Subdomain Takeovers

DNS Hygiene
and
Change Management

$ whoami

Panda

panda@protectedbypanda.com

@fuzzing_panda

cybermedsummit.org

RaiseMe @ShellConLa

Preview of Coming Attractions

1. How browsers connect to websites
   a. Uniform Resource Locator (URL)
   b. Domain Name System (DNS)

2. Subdomain Takeovers
   a. How to attack subdomains
   b. How to defend subdomains

How do browsers connect to websites?

Uniform Resource Locator (URL)

"the address of a given unique resource on the Web"

Moz://a MDN Web Docs

Example of a URL

http://www.example.com:80

Protocol

http://www.example.com:80

Protocol://Fully Qualified Domain Name (FQDN)

http://www.example.com:80

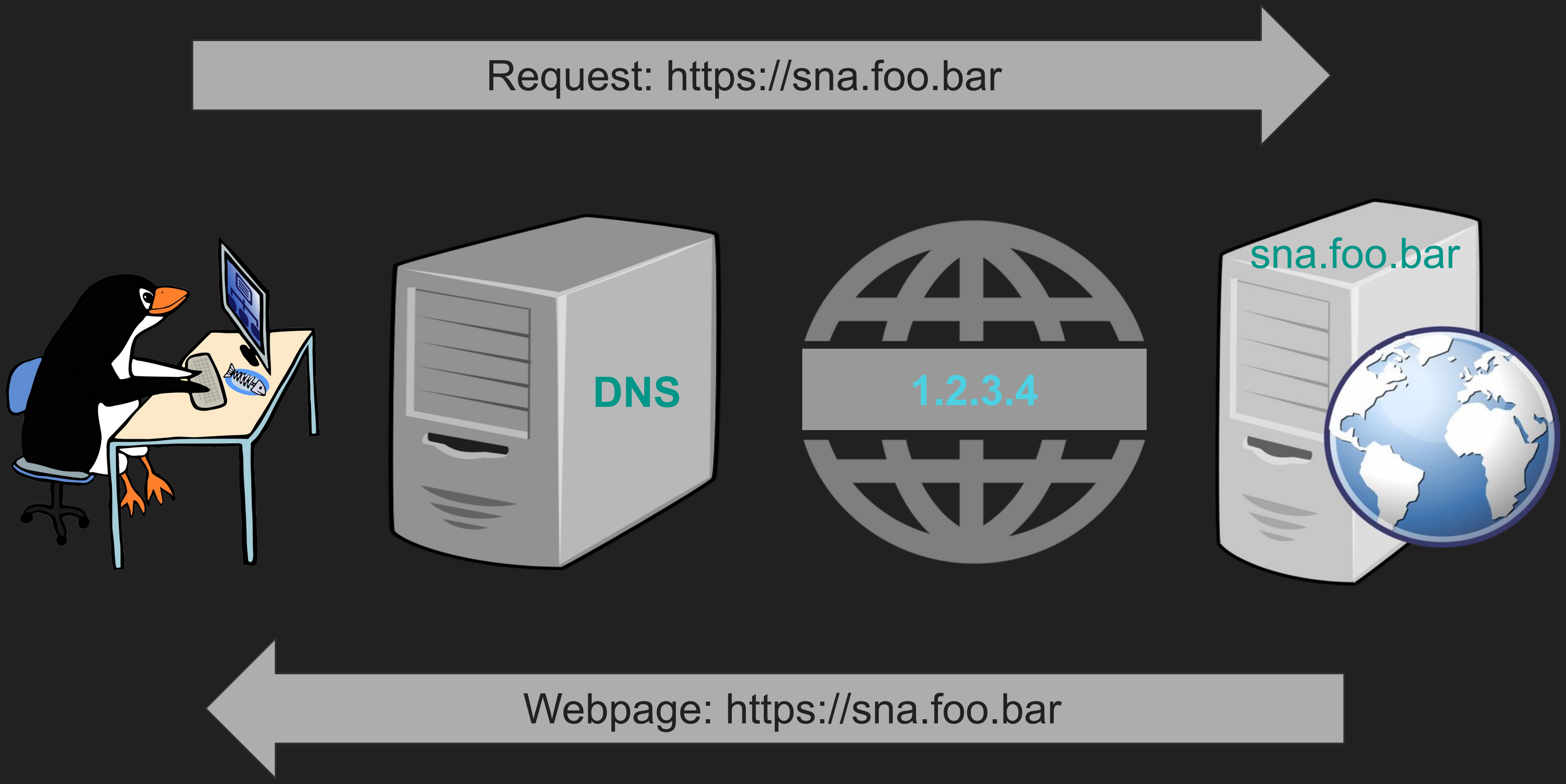
Protocol://FQDN:Port

http://www.example.com:80

Domain Name System (DNS)

Hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network

DNS as a Phonebook



Request: https://sna.foo.bar

Webpage: https://sna.foo.bar

Subdomain Takeover

Occurs when an attacker sets up a hosting account that can serve potentially malicious content from your domain because of misconfigured DNS.

Consequences of a Subdomain Takeover

Exploitation	**Consequence**
Steal cookies	Unauthorized access to accounts and systems
Harvest credentials	Unauthorized access to accounts and systems
Spread malware	Stop business
Display offensive or competitor content	Brand damage

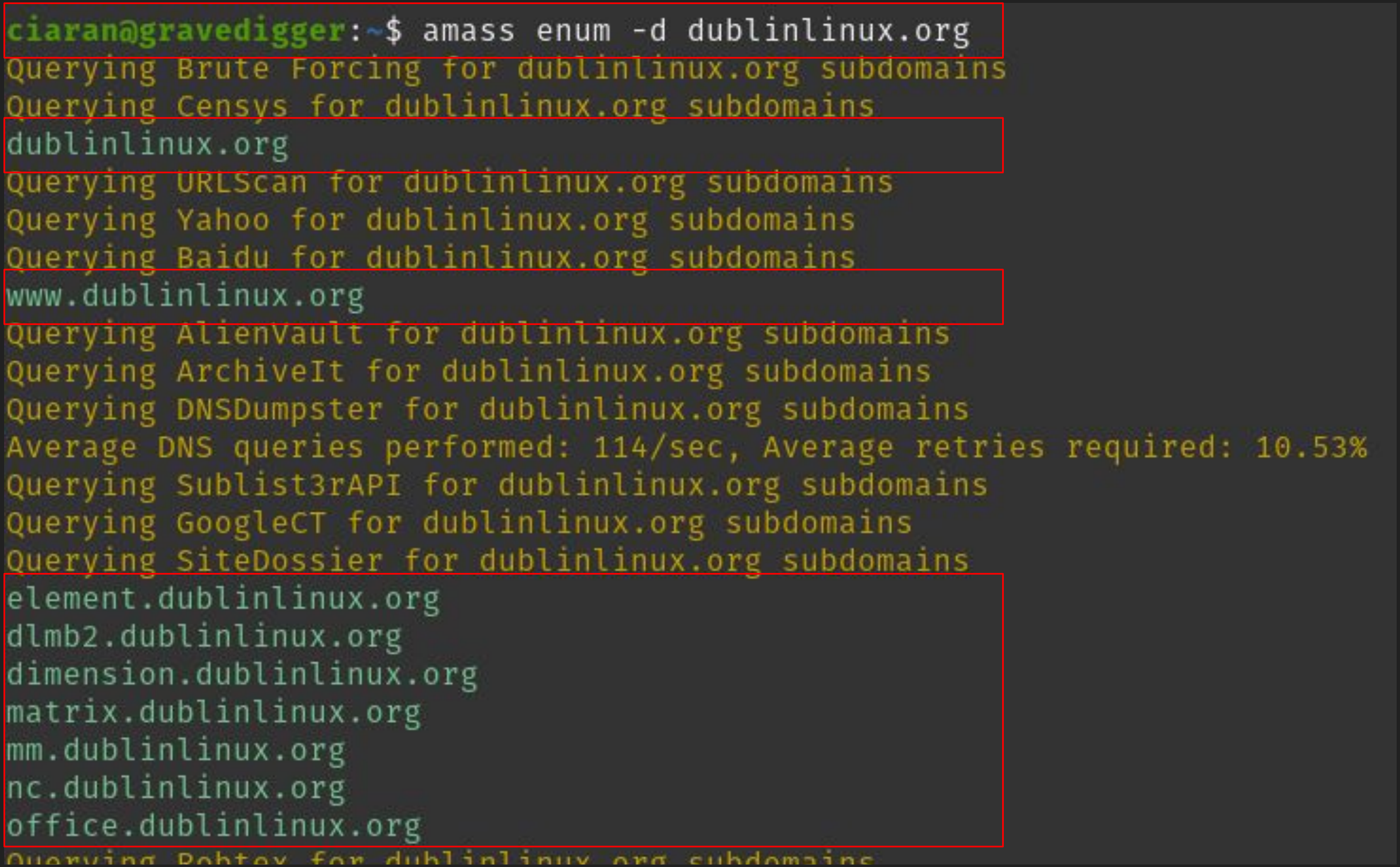
Attacking Vulnerable Subdomains

Attacking Vulnerable Subdomains

1. Get a list of subdomains.
2. Check for expired services or resources.
3. Swoop the expired services or resources.
4. Serve desired content.

How do attackers get a list of subdomains?

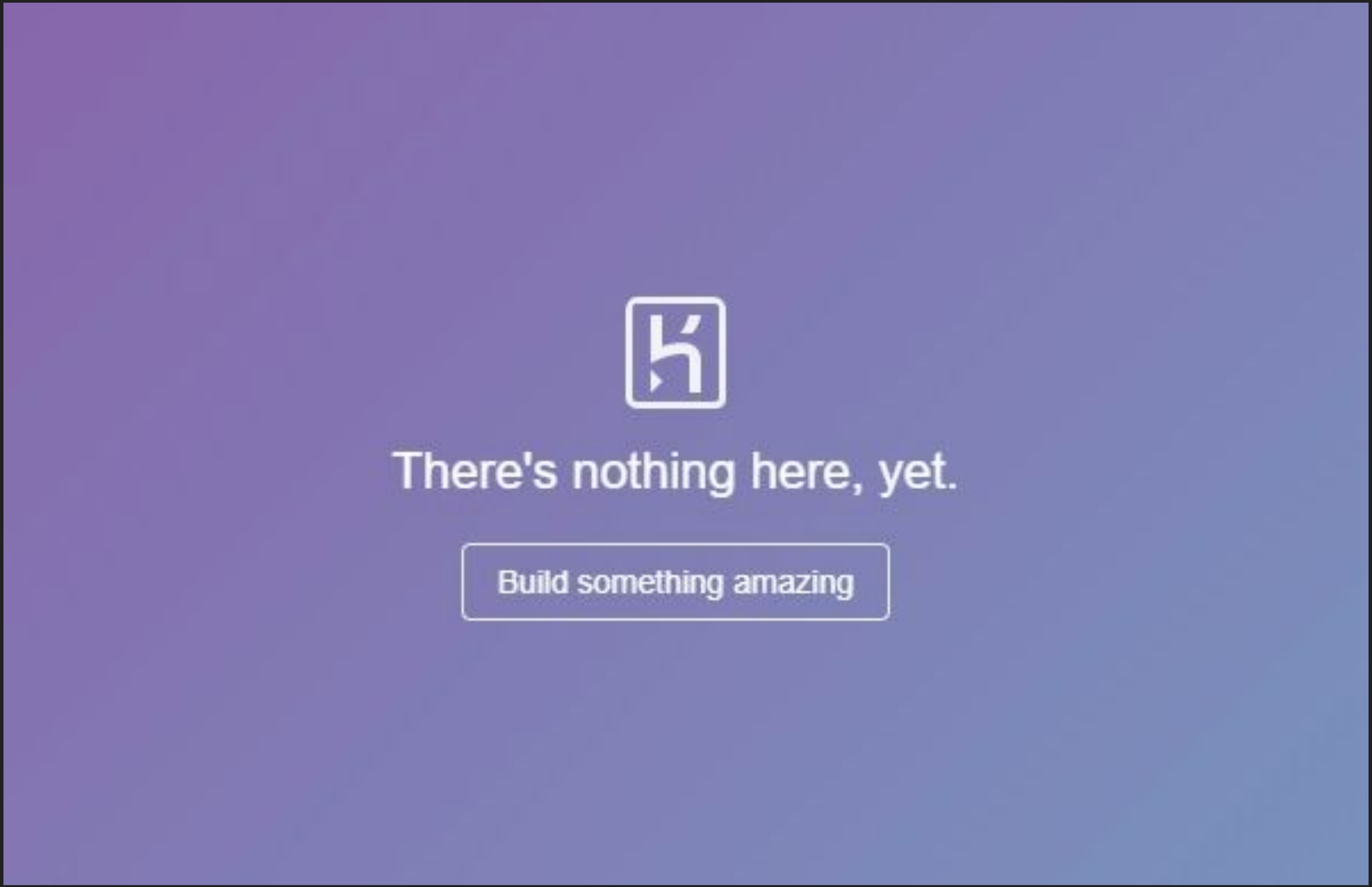
Example Domain Enumeration: Amass



```
ciaran@gravedigger:~$ amass enum -d dublinlinux.org
Querying Brute Forcing for dublinlinux.org subdomains
Querying Censys for dublinlinux.org subdomains
dublinlinux.org
Querying URLScan for dublinlinux.org subdomains
Querying Yahoo for dublinlinux.org subdomains
Querying Baidu for dublinlinux.org subdomains
www.dublinlinux.org
Querying AlienVault for dublinlinux.org subdomains
Querying ArchiveIt for dublinlinux.org subdomains
Querying DNSDumpster for dublinlinux.org subdomains
Average DNS queries performed: 114/sec, Average retries required: 10.53%
Querying Sublist3rAPI for dublinlinux.org subdomains
Querying GoogleCT for dublinlinux.org subdomains
Querying SiteDossier for dublinlinux.org subdomains
element.dublinlinux.org
dlmb2.dublinlinux.org
dimension.dublinlinux.org
matrix.dublinlinux.org
mm.dublinlinux.org
nc.dublinlinux.org
office.dublinlinux.org
Querying Robtex for dublinlinux.org subdomains
```

