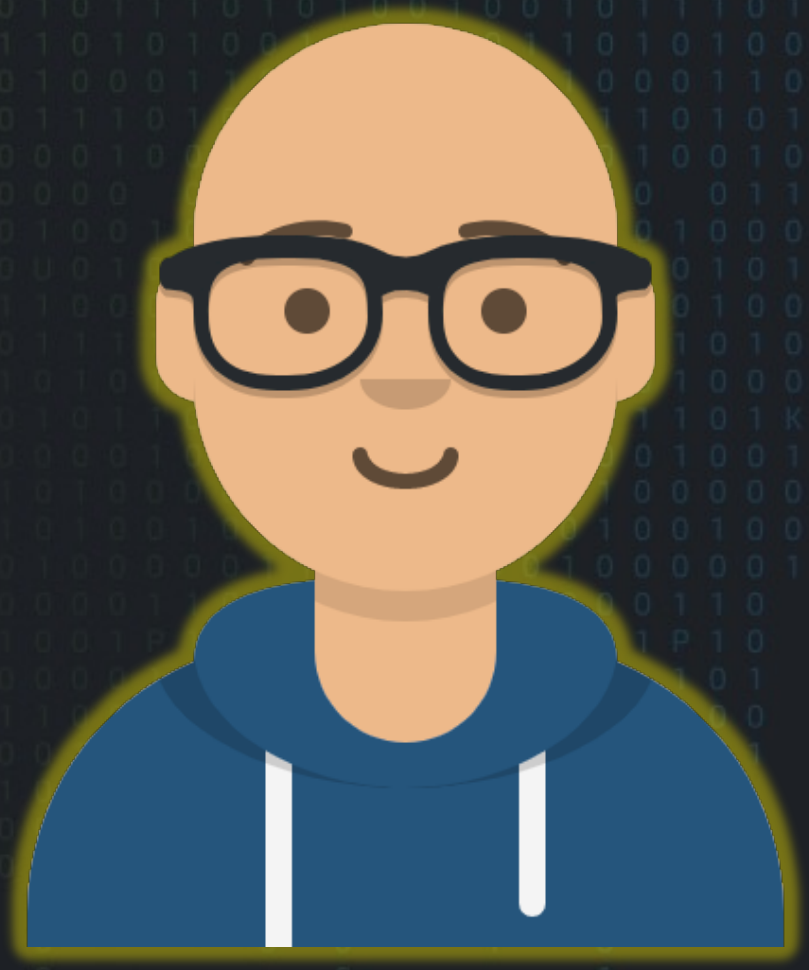
Subdomain Hijacking

Daniel Oates-Lee

#> whoami

Director – Punk Security

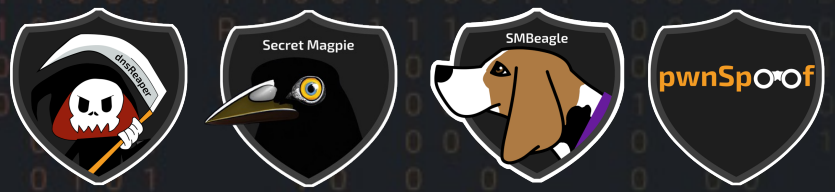
- DevSecOps enthusiast
- Automator
- Security guy
- Geek



#> whoarewe

Punk Security

- DevSecOps consultancy
- 4 x Opensource tools



- Home of the DevSecOps CTF

The agenda

- How does DNS work?
- Methods to attack subdomains
- Why should you care?
- How you can defend your org!

