

INITD COMMUNITY



Subdomain**Takeover**



THE ULTIMATE GUIDE
FOR BASIC SUBDOMAIN
TAKEOVER WITH PRACTICAL

BY
Touhid M. Shaikh

Special Thanks!!

We are InitD

Harshal Ghaisas - Logo Designer
Shrutirupa Banerjee, Sachin Sase and
Sagar Sharma - Members



TABLE OF contents

1. Introduction
2. What is Subdomain?
3. What is Subdomain Takeover?
4. All About CNAME.
5. How to find CNAME Records?
6. What is Subdomain Takeover Lab?
7. Let's Takeover Subdomain.
 - Github Pages
 - AWS S3 Bucket
 - Tilda
8. Mitigation
9. Bibliography

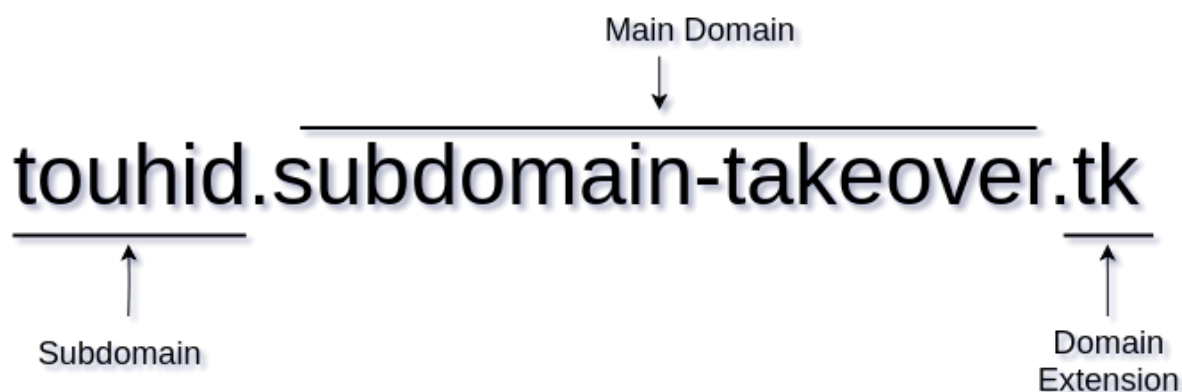


INTRODUCTION

Subdomain takeover vulnerabilities occur when a subdomain (subdomain.example.com) is pointing to a service (e.g. Amazon S3, GitHub pages, Heroku, etc.) that has been removed or deleted.

This allows an attacker to set up a page on the service that was being used and point their page to that subdomain. For example, if subdomain.example.com was pointing to a GitHub page and the user decided to delete their GitHub page, an attacker can now create a GitHub page, add a CNAME file containing subdomain.example.com, and claim subdomain.example.com.

What is Subdomain?



(Fig: 1).

Subdomain is a part of main domain. In the above picture(Fig: 1). I have explained a subdomain. The main domain name is subdomain-takeover with extension .tk and part of this main domain is touhid which is called subdomain of this main domain.

What is Subdomain Takeover?

Subdomain Takeover is a type of vulnerability which occurs due to Mis-configuration DNS CNAME, NS, MX records.

Scenario Example:

When a company or individual has configured a DNS CNAME entry for one of its subdomains pointing to an external service (ex: Heroku, Github Pages, Bitbucket, Tilda, AWS S3 Bucket, Shopify, etc) but the service is no longer utilized by that company. In that condition, An attacker could register to the external service and claim the affected subdomain to configure his/her service's to point affected subdomain.

All About CNAME

CNAME stands for Canonical Name is a type of Domain Name System(DNS) record that maps an alias name to a true or canonical domain name. CNAME records are typically used to map a subdomain such as www, mail, cpanel, blog etc to the domain hosting that subdomain's content.



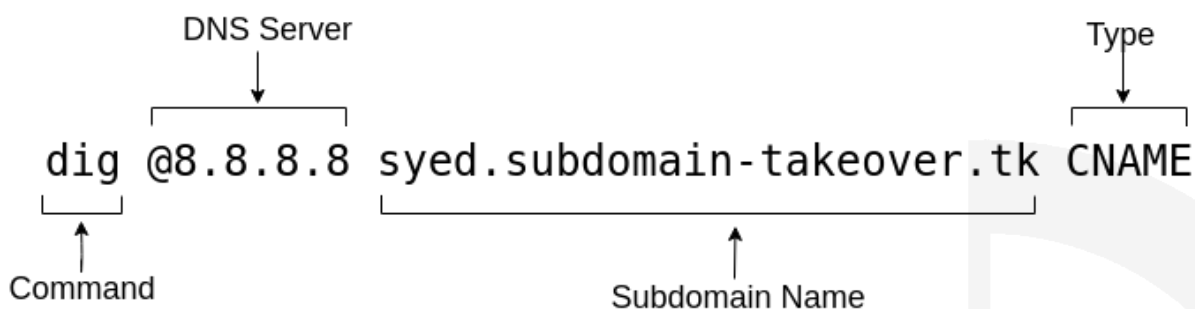
How to find CNAME records?

There is N-Number of ways to find the CNAME record to associate subdomain. In this section, I'll show you a few of techniques to find the CNAME record of the specific subdomain.