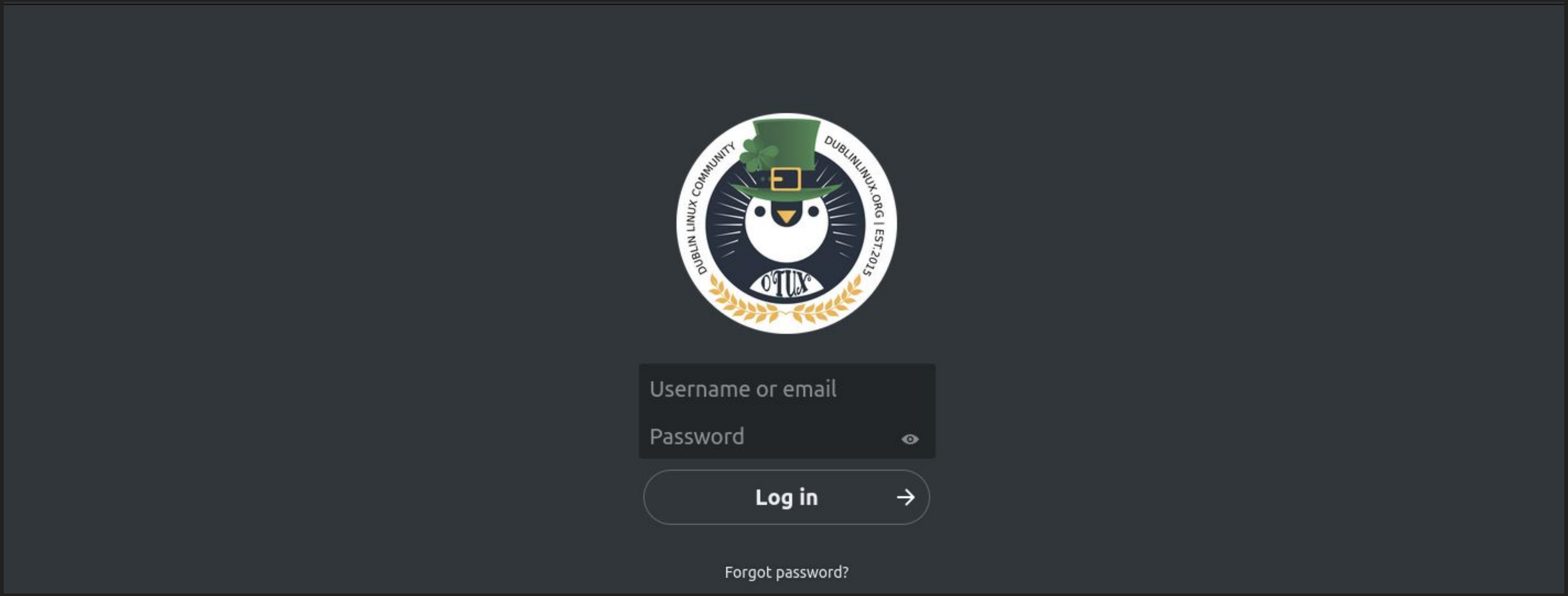
How do attackers check for expired services or resources?