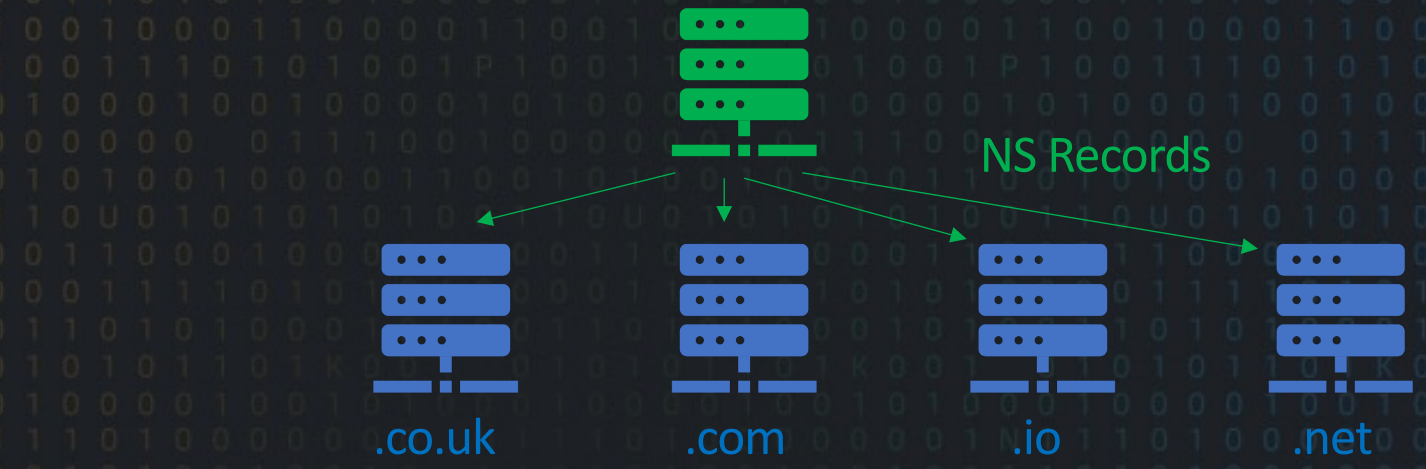
An intro to DNS

An intro to DNS

root hint servers

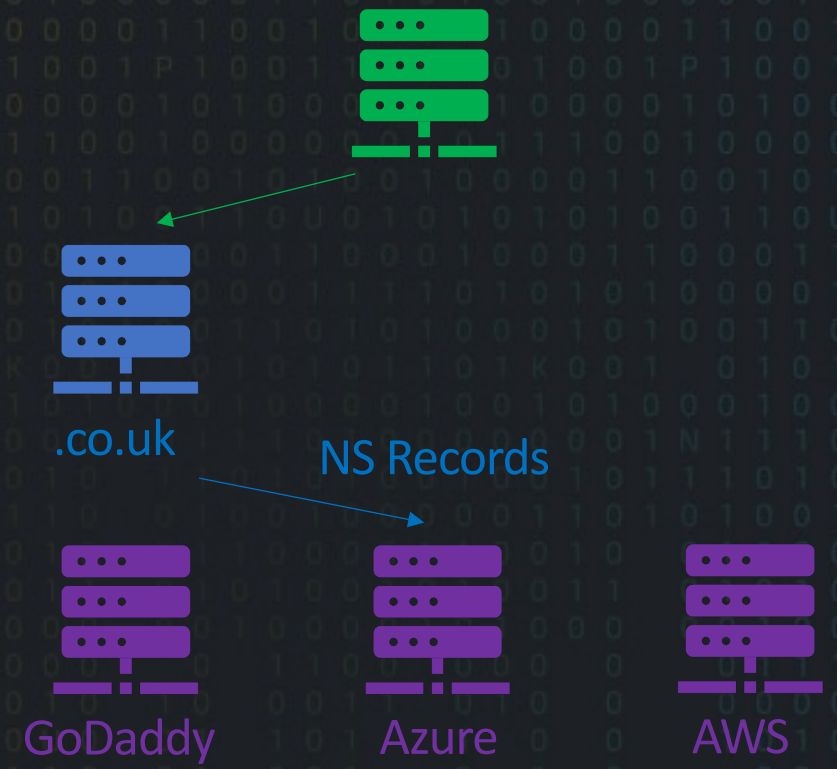
An intro to DNS

TLD servers

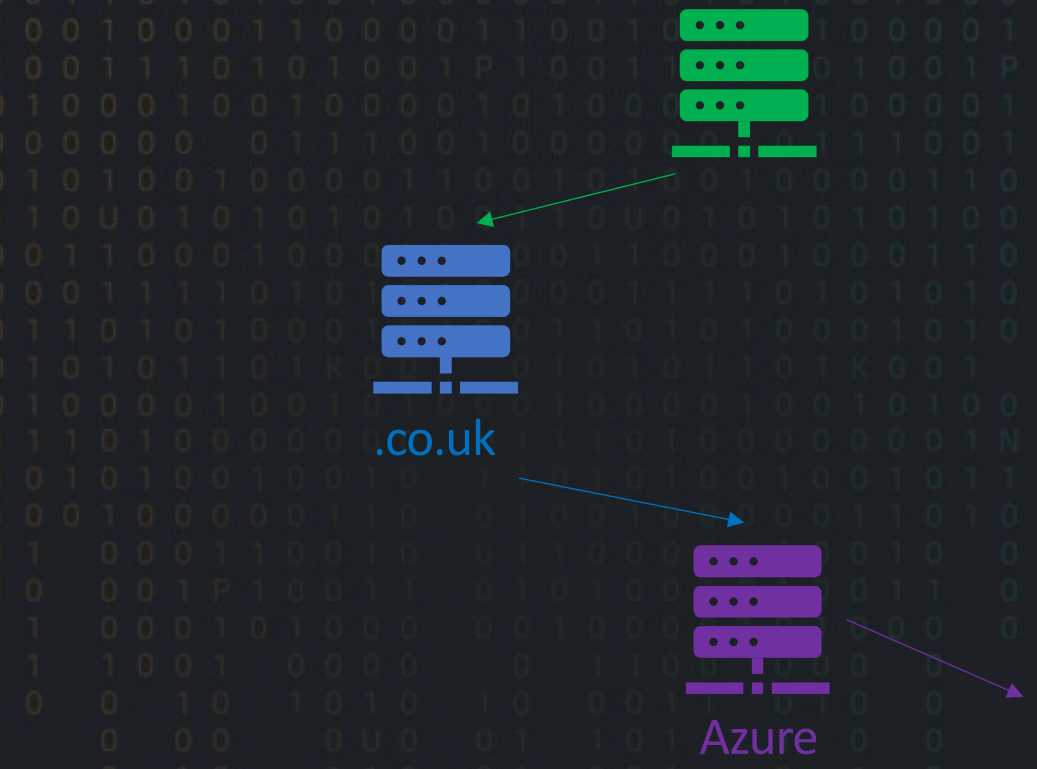


An intro to DNS

DNS Hosts



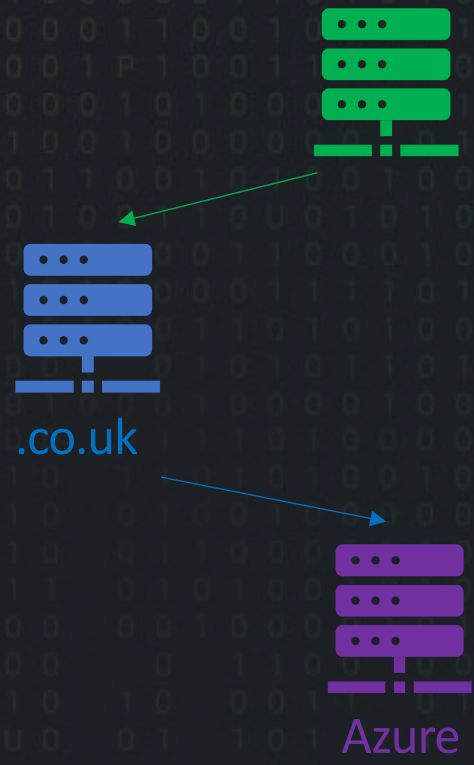
An intro to DNS



RECORDS:

- A
- AAAA
- CNAME
- NS

An intro to DNS



NO ACCESS

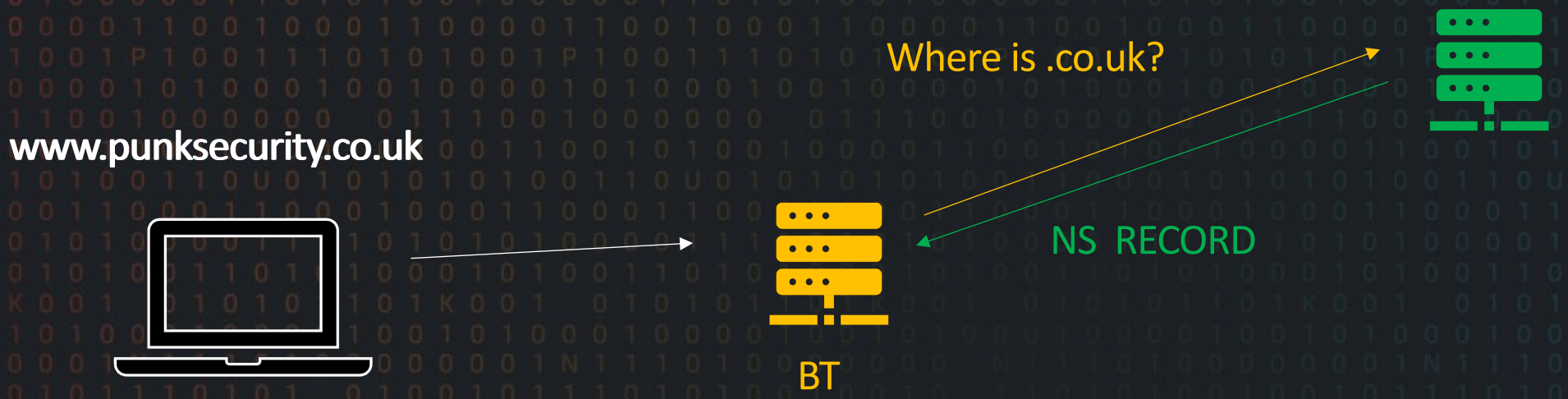
CONFIGURE VIA REGISTRAR

CONFIGURABLE

An intro to DNS

www.punksecurity.co.uk

An intro to DNS



An intro to DNS

www.punksecurity.co.uk

BT

Where is
punksecurity.co.uk?

NS RECORD

.co.uk

An intro to DNS

www.punksecurity.co.uk

BT

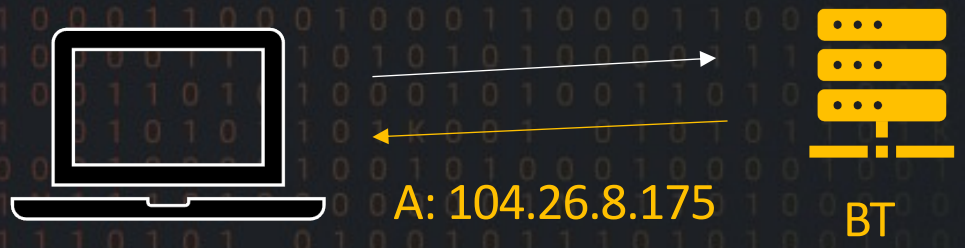
Where is
www.punksecurity.co.uk?

