Virtual Host Basics

hackinghub.io

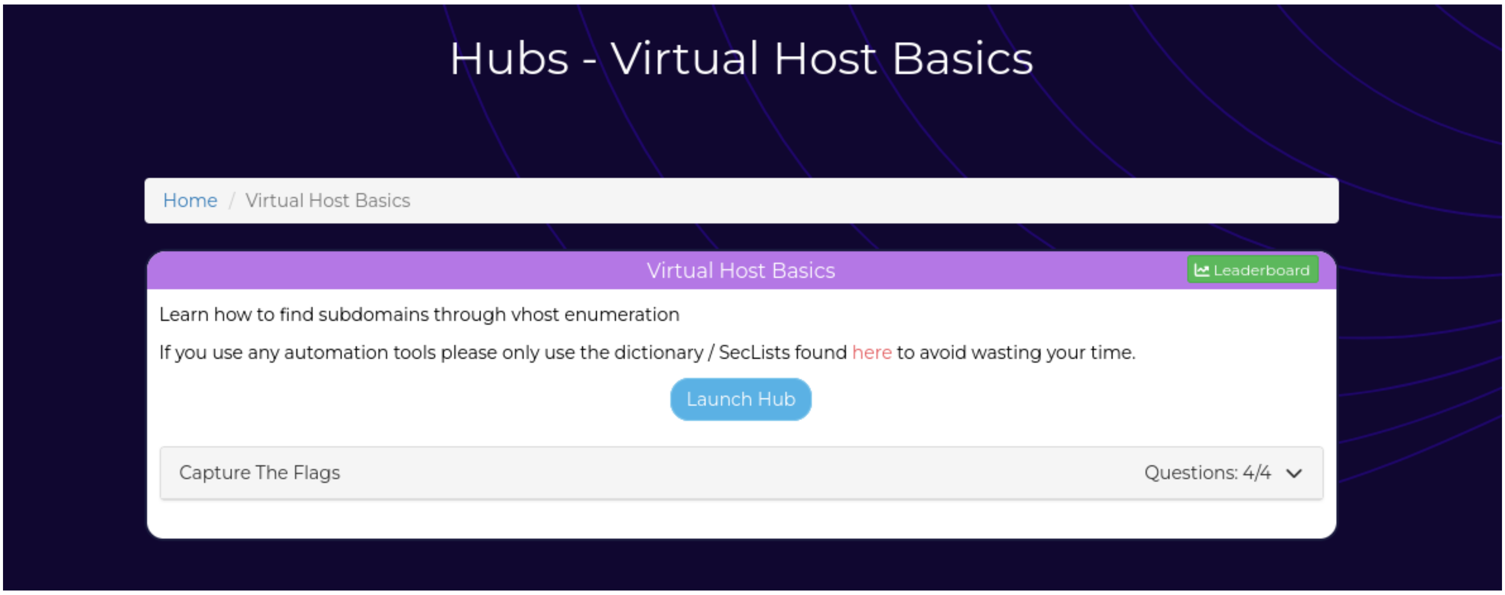
Hubs - Virtual Host Basics

Type: #WEB #blackbox
Difficulty: #easy
SOLVED by: #myself
TOOL USED: #gobuster #host #feroxbuster
TOPIC: #api #vhost

Writeup Date:2023-09-20
URL = *.nzkh4v4n.ctfio.com

---

the challenge description



Hubs - Virtual Host Basics

Home / Virtual Host Basics

Virtual Host Basics

Learn how to find subdomains through vhost enumeration

If you use any automation tools please only use the dictionary / SecLists found here to avoid wasting your time.

Capture The Flags

Questions: 4/4

```
$ rustscan -a www.nzkh4v4n.ctfio.com --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/musashi/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 206.189.31.119:22
Open 206.189.31.119:80
Open 206.189.31.119:9999
```

GOBUSTER VHOST VS DNS

VHOSTING

```
—$ gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u
http://nzkh4v4n.ctfio.com  --append-domain -t 100
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://nzkh4v4n.ctfio.com
[+] Method:          GET
[+] Threads:         100
[+] Wordlist:        /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.2.0-dev
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
2023/09/20 07:24:31 Starting gobuster in VHOST enumeration mode
===============================================================
Found: www.nzkh4v4n.ctfio.com Status: 200 [Size: 2275]
Found: app.nzkh4v4n.ctfio.com Status: 200 [Size: 625]
Found: marketing.nzkh4v4n.ctfio.com Status: 200 [Size: 1371]
Found: zeus.nzkh4v4n.ctfio.com Status: 200 [Size: 72]
Progress: 4989 / 4990 (99.98%)===============================================================
2023/09/20 07:24:35 Finished
===============================================================
```

