Subdomain Takeovers

Cactus Con 12

Anthony Pipia

Agenda

- ➔ About Me
- ➔ What is Subdomain Takeover
  - ◆ How?
- ➔ Dangers of Subdomain Takeover
  - ◆ What are the risks?
- ➔ Detect and Remediate
  - ◆ Ways to find and fix it yourself

Image Credit: ThreatNG

About Me

- ASU Graduate
- Started in Vulnerability Management
  - 2 yrs
- AppSec & Consulting Experience
  - 5 yrs
- Automation Focused
- Cybersecurity Instructor

Subdomain Takeovers - Bug Bounty

Bugcrowd’s Vulnerability Rating Taxonomy:

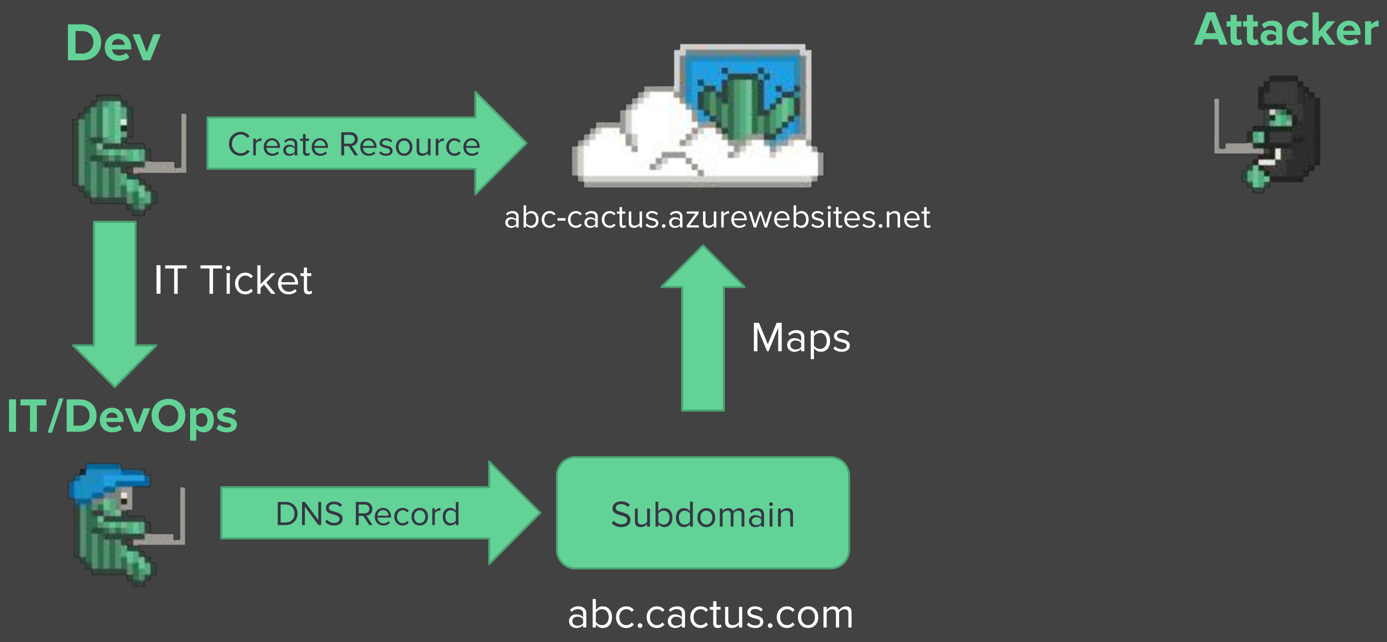
- ➔ High Impact Subdomain Takeover: **P2** (High)
- ➔ Basic Subdomain Takeover: **P3** (Medium)

Bugcrowd’s Recommended Rewards

- ➔ P2: $1,500 - $7,500
- ➔ P3: $500 - $2,500

Subdomain Takeovers accounted for **22%** of the Bug Bounty reports submitted to our program

What is Subdomain Takeover?



