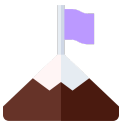


TakeOver

`security` `Enumeration` `Web` `Subdomains`

> Hello there,
>
> I am the CEO and one of the co-founders of **futurevera.thm**. In Futurevera, we believe that the future is in space. We do a lot of space research and write blogs about it. We used to help students with space questions, but we are rebuilding our support.
>
> Recently blackhat hackers approached us saying they could takeover and are asking us for a big ransom. Please help us to find what they can takeover.
>
> Our website is located at `https://futurevera.thm`
>
> Hint: Don't forget to add the 10.10.234.236 in /etc/hosts for futurevera.thm ;)

Enumeration

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn futurevera.thm
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-06 06:43 EDT
Nmap scan report for futurevera.thm (10.10.234.236)
Host is up (0.18s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
```

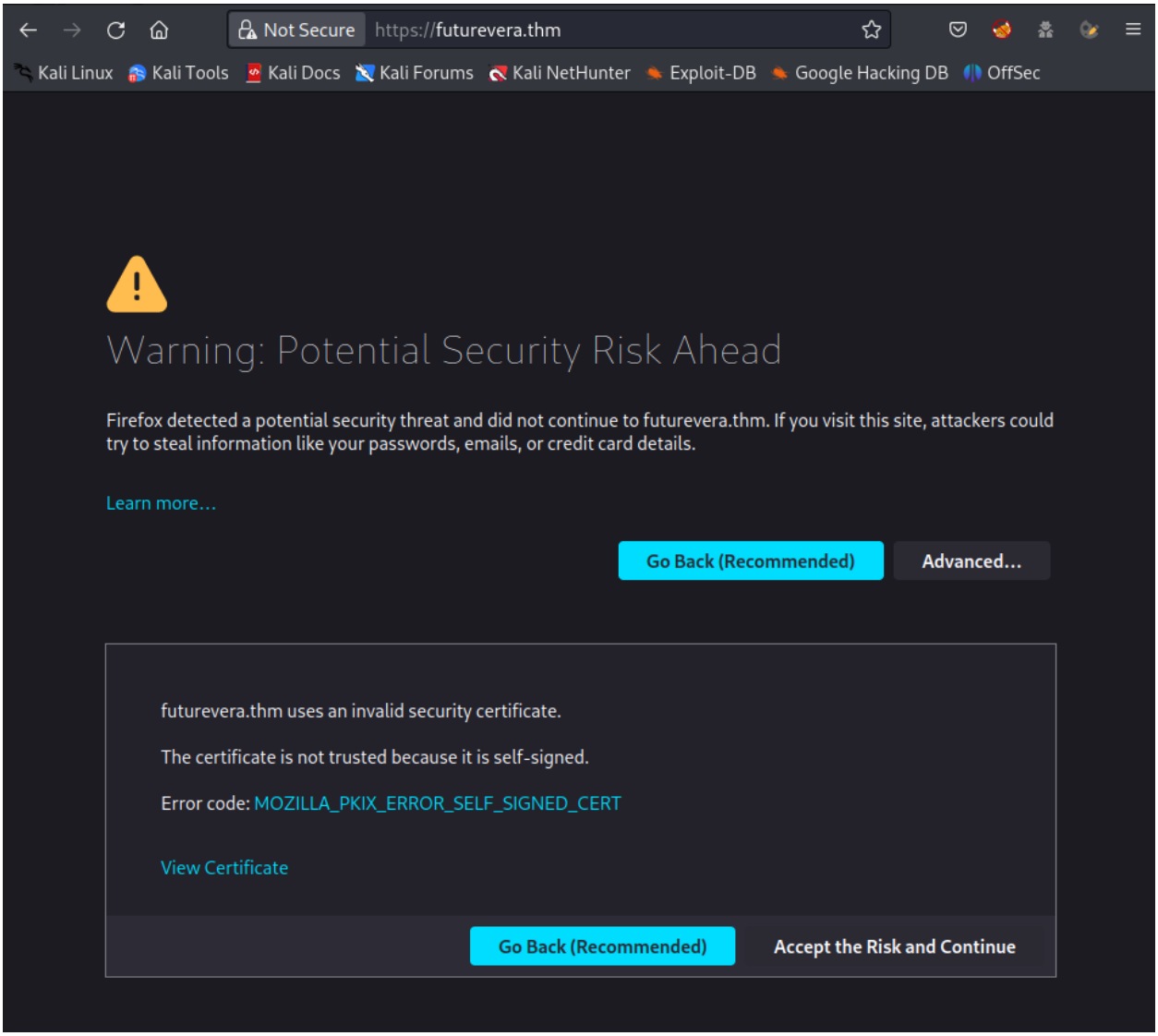
```
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 14.05 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -Pn -p 22,80,443 futurevera.thm
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-06 06:43 EDT
Nmap scan report for futurevera.thm (10.10.234.236)
Host is up (0.18s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 dd29a70c05691ff6260ad928cd40f020 (RSA)
|   256 cb2ea86d0366e970eb96e1f5ba25cb4e (ECDSA)
|_  256 50d34ba8a24d1d79e17dacbbff0b2413 (ED25519)
80/tcp  open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to https://futurevera.thm/
|_http-server-header: Apache/2.4.41 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.4.41
| ssl-cert: Subject: commonName=futurevera.thm/organizationName=Futurevera/stateOrProvince
Name=Oregon/countryName=US
| Not valid before: 2022-03-13T10:05:19
|_Not valid after:  2023-03-13T10:05:19
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
|_http-title: FutureVera
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera
 (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG
 FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%),
 Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   193.80 ms 10.8.0.1
2   193.89 ms futurevera.thm (10.10.234.236)

