

CSP

Cookie

1 DNS **www.azureresky.live** CNAME **dlersec.azureedge.net** dlersec.azureedge.net  
**www.azureresky.live** CNAME

2 DNS ( blog.raven-medicine.com) **blog.ravenmedicine.com** CNAME **blog.ravenmedicine.azureedge.net** (

```
r—(root kali)-[~/Desktop]
L—# host -t cname app-cloud.dev.example.com
app-cloud.dev.example.com is an alias for app-cloud-dev-eus.azurewebsites.net.
```

```
r—(root kali)-[~/Desktop]
L—# host app-cloud-dev-eus.azurewebsites.net
Host app-cloud-dev-eus.azurewebsites.net not found: 3(NXDOMAIN)
```

```
import sys
import dns.resolver

if len(sys.argv)!=2:
    print("Usage: python3 subdomain.py target.txt")
file=sys.argv[1]
target=[]
vuln=[]

with open(file,"r") as fp:
    for line in fp:
        try:
            target.append(line.strip())
        except:
```

```

        #print(line)
        print('Error')
print("Read "+str(len(target))+" subdomains")

for sub in target:
    try:
        cname = str(dns.resolver.resolve(sub, 'cname')[0])
        cname=cname[0: len(cname)-1]
        try:
            host=dns.resolver.resolve(cname, 'A')
        except:
            print(sub+" is vulnerable to subdomain takeover")
            vuln.append(sub)
            pass
    except:
        pass

print("\n\nThe following subdomains are vulnerable to subdomain take over")
for i in vuln:
    print(i)

```

```

Read 805 subdomains
activation.██████████.com is vulnerable to subdomain takeover
activation-dev.██████████.com is vulnerable to subdomain takeover
www.consumerservices.██████████.com is vulnerable to subdomain takeover
reviews.██████████.com is vulnerable to subdomain takeover
hdm-dev.██████████.com is vulnerable to subdomain takeover
craftcms.██████████.com is vulnerable to subdomain takeover
pao-app-cloud.dev.██████████.com is vulnerable to subdomain takeover
jdesss.██████████.com is vulnerable to subdomain takeover
pao-cloud-mv4.██████████.com is vulnerable to subdomain takeover

The following subdomains are vulnerable to subdomain take over
activation.██████████.com
activation-dev.██████████.com
www.consumerservices.██████████.com
reviews.██████████.com
hdm-dev.██████████.com
(██████████).com
pao-app-cloud.██████████.com
jdesss.██████████.com
(██████████).com

```

DNS <https://github.com/EdOverflow/can-i-take-over-xyz>

Revision #5

Created 20 February 2023 15:22:47 by

Updated 18 October 2023 03:57:24 by unknown