Executive Summary

This report is intended to round up the information gathered and method utilized for enumeration of multiple machines.

In most machines there was sufficient information uncovered to, most likely, successfully exploit and *own* the machine. Having said this, due to time constraints and the defined scope for this report, only enumeration and possible exploitation vector identification, were covered.

Index

The following machines were explored:

Tools and Environment

- Nmap
- Amass
- OWASP ZAP
- gobuster
- dirsearch
- wfuzz
- Postman
- BurpSuite

Format Machine

Steps to Reproduce

1. Port Mapping

Begin by using `nmap` to map the machine open ports. When doing you will find that the machine exposes three ports.

```
└──╼ $nmap -T4 -A 10.10.11.213
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-29 21:40 WEST
Nmap scan report for 10.10.11.213
Host is up (0.098s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 c397ce837d255d5dedb545cdf20b054f (RSA)
|   256 b3aa30352b997d20feb6758840a517c1 (ECDSA)
|_  256 fab37d6e1abcd14b68edd6e8976727d7 (ED25519)
80/tcp   open  http    nginx 1.18.0
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0
3000/tcp open  http    nginx 1.18.0
|_http-title: Did not follow redirect to http://microblog.htb:3000/
|_http-server-header: nginx/1.18.0
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 37.29 seconds
```

2. Visit addresses

By running `curl` to the same address, we can see that a **domain** called *microblog* and a subdomain called *app* are expected.

Know this, you can add to these entries `/etc/hosts` since running `nslookup` results in no external server being able to resolve the hostname to this IP address.

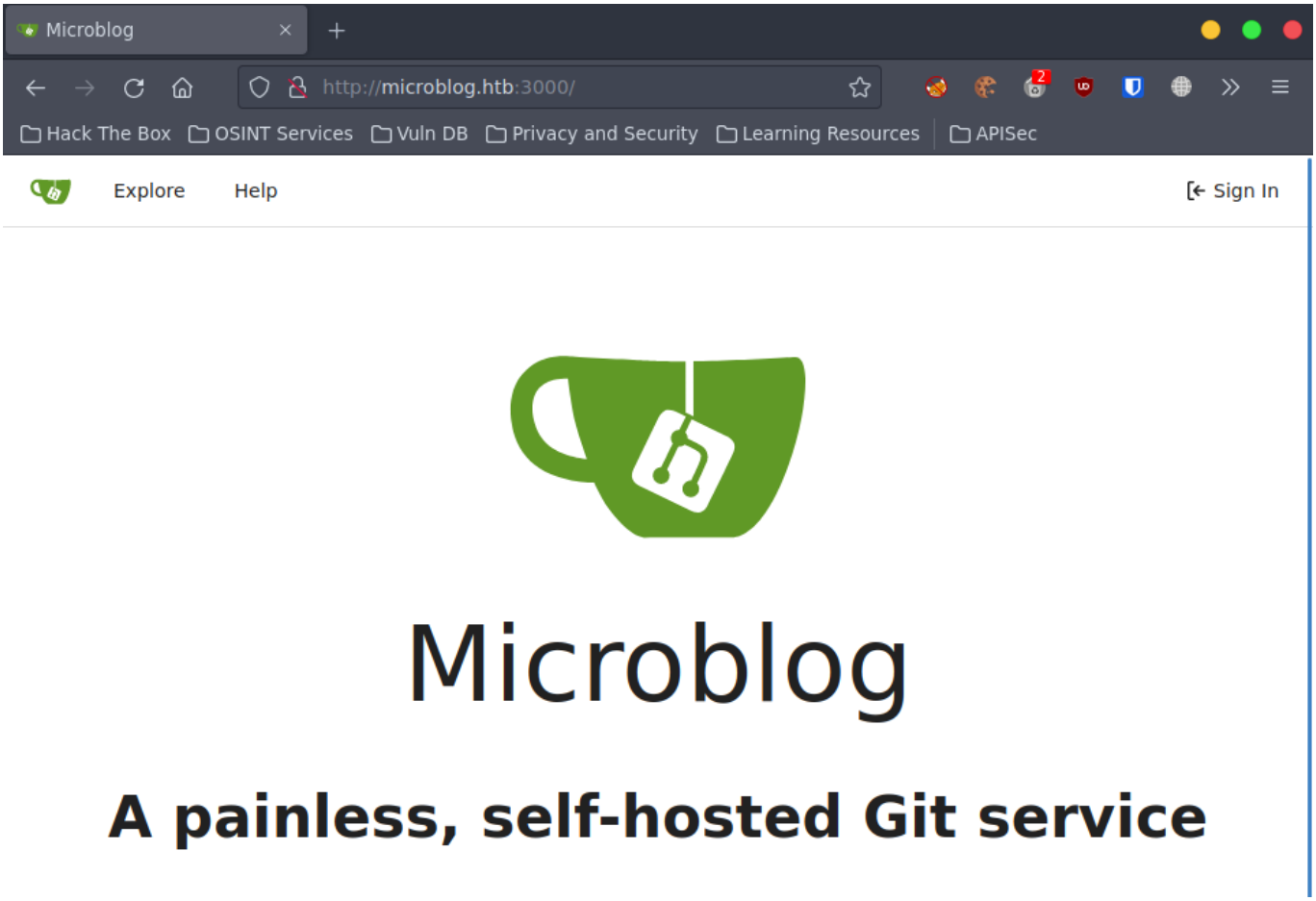
```
└──╼ $nslookup 10.10.11.213
** server can't find 213.11.10.10.in-addr.arpa: NXDOMAIN
```

```
 9 10.10.11.213 microblog.htb$
10 10.10.11.213 app.microblog.htb$
```

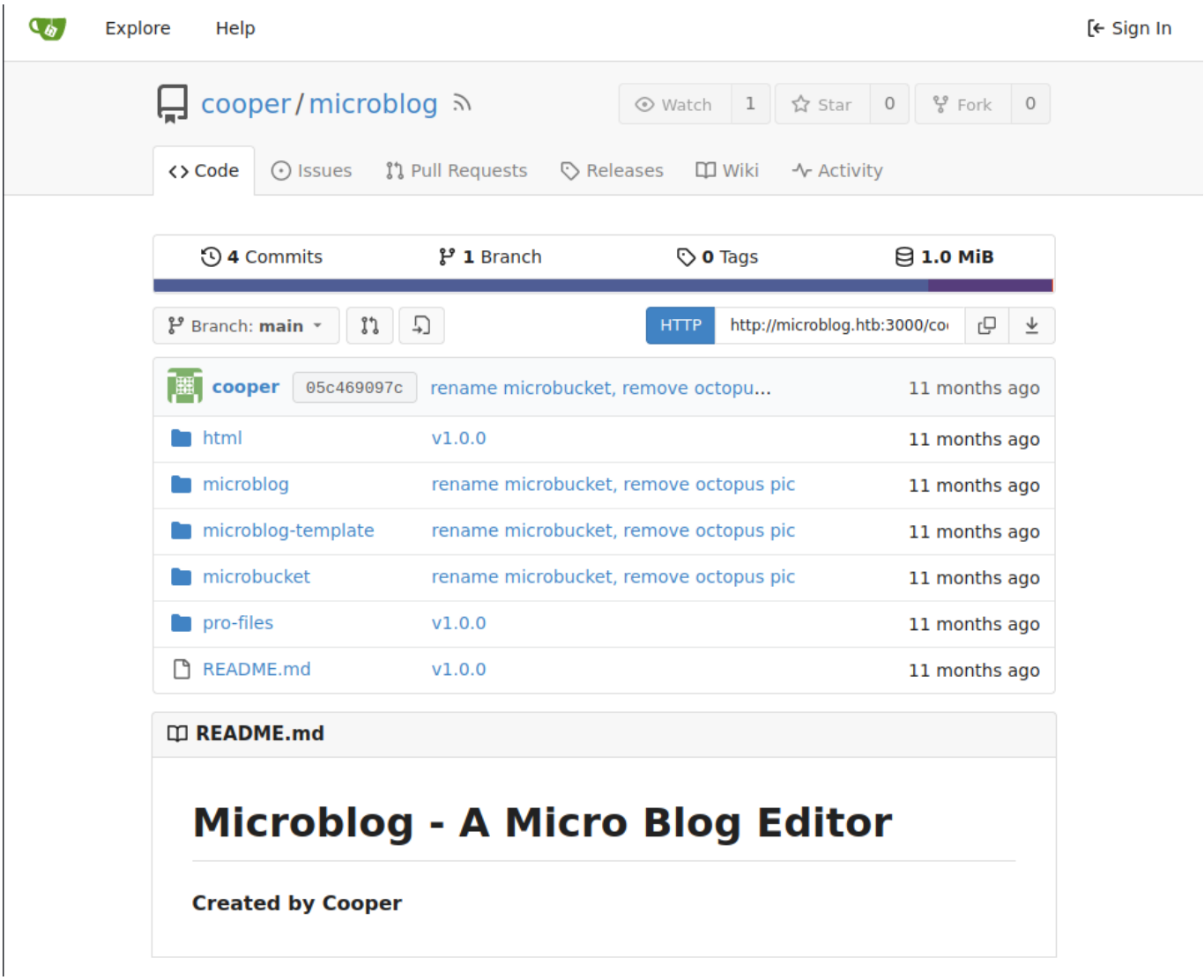
3. Visiting domains

3.1 http://microblog.htb:3000

Visiting this domain you discover an exposed self-hosted Git repository.

