Why GitHub? Enterprise Explore Marketplace Pricing Search / Sign in Sign up

haccer / **subjack**

Watch 35 Star 727 Fork 122

Code Issues 10 Pull requests 4 Security Insights

Subdomain Takeover tool written in Go

go golang hostile subdomain takeover subdomain-takeover bug-bounty pentesting infosec bugbounty security

170 commits **1** branch **0** packages **10** releases **2** contributors Apache-2.0

Branch: **master** New pull request Find file Clone or download

haccer rm CloudFront ✓ Latest commit `b800ca4` on Jul 31

subjack	Add TLS skip verify & change format	11 months ago
.appveyor.yml	Changes to README.md for Godoc	2 years ago
.gitignore	Create .gitignore	2 years ago
.travis.yml	Create .travis.yml	2 years ago
LICENSE	Initial commit	2 years ago
README.md	Update README.md	last year
fingerprints.json	rm CloudFront	4 months ago
main.go	Add new -m option	last year

README.md

subjack

build passing | Windows - OK | go report A+ | godoc reference | license Apache-2.0

Subjack is a Subdomain Takeover tool written in Go designed to scan a list of subdomains concurrently and identify ones that are able to be hijacked. With Go's speed and efficiency, this tool really stands out when it comes to mass-testing. Always double check the results manually to rule out false positives.

Subjack will also check for subdomains attached to domains that don't exist (NXDOMAIN) and are **available to be registered**. No need for dig ever again! This is still cross-compatible too.

What's New? (Last Updated 09/17/18)

- Custom fingerprint support
- New Services (Re-added Zendesk && Added Readme, Bitly, and more)
- Slight performance enhancements

Installing

Requires Go

```
go get github.com/haccer/subjack
```

How To Use:

Examples:

- `./subjack -w subdomains.txt -t 100 -timeout 30 -o results.txt -ssl`

Options:

- `-w domains.txt` is your list of subdomains.
- `-t` is the number of threads (Default: 10 threads).
- `-timeout` is the seconds to wait before timeout connection (Default: 10 seconds).
- `-o results.txt` where to save results to. For JSON: `-o results.json`
- `-ssl` enforces HTTPS requests which may return a different set of results and increase accuracy.
- `-a` skips CNAME check and sends requests to every URL. **(Recommended)**
- `-m` flag the presence of a dead record, but valid CNAME entry.
- `-v` verbose. Display more information per each request.
- `-c` Path to configuration file.

Practical Use

You can use scanio.sh which is kind of a PoC script to mass-locate vulnerable subdomains using results from Rapid7's Project Sonar. This script parses and greps through the dump for desired CNAME records and makes a large list of subdomains to check with subjack if they're vulnerable to Hostile Subdomain Takeover. Of course this isn't the only method to get a large amount of data to test. **Please use this responsibly ;)**

Adding subjack to your workflow

```go
package main

import (
        "fmt"
        "encoding/json"
        "io/ioutil"
        "strings"

        "github.com/haccer/subjack/subjack"
)


func main() {
        var fingerprints []subjack.Fingerprints
        config, _ := ioutil.ReadFile("custom_fingerprints.json")
        json.Unmarshal(config, &fingerprints)

        subdomain := "dead.cody.su"
        /* Use subjack's advanced detection to identify
        if the subdomain is able to be taken over. */
        service := subjack.Identify(subdomain, false, 10, fingerprints)

        if service != "" {
                service = strings.ToLower(service)
                fmt.Printf("%s is pointing to a vulnerable %s service.\n", subdomain, service)
        }
}
```

See the godoc for more functions.

FAQ

Q: What should my wordlist look like?

A: Your wordlist should include a list of subdomains you're checking and should look something like:

```
assets.cody.su
assets.github.com
b.cody.su
big.example.com
cdn.cody.su
dev.cody.su
dev2.twitter.com
```

References

Extra information about Hostile Subdomain Takeovers:

- https://github.com/EdOverflow/can-i-take-over-xyz
- https://labs.detectify.com/2014/10/21/hostile-subdomain-takeover-using-herokugithubdesk-more/