Flag Validator (50)

Description

http://tenjin.compfest.web.id:10339

calculate.php:

```
<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8">
            <title>Mari berhitung!</title>
        </head>
        <body>
            <br>
            <br>
            <div style="text-align:center ">
                <form action="./calculate.php" method="post" class="">
                    <input type="text" name="calc">
                    <input type="submit">
                </form>
                <?php
                $pattern = "/([0-9]\s?[\+\/\-\*]\s?[0-9])/";
                if(preg_match($pattern, $_POST['calc'])){
                    $toeval = "return " . $_POST['calc'] . ";";
                    $val = eval($toeval);
                    print("<h3>$val</h3>");
                }
                ?>
        </div>
    </body>
</html>
```

Write up

- Opening the website gives us a simple calculator, try entering `1 + 1` and it gives us `2.`
- We can see from the code provided it uses PHP `eval` to evaluate the math expression
- However it uses RegEx matching to prevent malicious code from being `eval`'d, as an example if you enter `system('id');` it won't return anything
- The RegEx matches `[number] [math expression] [number]` but it is not strict, so we can, for example, enter `asd 1 + 1 asd` and it still passes the filter
- We can then enter `system('id'); 1 + 1` and it `exec`'d successfully
- Then we can just `ls` and see:

```
Dockerfile calculate.php docker-compose.yml flag.txt index.php
```

- `cat`-ing the file `flag.txt` gives us the flag: `COMPFEST9{omg_that_regex_is_not_strong_enough}`