[ok] started...

- Dig Command

```
$ dig @8.8.8.8 syed.subdomain-takeover.tk CNAME
```



DNS Server: Here we can use any DNS Server. I have used the Google Public DNS(8.8.8.8) Server name. But you can use any of DNS servers like Your Private DNS server or any Anonymous DNS server name also.

Subdomain Name: Here, I have to ask record to my DNS server.

Type: I have asked for specific CNAME record only to DNS Server.

How to find CNAME records? (cont'd)

OUTPUT:

```
; <<>> DiG 9.11.5-P1-1-Debian <<>> @8.8.8.8 syed.subdomain-takeover.tk CNAME
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38864
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;syed.subdomain-takeover.tk.      IN      CNAME

;; ANSWER SECTION:
syed.subdomain-takeover.tk. 3599 IN      CNAME   touhidshaikh.github.io.

;; Query time: 365 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jan 30 19:39:49 IST 2019
;; MSG SIZE rcvd: 91
```



How to find CNAME records? (cont'd)

- Host Command

```
$ host syed.subdomain-takeover.tk
```

OUTPUT:

```
syed.subdomain-takeover.tk is an alias for touhidshaikh.github.io.  
touhidshaikh.github.io has address 185.199.108.153  
touhidshaikh.github.io has address 185.199.109.153  
touhidshaikh.github.io has address 185.199.111.153  
touhidshaikh.github.io has address 185.199.110.153
```



There is N-Number of tools to check DNS record in various visual formats. You can use DNS recon tools also to check multiple DNS.

What is Subdomain Takeover Lab?

Subdomain Takeover Lab is Initiative of InitD Community for all(Infosec Guys). Here, its legal to takeover subdomain and host anything(Read Rules). Hackers can explore thier Subdomain Takeover Skills with a vulnerable subdomain of subdomain-takeover.tk domain. You can find more than 100 subdomain which is Mis-Configured DNS record such as CNAME, MX, NS records.

Subdomain Takeover Lab Link: <https://subdomain-takeover.tk>

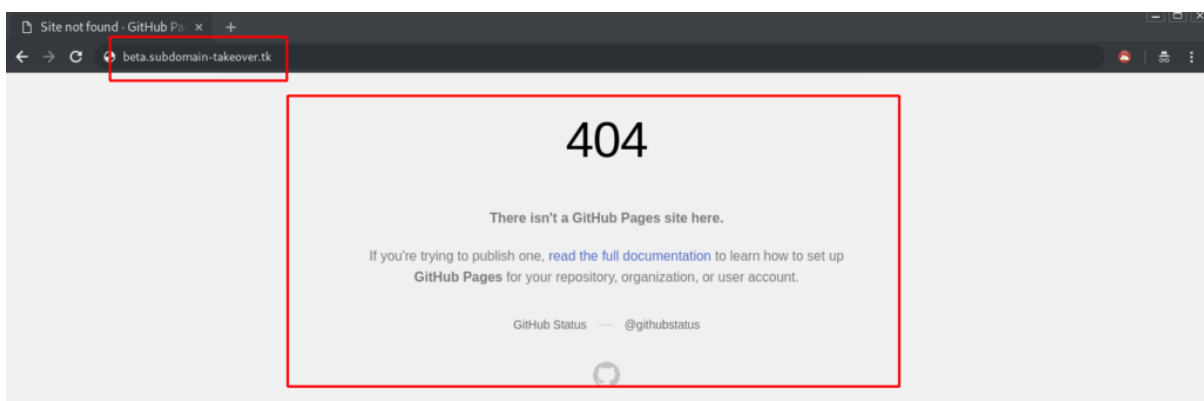
Let's Takeover Subdomain

Enough Talk! Lets start Hands-on.

Github Pages

Vulnerable Subdomain: beta.subdomain-takeover.tk

Let's Visit this URL.



In above an image. we got **404 Error** page. its means, this subdomain has no longer

GitHub Page.

In short, we can claim this Subdomain by pointing our GitHub page to this subdomain. Let's confirm CNAME records by Dig Command.

```
touhid@kali:/tmp$ dig @8.8.8.8 beta.subdomain-takeover.tk CNAME
; <<>> DiG 9.11.5-P1-1-Debian <<>> @8.8.8.8 beta.subdomain-takeover.tk CNAME
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35643
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 512
;; QUESTION SECTION:
;beta.subdomain-takeover.tk.      IN      CNAME

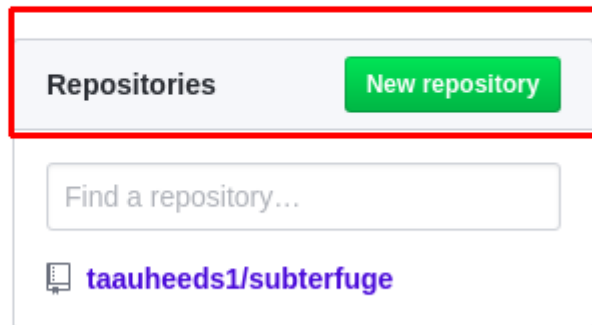
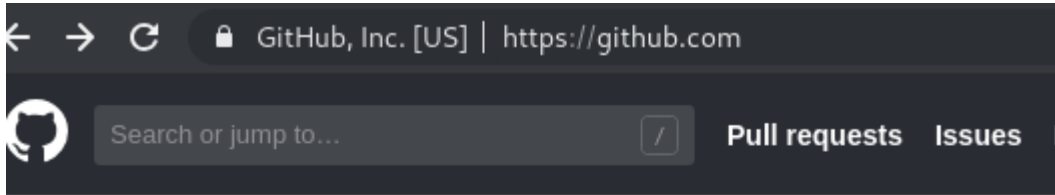
;; ANSWER SECTION:
beta.subdomain-takeover.tk. 14399 IN    CNAME   touhidshaikh.github.io.

;; Query time: 4315 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Jan 07 15:56:25 IST 2019
;; MSG SIZE rcvd: 91

touhid@kali:/tmp$
```