DNS

```
$ gobuster dns -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -d nzkh4v4n.ctfio.com
-t 100
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     nzkh4v4n.ctfio.com
[+] Threads:    100
[+] Timeout:    1s
[+] Wordlist:   /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
===============================================================
2023/09/20 07:26:13 Starting gobuster in DNS enumeration mode
===============================================================
Found: app.nzkh4v4n.ctfio.com

Progress: 4989 / 4990 (99.98%)===============================================================
2023/09/20 07:27:04 Finished
===============================================================
```

doing

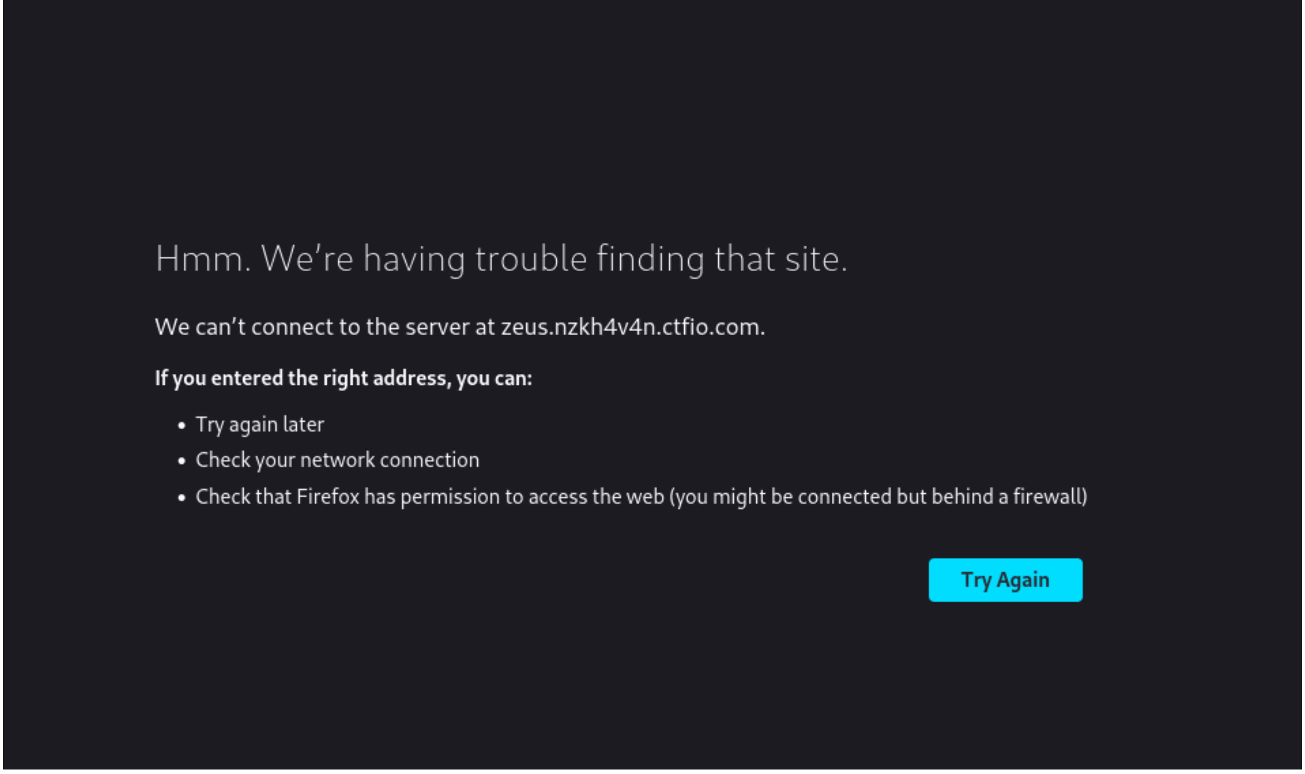
```
host nzkh4v4n.ctfio.com                                    nzkh4v4n.ctfio.com has address 206.189.31.119
```

we have IP address how to know if it's vhosting or not

we can use curl and supply HEADER HOST: localhost/subdomain
and see if they are different response here's example

```
curl 206.189.31.119 -H "HOST: zeus.nzkh4v4n.ctfio.com"
EvilCorp API Server
For customer data use {host}.zeus.nzkh4v4n.ctfio.com
```

NOTE: if u can't access those site through the browser
with error like this :



Hmm. We're having trouble finding that site.