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.17 seconds
```

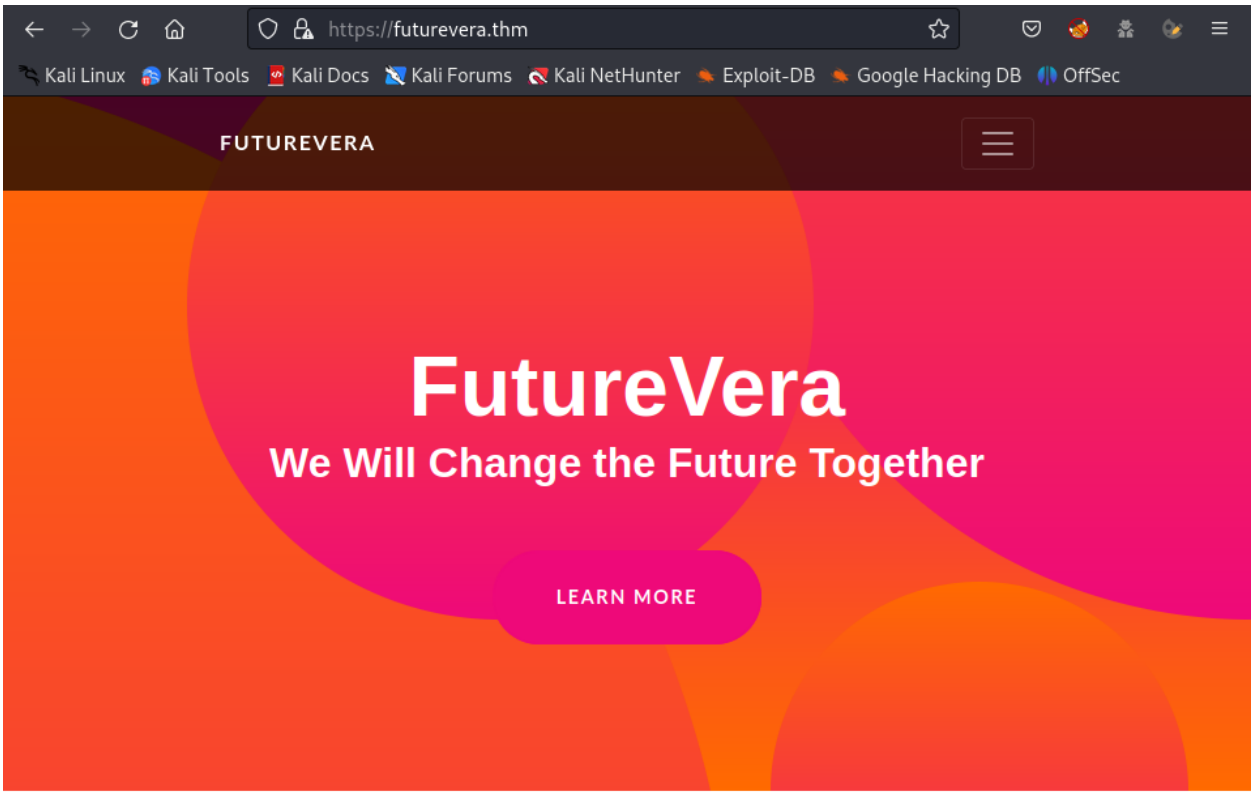
Add the `host` and `ip address` to the `/etc/hosts`