Dev

Create Resource

abc-cactus.azurewebsites.net

Attacker

IT Ticket

Maps

IT/DevOps

DNS Record

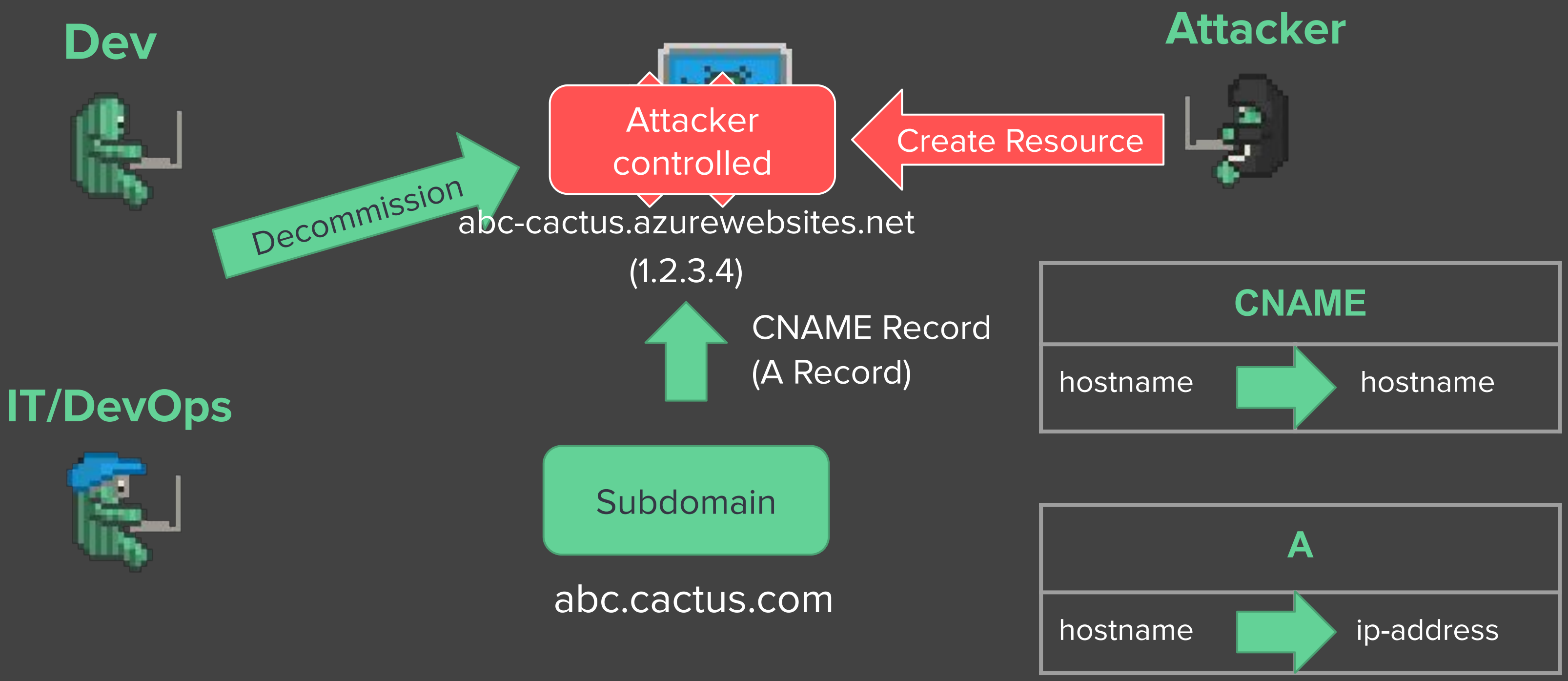
Subdomain

abc.cactus.com

What is Subdomain Takeover?

Subdomain Takeover

VULNERABLE



CNAME		
hostname	→	hostname

A		
hostname	→	ip-address

Subdomain Takeover Risks

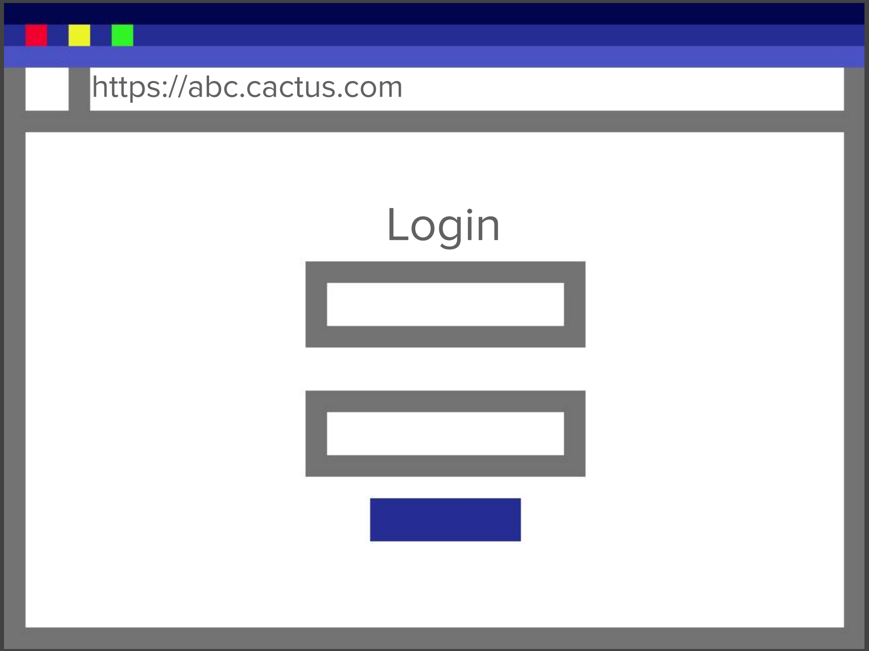
At a minimum:

Subdomain Takeover Risks

At a minimum:

➔ Excellent Phishing Spot

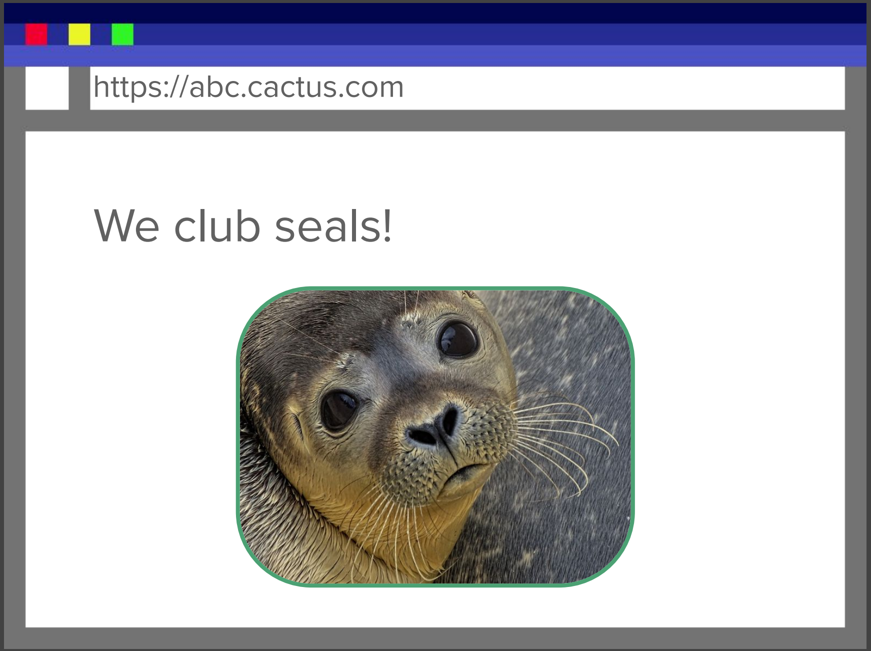
- Fake login page
- Links to use in emails that look legitimate



Subdomain Takeover Risks

At a minimum:

- Excellent Phishing Spot
  - Fake login page
  - Links to use in emails that look legitimate
- Defacement / Reputation
  - Control the content on the site



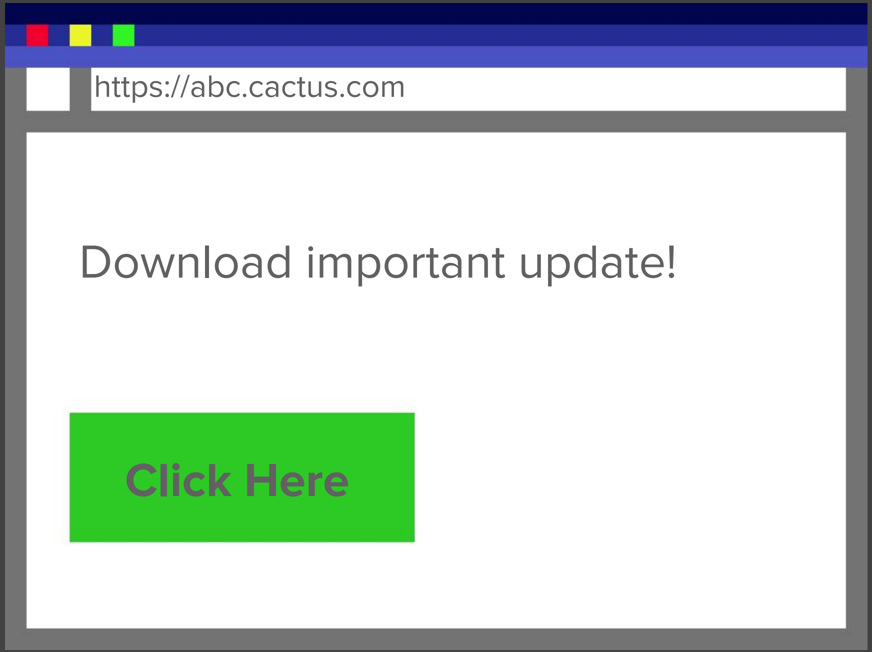
https://abc.cactus.com

We club seals!