We can't connect to the server at zeus.nzkh4v4n.ctfio.com.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be connected but behind a firewall)

then edit the /etc/hosts file
with ip and the domain name
for example
206.189.31.119 zeus.nzkh4v4n.ctfio.com marketing.nzkh4v4n.ctfio.com

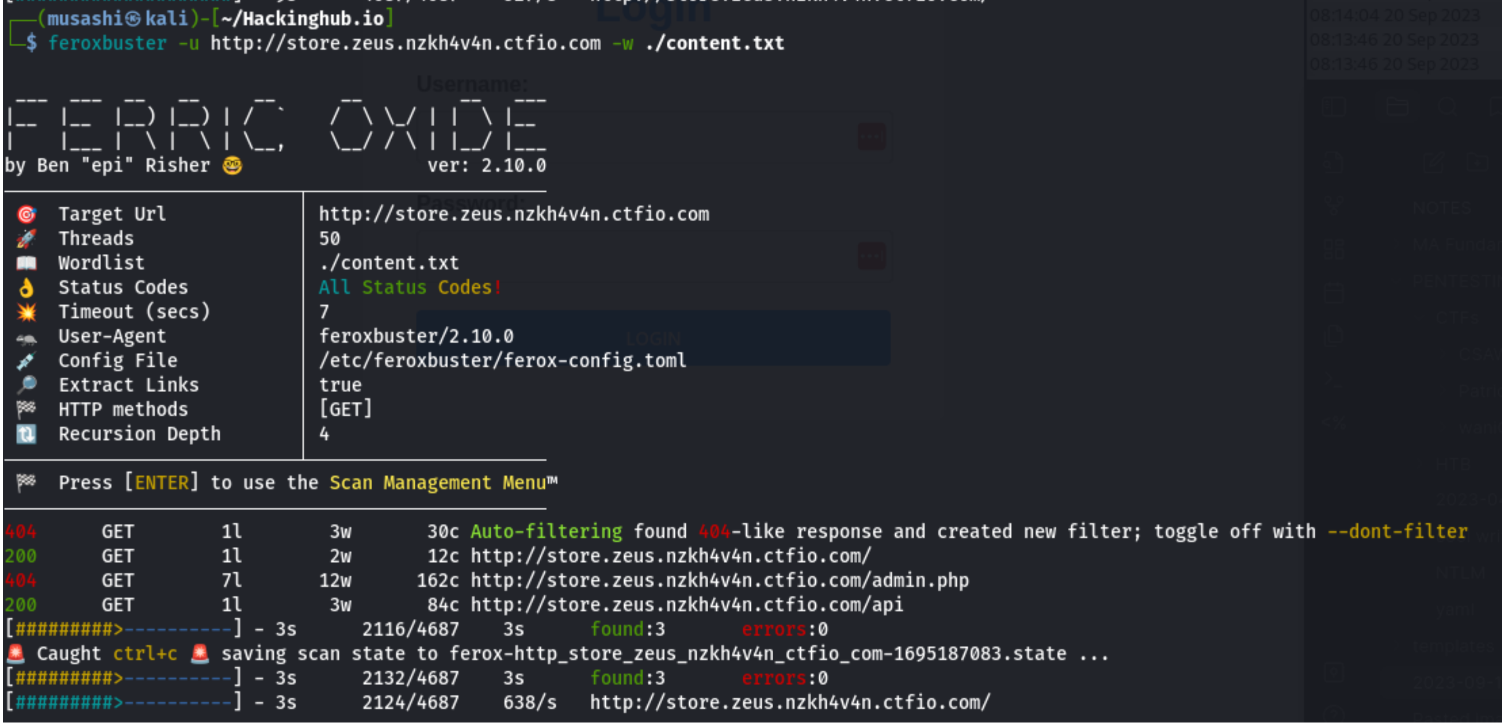
```
curl 206.189.31.119 -H "HOST: "marketing.nzkh4v4n.ctfio.com"
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>EvilCorp Marketing Intranet</title>
    <link rel="stylesheet" href="/style.css">
</head>
<body>
<header>
    <h1>Welcome to EvilCorp Marketing Intranet</h1>
    <nav>
        <ul>
            <li><a href="#home">Home</a></li>
            <li><a href="#news">News</a></li>
            <li><a href="#events">Events</a></li>
            <li><a href="#documents">Documents</a></li>
            <li><a href="#contact">Contact</a></li>
        </ul>
    </nav>
</header>
<main>
    <section id="home">
        <h2>Flags</h2>
        <p>FLAG_TWO{925494afdb0024a6add21a5b9ee9f3f0}</p>
    </section>
    <section id="news">
        <h2>News</h2>
        <!-- Your content for the news section goes here -->
    </section>
    <section id="events">
        <h2>Events</h2>
        <!-- Your content for the events section goes here -->
    </section>
    <section id="documents">
        <h2>Documents</h2>
        <!-- Your content for the documents section goes here -->
    </section>
    <section id="contact">
        <h2>Contact</h2>
        <!-- Your content for the contact section goes here -->
    </section>
</main>
<footer>
    <p>&copy; 2023 EvilCorp Marketing. All rights reserved.</p>
</footer>
</body>
</html>
```

```
curl 206.189.31.119 -H "HOST: localhost"
{"status":"OK","flag":"FLAG_ONE{95fe9f9e8bf849aec6a8de02fee14d57}"}
```