A: 104.26.8.175

Azure

An intro to DNS

www.punksecurity.co.uk



what are subdomains?

punksecurity.co.uk

www.punksecurity.co.uk

blog.punksecurity.co.uk

docs.punksecurity.co.uk

Scenario #1
SaaS pages takeover

what are subdomains takeovers?

punksecurity.co.uk

www.punksecurity.co.uk

blog.punksecurity.co.uk

docs.punksecurity.co.uk

CNAME
punksecurity-docs.github.io


KEEP
CALM
ITS
DEMO
TIME!!!

Scenario #2
NS Takeover

What is NS delegation

punksecurity.co.uk

www.punksecurity.co.uk

Main DNS Server

NS delegation

punksecurity.co.uk

www.punksecurity.co.uk

dev.punksecurity.co.uk

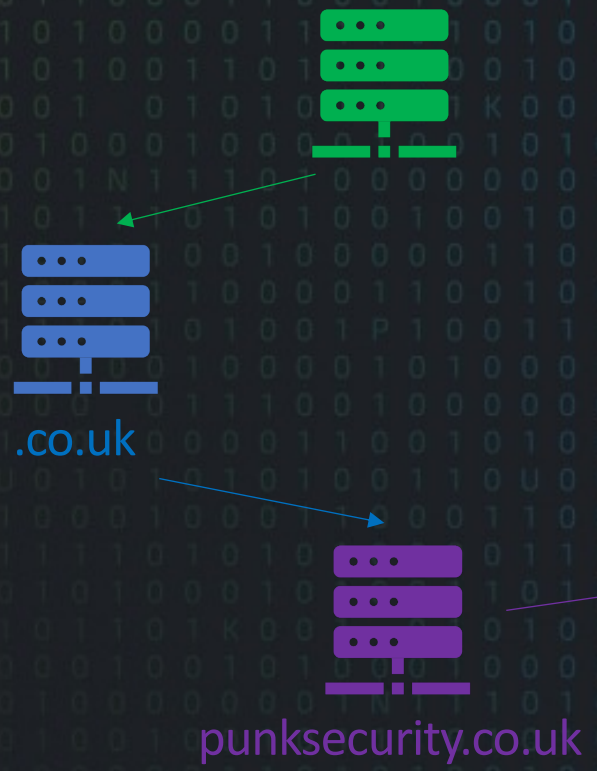
Main DNS Server

NS Record to Developers DNS Server

www.dev.punksecurity.co.uk

Developers DNS Server

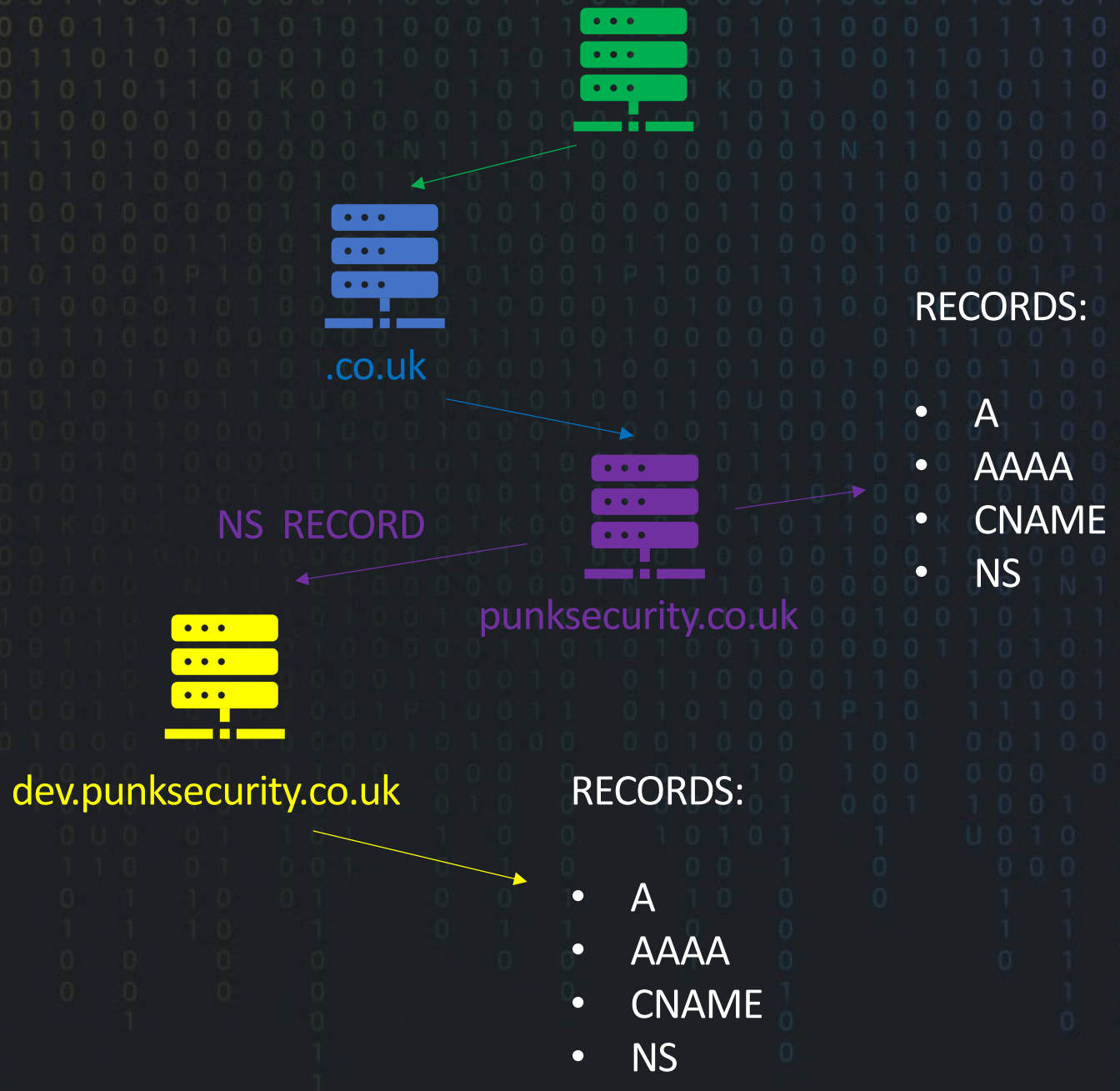
NS delegation

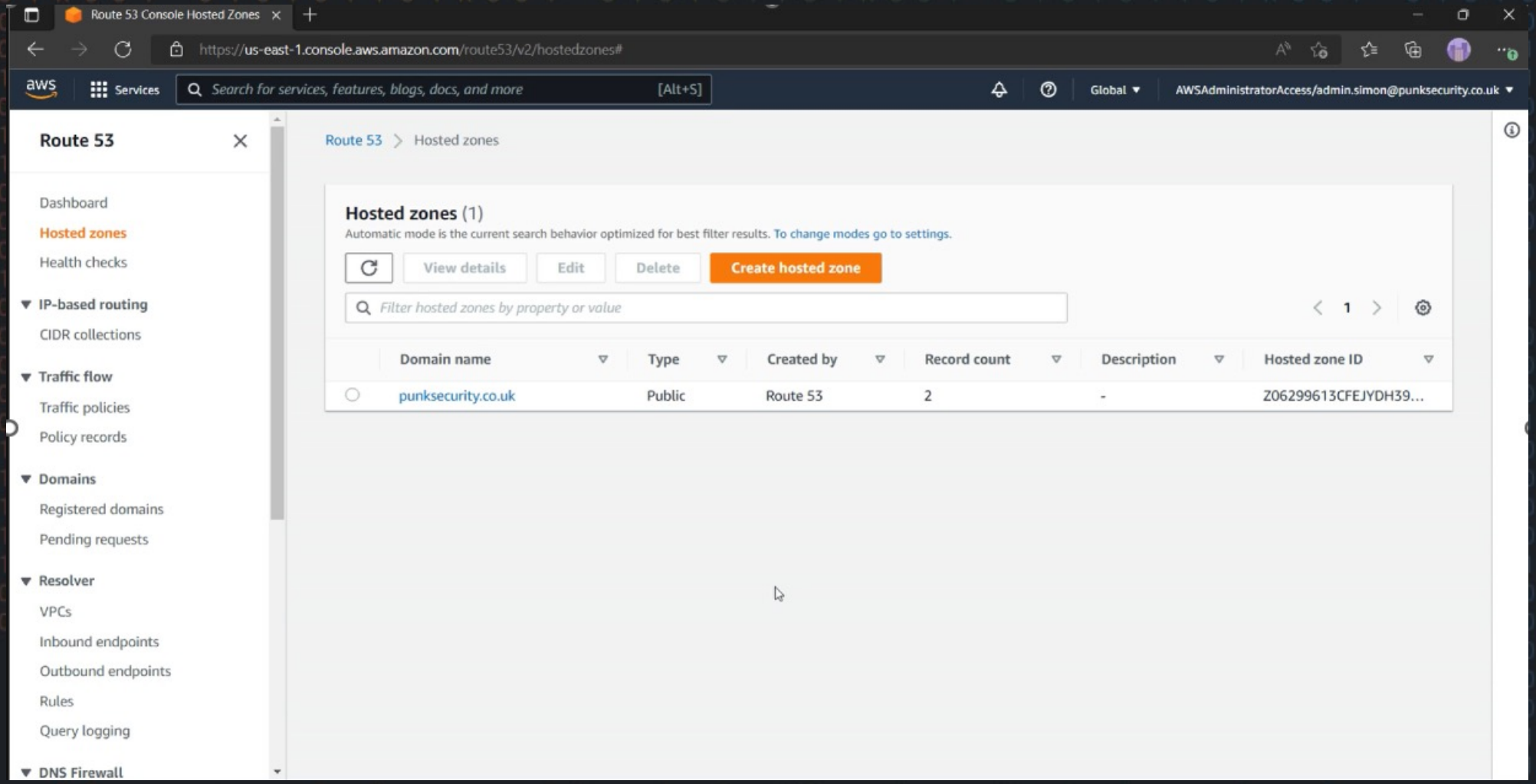


RECORDS:

- A
- AAAA
- CNAME
- NS

NS delegation




Route 53 Console Hosted Zones
https://us-east-1.console.aws.amazon.com/route53/v2/hostedzones#
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
AWSAdministratorAccess/admin.simon@punksecurity.co.uk
Route 53
Dashboard
Hosted zones
Health checks
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Query logging
DNS Firewall
Route 53 > Hosted zones
Hosted zones (1)
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
View details
Edit
Delete
Create hosted zone
Filter hosted zones by property or value
1
Domain name
Type
Created by
Record count
Description
Hosted zone ID
punksecurity.co.uk
Public
Route 53
2
-
Z06299613CFEJYDH39...

Route 53

Dashboard
Hosted zones
Health checks

IP-based routing
CIDR collections

Traffic flow
Traffic policies
Policy records

Domains
Registered domains
Pending requests

Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Query logging

DNS Firewall

Hosted zones (1)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

