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_contens($filename,$content)

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