Great this subdomain pointed to **github.io**

Let's Login to GitHub and Create a Repository with any name.





Make a New repository or you can use you exist repository.

Create a new repository

A repository contains all the files for your project, including the revision history.

Owner **Repository name**

 taauheeds1 ▾ / github 

Great repository names are short and memorable. Need inspiration? How about [fantastic-doodle](#).

Description (optional)

testing subdomain takeover

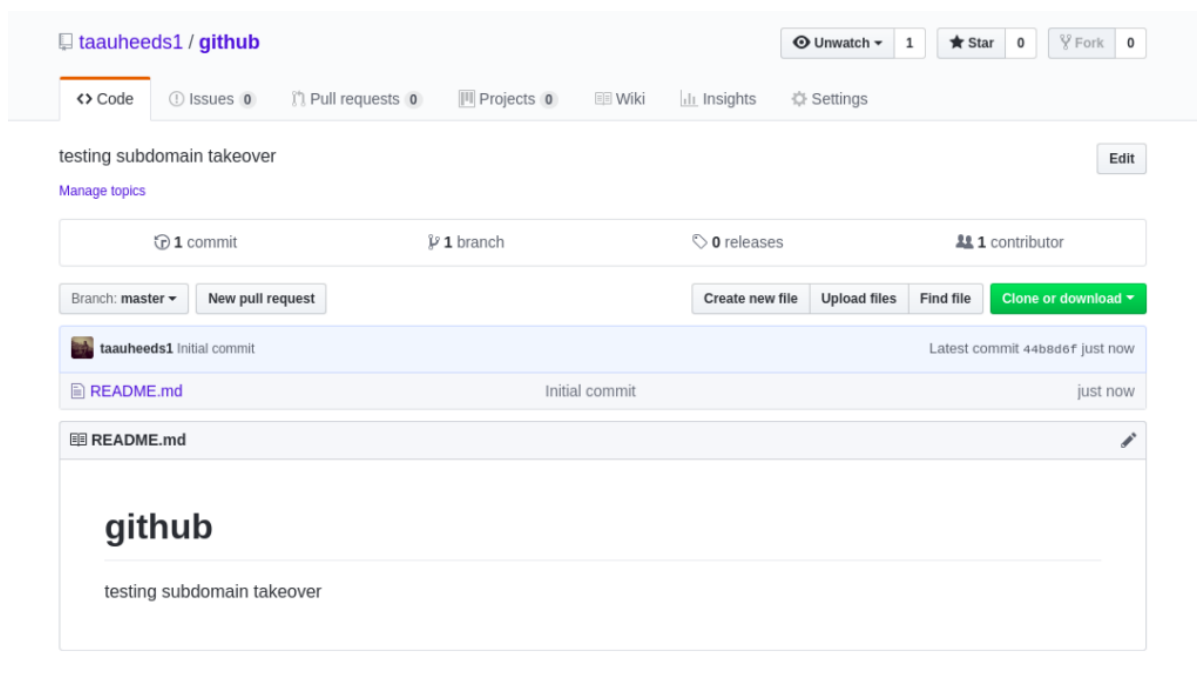
- Public**
Anyone can see this repository. You choose who can commit.
- Private**
You choose who can see and commit to this repository.

Initialize this repository with a README
This will let you immediately clone the repository to your computer. Skip this step if you're importing an existing repository.

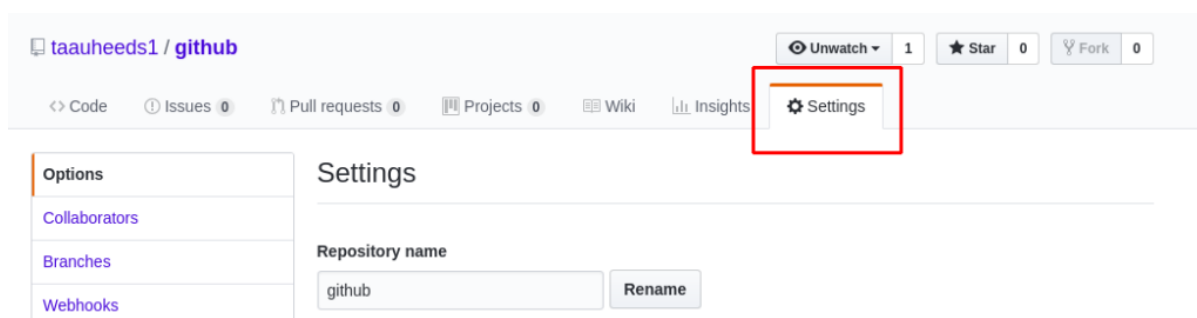
Add .gitignore: **None** ▾ Add a license: **None** ▾ 

Create repository

After Creating you repository. its will shows like below.



now go to repository setting.