```
<TARGET_IP>   futurevera.thm
```

First of all, If you try to connect to the target `http` service → The web browser would block you with this error:



Therefore, to go through this one, you need to click on `Advanced...` and then `Accept the Risk and Continue`



The `Directories Scanning` in normal mode is not really helpful

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --no-error -t 40 -u https://futurev
era.thm -k
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://futurevera.thm
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/06 07:03:23 Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 319] [--> https://futurevera.thm/assets/]
/css                  (Status: 301) [Size: 316] [--> https://futurevera.thm/css/]
/js                   (Status: 301) [Size: 315] [--> https://futurevera.thm/js/]
Progress: 67387 / 220564 (30.55%)^C
[!] Keyboard interrupt detected, terminating.

===============================================================
2023/07/06 07:08:44 Finished
===============================================================
```

Foothold

Let's modify the command line to use the `dns` mode:

```
gobuster vhost -w Subdomain.txt -u https://futurevera.thm -k --append-domain
```

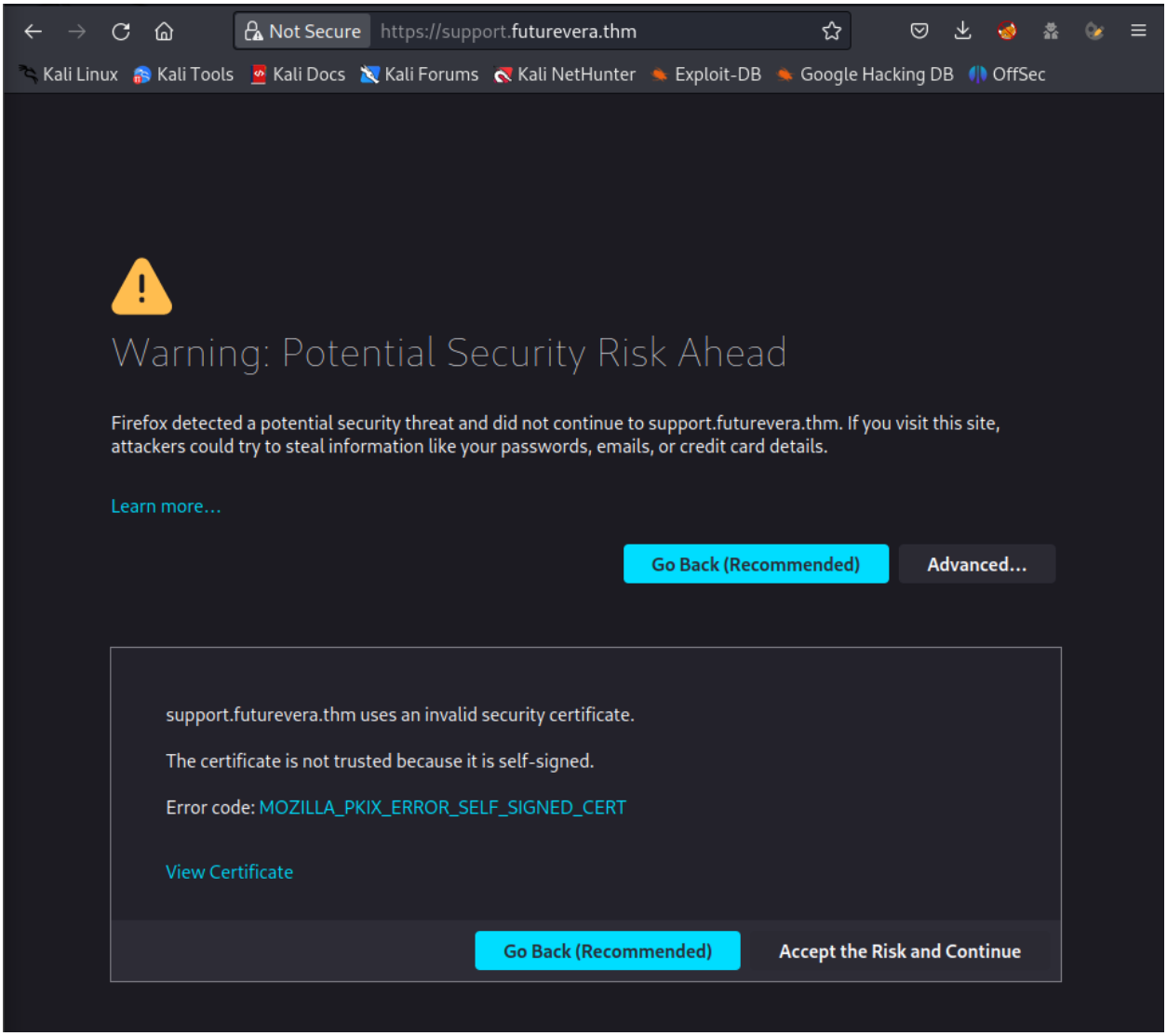
Here I used the wordlist of subdomain form this source

```
┌──(kali㉿kali)-[~/wordlists]
└─$ gobuster vhost -w Subdomain.txt -u https://futurevera.thm -k --append-domain
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             https://futurevera.thm
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        Subdomain.txt
[+] User Agent:      gobuster/3.5
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
2023/07/06 07:40:24 Starting gobuster in VHOST enumeration mode
===============================================================
Found: blog.futurevera.thm Status: 421 [Size: 408]
Found: support.futurevera.thm Status: 421 [Size: 411]
Found: *.blog.futurevera.thm Status: 400 [Size: 307]
Found: *.mail.futurevera.thm Status: 400 [Size: 307]
Found: m..futurevera.thm Status: 400 [Size: 307]
Found: *.red.futurevera.thm Status: 400 [Size: 307]
Found: *.dev.futurevera.thm Status: 400 [Size: 307]
```