Subdomain Takeover Risks

At a minimum:

- Excellent Phishing Spot
  - Fake login page
  - Links to use in emails that look legitimate
- Defacement / Reputation
  - Control the content on the site
- Serve Malware
  - Trusted URL makes users more comfortable downloading files



https://abc.cactus.com

Download important update!

Subdomain Takeover Risks

At a minimum:

- Excellent Phishing Spot
  - Fake login page
  - Links to use in emails that look legitimate
- Defacement / Reputation
  - Control the content on the site
- Serve Malware
  - Trusted URL makes users more comfortable downloading files

Other potential risks:

- Stealing user cookies / sessions
  - Depends on configuration

Subdomain Takeover Risks

At a minimum:

- Excellent Phishing Spot
  - Fake login page
  - Links to use in emails that look legitimate
- Defacement / Reputation
  - Control the content on the site
- Serve Malware
  - Trusted URL makes users more comfortable downloading files

Other potential risks:

- Stealing user cookies / sessions
  - Depends on configuration
- Cross-Site Scripting (XSS) attacks
  - Depends on configuration

Subdomain Takeover Risks

At a minimum:

- Excellent Phishing Spot
  - Fake login page
  - Links to use in emails that look legitimate
- Defacement / Reputation
  - Control the content on the site
- Serve Malware
  - Trusted URL makes users more comfortable downloading files

Other potential risks:

- Stealing user cookies / sessions
  - Depends on configuration
- Cross-Site Scripting (XSS) attacks
  - Depends on configuration

Stealing Cookies

Protected by default

- ➔ Same Origin Policy (SOP)
- ➔ Default behavior of cookie without Domain attribute

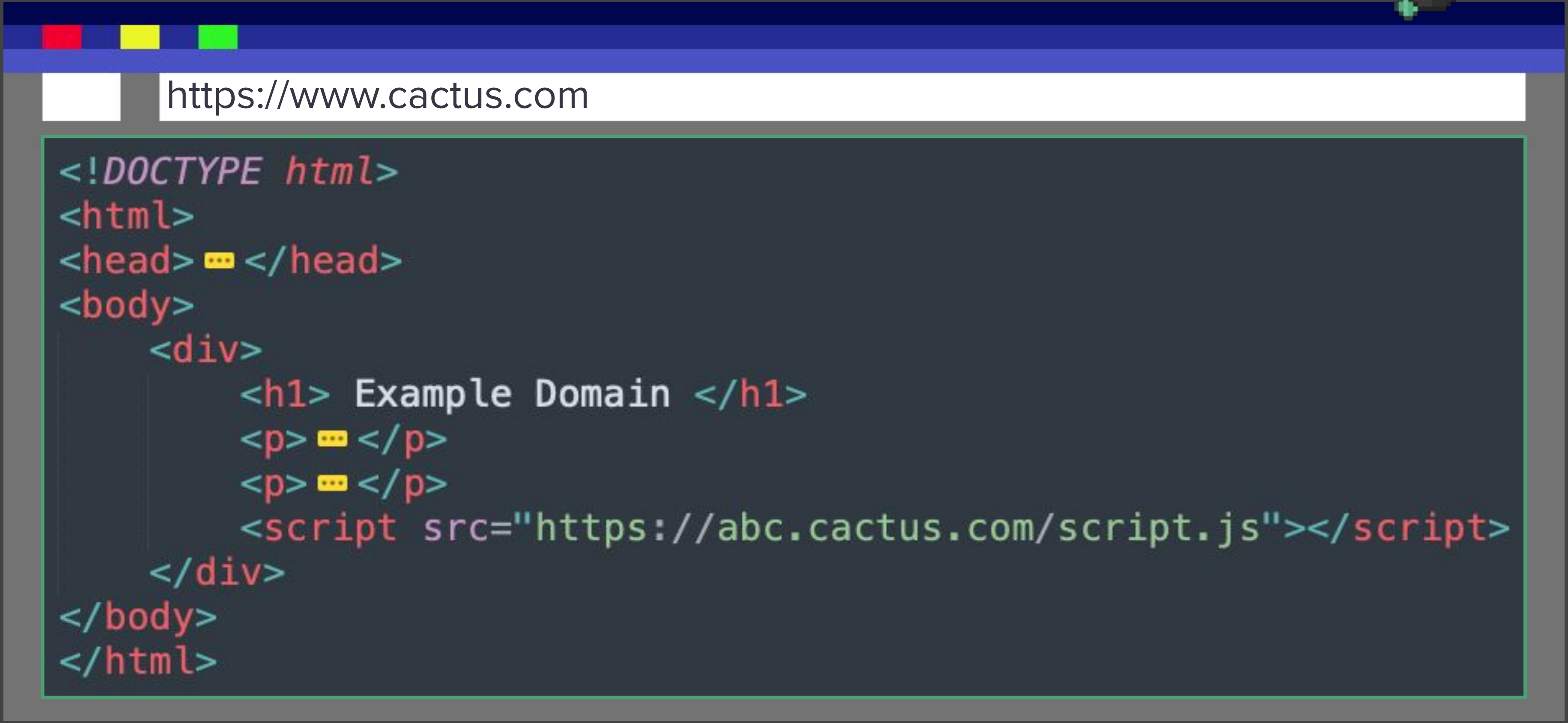
In the context of Subdomain Takeovers, your cookies are protected if you **don’t set the Domain** attribute to the higher-level domain.