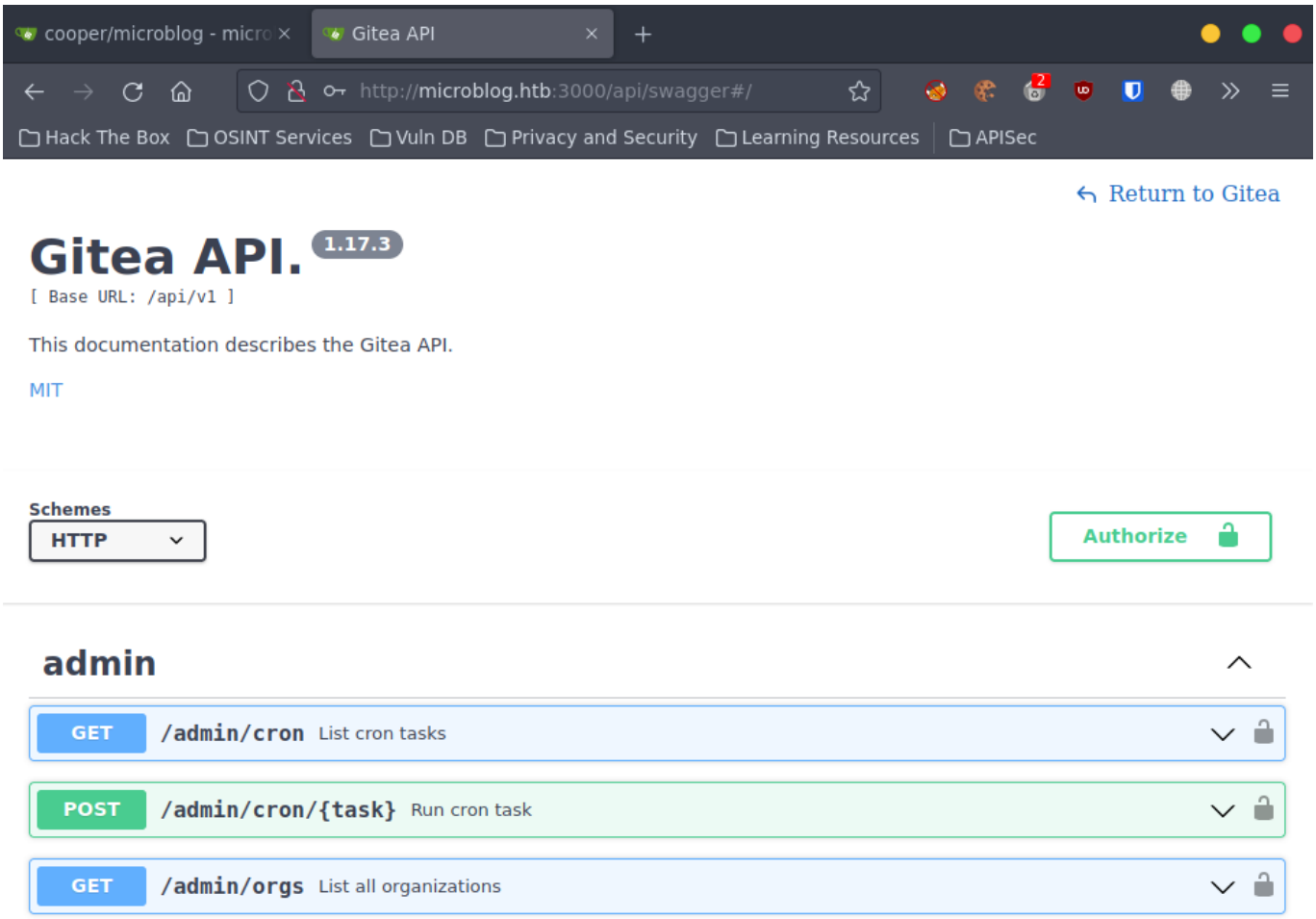


Exploring this you can discover a repository which appears to contain the code for an website.



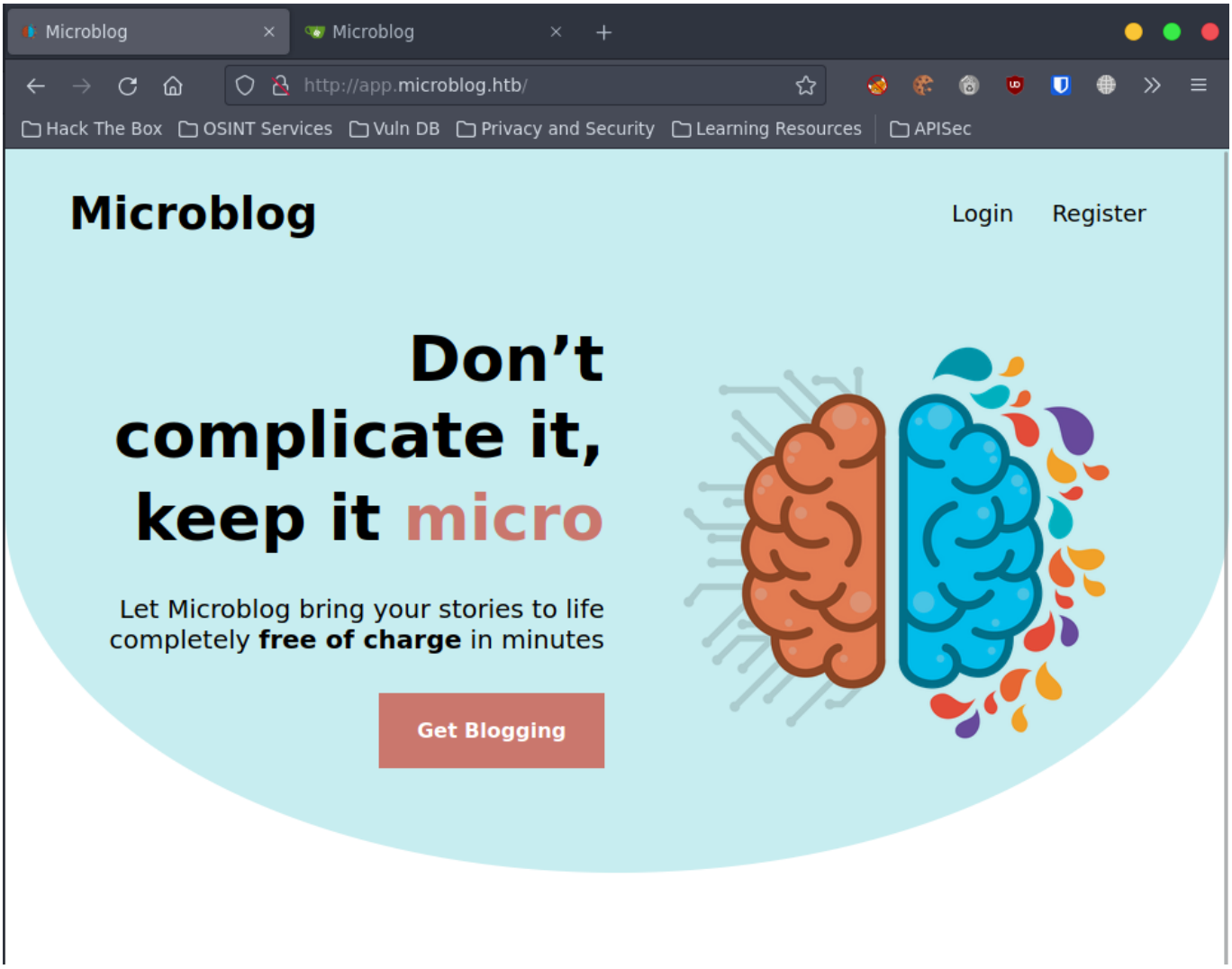
3.1.1 Swagger API

You will also find that an API is exposed, with the bonus of having the documentation available. This could be exploited in order to gain access of the repository service.



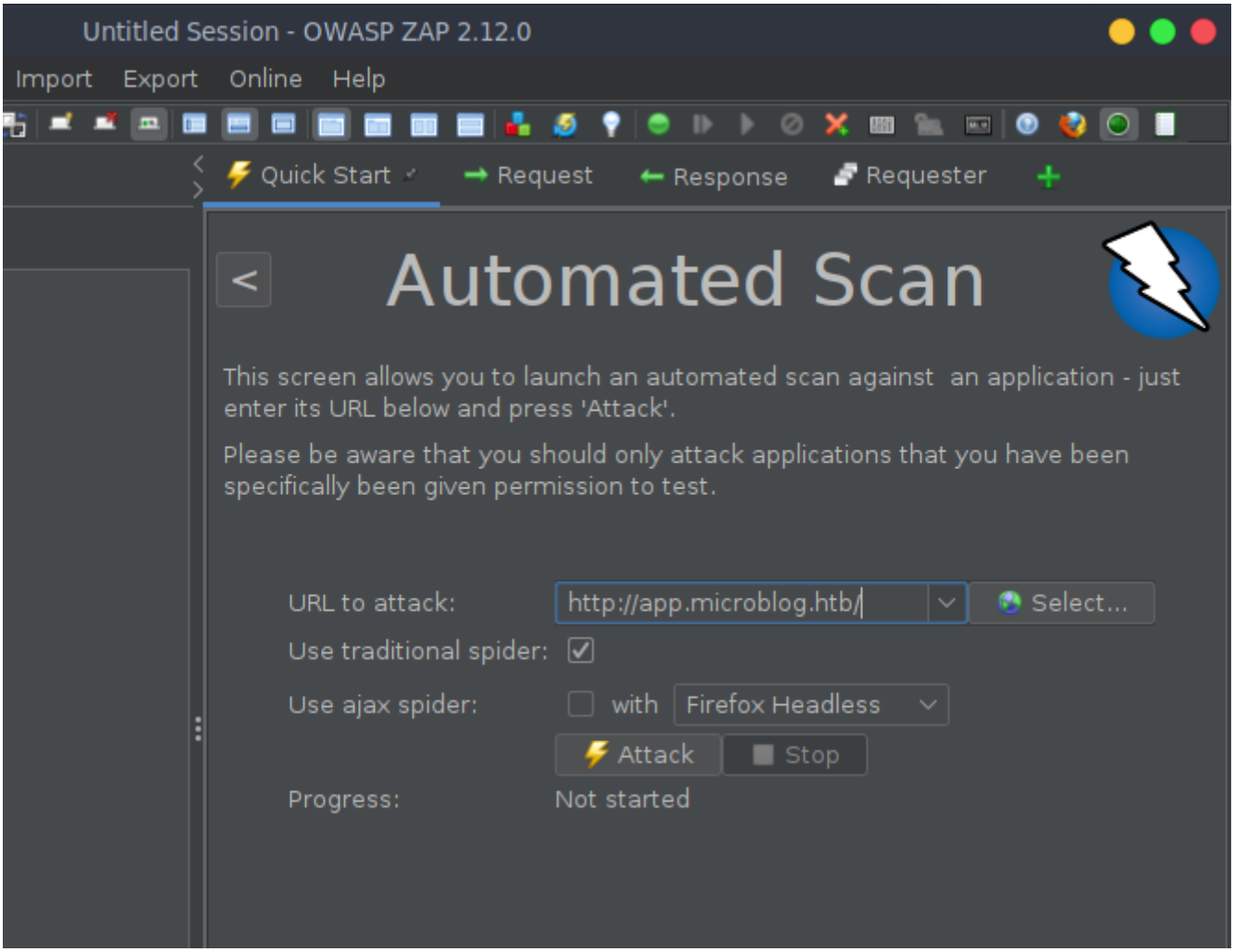
3.2 http://app.microblog.htb:80

You will now be able to visit the website that is described by the code in the previous repo.