View details | Edit | Delete | Create hosted zone

Filter hosted zones by property or value

1

Domain name	Type	Created by	Record count	Description	Hosted zone ID
punksecurity.co.uk	Public	Route 53	2	-	Z06299613CFEJYDH39...

NS takeover

punksecurity.co.uk

www.punksecurity.co.uk

dev.punksecurity.co.uk

Main DNS Server

NS Record to Developers DNS Server

developers.punksecurity.co.uk

Incorrect NS Record

How can we exploit this?

TARGET:
ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com

ns-300.awsdns-31.net
ns-200.awsdns-35.co.uk
ns-100.awsdns.co.uk
ns-400.awsdns-12.com

How can we exploit this?

TARGET:
ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com

ns-300 net
ns- uk
ns-10 wsdns.c k
ns-400.awsdns-12.com

How can we exploit this?

TARGET:
ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com

ns-300 net
ns- uk
ns-10 wsdns.co k
ns-400.awsdns-12.com

ns-300.awsdns-31.net
ns-200.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com

How can we exploit this?

TARGET:
ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com

ns-300 net
ns- uk
ns-10 wsdns.co k
ns-400.awsdns-12.com

ns-300.awsdns-31.net
ns-200.awsdns-35.co.uk
ns-1507.awsdns.co.uk
ns-99.awsdns-12.com

ns-766.awsdns-31.net
ns-1819.awsdns-35.co.uk
ns-100.awsdns.co.uk
ns-400.awsdns-12.com

How is DevOps making it worse?

Gene Kim / Geoffrey Moore

Core vs Context

Ticketing systems

How is DevOps making it worse?

- ClickOps - old copy and pasting
- Delegation is more rife than ever
- Lack of access controls

so what?

so what?

Credible phishing links

support.invisionpower.com

new.rubyonrails.org

signup.uber.com

so what?

Credible email addresses

info@support.invisionpower.com

support@new.rubyonrails.org

help@signup.uber.com

so what?

- Loosely scoped cookies

so what?

Loosely scoped cookies

punksecurity.co.uk

www.punksecurity.co.uk

blog.punksecurity.co.uk

so what?