A setting of `Domain=cactus.com` will cause the cookie to be sent to `abc.cactus.com`

Cookie Attribute	Hacker Subdomain	Vulnerable
`Domain=cactus.com`	`abc.cactus.com`	Unsafe
`Domain=www.cactus.com`	`abc.cactus.com`	Safe

Subdomain Takeover can’t be used to steal sensitive cookies if **the cookies are properly protected.**

Cross-Site Scripting (XSS)



https://www.cactus.com

```
<!DOCTYPE html>
<html>
<head> ⋯ </head>
<body>
    <div>
        <h1> Example Domain </h1>
        <p> ⋯ </p>
        <p> ⋯ </p>
        <script src="https://abc.cactus.com/script.js"></script>
    </div>
</body>
</html>
```

Cross-Site Scripting (XSS)

Subdomain Takeover can be used to bypass the Content Security Policy header.

“The **Content-Security-Policy** header allows you to restrict which resources (such as JavaScript, CSS, Images, etc.) can be loaded, and the URLs that they can be loaded from.”
- https://content-security-policy.com/

Cross-Site Scripting (XSS)

Subdomain Takeover can be used to bypass the Content Security Policy header.

“The **Content-Security-Policy** header allows you to restrict which resources (such as JavaScript, CSS, Images, etc.) can be loaded, and the URLs that they can be loaded from.”
- https://content-security-policy.com/

Example:

```
Content-Security-Policy: default-src 'self'; img-src 'self'
cdn.cactus.com; script-src ‘self’ abc.cactus.com;
```

Cross-Site Scripting (XSS)

Subdomain Takeover can be used to bypass the Content Security Policy header.

“The **Content-Security-Policy** header allows you to restrict which resources (such as JavaScript, CSS, Images, etc.) can be loaded, and the URLs that they can be loaded from.” - https://content-security-policy.com/

Example:

```
Content-Security-Policy: default-src 'self'; img-src 'self'
cdn.cactus.com; script-src ‘self’ abc.cactus.com;
```

Cross-Site Scripting payloads that use **abc.cactus.com** as a source will execute.

Detect and Remediate

This is a **DNS hygiene** issue

1. Find all DNS records that point to cloud resources you **no longer own**.
2. **Remove** those DNS records.

“**Find them** and **destroy them.**”

- Mr. Smith

Detect and Remediate

This is a **DNS hygiene** issue

1. Find all DNS records that point to cloud resources you **no longer own**.
2. **Remove** those DNS records.

DNS Record System

Name	Content
xyz.cactus.com	xyz-cactus.azurewebsites.net
~~abc.c om~~	~~abc-cactu websites.net~~
~~abc.c om~~	~~1.2.3.4~~

> “**Find them** and **destroy them.**”
>
> \- Mr. Smith

Detect and Remediate

1. Gather all DNS Records that point to cloud resources
2. Determine if the resource still exists
3. Delete the DNS record if it the resource no longer exists

dnsReaper

Github: punk-security/dnsReaper

Detect and Remediate

What about A Records?

➔ Find all A-records that point to Cloud IP Addresses

- Azure: `https://www.azurespeed.com/api/ipAddress?ipOrDomain=<IP>`
- AWS: `https://awsips.co/ip-ranges.json`

➔ Find all public IP addresses in cloud environment (Azure Example)

- Use Resource Graph query:

```
resources | where type contains 'publicIPAddresses' and
isnotempty(properties.ipAddress) | project
properties.ipAddress, subscriptionId"
```

➔ Remove Records

- If the record points to an IP not in your list from Azure, remove the record.
- If you don’t want to automate deleting records (dangerous), have the script send a slack message.