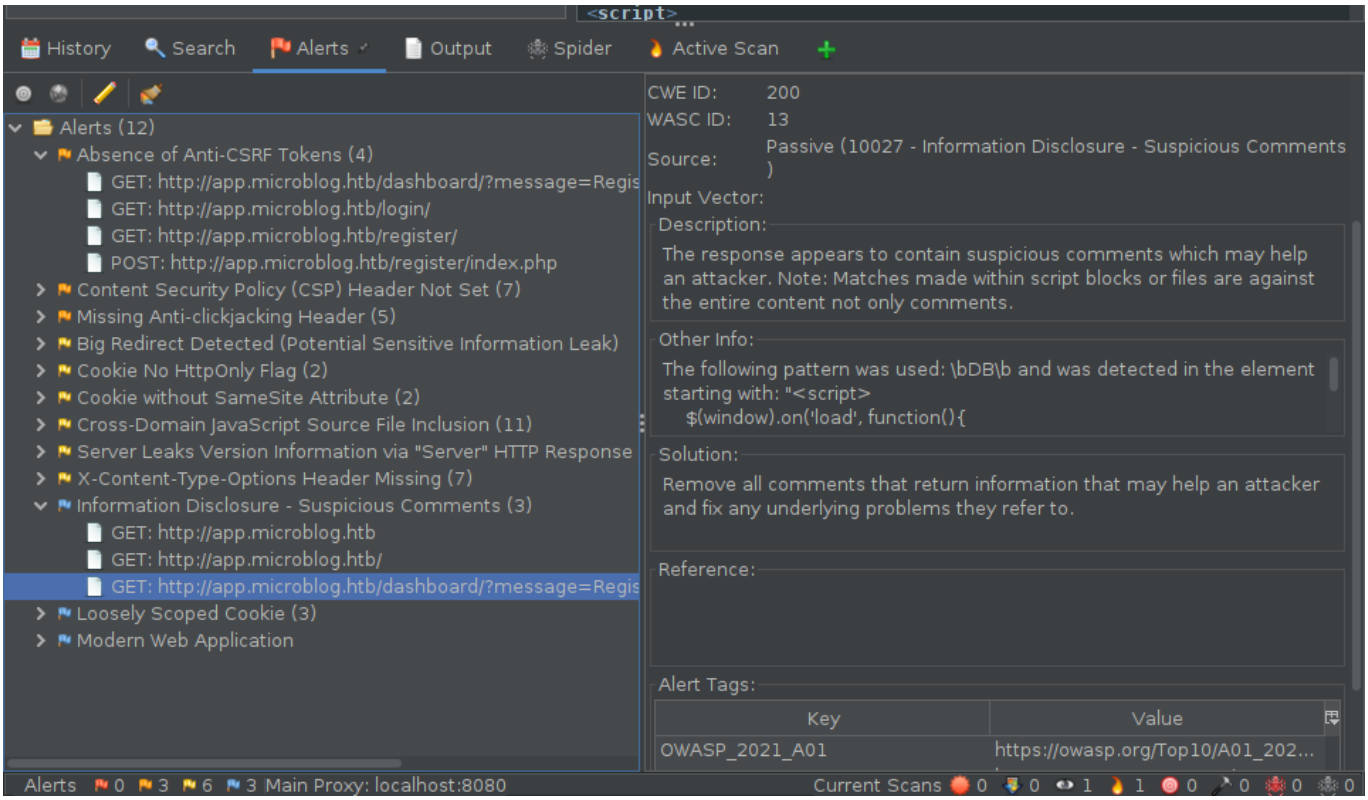


3.2.1 Spider

We will now run **OWASP ZAP** *spider* in order to easily explore the website.



As you can see, there are various alerts raised by ZAP that should be addressed.

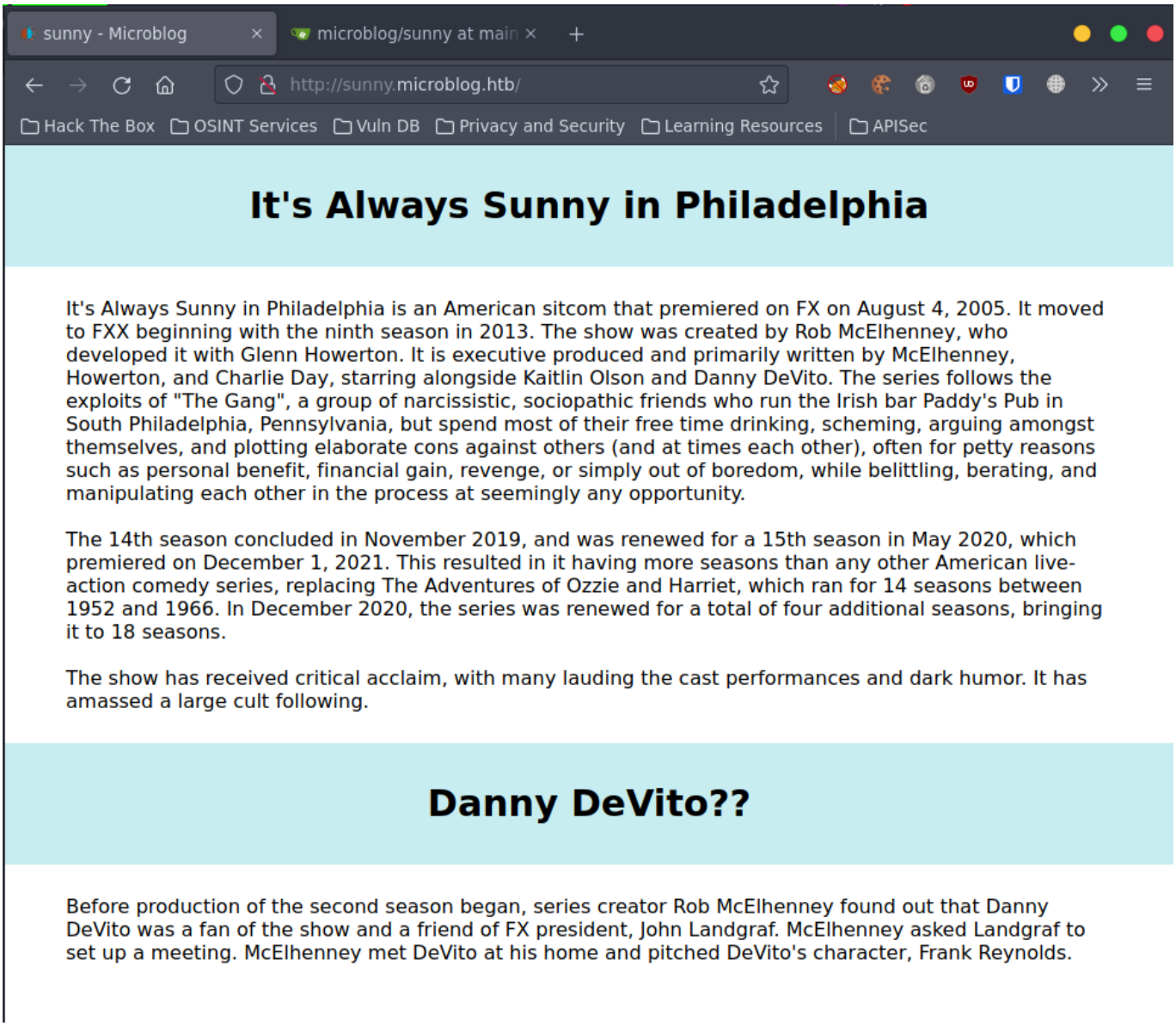


3.3 Fuzzing domains

Since in the repository it seemed has there would be more that just this simple pages, it might be a good idea to fuzz the domain in search for other subdomains and paths that may not be visible. Sure enough, another subdomain is found, *sunny*.

```
└──╼ $wfuzz -c -f sub-fighter -w /opt/SecLists/Discovery/DNS/subdomains-top1mill
ion-5000.txt -u "http://microblog.htb" -H "Host: FUZZ.microblog.htb" --hl 125 --
hc 404
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://microblog.htb/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000111:   200        83 L     306 W      3973 Ch     "app"
000001619:   200        42 L     434 W      3731 Ch     "sunny"
```

After adding this subdomain to the hosts DNS resolution file, this is what you can find.



Attack Surface Overview

For this machine the base attack surface should now be sufficient to carry out a deeper exploration. The most common approach would be to try and use BurpSuite and exploit the API by proxing the traffic and creating a test account and interact as much as possible with the application.

PC Machine

Steps to Reproduce

1. Port Mapping

Beginning with `nmap`, we can see that is at least does not respond to pings. But it show an open SSH port if run with the `-Pn` option.

```
└─$ nmap -Pn 10.10.11.214
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-30 23:04 WEST
Nmap scan report for 10.10.11.214
Host is up (0.10s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 15.63 seconds
```

However, as `nmap` reports, it only filtered 999 ports, it may be possible that there are other exposed ports in the entire gama of 65535 ports. To accommodate that we will specify the entire port range. This produces interesting results with another open port found.

```
└─$ nmap -Pn -r -p1-65535 10.10.11.214
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-30 23:14 WEST
Nmap scan report for 10.10.11.214
Host is up (0.072s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
50051/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 202.55 seconds
```

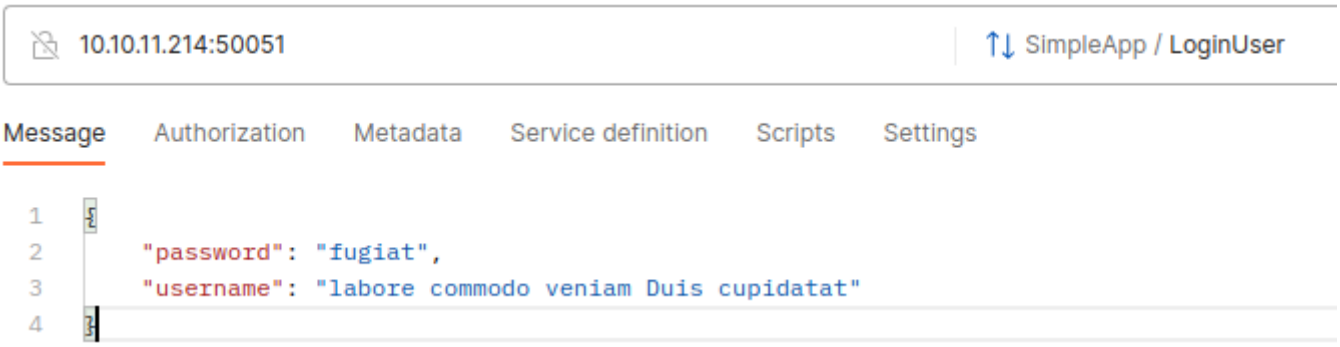
2. Testing port 50051

When trying to run ´curl´ to this address and port, the output is return as in some form of binary. This is common when the connection is trying by crossing different protocols, and you can expect that whatever the connection protocol is, dos not support http.

```
└─$ curl --http0.9 --output - 10.10.11.214:50051
????? ?┌─[test@parrot]─[~]
```

By researching online, one can discover that **gRPC** usually uses port 50051 and this types of default port specification should always be considered for testing, and so we did.