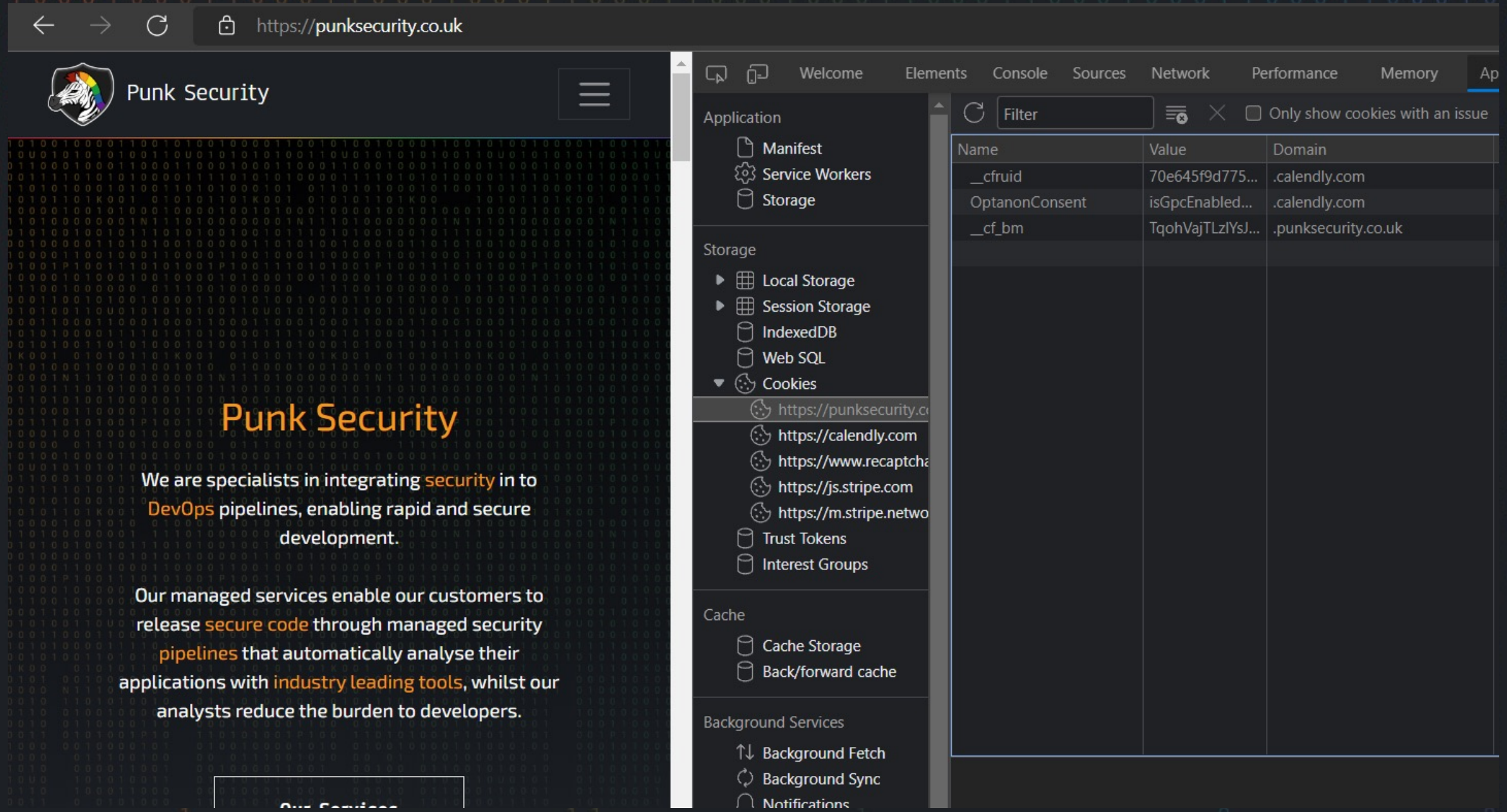
Loosely scoped cookies

punksecurity.co.uk

www.punksecurity.co.uk

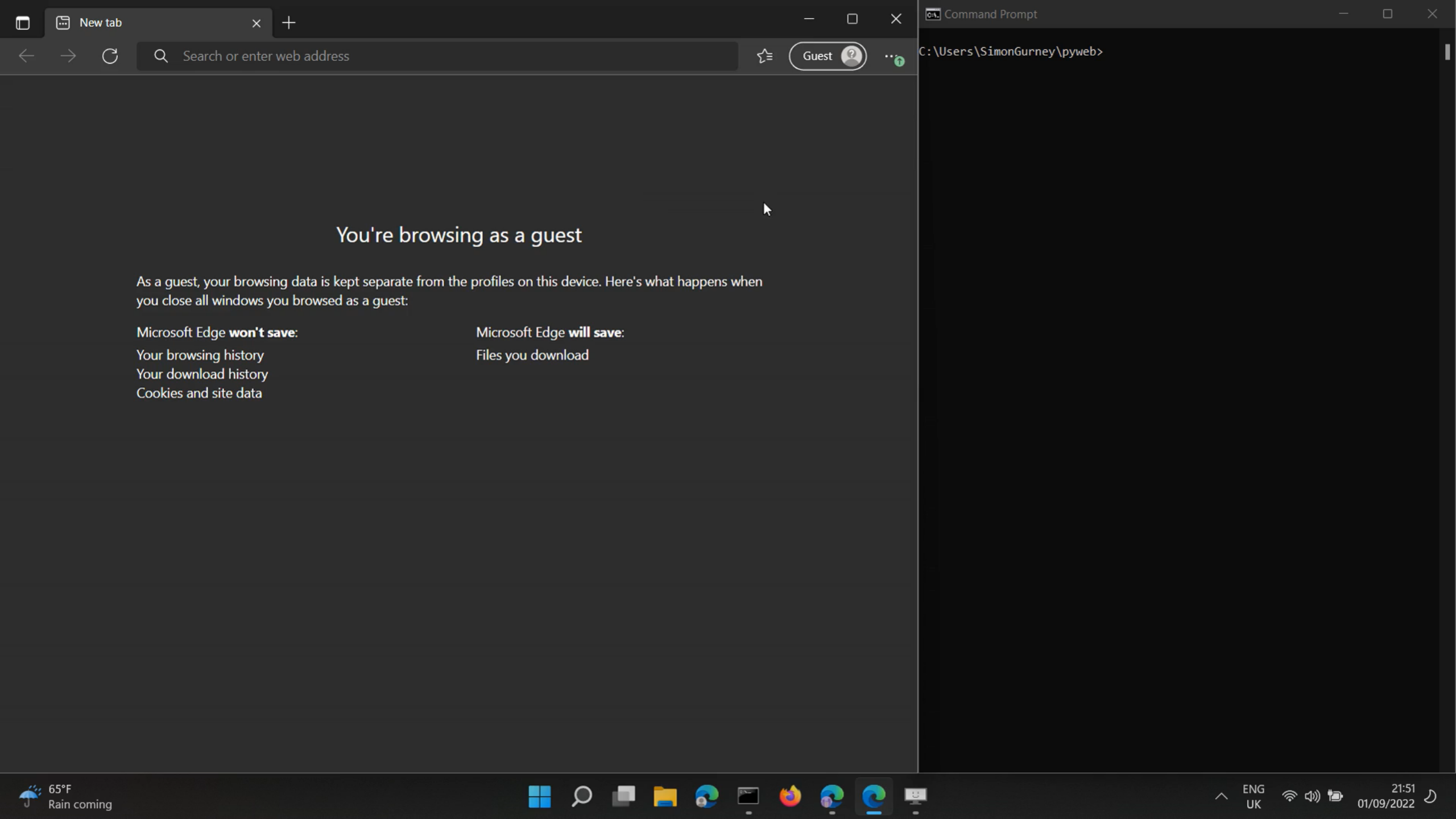
blog.punksecurity.co.uk

www.developers.punksecurity.co.uk


https://punksecurity.co.uk
Punk Security
Punk Security
We are specialists in integrating security in to DevOps pipelines, enabling rapid and secure development.
Our managed services enable our customers to release secure code through managed security pipelines that automatically analyse their applications with industry leading tools, whilst our analysts reduce the burden to developers.
Welcome
Elements
Console
Sources
Network
Performance
Memory
Application
Manifest
Service Workers
Storage
Storage
Local Storage
Session Storage
IndexedDB
Web SQL
Cookies
https://punksecurity.c
https://calendly.com
https://www.recaptcha
https://js.stripe.com
https://m.stripe.netwo
Trust Tokens
Interest Groups
Cache
Cache Storage
Back/forward cache
Background Services
Background Fetch
Background Sync
Notifications
Filter
Only show cookies with an issue
Name
Value
Domain
__cfruid
70e645f9d775...
.calendly.com
OptanonConsent
isGpcEnabled...
.calendly.com
__cf_bm
TqohVajTLzIYsJ...
.punksecurity.co.uk

	Domain	P
...	.calendly.com	/
..	.calendly.com	/
l...	.punksecurity.co.uk	/

DEMO #3
Stealing loosely scoped cookies


New tab
Search or enter web address
Guest
You're browsing as a guest
As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:
Microsoft Edge won't save:
Your browsing history
Your download history
Cookies and site data
Microsoft Edge will save:
Files you download
Command Prompt
C:\Users\SimonGurney\pyweb>
65°F
Rain coming
ENG
UK
21:51
01/09/2022

how do we defend?