In **Setting** Go to the **Github Page** Section.

GitHub Pages

GitHub Pages is designed to host your personal, organization, or project pages from a GitHub repository.

Source
GitHub Pages is currently disabled. Select a source below to enable GitHub Pages for this repository. [Learn more.](#)

None ▾ **Save**

Theme Chooser
Select a theme to publish your site with a Jekyll theme using the master branch. [Learn more.](#)

Choose a theme

Change *None* to Your *Master* Repository and hit **Save**.

GitHub Pages

GitHub Pages is designed to host your personal, organization, or project pages from a GitHub repository.

Your site is ready to be published at <https://taauheeds1.github.io/github/>.

Source

Your GitHub Pages site is currently being built from the master branch. [Learn more.](#)

master branch ▾

Save

Theme Chooser

Select a theme to publish your site with a Jekyll theme. [Learn more.](#)

Choose a theme

Custom domain

Custom domains allow you to serve your site from a domain other than `taauheeds1.github.io`. [Learn more.](#)

Save

Enforce HTTPS

— Required for your site because you are using the default domain (`taauheeds1.github.io`)

HTTPS provides a layer of encryption that prevents others from snooping on or tampering with traffic to your site. When HTTPS is enforced, your site will only be served over HTTPS. [Learn more.](#)

Now add *subdomain* name here which you *want to takeover*. in my case, Custom domain will be **beta.subdomain-takeover.tk**

And you can use HTTPS connection. i just avoid **Enforce HTTPS** .

GitHub Pages

GitHub Pages is designed to host your personal, organization, or project pages from a GitHub repository.

Your site is ready to be published at <http://beta.subdomain-takeover.tk/>.

Source

Your GitHub Pages site is currently being built from the master branch. [Learn more.](#)

master branch ▾

Save

Theme Chooser

Select a theme to publish your site with a Jekyll theme. [Learn more.](#)

Choose a theme

Custom domain

Custom domains allow you to serve your site from a domain other than `taauheeds1.github.io`. [Learn more.](#)

beta.subdomain-takeover.tk

Save

Enforce HTTPS

HTTPS provides a layer of encryption that prevents others from snooping on or tampering with traffic to your site. When HTTPS is enforced, your site will only be served over HTTPS. [Learn more.](#)

Now Visit beta.subdomain-takeover.tk

↳ → ⓘ Not secure | beta.subdomain-takeover.tk

github

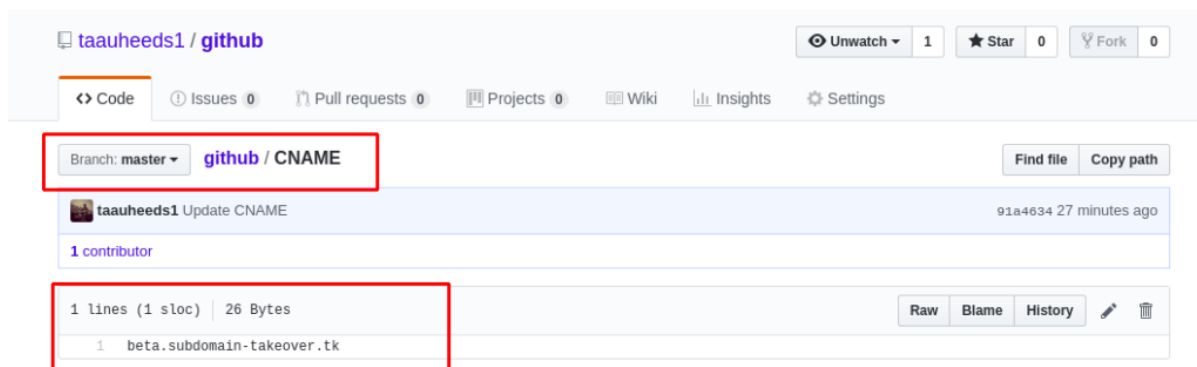
testing subdomain takeover

Congratulation !! You have Successfully Takeover

beta.subdomain-takeover.tk

There is another alternative way to doing same thing with minimum step.

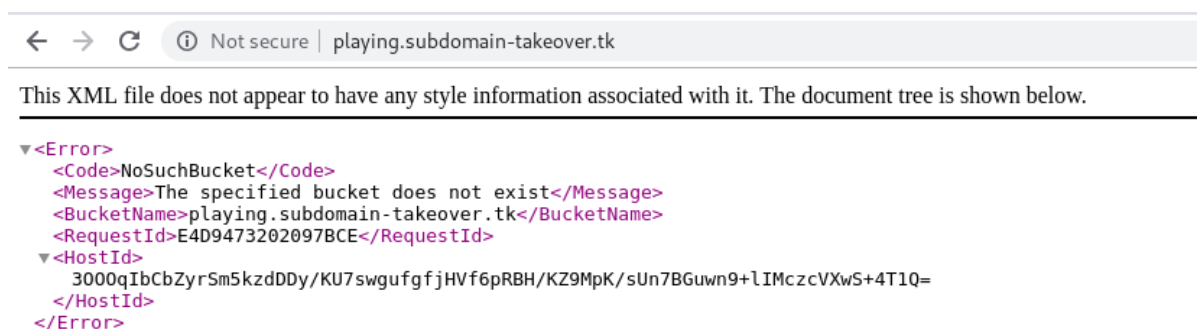
You Need to add a **CNAME** file with your desired subdomain name.