Check for default expired service pages.

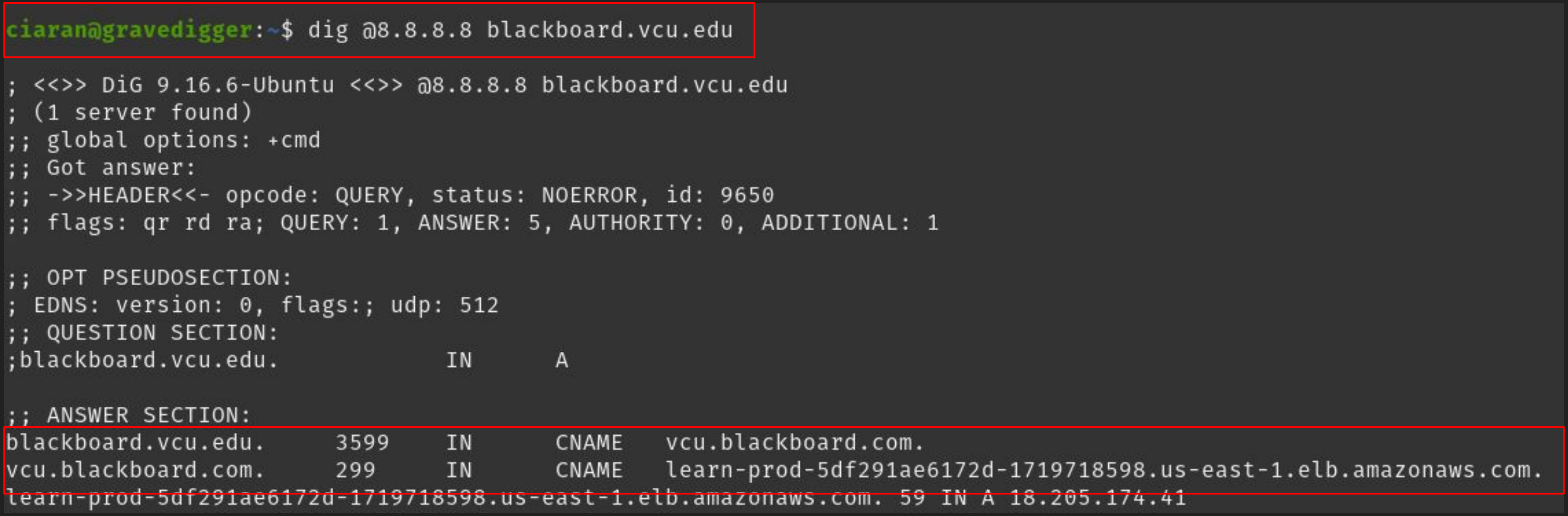


There's nothing here, yet.

Heroku expired services page


DUBLIN LINUX COMMUNITY
DUBLINLINUX.ORG | EST.2015
TUX
Username or email
Password
Log in
Forgot password?