so we will continue on zeus.nzkh4v4n.ctfio.com domain because this message
For customer data use {host}.zeus.nzkh4v4n.ctfio.com is interesting

```
gobuster vhost -w ./subdomains.txt -u http://zeus.nzkh4v4n.ctfio.com  --append-domain -t 100
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://zeus.nzkh4v4n.ctfio.com
[+] Method:          GET
[+] Threads:         100
[+] Wordlist:        ./subdomains.txt
[+] User Agent:      gobuster/3.2.0-dev
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
2023/09/20 08:06:44 Starting gobuster in VHOST enumeration mode
===============================================================
Found: a.auth-ns.zeus.nzkh4v4n.ctfio.com Status: 200 [Size: 670]
Found: b.auth-ns.zeus.nzkh4v4n.ctfio.com Status: 200 [Size: 670]
Found: c.auth-ns.zeus.nzkh4v4n.ctfio.com Status: 200 [Size: 670]
Found: ipv6.teredo.zeus.nzkh4v4n.ctfio.com Status: 200 [Size: 670]
Found: store.zeus.nzkh4v4n.ctfio.com Status: 200 [Size: 12]
===============================================================
2023/09/20 08:06:46 Finished
===============================================================
```

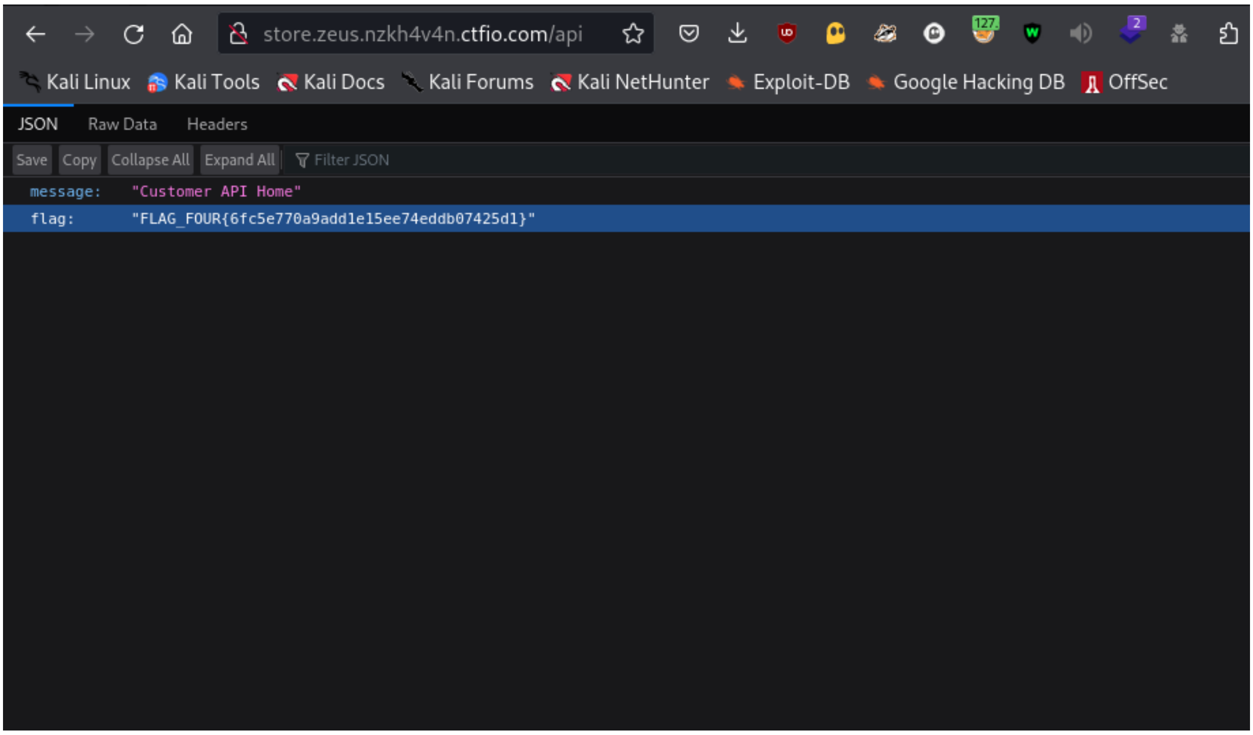
store.zeus.nzkh4v4n.ctfio.com is interesting one
and i checked all the above with curl they all returned nginx expect store
we now can continue with content discovery api endpoints



```