Using Postman, you can try to make requests to this address. Postman offers some simple template for request paths, and you can use the *LoginUse* with the example message also provided.



Attack Surface Overview

From were, you should be able to further exploit by trying to brute-force the login request and advance.

Jupiter Machine

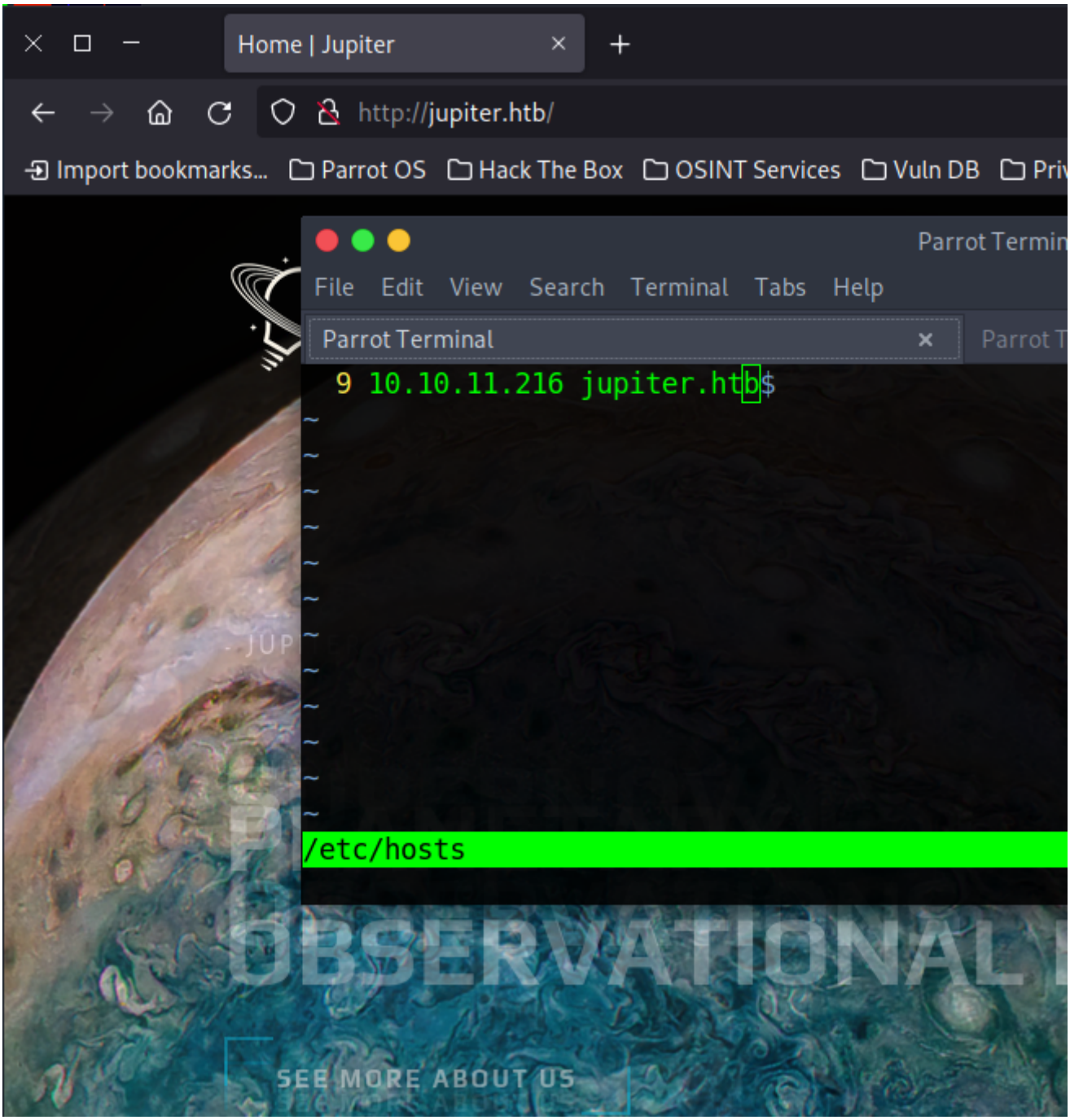
Steps to Reproduce

1. Port Mapping

Use nmap to search the complete range of ports.

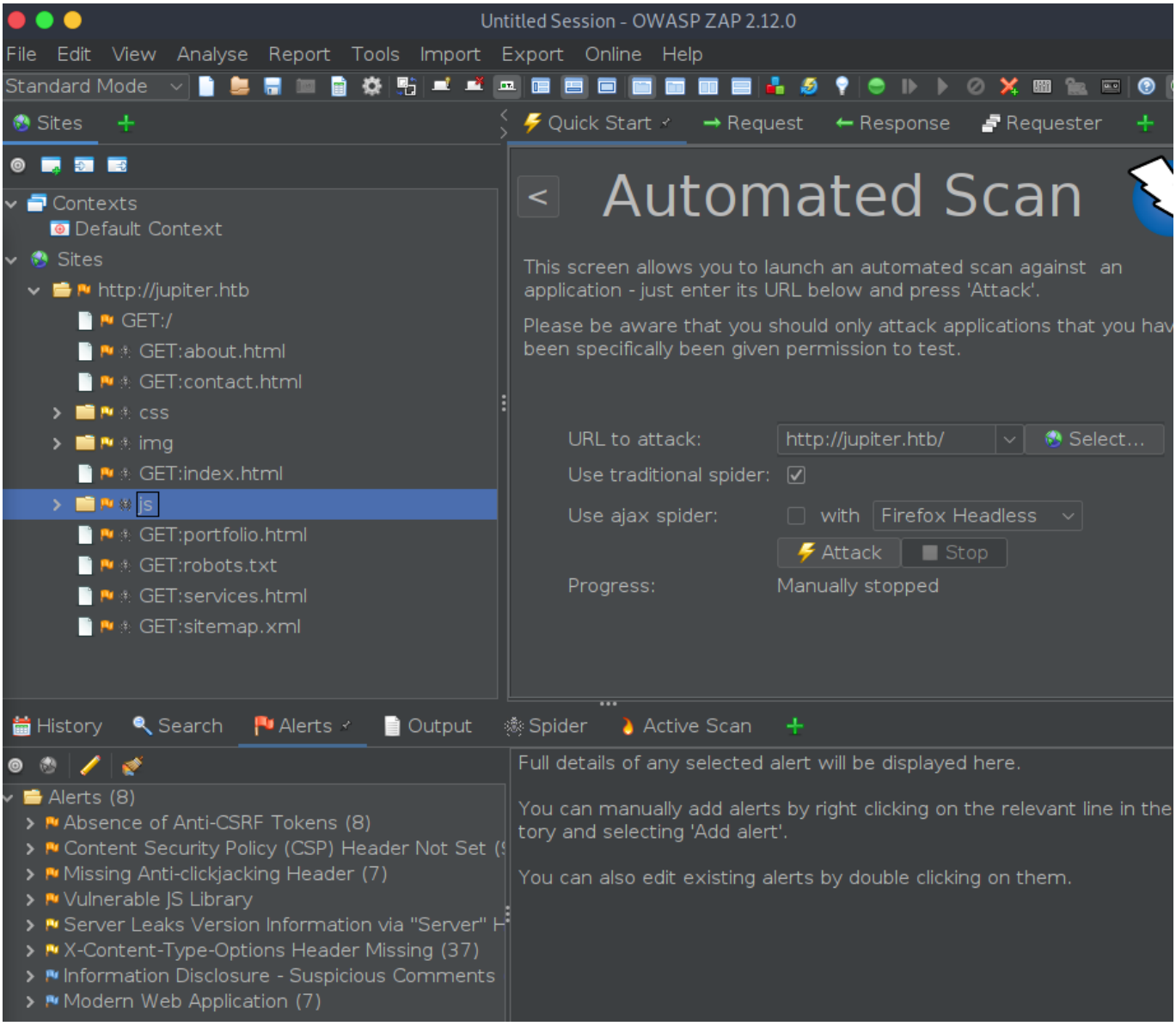
```
┌─[✗]─[test@parrot]─[~]
└──╼ $nmap --min-rate 4000  -p1-65535 10.10.11.216
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-01 11:13 WEST
Nmap scan report for 10.10.11.216
Host is up (0.075s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
5125/tcp  filtered unknown
36651/tcp filtered unknown
42610/tcp filtered unknown
46615/tcp filtered unknown
60044/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 21.23 seconds
```

Knowing a http service is available, you can visit the browse and add to `/etc/hosts` the domain that results from the address search


Home | Jupiter
http://jupiter.htb/
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Parrot Termin
File Edit View Search Terminal Tabs Help
Parrot Terminal
9 10.10.11.216 jupiter.htb$
/etc/hosts
OBSERVATIONAL
SEE MORE ABOUT US

2. Web Application mapping

Using ZAP map the website to quickly *spider* through it.



