconfiguration Scanner

[release](#) [v0.2-beta](#) [closed issues 5](#)

Introduction

Corsy is a lightweight program that scans for all known misconfigurations in CORS implementations.

```
C O R S Y {v0.1-beta}

[+] Misconfiguration found!
[!] Title: Post-domain wildcard
[!] Description: The origin verification is flawed, it allows requests from a host that has
this host as a prefix.
[!] Severity: High
[!] Exploitation: Make requests from target.com.attacker.com
```

Requirements

Corsy only works with `Python 3` and has the following dependencies:

- `tld`
- `requests`

To install these dependencies, navigate to Corsy directory and execute `pip3 install -r requirements.txt`

Usage

Using Corsy is pretty simple

```
python3 corsy.py -u https://example.com
```

A delay between consecutive requests can be specified with `-d` option.

Note: This is a beta version, features such as JSON output and scanning multiple hosts will be added later.

Tests implemented

- Pre-domain bypass
- Post-domain bypass
- Backtick bypass
- Null origin bypass
- Unescaped dot bypass
- Invalid value
- Wild card value
- Origin reflection test
- Third party allowance test
- HTTP allowance test

Support the developer

Liked the project? Donate a few bucks to motivate me to keep writing code for free.