AWS S3 Bucket

Vulnerable Subdomain: *playing.subdomain-takeover.tk*

Let's Visit this URL.



We Got Error **NoSuchBucket**

This is good sign if you're going to takeover the subdomain.

Lets Verify this by looking for CNAME Records.

```
root@kali:/home/touhid# dig @8.8.8.8 playing.subdomain-takeover.tk CNAME

; <<>> DiG 9.11.5-P1-1-Debian <<>> @8.8.8.8 playing.subdomain-takeover.tk CNAME
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 4370
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;playing.subdomain-takeover.tk. IN      CNAME

;; ANSWER SECTION:
playing.subdomain-takeover.tk. 3599 IN CNAME   playing.subdomain-takeover.tk.s3.amazonaws.com.

;; Query time: 308 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jan 30 20:48:08 IST 2019
;; MSG SIZE rcvd: 118
```

Ahhh ! Good News its pointing to AWS S3 Bucket.

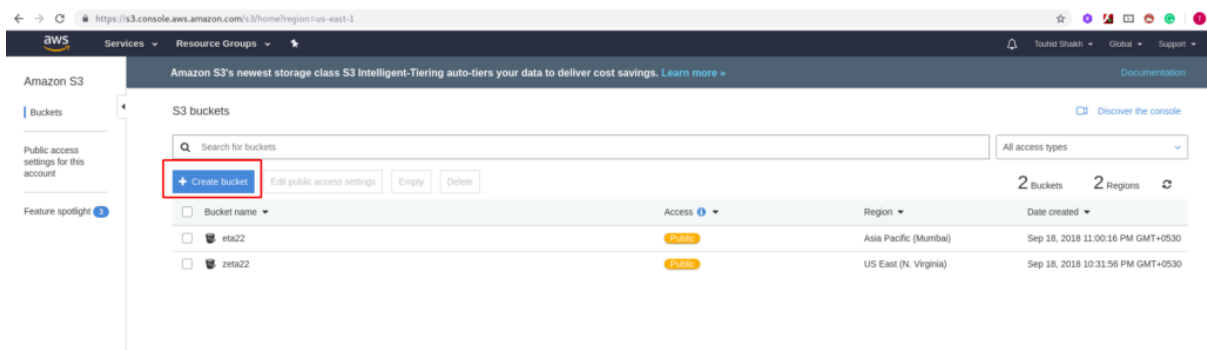
Now You Need a AWS Account to create a Bucket and claim this subdomain.

Let's start Takeover.

Login to <https://console.aws.amazon.com/>

and move to <https://s3.console.aws.amazon.com/s3/home>

Click Create Bucket.



Set Bucket name to source domain name (i.e., the domain you want to take over)

1 Name and region 2 Configure options 3 Set permissions 4 Review

Name and region

Bucket name ⓘ

playing.subdomain-takeover.tk

Region

US East (N. Virginia) ▾

Copy settings from an existing bucket

Select bucket (optional) 2 Buckets ▾

Create Cancel Next

Click Next multiple times to finish.

S3 buckets [Discover the console](#)

Search for buckets All access types ▾

[+ Create bucket](#) [Edit public access settings](#) [Empty](#) [Delete](#) 3 Buckets 2 Regions ↻

<input type="checkbox"/> Bucket name ▾	Access ⓘ ▾	Region ▾	Date created ▾
<input type="checkbox"/> eta22	Public	Asia Pacific (Mumbai)	Sep 18, 2018 11:00:16 PM GMT+0530
<input type="checkbox"/> playing.subdomain-takeover.tk	Public	US East (N. Virginia)	Jan 30, 2019 9:18:51 PM GMT+0530
<input type="checkbox"/> zeta22	Public	US East (N. Virginia)	Sep 18, 2018 10:31:56 PM GMT+0530

Open the created bucket.