After scanning subdomains, we found 2 domains → Add them into `/etc/hosts` file

```
<TARGET_IP>   futurevera.thm blog.futurevera.thm support.futurevera.thm
```

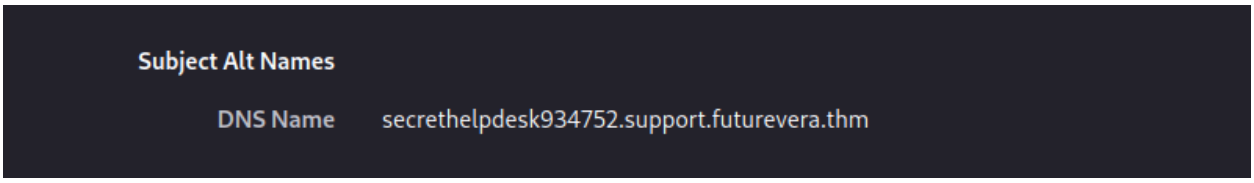
View both of them on the web browser would display the TLS errors



For this situation, click on `View Certificate` to look for other interested things

At the subdomain `blog` , I found nothing.

At the subdomain `support` , I found this



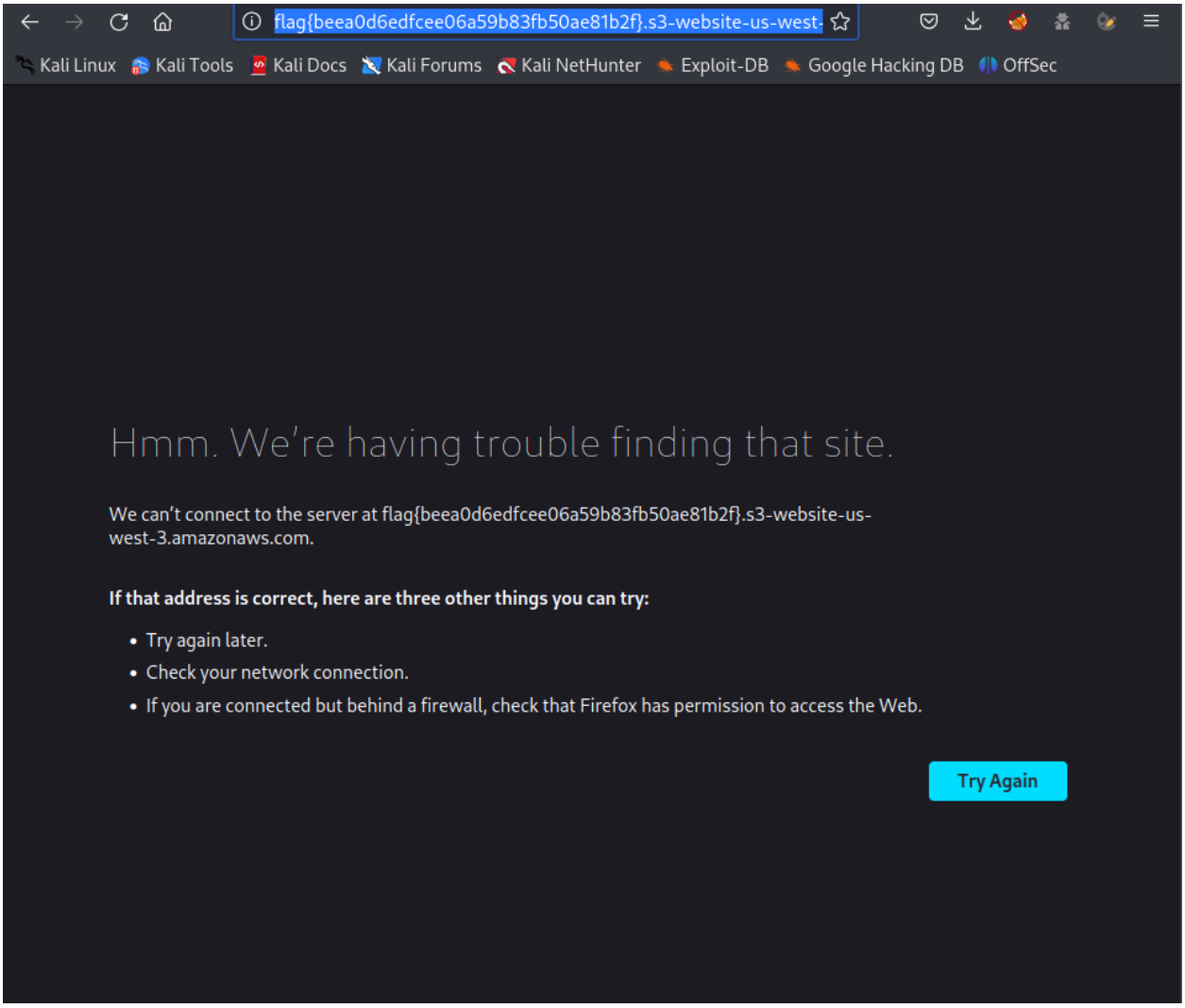

```
DNS Name    secrethelpdesk934752.support.futurevera.thm
```

Add the **DNS** above into the `/etc/hosts`

```
<TARGET_IP> futurevera.thm blog.futurevera.thm support.futurevera.thm secrethelpdesk93475
2.support.futurevera.thm
```

Then use web browser to brows to the target **dns** → It would redirect us to this **URL**

```
http://flag{beea0d6edfcee06a59b83fb50ae81b2f}.s3-website-us-west-3.amazonaws.com/
```


flag{beea0d6edfcee06a59b83fb50ae81b2f}.s3-website-us-west-
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Hmm. We're having trouble finding that site.
We can't connect to the server at flag{beea0d6edfcee06a59b83fb50ae81b2f}.s3-website-us-west-3.amazonaws.com.
If that address is correct, here are three other things you can try:
Try again later.
Check your network connection.
If you are connected but behind a firewall, check that Firefox has permission to access the Web.
Try Again