- Periodic audits / DNS hygiene

how do we defend?

Periodic audits / DNS hygiene

Bug bounty programs

how do we defend?

Periodic audits / DNS hygiene

Bug bounty programs

Extend our pen testing scopes

how do we defend?

- Periodic audits / DNS hygiene
- Bug bounty programs
- Extend our pen testing scopes
- IaC - Terraform

how do we defend?

- Periodic audits / DNS hygiene
- Bug bounty programs
- Extend our pen testing scopes
- IaC - Terraform
- dnsReaper

#> docker run punksecurity/dnsReaper

Give it domains, or have it fetch them

#> docker run punksecurity/dnsReaper

Give it domains, or have it fetch them

Tests all domains with nearly 60 signatures

- Pattern match the record
- Pattern match the web response

#> docker run punksecurity/dnsReaper

Give it domains, or have it fetch them

Tests all domains with nearly 60 signatures

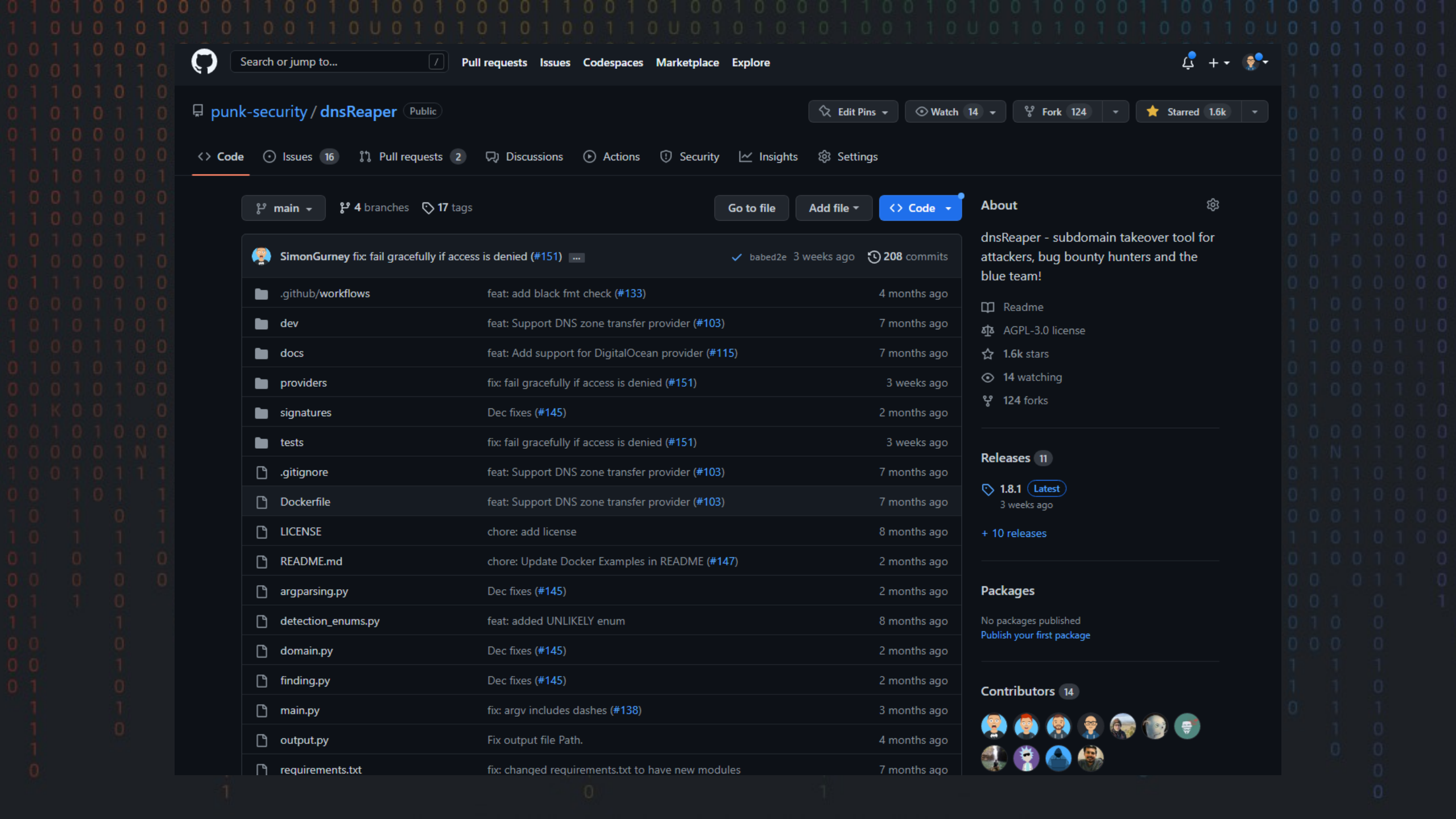
- Pattern match the record
- Pattern match the web response