┌──(musashi㉿kali)-[~/Hackinghub.io]
└─$ feroxbuster -u http://store.zeus.nzkh4v4n.ctfio.com -w ./content.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.0
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://store.zeus.nzkh4v4n.ctfio.com
 🚀  Threads               │ 50
 📖  Wordlist              │ ./content.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.10.0
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎  Extract Links         │ true
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        1l        3w       30c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        1l        2w       12c http://store.zeus.nzkh4v4n.ctfio.com/
404      GET        7l       12w      162c http://store.zeus.nzkh4v4n.ctfio.com/admin.php
200      GET        1l        3w       84c http://store.zeus.nzkh4v4n.ctfio.com/api
[#########>----------] - 3s      2116/4687    3s      found:3       errors:0
🚨 Caught ctrl+c 🚨 saving scan state to ferox-http_store_zeus_nzkh4v4n_ctfio_com-1695187083.state ...
[#########>----------] - 3s      2132/4687    3s      found:3       errors:0
[#########>----------] - 3s      2124/4687    638/s   http://store.zeus.nzkh4v4n.ctfio.com/
```

and we have /api with 200 we visit it

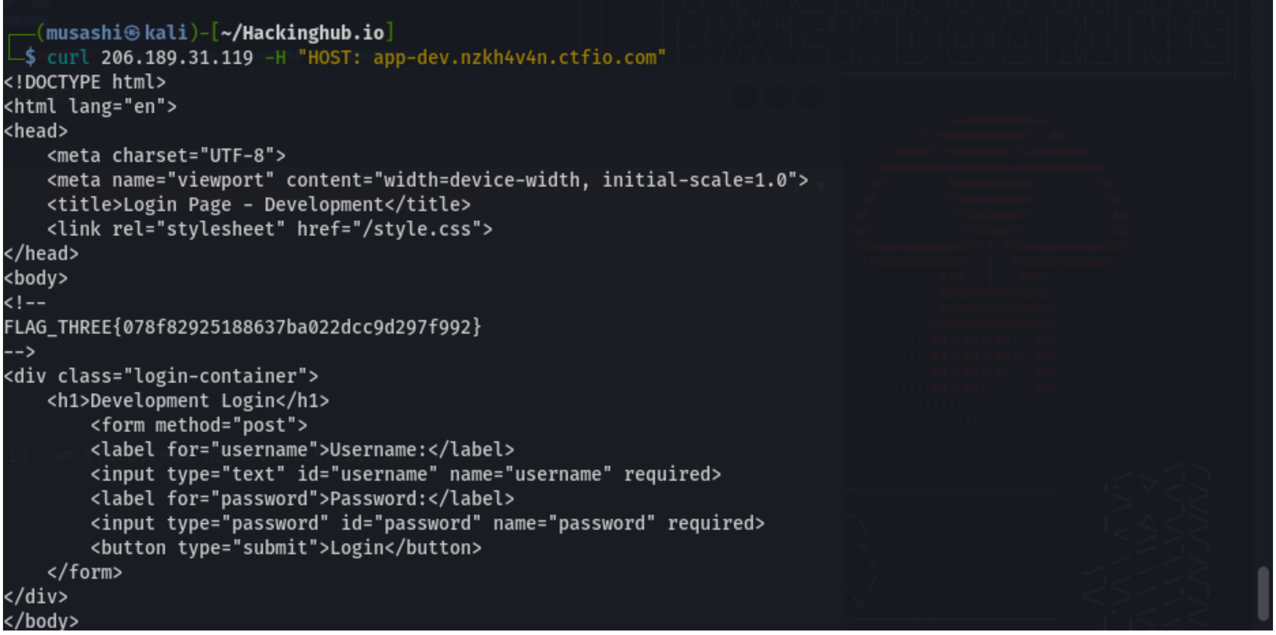


```
message:   "Customer API Home"
flag:      "FLAG_FOUR{6fc5e770a9add1e15ee74eddb07425d1}"
```