Detect and Remediate - A Records

DNS

A	lmnop.cactus.com	5.4.3.2
A	sql.cactus.com	1.3.3.7
A	dev.cactus.com	8.3.4.7
A	abc.cactus.com	1.2.3.4
A	xyz.cactus.com	3.2.4.1

Cloud Environment

4.3.5.1
5.4.3.2
8.7.5.4
1.3.3.7
7.7.7.7

Detect and Remediate - A Records

DNS

A	lmnop.cactus.com	5.4.3.2
A	sql.cactus.com	1.3.3.7
A	dev.cactus.com	8.3.4.7
A	abc.cactus.com	1.2.3.4
A	xyz.cactus.com	3.2.4.1

Cloud Environment

4.3.5.1
5.4.3.2
8.7.5.4
1.3.3.7
7.7.7.7

Is IP Address owned by cloud provider?
(ex. azurespeed.com, awsips.co)

```
https://www.azurespeed.com/api/ipAddress?ipOrDomain=<IP>
https://awsips.co/ip-ranges.json
```

Detect and Remediate - A Records

DNS

A	lmnop.cactus.com	5.4.3.2	
A	sql.cactus.com	1.3.3.7	
A	dev.cactus.com	8.3.4.7	❌
A	abc.cactus.com	1.2.3.4	
A	xyz.cactus.com	3.2.4.1	❌

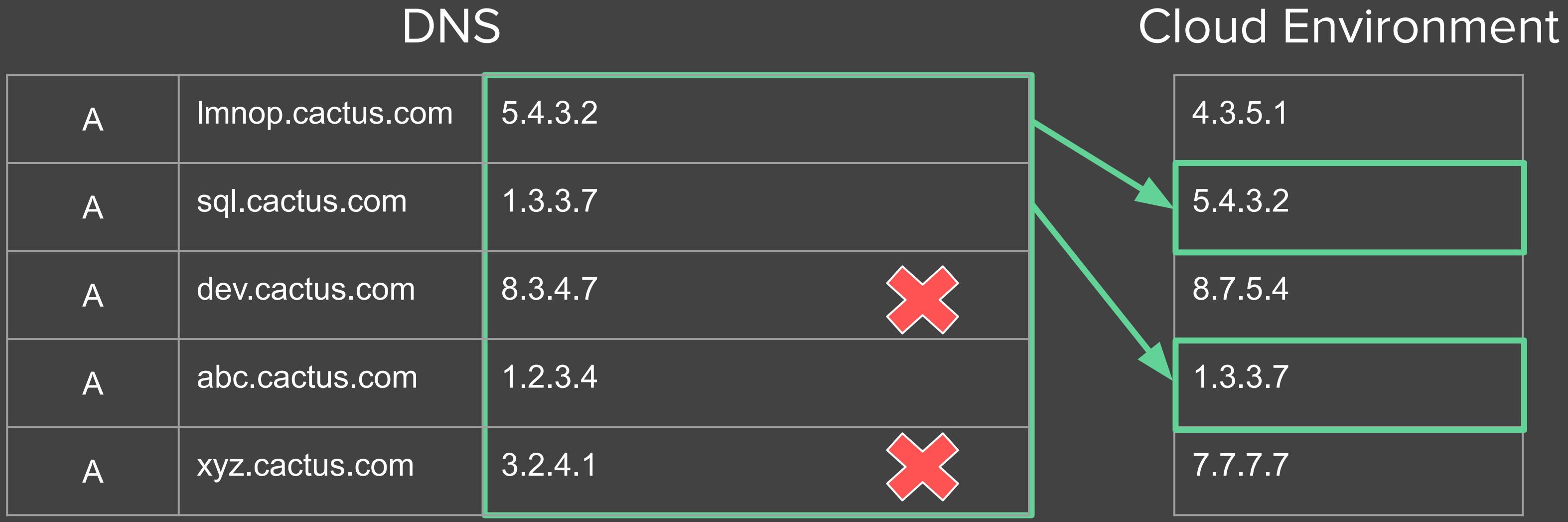
Cloud Environment

4.3.5.1
5.4.3.2
8.7.5.4
1.3.3.7
7.7.7.7

Is IP Address owned by cloud provider?
(ex. azurespeed.com, awsips.co)

```
https://www.azurespeed.com/api/ipAddress?ipOrDomain=<IP>
https://awsips.co/ip-ranges.json
```