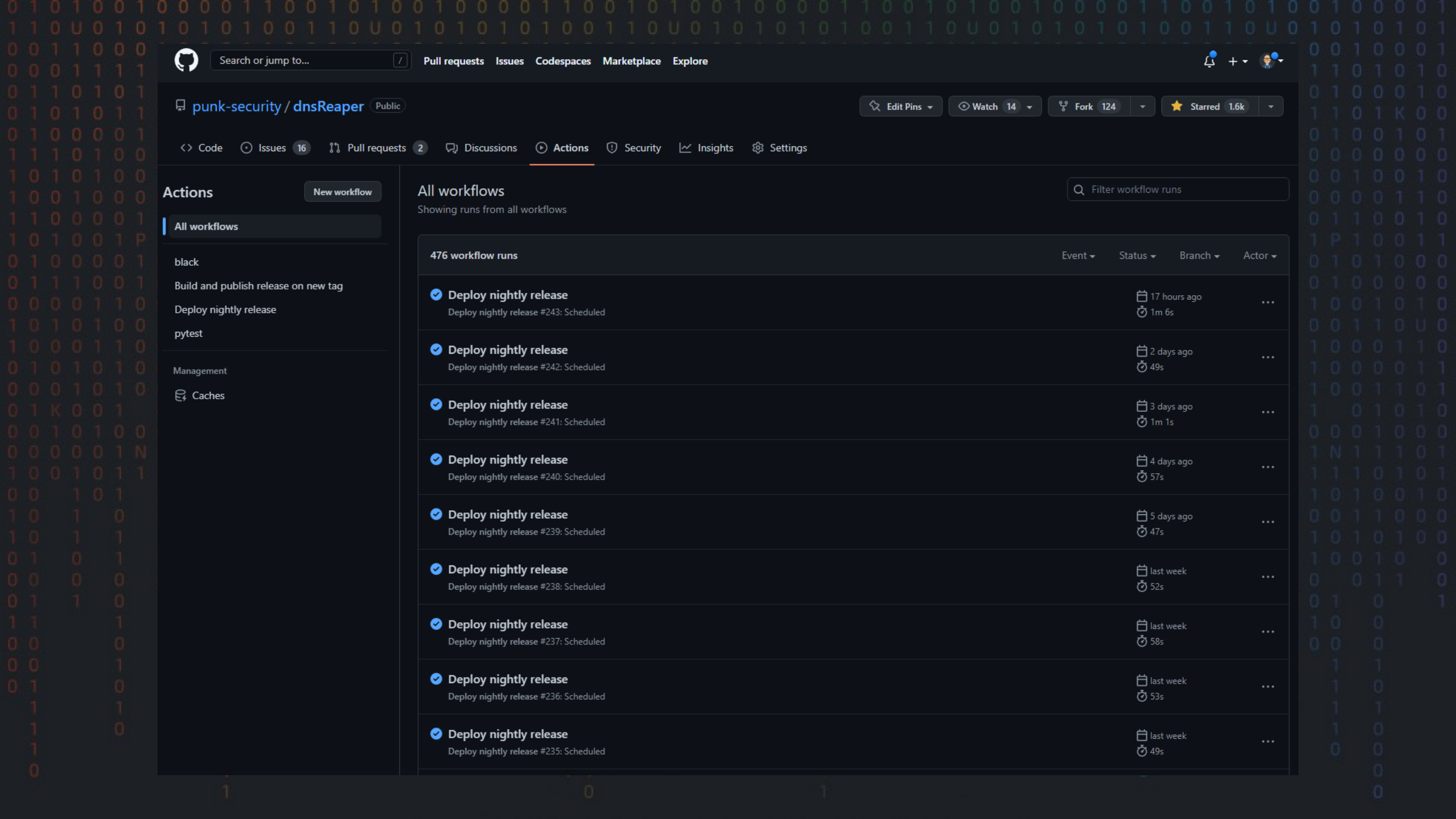
Reports to screen, csv and json

use cases

- Audit a DNS configuration
- Scan for bounties $ $ $
- Prevent bad deployments

dnsReaper


Search or jump to...
Pull requests
Issues
Codespaces
Marketplace
Explore
punk-security / dnsReaper
Public
Edit Pins
Watch 14
Fork 124
Starred 1.6k
Code
Issues 16
Pull requests 2
Discussions
Actions
Security
Insights
Settings
main
4 branches
17 tags
Go to file
Add file
Code
SimonGurney fix: fail gracefully if access is denied (#151)
babed2e 3 weeks ago
208 commits
.github/workflows feat: add black fmt check (#133) 4 months ago
dev feat: Support DNS zone transfer provider (#103) 7 months ago
docs feat: Add support for DigitalOcean provider (#115) 7 months ago
providers fix: fail gracefully if access is denied (#151) 3 weeks ago
signatures Dec fixes (#145) 2 months ago
tests fix: fail gracefully if access is denied (#151) 3 weeks ago
.gitignore feat: Support DNS zone transfer provider (#103) 7 months ago
Dockerfile feat: Support DNS zone transfer provider (#103) 7 months ago
LICENSE chore: add license 8 months ago
README.md chore: Update Docker Examples in README (#147) 2 months ago
argparsing.py Dec fixes (#145) 2 months ago
detection_enums.py feat: added UNLIKELY enum 8 months ago
domain.py Dec fixes (#145) 2 months ago
finding.py Dec fixes (#145) 2 months ago
main.py fix: argv includes dashes (#138) 3 months ago
output.py Fix output file Path. 4 months ago
requirements.txt fix: changed requirements.txt to have new modules 7 months ago
About
dnsReaper - subdomain takeover tool for attackers, bug bounty hunters and the blue team!
Readme
AGPL-3.0 license
1.6k stars
14 watching
124 forks
Releases 11
1.8.1 Latest
3 weeks ago
+ 10 releases
Packages
No packages published
Publish your first package
Contributors 14


Search or jump to...
Pull requests
Issues
Codespaces
Marketplace
Explore
punk-security / dnsReaper
Public
Edit Pins
Watch 14
Fork 124
Starred 1.6k
Code
Issues 16
Pull requests 2
Discussions
Actions
Security
Insights
Settings
Actions
New workflow
All workflows
black
Build and publish release on new tag
Deploy nightly release
pytest
Management
Caches
All workflows
Showing runs from all workflows
Filter workflow runs
476 workflow runs
Event
Status
Branch
Actor
Deploy nightly release
Deploy nightly release #243: Scheduled
17 hours ago
1m 6s
Deploy nightly release
Deploy nightly release #242: Scheduled
2 days ago
49s
Deploy nightly release
Deploy nightly release #241: Scheduled
3 days ago
1m 1s
Deploy nightly release
Deploy nightly release #240: Scheduled
4 days ago
57s
Deploy nightly release
Deploy nightly release #239: Scheduled
5 days ago
47s
Deploy nightly release
Deploy nightly release #238: Scheduled
last week
52s
Deploy nightly release
Deploy nightly release #237: Scheduled
last week
58s
Deploy nightly release
Deploy nightly release #236: Scheduled
last week
53s
Deploy nightly release
Deploy nightly release #235: Scheduled
last week
49s

