SUBDOMAIN TAKEOVER

What is Subdomain?

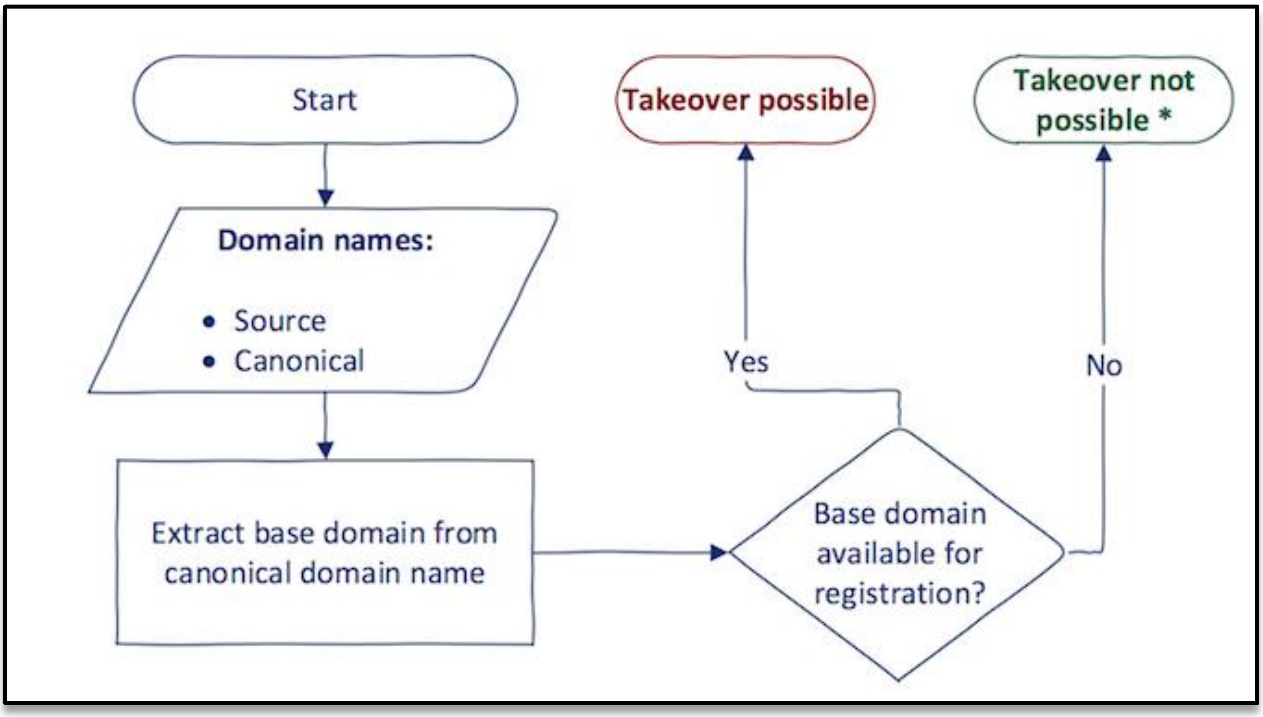
A subdomain is an additional part to your main domain name. Subdomains are created to organize and navigate to different sections of your website. You can create multiple subdomains or child domains on your main domain.

For example: store.yourwebsite.com

What is Subdomain takeover Vulnerability

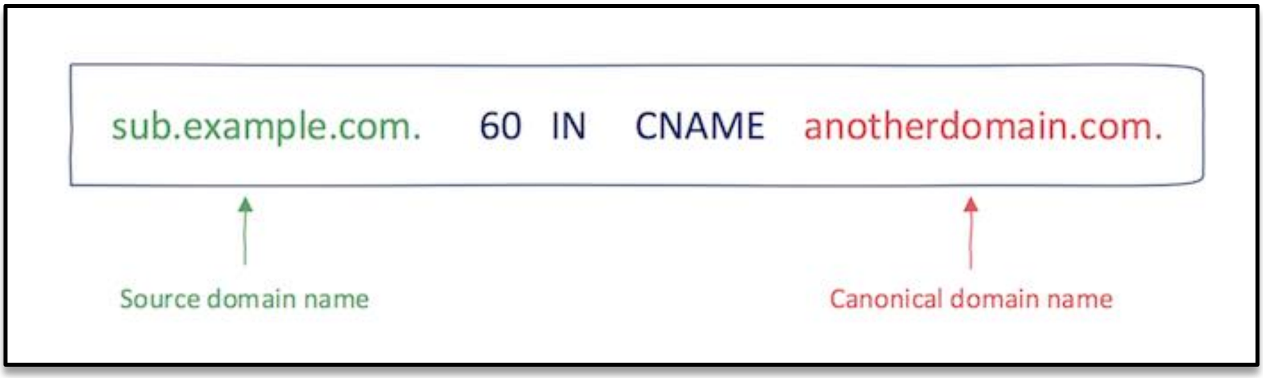
A subdomain takeover occurs when an attacker gains control over a subdomain of a target domain.