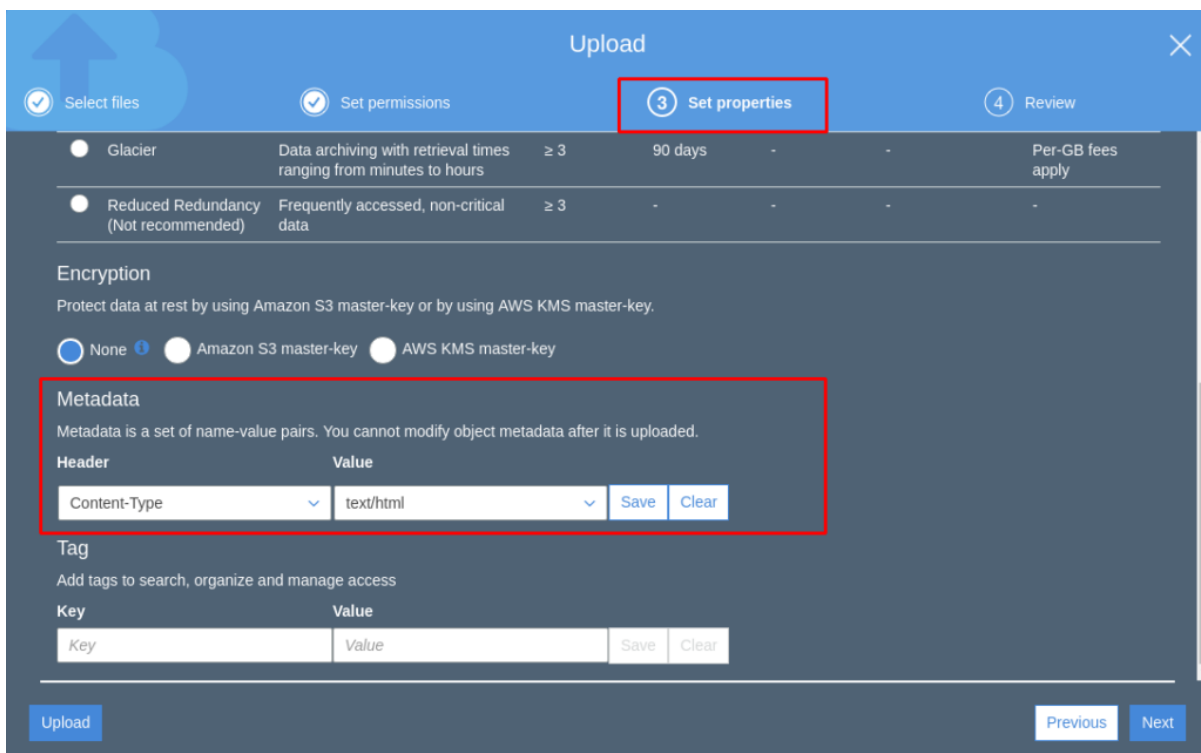
Click Upload

Select the file which will be used for PoC (HTML or TXT file). I recommend naming it differently than *index.html*; you can use *PoC* (without extension)

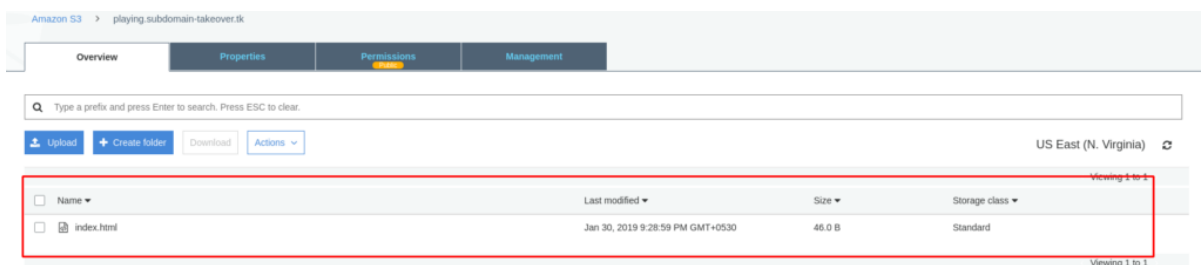
In *Set Permissions* tab select *Grant public read access to this object(s)*

In *Set Properties* tab *Go To Metadata*

In Header, select *Content-Type* and value should reflect the type of document which you going to upload. In Our Case HTML, choose *text/html*.



Click to Upload.



If Everything done properly. You'll Get the subdomain. Lets visit and verify successful takeover.

AWS S3 Takeover by TOuhid Shaikh

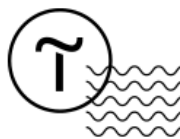
Congratulation !!

Tilda (Using A Record)

For Tilda, You need a premium account or at least a Feel Trail Account on <https://tilda.cc>
(We Recommend a Premium Account)

Lets Visit Vulnerable domain and check its available for takeover or not.

Vulnerable Subdomain: tilda.subdomain-takeover.tk



Domain has been assigned.