dnsReaper/aws.md at main · pun

https://github.com/punk-security/dnsReaper/blob/main/docs/aws.md

Guest

47 lines (38 sloc) | 1.41 KB

Raw Blame

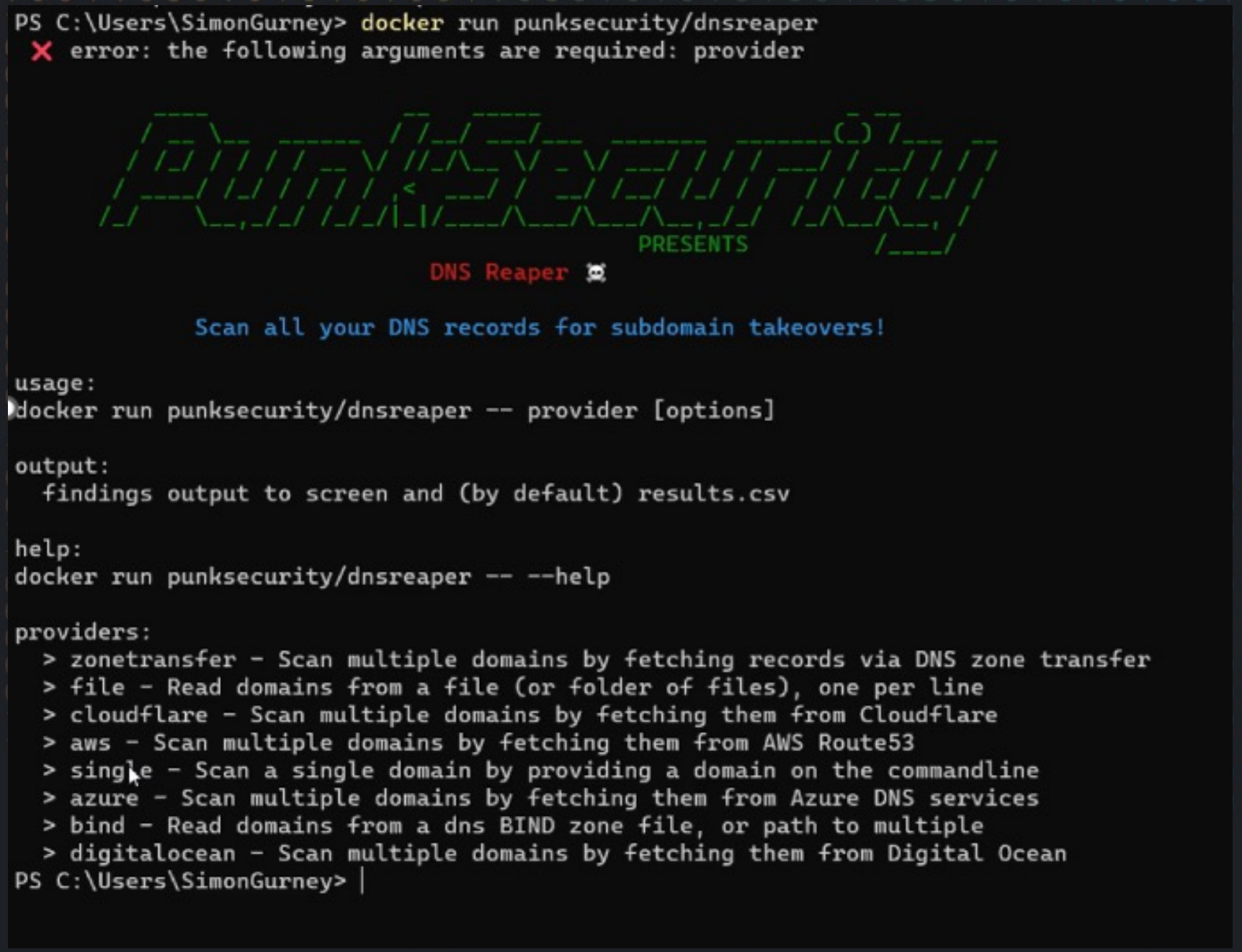
Requirements

As a minimum you need:

- GetHostedZone
- ListHostedZones
- ListResourceRecordSets

A suggested inline policy for the account would be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets"
            ],
            "Resource": "*"
        }
    ]
}
```


PS C:\Users\SimonGurney> docker run punksecurity/dnsreaper
error: the following arguments are required: provider
PRESENTS
DNS Reaper
Scan all your DNS records for subdomain takeovers!
usage:
docker run punksecurity/dnsreaper -- provider [options]
output:
findings output to screen and (by default) results.csv
help:
docker run punksecurity/dnsreaper -- --help
providers:
> zonetransfer - Scan multiple domains by fetching records via DNS zone transfer
> file - Read domains from a file (or folder of files), one per line
> cloudflare - Scan multiple domains by fetching them from Cloudflare
> aws - Scan multiple domains by fetching them from AWS Route53
> single - Scan a single domain by providing a domain on the commandline
> azure - Scan multiple domains by fetching them from Azure DNS services
> bind - Read domains from a dns BIND zone file, or path to multiple
> digitalocean - Scan multiple domains by fetching them from Digital Ocean
PS C:\Users\SimonGurney>

```
PS C:\Users\SimonGurney> docker run punksecurity/dnsreaper aws --aws-access-key-id AKIAUIG46DC3VB7C4SHA --aws-access-key-secret rHrhuWmfLPiSxBSYjOoJ5IzLYp06
ToHdNvBHI02D
```

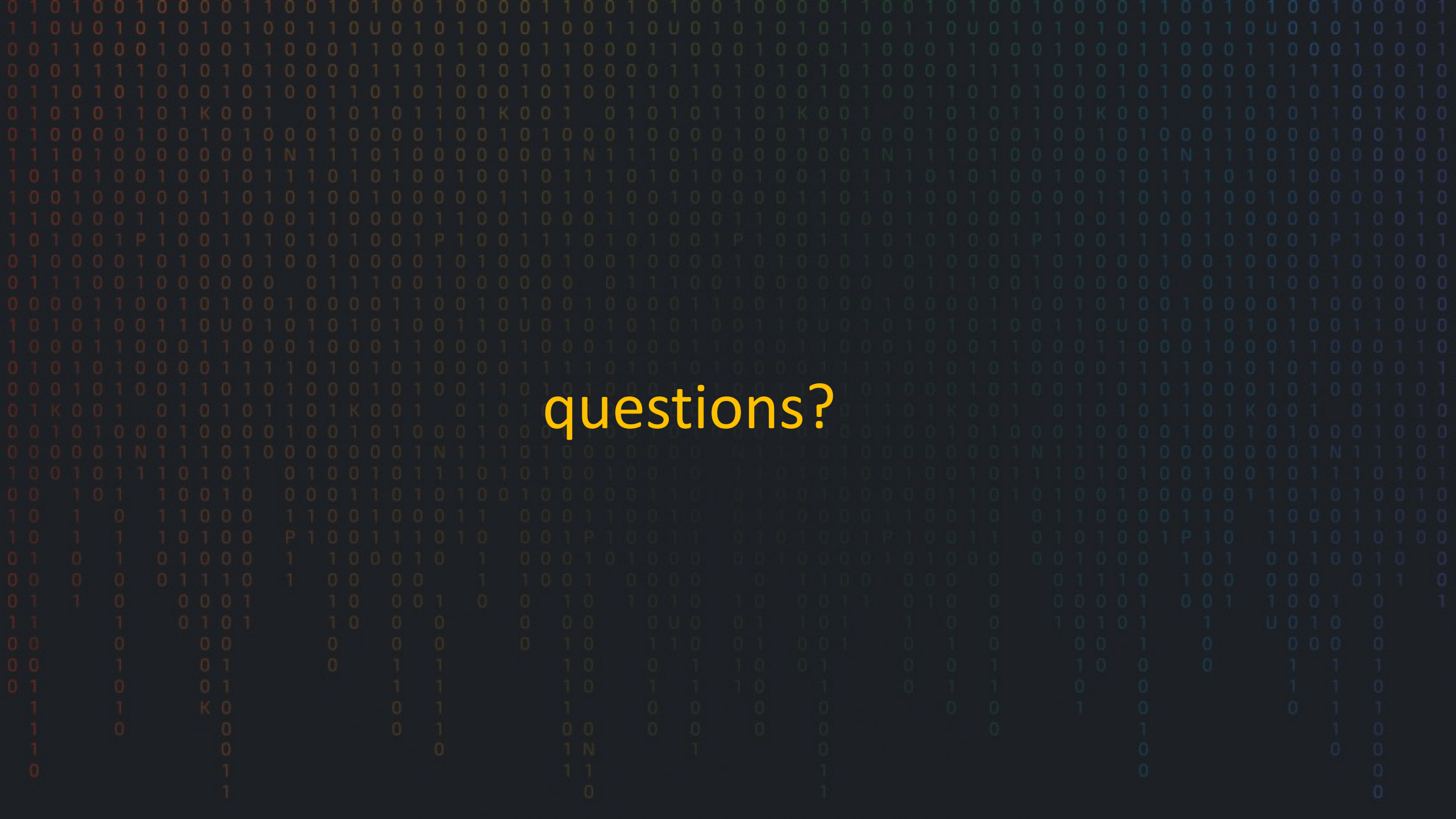

```
DNS Reaper

Scan all your DNS records for subdomain takeovers!

Got 3 records from aws
Testing with 59 signatures


We found 2 takeovers
-- DOMAIN 'developers.punksecurity.co.uk' :: SIGNATURE '_generic_zone_missing_on_ns' :: CONFIDENCE 'POTENTIAL'
NS: ns-766.awsdns-31.net,ns-1819.awsdns-35.co.uk,ns-1507.awsdns-60.org,ns-99.awsdns-12.com
-- DOMAIN 'developers.punksecurity.co.uk' :: SIGNATURE 'aws_ns' :: CONFIDENCE 'CONFIRMED'
NS: ns-766.awsdns-31.net,ns-1819.awsdns-35.co.uk,ns-1507.awsdns-60.org,ns-99.awsdns-12.com

 We completed in 1.68 seconds
...Thats all folks!
PS C:\Users\SimonGurney>
```


questions?

Punk Security

Automating quality and security checks