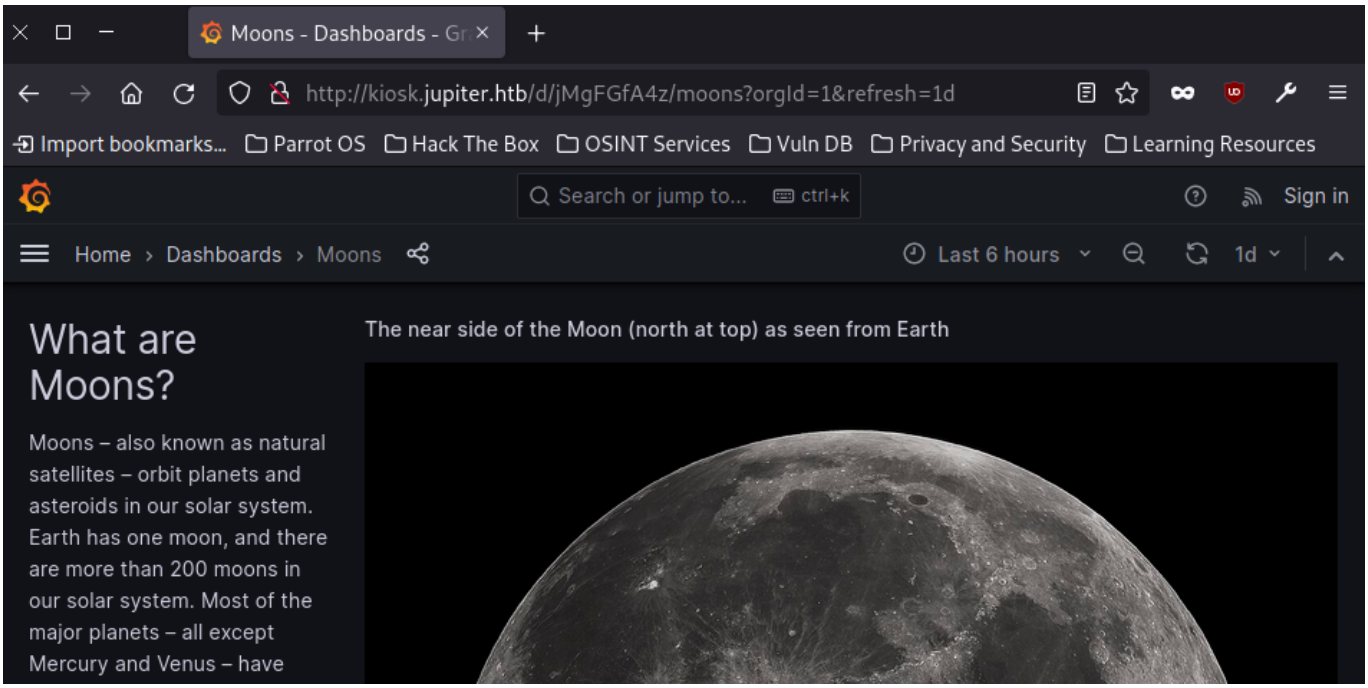
3. Fuzzing

Subdomain

One subdomain *kiosk* is found, add it to the `/etc/hosts` to view it in the browser.

```
┌─[test@parrot]─[~]
└──╼ $wfuzz -c -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u "http://
jupiter.htb" -H "Host: FUZZ.jupiter.htb" --sc 200
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl.
 Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://jupiter.htb/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000001955:   200        211 L    798 W      34390 Ch    "kiosk"
```

This will result in access to a Grafana dashboard.



Attack Surface Overview

From were, you should be able to further exploit by exploring the data visible in the Grafana dashboard.

Pilgrimage Machine

Steps to Reproduce

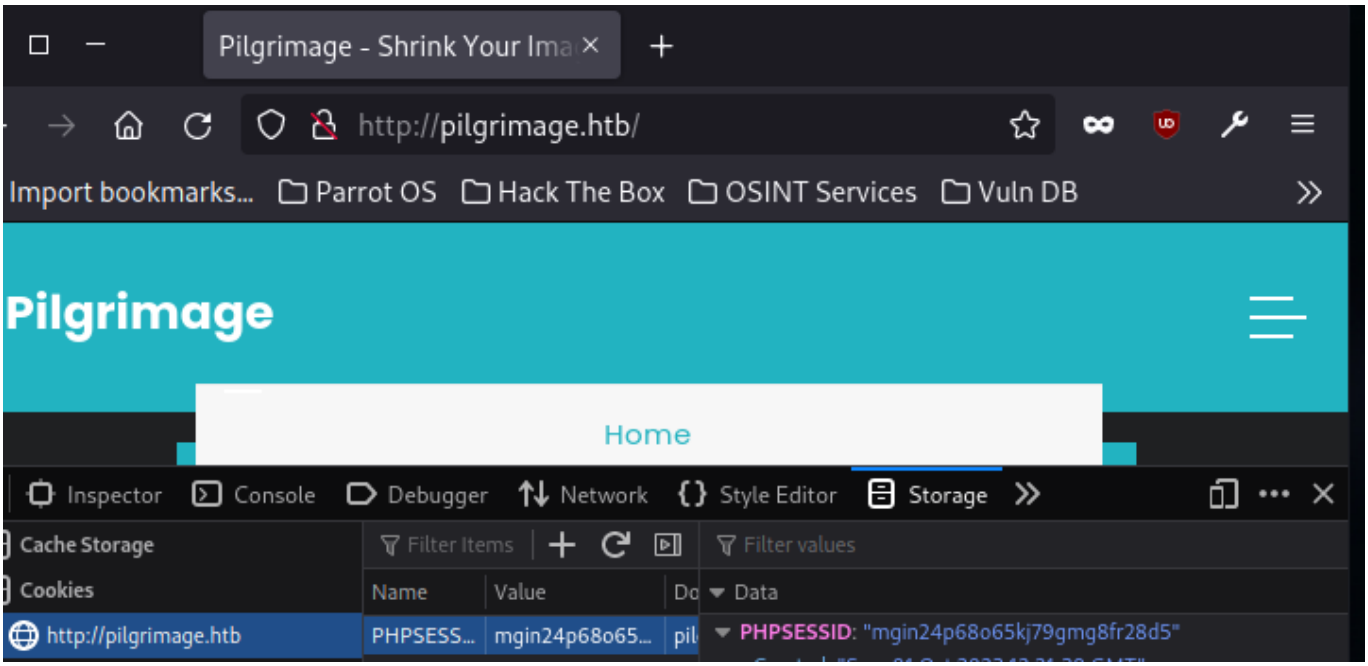
1. Port Mapping

```
┌─[test@parrot]─[~]
└──╼ $nmap -p1-65535 -T4 10.10.11.219
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-01 12:48 WEST
Nmap scan report for 10.10.11.219
Host is up (0.12s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 463.28 seconds
```

2. Website Exploration

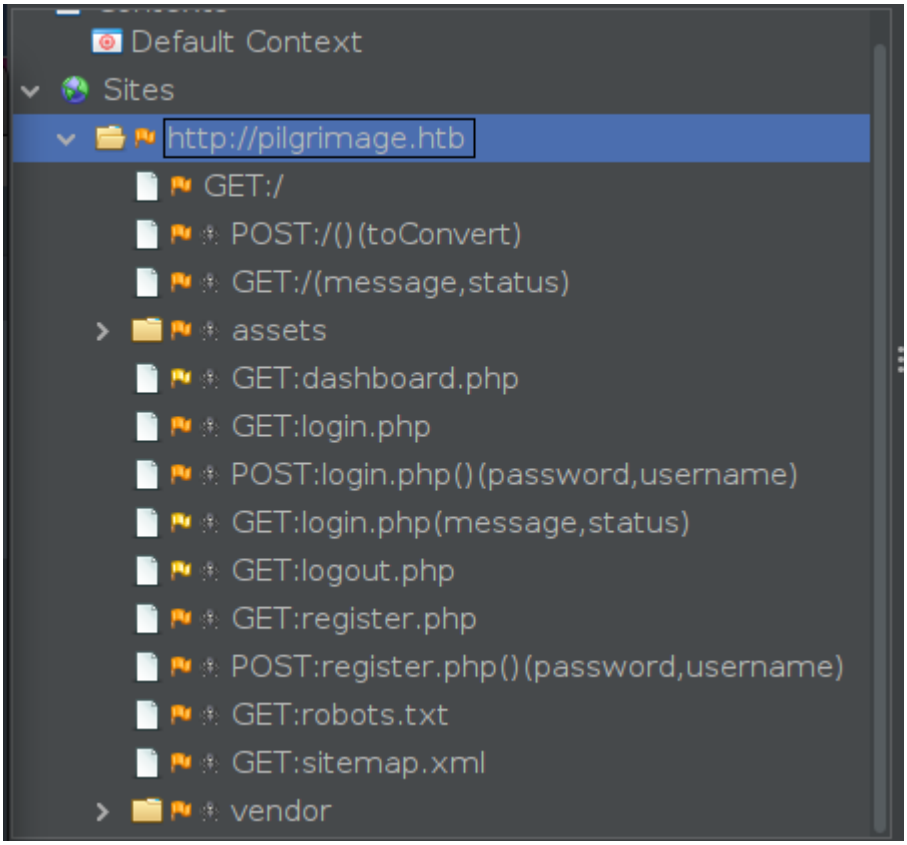
We can see that the site allow to upload a file. This always a risky operation so it should be further explored.

For now, from simply inspecting the resources, you can discover that this web application is built using PHP.



3. Site map

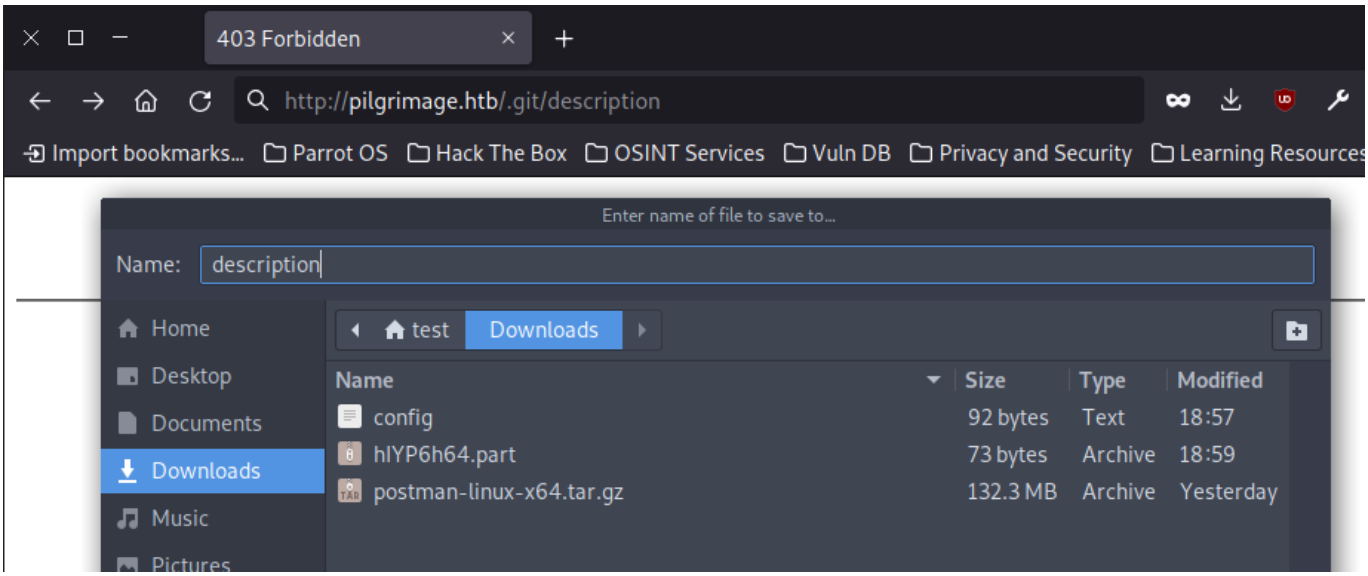
Create a website map with ZAP, and you will be able to get an approximation of the layout.