Detect and Remediate - A Records



DNS

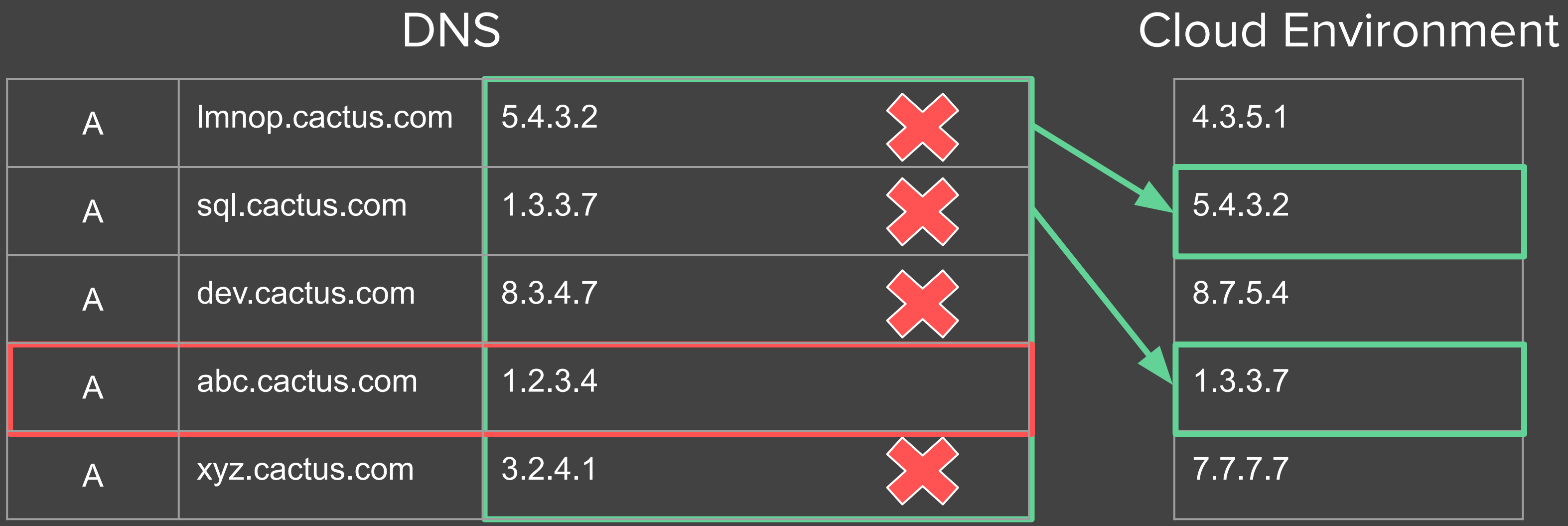
A	lmnop.cactus.com	5.4.3.2
A	sql.cactus.com	1.3.3.7
A	dev.cactus.com	8.3.4.7 ✗
A	abc.cactus.com	1.2.3.4
A	xyz.cactus.com	3.2.4.1 ✗

Cloud Environment

4.3.5.1
5.4.3.2
8.7.5.4
1.3.3.7
7.7.7.7

Check remaining records against list of public ip addresses in your cloud environment

Detect and Remediate - A Records



DNS

A	lmnop.cactus.com	5.4.3.2 ✗
A	sql.cactus.com	1.3.3.7 ✗
A	dev.cactus.com	8.3.4.7 ✗
A	abc.cactus.com	1.2.3.4
A	xyz.cactus.com	3.2.4.1 ✗

Cloud Environment

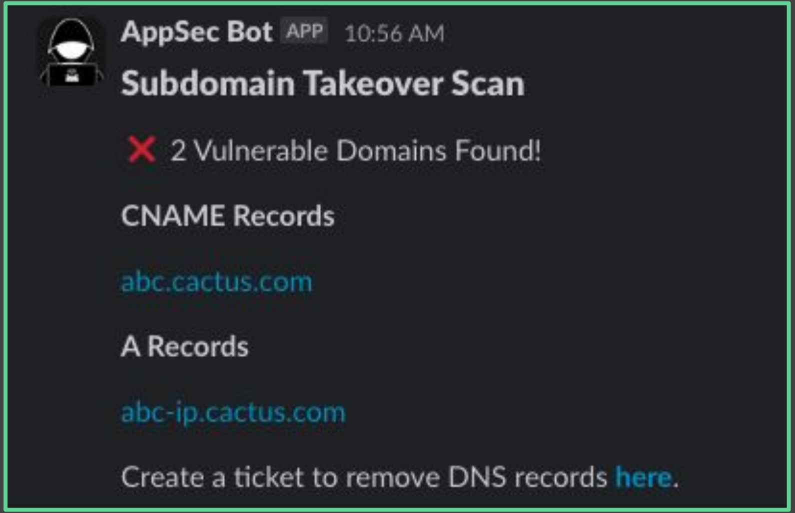
4.3.5.1
5.4.3.2
8.7.5.4
1.3.3.7
7.7.7.7

Any remaining records are vulnerable to

`Subdomain Takeover`

Detect and Remediate - Automation

1. Run dnsReaper with DNS API token and save the results in a json file.
2. Run custom A-Record scan using the same DNS API token along with an Azure PAT Token to get public IP Addresses.
3. Append results to the json file from dnsReaper.
4. Processes the results and send a slack message with vulnerable subdomains.