Typically, this happens when the subdomain has a canonical name **CNAME [A Canonical Name record is a type of resource record in the Domain Name System that maps one domain name to another. This can prove convenient when running multiple services from a single IP address]** in the Domain Name System (DNS), but no host is providing content for it.


Start
Takeover possible
Takeover not possible *
Domain names:
Source
Canonical
Yes
No
Extract base domain from canonical domain name
Base domain available for registration?

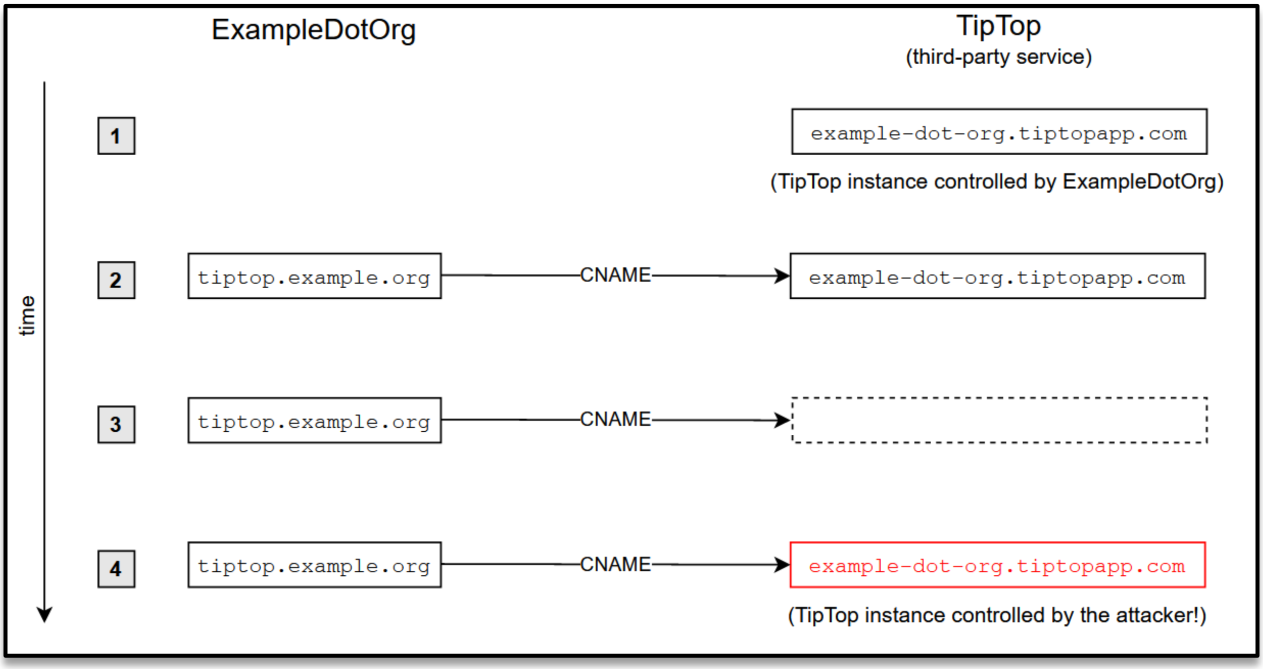
This can happen because either a virtual host hasn't been published yet or a virtual host has been removed.

An attacker can take over that subdomain by providing their own virtual host and then hosting their own content for it.



A Typical Scenario:

To fix ideas, let's go over a typical subdomain-takeover scenario. Let's assume that your organization, ExampleDotOrg, whose domain name is example.org, wants to use some service from a vendor called TipTop.


ExampleDotOrg
TipTop
(third-party service)
time
1
example-dot-org.tiptopapp.com
(TipTop instance controlled by ExampleDotOrg)
2
tiptop.example.org
CNAME
example-dot-org.tiptopapp.com
3
tiptop.example.org
CNAME
4
tiptop.example.org
CNAME
example-dot-org.tiptopapp.com
(TipTop instance controlled by the attacker!)