4. Exposed git

When `dirsearch` is run, a `.git` path is found, and when trying to access it, it is possible to retrieve its contents!

```
└─$dirsearch -u http://pilgrimage.htb

  _|. _ _  _  _  _ _|_    v0.4.3.post1
 (_|| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/test/reports/http_pilgrimage.htb/_23-10-01_19-55-33.txt

Target: http://pilgrimage.htb/

[19:55:33] Starting:
[19:55:36] 301 -  169B  - /.git  ->  http://pilgrimage.htb/.git/
[19:55:36] 403 -  555B  - /.git/branches/
[19:55:36] 200 -    2KB - /.git/COMMIT_EDITMSG
[19:55:36] 403 -  555B  - /.git/
[19:55:36] 200 -   92B  - /.git/config
[19:55:36] 200 -   23B  - /.git/HEAD
[19:55:36] 200 -   73B  - /.git/description
```



Attack Surface Overview

For here you should be able to find critical information about the repository, maybe even credentials.

Further exploring the paths, mainly those most common in PHP would also be relevant.

SAU Machine

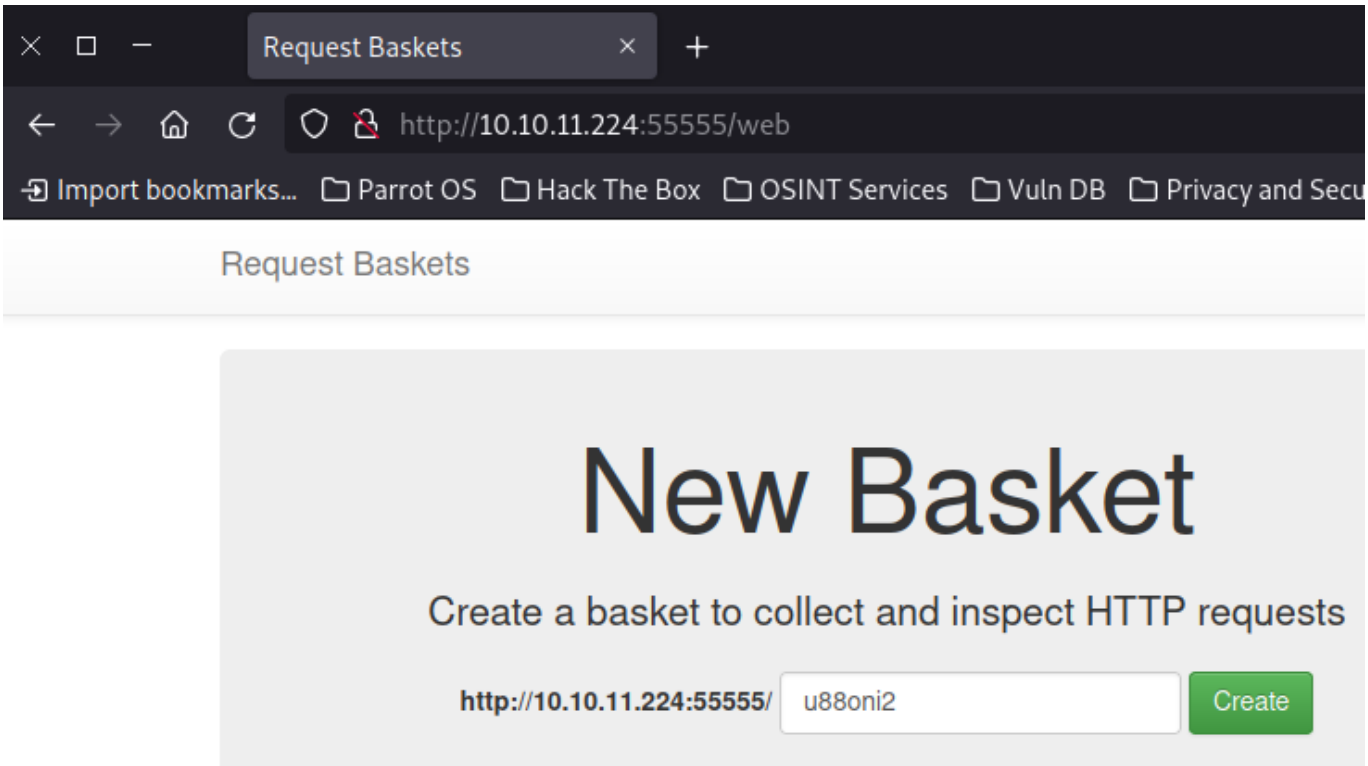
Steps to Reproduce

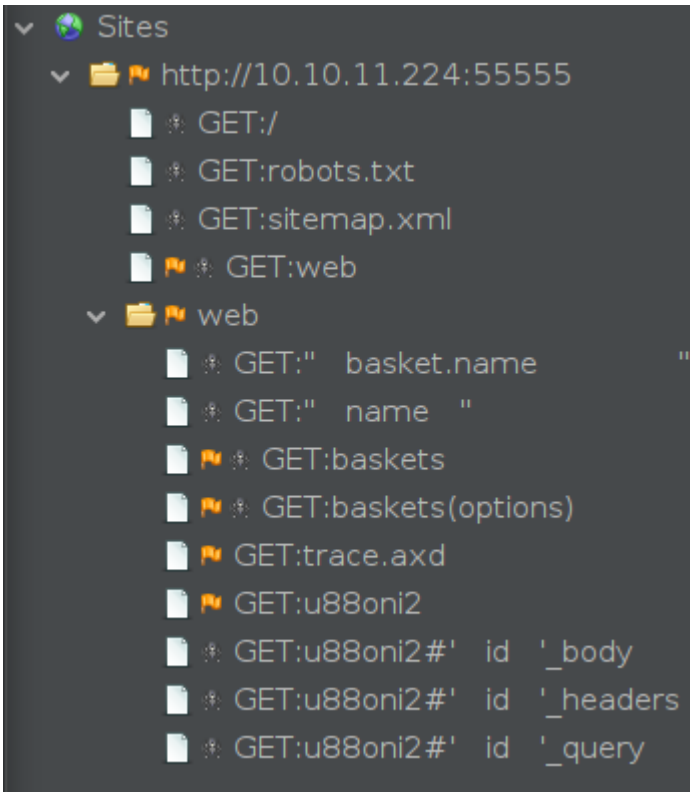
1. Port Mapping

```
┌─[test@parrot]─[~]
└──╼ $nmap -p1-65535 --min-rate 4000 10.10.11.224
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-01 20:31 WEST
Warning: 10.10.11.224 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.224
Host is up (0.078s latency).
Not shown: 64335 closed tcp ports (conn-refused), 1198 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
55555/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 37.94 seconds
```

```
└──╼ $curl 10.10.11.224:55555
<a href="/web">Found</a>.
```

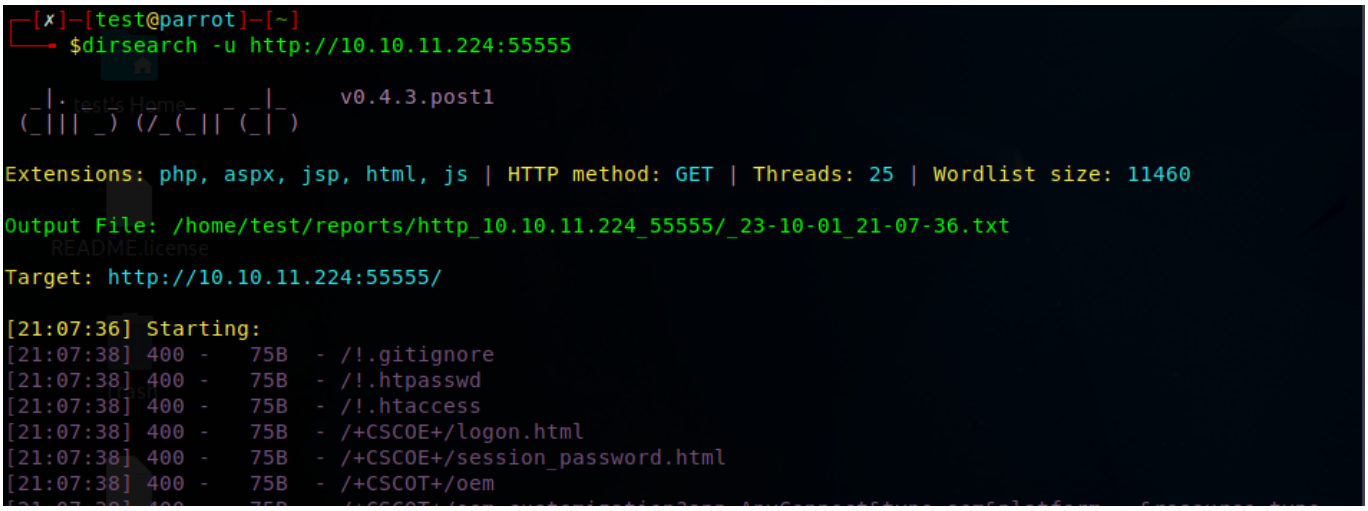
2. Website





3. Paths

Knowing baskets following are identified by the path, fuzzing the path may result in interesting finds. This appears to be a storage basket service, so usernames should be common. Unfortunately nothing is found.



Attack Surface Overview

This type of request baskets can have multiple services depending on them, and it should be possible to gain access to the service with some known exploit that allows us to traverse the baskets.