and boom we have flag number 4

flag three i tried to bruteforce app.nzkh4v4n.ctfio.com
with username and password list was provided by hackinghub.io but it would took me so long

i tried to enumerate directory/files didn't find anything except style.css
so i watched ben's video and i saw him using app-dev
not just app so i tested app-dev with curl

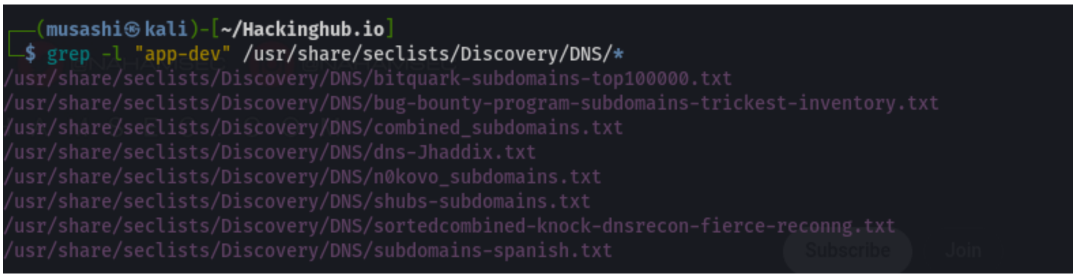


```
┌──(musashi㉿kali)-[~/Hackinghub.io]
└─$ curl 206.189.31.119 -H "HOST: app-dev.nzkh4v4n.ctfio.com"
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Login Page - Development</title>
    <link rel="stylesheet" href="/style.css">
</head>
<body>
<!--
FLAG_THREE{078f82925188637ba022dcc9d297f992}
-->
<div class="login-container">
    <h1>Development Login</h1>
        <form method="post">
        <label for="username">Username:</label>
        <input type="text" id="username" name="username" required>
        <label for="password">Password:</label>
        <input type="password" id="password" name="password" required>
        <button type="submit">Login</button>
    </form>
</div>
</body>
```

and we got the flag there.
done

lesson learned: don't rely on one subdomain list
because even i was provided with subdomain from the challenge it didn't contain the app-dev

so i wanted to know where is app-dev in my seclist/DNS/*



```
┌──(musashi㉿kali)-[~/Hackinghub.io]
└─$ grep -l "app-dev" /usr/share/seclists/Discovery/DNS/*
/usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
/usr/share/seclists/Discovery/DNS/bug-bounty-program-subdomains-trickest-inventory.txt
/usr/share/seclists/Discovery/DNS/combined_subdomains.txt
/usr/share/seclists/Discovery/DNS/dns-Jhaddix.txt
/usr/share/seclists/Discovery/DNS/n0kovo_subdomains.txt
/usr/share/seclists/Discovery/DNS/shubs-subdomains.txt
/usr/share/seclists/Discovery/DNS/sortedcombined-knock-dnsrecon-fierce-reconng.txt
/usr/share/seclists/Discovery/DNS/subdomains-spanish.txt
```

with grep -l i found out that my usual go to lists aka

- /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
- /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
- /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt

didn't contain app-dev. so if you stuck on any point do more enumeration
u will get your foothold eventually

> Character develops itself in the stream of life.
> — *Johann Wolfgang von Goethe*