AppSec Bot APP 10:56 AM

Subdomain Takeover Scan

❌ 2 Vulnerable Domains Found!

CNAME Records

abc.cactus.com

A Records

abc-ip.cactus.com

Create a ticket to remove DNS records here.

Detect and Remediate - Automation

Scripts & Tools

➔ https://github.com/Apipia/cactus-con-12 - Python (a-record scanning)

➔ dnsReaper - Python

➔ Azure Get-DanglingDNSRecords - Powershell Script

➔ recon-ng - Web Reconnaissance framework

➔ theHarvester - OSINT intelligence gathering tool

➔ Sublist3r - OSINT subdomain enumeration tool

➔ dnsrecon - DNS Enumeration Script

Detect and Remediate - Paid Solution

Paid Tools and Services

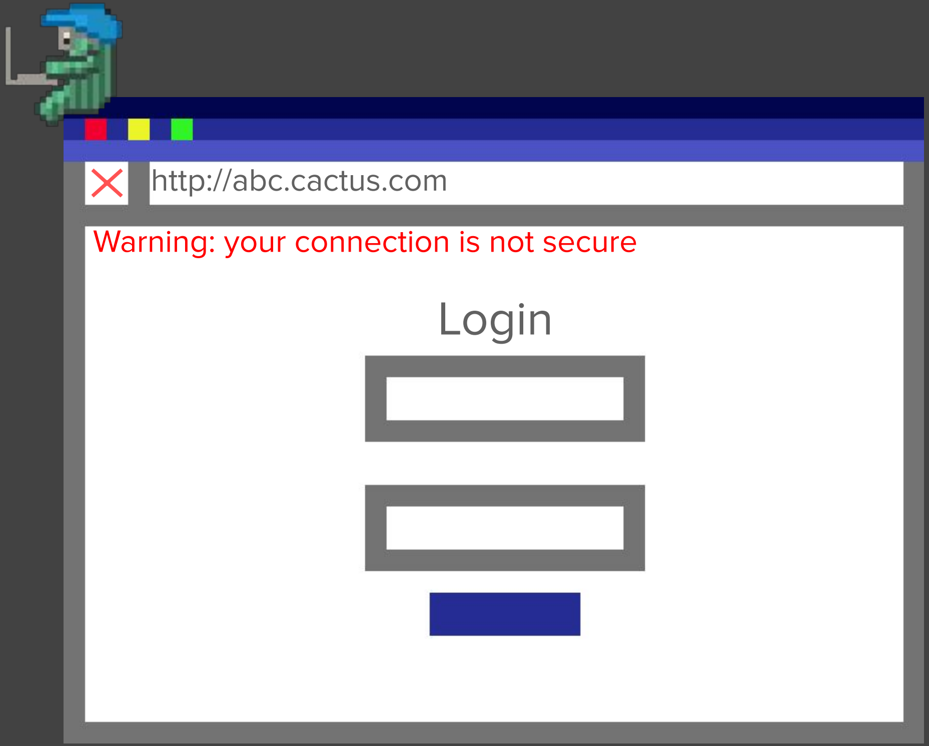
- Bug Bounty Program
- External Pentest Scope
- ThreatNG - Subdomain Takeover
- Paloalto Networks - Prisma
- Detectify

Prevention

1. **Improve decommission process** to ensure DNS records are deleted first, then proceed with cloud resource decommissioning

Reduce Risk

1. **CAA DNS Certificate**
2. Don’t set **Domain** attribute on sensitive cookies



http://abc.cactus.com

Warning: your connection is not secure

Thank you!

Q&A

https://www.linkedin.com/in/anthonypipia

https://github.com/Apipia/cactus-con-12

References

- OWASP | Test for Subdomain Takeover
  https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/10-Test_for_Subdomain_Takeover
- Hacker One | Guide to Subdomain Takeover
  https://www.hackerone.com/application-security/guide-subdomain-takeovers
- 0xpatrik | Subdomain Takeover
  https://0xpatrik.com/subdomain-takeover-basics/
  https://0xpatrik.com/subdomain-takeover/
- Hacktricks.xyz | Subdomain Takeover
  https://book.hacktricks.xyz/pentesting-web/domain-subdomain-takeover
- ThreatNG | Subdomain Takeover
  https://www.threatngsecurity.com/subdomain-takeover