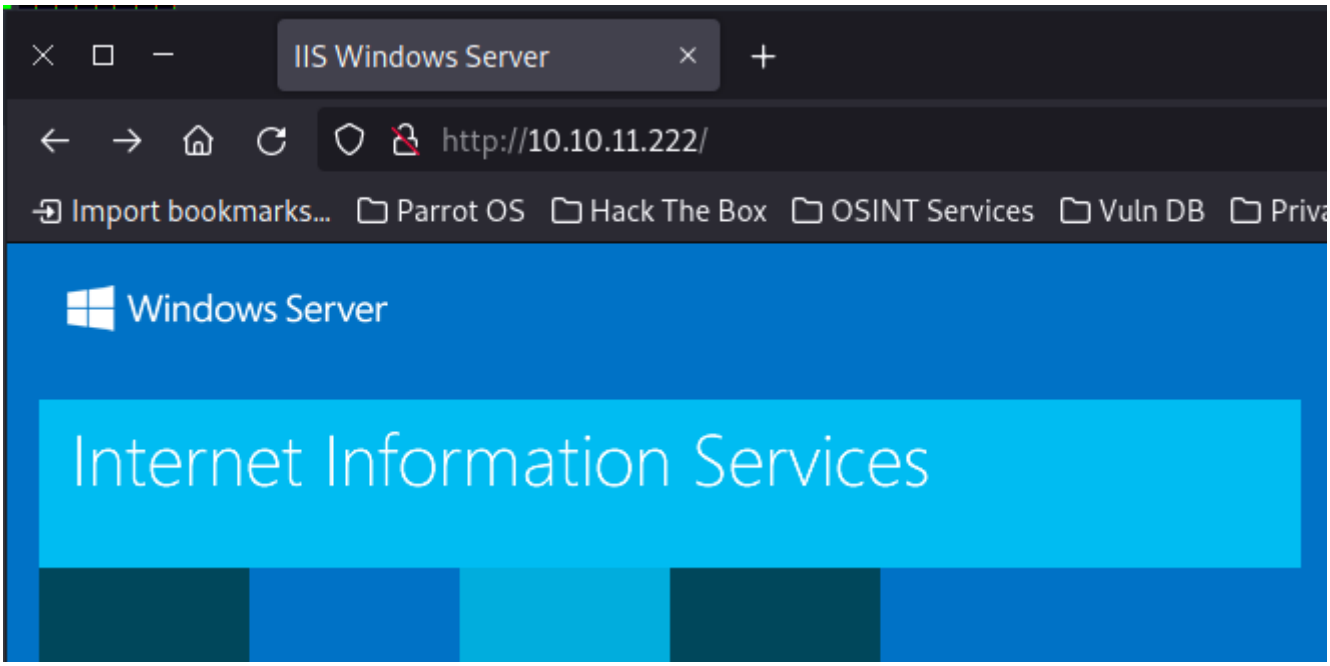
Authority Machine

Steps to Reproduce

1. Port Mapping

As usual, use nmap to scan for ports, a gather as much information as possible.

```
┌──[✗]─[test@parrot]─[~]
└──╼ $sudo nmap -sV -O 10.10.11.222
[sudo] password for test:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-01 21:37 WEST
Nmap scan report for 10.10.11.222
Host is up (0.12s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-10-02 00:39:44Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Defaul
t-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Defaul
t-First-Site-Name)
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Defaul
t-First-Site-Name)
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Defaul
t-First-Site-Name)
8443/tcp open  ssl/https-alt
```



A port 53 is open, you should run `nslookup`

```
┌──[✗]─[test@parrot]─[~]
└──╼ $nslookup
> server 10.10.11.222
Default server: 10.10.11.222
Address: 10.10.11.222#53
> localhost
;; communications error to 10.10.11.222#53: timed out
Server:         10.10.11.222
Address:        10.10.11.222#53

Non-authoritative answer:
Name:   localhost
Address: 127.0.0.1
** server can't find localhost: SERVFAIL
```

2. SMB Mapping

Samba is quite an "*outdated*" mechanism for storage, and comes with flaws, so you should always enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and maybe even execute remote commands.

```
┌──[test@parrot]─[~]
└──╼ $smbmap -u "" -p "" -P 445 -H 10.10.11.222 && smbmap -u "guest" -p "" -P 445 -H 10.10.11.222
[+] IP: 10.10.11.222:445        Name: 10.10.11.222
[+] IP: 10.10.11.222:445        Name: 10.10.11.222
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Department Shares                                       NO ACCESS
        Development                                             READ ONLY
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        SYSVOL                                                  NO ACCESS       Logon server share
```

Attack Surface Overview

From this point, one should consider mounting the samba drive and further explore any exposed information, which can prove quite insightful.

Gofer Machine

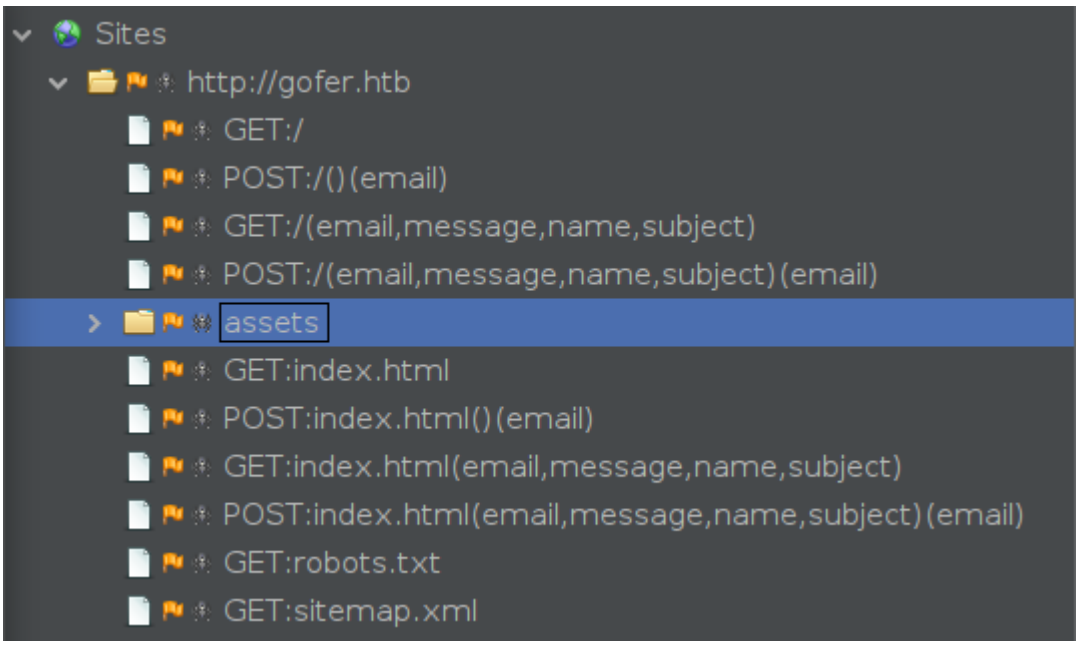
Steps to Reproduce

1. Port Mapping

```
┌──[test@parrot]─[~]
└──╼ $sudo nmap -sV -O 10.10.11.225
[sudo] password for test:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-01 22:04 WEST
Nmap scan report for 10.10.11.225
Host is up (0.12s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
25/tcp   filtered smtp
80/tcp   open     http        Apache httpd 2.4.56
139/tcp  open     netbios-ssn Samba smbd 4.6.2
445/tcp  open     netbios-ssn Samba smbd 4.6.2
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=10/1%OT=22%CT=1%CU=33863%PV=Y%DS=2%DC=I%G=Y%TM=6519DF0
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M53AST11NW7%O2=M53AST11NW7%O3=M53ANNT11NW7%O4=M53AST11NW7%O5=M53AST1
OS:1NW7%O6=M53AST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M53ANNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: Host: gofer.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.63 seconds
```

2. Website Exploration

Not much at first sight, seems like a simple One-Page Website.

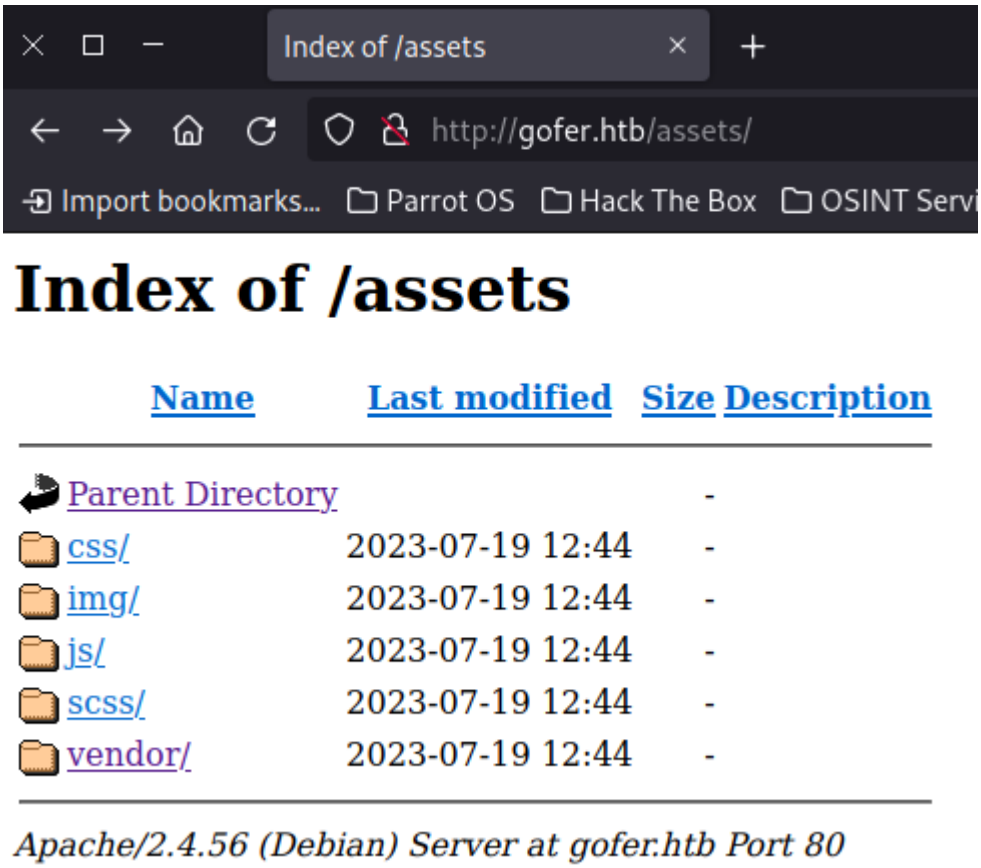


3. Samba search

```
┌─[test@parrot]─[~]
└──╼ $smbmap -u "" -p "" -P 445 -H 10.10.11.222 && smbmap -u "" -p "" -P 139 -H 10.10.11.225
[+] IP: 10.10.11.222:445        Name: 10.10.11.222
[+] IP: 10.10.11.225:139        Name: gofer.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        shares                                                  READ ONLY
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.13.1
3-Debian)
[!] Error:  (<class 'impacket.nmb.NetBIOSTimeout'>, 'smbmap', 1337)
```