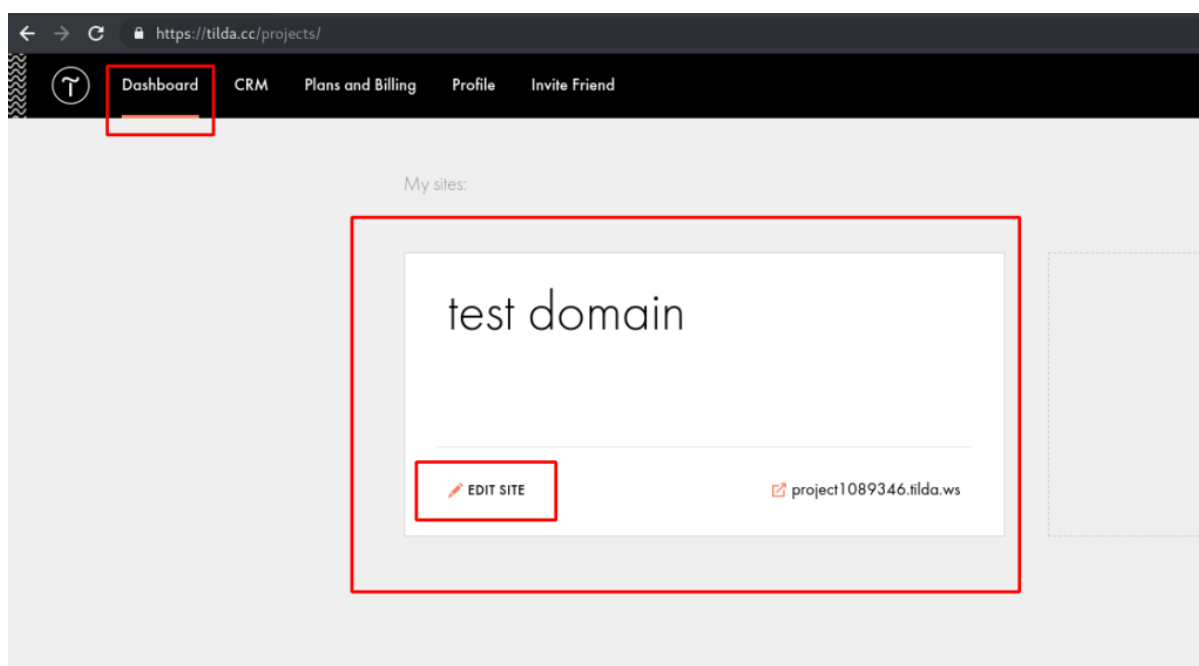
Please go to the site settings and put the domain name in the Domain tab.

We Got This Page ... Its Seems Vulnerable lets dig into and takeover this subdomain.

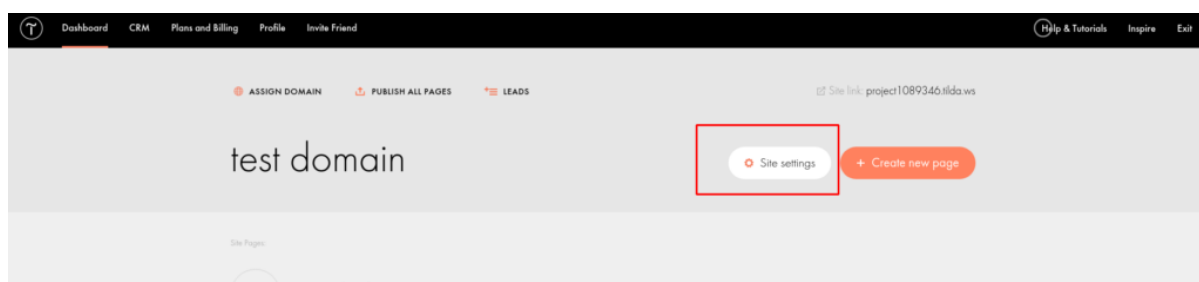
Let's Takeover. ☐

I am Assuming

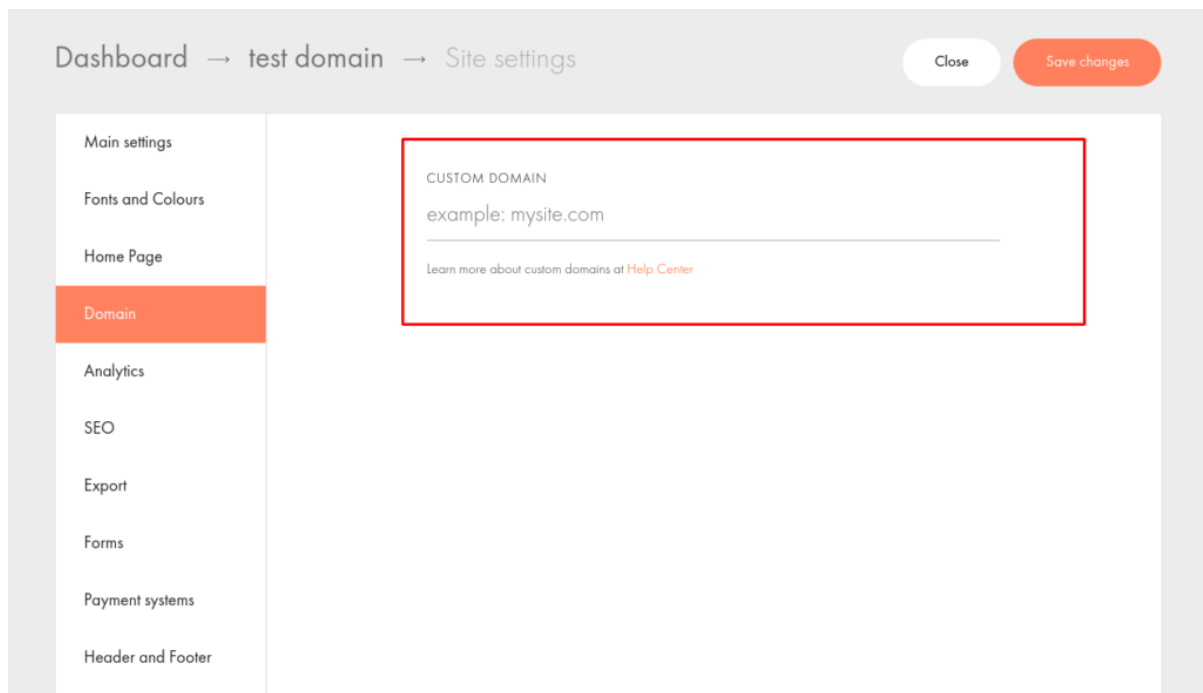
Create A Project and Click on **Edit Site.**