“digging” into the details of one subdomain



```
ciaran@gravedigger:~$ dig @8.8.8.8 blackboard.vcu.edu

; <<>> DiG 9.16.6-Ubuntu <<>> @8.8.8.8 blackboard.vcu.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9650
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;blackboard.vcu.edu.            IN      A

;; ANSWER SECTION:
blackboard.vcu.edu.     3599    IN      CNAME   vcu.blackboard.com.
vcu.blackboard.com.     299     IN      CNAME   learn-prod-5df291ae6172d-1719718598.us-east-1.elb.amazonaws.com.
learn-prod-5df291ae6172d-1719718598.us-east-1.elb.amazonaws.com. 59 IN A 18.205.174.41
```

Subdomain Takeover Types

Subdomain Takeover Types

Canonical Name (CNAME) Subdomain Takeover

Nameserver Records (NS Records) Subdomain Takeover

Mail Server Records (MX Records) Subdomain Takeover

Second-order Subdomain Takeover

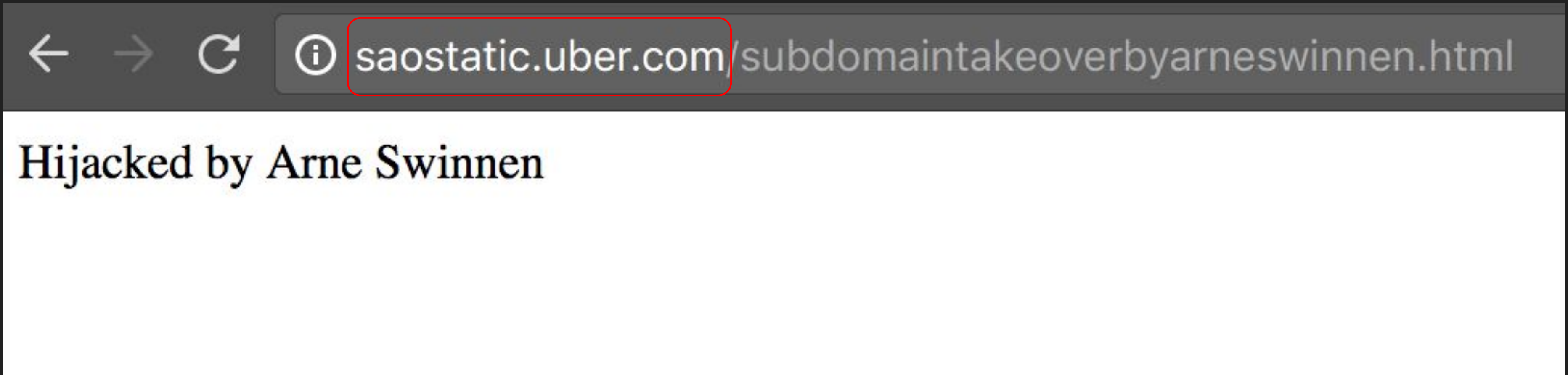
How real is the risk

Uber

Uber

Vulnerable subdomain

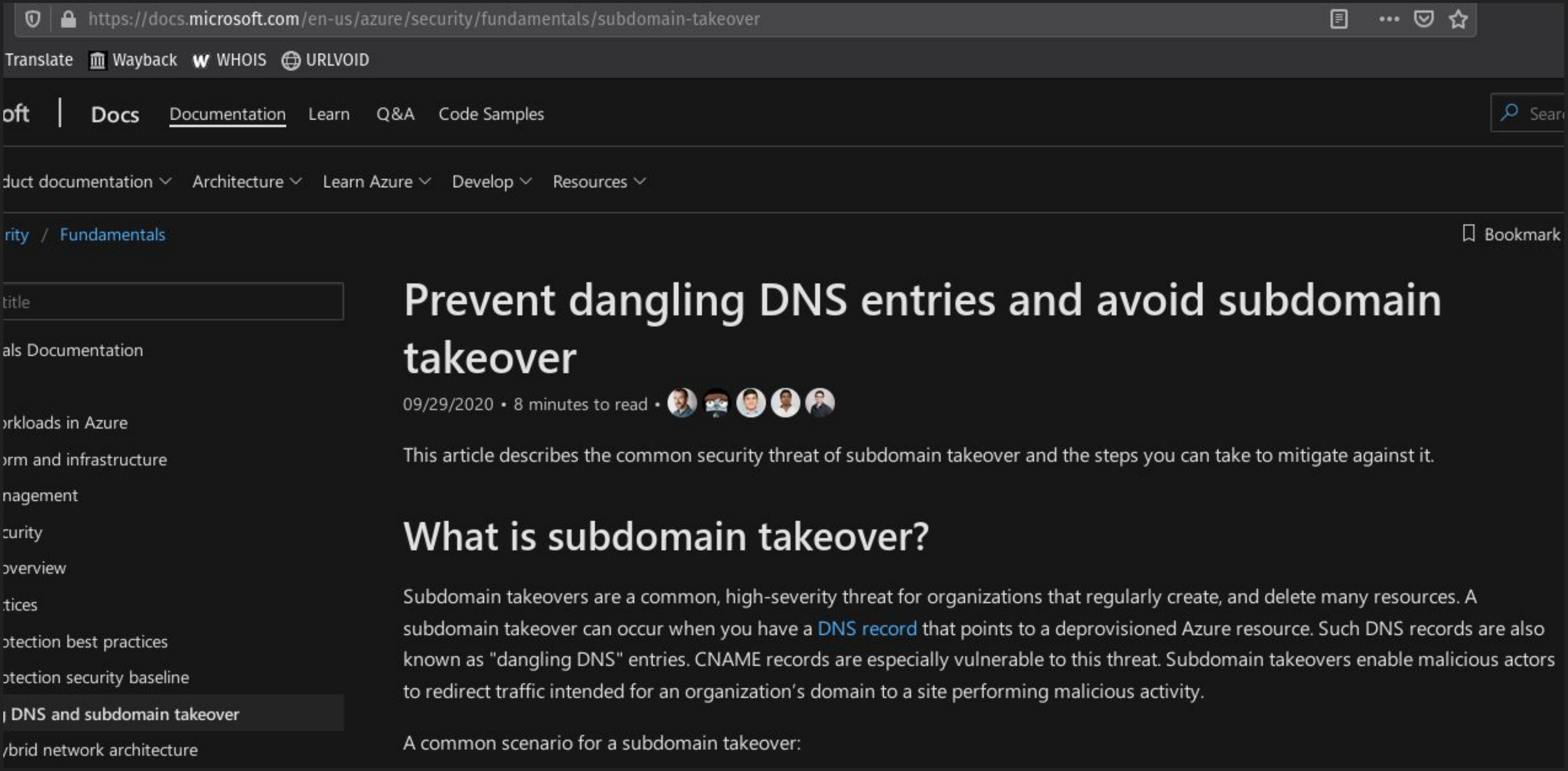
Single Sign-On (SSO) with vulnerable session cookies



saostatic.uber.com/subdomaintakeoverbyarneswinnen.html

Hijacked by Arne Swinnen

Is there protection with major hosting providers?



Prevent dangling DNS entries and avoid subdomain takeover

09/29/2020 • 8 minutes to read •

This article describes the common security threat of subdomain takeover and the steps you can take to mitigate against it.

What is subdomain takeover?