4. Domain and Path Fuzzing

```
┌─[test@parrot]─[~]
└──╼ $dirsearch -u gofer.htb

  _|. _ _  _  _  _ _|_    v0.4.3.post1
 (_|| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/test/reports/_gofer.htb/_23-10-01_22-19-46.txt

Target: http://gofer.htb/

[22:19:46] Starting:
[22:19:52] 403 -  274B  - /.ht_wsr.txt
[22:19:52] 403 -  274B  - /.htaccess.bak1
[22:19:52] 403 -  274B  - /.htaccess.orig
[22:19:52] 403 -  274B  - /.htaccess.sample
[22:19:52] 403 -  274B  - /.htaccess_extra
[22:19:52] 403 -  274B  - /.htaccess_orig
[22:19:52] 403 -  274B  - /.htaccess.save
[22:19:52] 403 -  274B  - /.htaccess_sc
[22:19:52] 403 -  274B  - /.htaccessOLD
[22:19:52] 403 -  274B  - /.htaccessBAK
[22:19:52] 403 -  274B  - /.htaccessOLD2
[22:19:52] 403 -  274B  - /.htm
[22:19:52] 403 -  274B  - /.html
[22:19:52] 403 -  274B  - /.httr-oauth
[22:19:52] 403 -  274B  - /.htpasswd_test
[22:19:52] 403 -  274B  - /.htpasswds
[22:19:53] 403 -  274B  - /.php
[22:20:07] 301 -  307B  - /assets  ->  http://gofer.htb/assets/
[22:20:07] 200 -  477B  - /assets/
[22:20:37] 403 -  274B  - /server-status/
[22:20:37] 403 -  274B  - /server-status

Task Completed
```



Although no subdomains or relevant paths were discovered, there is still the assets folders for search.

Attack Surface Overview

In this target, the surface does not seem as large as others, but the samba storage would still be the primary target to explore further.

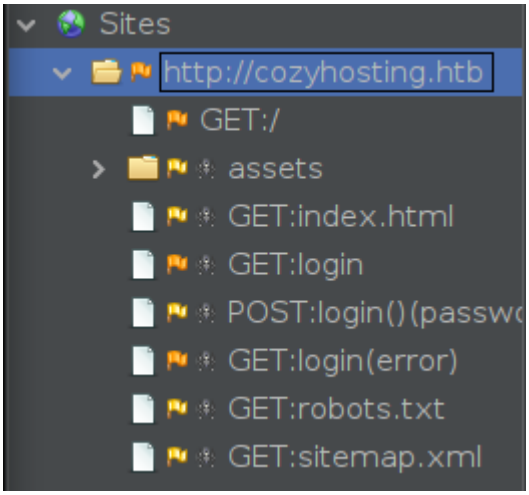
CozyHosting Machine

Steps to Reproduce

1. Port Mapping

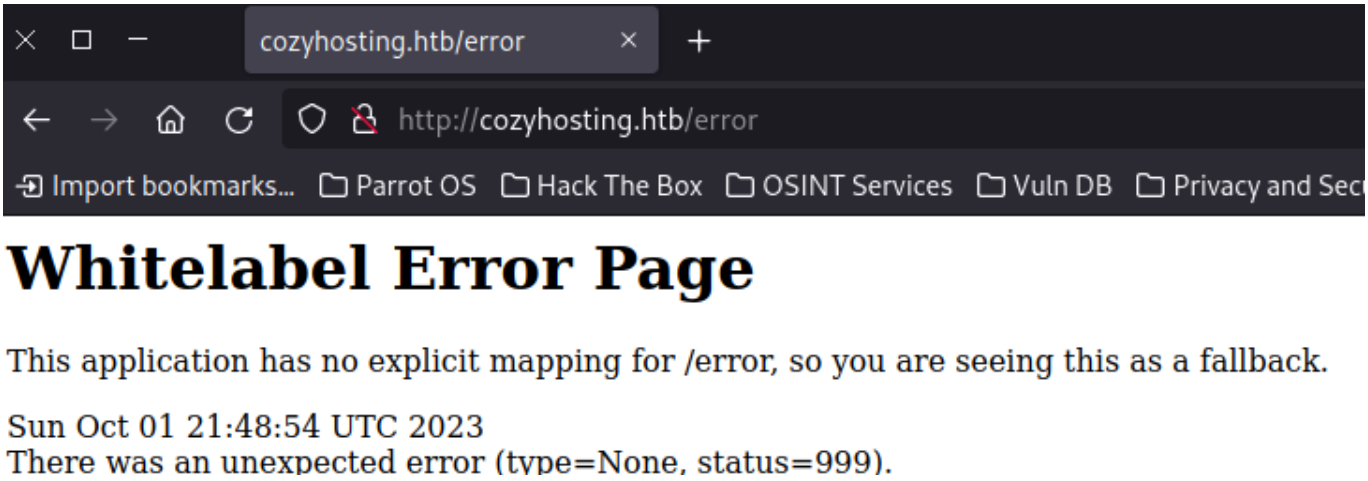
```
┌─[test@parrot]─[~]
└──╼ $sudo nmap -sV -O 10.10.11.230
[sudo] password for test:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-01 22:28 WEST
Nmap scan report for 10.10.11.230
Host is up (0.11s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=10/1%OT=22%CT=1%CU=30816%PV=Y%DS=2%DC=I%G=Y%TM=6519E47
OS:E%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=107%GCD=1%ISR=10B%TI=Z%CI=Z%TS=A)OPS(O1=M53AST11NW7%O2=M53AST11NW7%O
OS:3=M53ANNT11NW7%O4=M53AST11NW7%O5=M53AST11NW7%O6=M53AST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53ANNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.75 seconds
```

2. Website Exploring



```
[22:42:32] 200 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[22:42:40] 200 -    0B  - /engine/classes/swfupload//swfupload.swf
[22:42:40] 200 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
[22:42:40] 500 -   73B  - /error
[22:42:41] 200 -    0B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[22:42:41] 200 -    0B  - /extjs/resources//charts.swf
[22:42:45] 200 -    0B  - /html/js/misc/swfupload//swfupload.swf
[22:42:49] 200 -    0B  - /jkstatus;
[22:42:51] 200 -    0B  - /login.wdm%2e
[22:42:51] 200 -    4KB - /login
[22:42:52] 204 -    0B  - /logout

Task Completed
```

This appeared during a `dirsearch` run, and errors should always be explored.



With a bit of online search, we can discover that this is a typical error of **SpringBoot**.

Attack Surface Overview

Knowing that this is application running SpringBoot, you should now explore the known paths and exploits used for this framework.

Clicker Machine

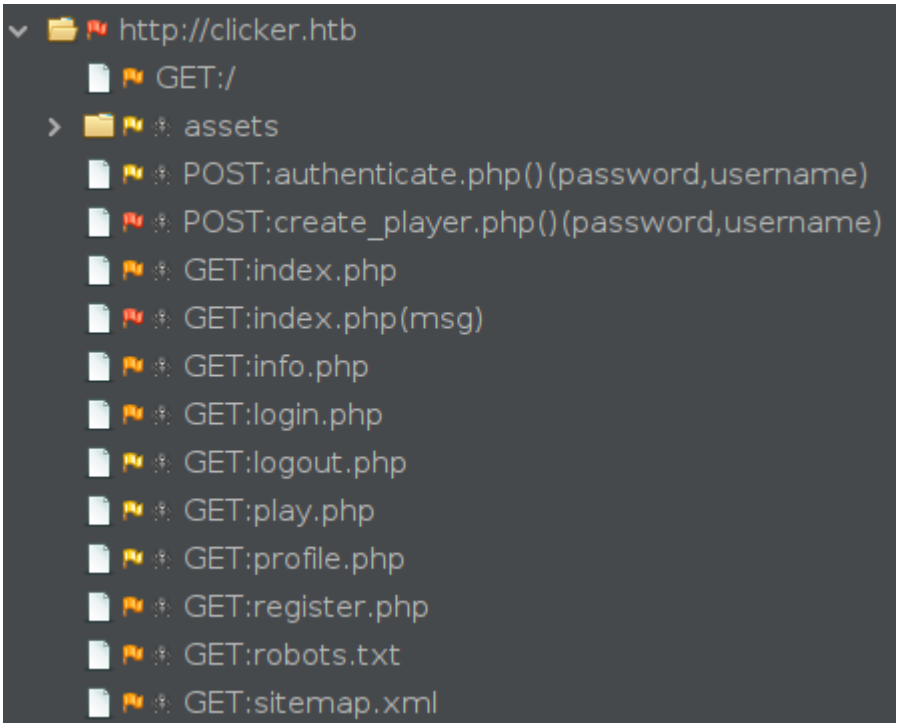
Steps to Reproduce

1. Port Mapping

```
┌─[test@parrot]─[~]
└──╼ $sudo nmap -sV -O 10.10.11.232
[sudo] password for test:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-01 22:54 WEST
Nmap scan report for 10.10.11.232
Host is up (0.12s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE   VERSION
22/tcp   open  ssh       OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http      Apache httpd 2.4.52 ((Ubuntu))
111/tcp  open  rpcbind   2-4 (RPC #100000)
2049/tcp open  nfs_acl   3 (RPC #100227)
8000/tcp open  http-alt?
```

With `nmap` we are able to discover a website and a nfs service, which is handy since is is a shared storages service.

2. Website Exploration



Always a faster to *zap* the website that manually discover since it is faster and allows for the exploration of the request format.

Attack Surface Overview

After knowing these too surfaces, one should start by trying to mount the nfs directory and search for more clues.

Fuzzing and subdomain enumeration were also tried, but did not resolve any relevant information.

Author

David José Araújo Ferreira, 93444 - davidaraujo@ua.pt

Report submitted for the Lab 01 of *Analysis and Vulnerability Exploitation* course at the University of Aveiro.