How to find Vulnerable Subdomain

The first step is to list every subdomain of the web application using a subdomain discovery tool (such as subfinder, sublister, knockpy, amass, or turbolister) and save the results in a file.

The next step is to use tools to detect vulnerable subdomains to scan the subdomain file.

Subzy:

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

Subjack:

```
go get -u -v github.com/lukasikic/subzy
```

Tko-subs:

```
go get github.com/anshumanbh/tko-subs
```

Sub404:

```
git clone https://github.com/r3curs1v3-pr0xy/sub404.git
```

Use dig to check the CNAME of the subdomain. Then, you may check to takeover the subdomain using

- Github
- AWS S3
- Shopify
- Unbounce (etc)

Impact of Subdomain takeover

Defacement: If possible, an attacker may decide to change the appearance of pages served by the vulnerable example.org subdomain to openly ridicule or embarrass your organization

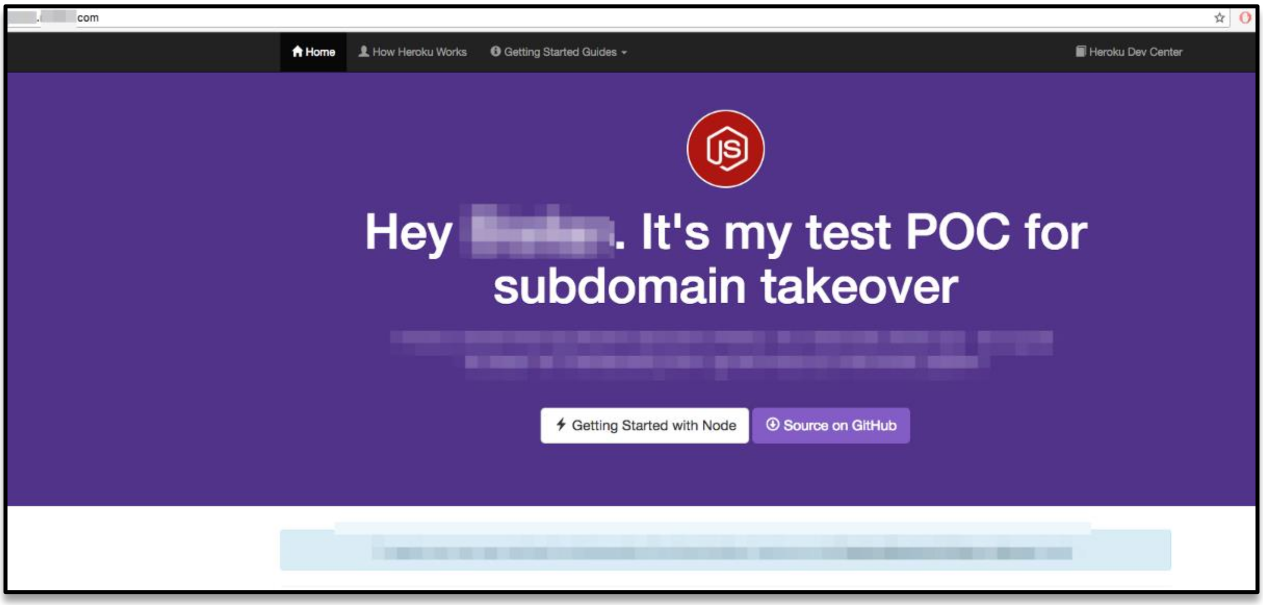
Phishing: Another obvious way to exploit a subdomain vulnerable to takeover is phishing.

Stealing Broadly Scoped Cookies: Run-of-the-mill phishing typically requires some gullibility and user interaction (beyond navigating to the malicious site) from the victim. A subdomain takeover is more powerful, though, as it may enable an attacker to steal sensitive cookies simply by the victim visiting the attacker's site.

Cross-Site Request Forgery: Cross-site request forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which [he or she is] currently authenticated.

Abusing Over trusting CORS-Aware Servers.

Defeating a Permissive Content Security Policy.



[redacted].com

Hey [redacted]. It's my test POC for subdomain takeover

[redacted]

[redacted]

Subdomain takeover References

https://bughacking.com/best-subdomain-takeover-tools-for-bug-bounty-hunting/

https://0xpatrik.com/subdomain-takeover-basics/

https://www.honeybadger.io/blog/subdomain-takeover/