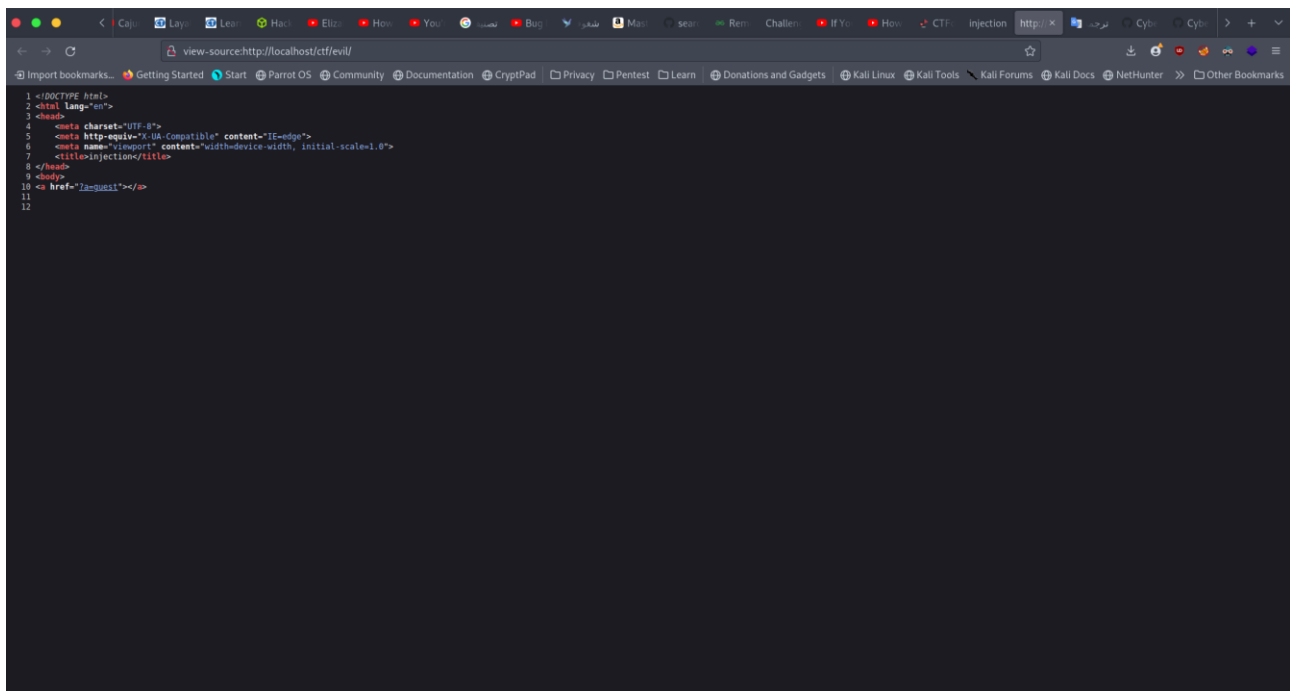




evil challenge | medium

Reported By:
AZZAM AL DUYULI

Reported To:
Academy of learning



```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta http-equiv="X-UA-Compatible" content="IE=edge">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <title>Injection</title>
8 </head>
9 <body>
10  <a href="?a=guest"></a>
11
12
```

When I started challenge I didn't see anything but in source code I see `<a>` tag inside it `?a=guest` and when I click it value for parameter `a` reflected in the page so I try write any word to know if there are any check process or don't. And clear for me that isn't there any check process so I try sql injection but also didn't work then check maybe it's php injection so I enter this payload

`guest;echo 5-2`

and I see this response → guest3

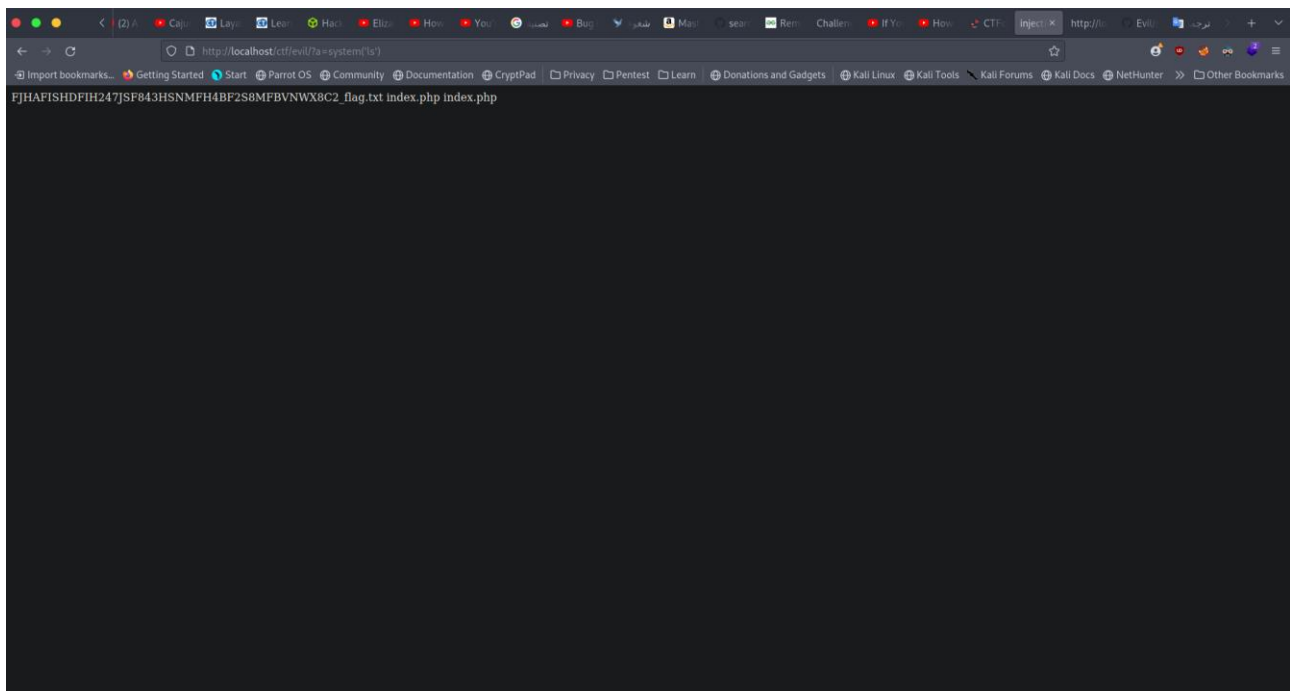
that mean the backend print guest And handle the subtraction process

So in php there are function called `system()` I can use it to execute command in the server so I put this payload → `system('ls')`

This payload will execute `ls` command in the server and then return the result to me in the page

And this was a result





So that worked and you can see there is file has a long name and end by `_flag.txt` so I read it by this payload → `system('cat%20FJHAFISHDFIH247JSF843HSNMFH4BF2S8MFBVNWX8C2_flag.txt')`

And I see the flag