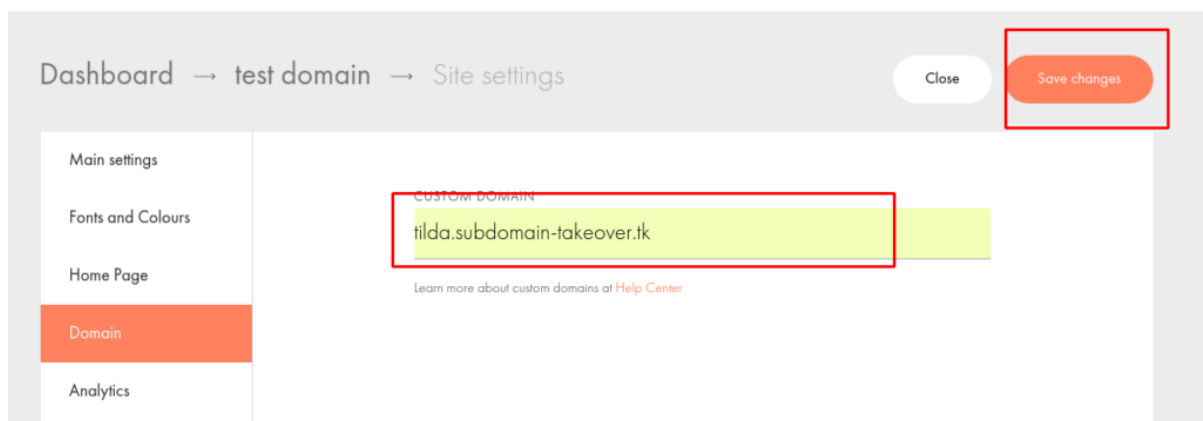
Go To **Site setting**



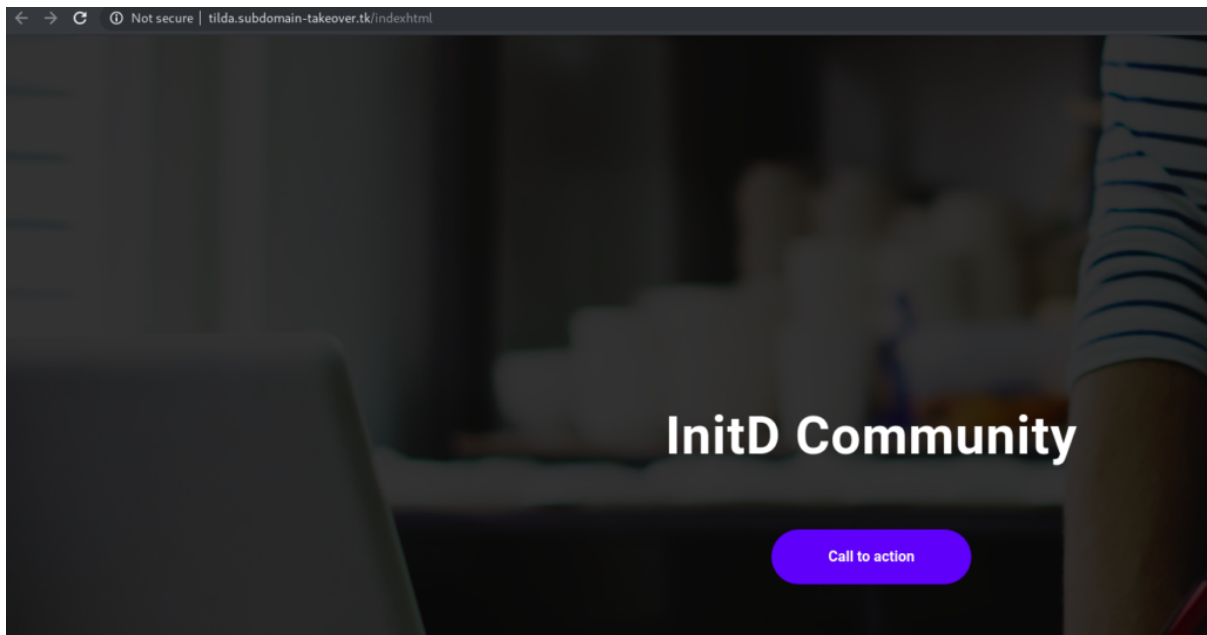
Click on Domain



Type You Subdomain Name a Click on **Save changes**.



If Everything is Perfect.... I Got The Subdomain.



I have Design some page in my project ☐

Congratulation.

Mitigation

Remove the unused Service's DNS Records from DNS Server.

Bibliography

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

Thanks For Reading.

Please Try or Subdomain Takeover LAB which is in BETA testing. If you Find any Difficulties please let us know.

END