Subdomain takeovers are a common, high-severity threat for organizations that regularly create, and delete many resources. A subdomain takeover can occur when you have a DNS record that points to a deprovisioned Azure resource. Such DNS records are also known as "dangling DNS" entries. CNAME records are especially vulnerable to this threat. Subdomain takeovers enable malicious actors to redirect traffic intended for an organization's domain to a site performing malicious activity.

A common scenario for a subdomain takeover:

https://docs.microsoft.com/en-us/azure/security/fundame ntals/subdomain-takeover

Defense

Remediating Vulnerable and Compromised Subdomains

- Align all DNS servers
  - Internal DNS servers
  - External DNS server
- Remediation varies depending on compromise

Subdomain Takeover
can be prevented.

Subdomain Takeover Prevention Methodology

Automate detection of vulnerable subdomains

Fix policies and procedures to improve change management

Challenges to Defending Subdomains

Browsers implicitly trust whatever the DNS server returns.

Users implicitly trust whatever the browser returns.

Inventory management needs to be disciplined.

Expired service detection needs to be continuous at scale.

Third-party management of resources needs to be disciplined.

Maintaining DNS hygiene needs to be disciplined.

Change Management needs to be disciplined.

Go raibh maith agaibh go léir.

Panda

panda@protectedbypanda.com

@fuzzing_panda

cybermedsummit.org

RaiseMe @ShellConLa