实验吧CTF_WEB(一)

原创

风凉ZZ 于 2016-09-26 23:50:09 发布 11488 收藏

更新ing~

1.题目：

你能跨过去吗
？，你是在问我吗？？？你是在怀疑我的能力吗？？？

解题链接： http://ctf1.shiyanbar.com/basic/xss/

解答：

点击链接后

将URL进行UnEscape解密 工具：http://tool.chinaz.com/Tools/Escape.aspx

+/v+是UTF—7编码

将ADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGsAZQB5ADoALwAlAG4AcwBmAG8AYwB1AHMA

进行base64解码得到

key:/%nsfocusXSStest%/

submit/%nsfocusXSStest%/得到过关KEY

相关：

1.utf7编码：

1>将字符转化为unicode码

2>将unicode码转化为二进制码

3>对二进制码重新进行分组，每6个一组，最后一组若不足6位用0补齐

4>根据改编的BASE64码表转化每一组所对应的字符
2.utf7解码：
1>根据改编后的base64码表获取每一个字符对应的代码
2>将代码转化为二进制
3>对二进制码重新进行分组，每16个一组，多余的部分舍弃
4>根据每组得到的unicode代码获取每个字符

2.因为utf-7编码特点，可以逃过绝大部分过滤检测，再配合常规的XSS手法，最简单的就是可以把 '<' 和 '>' 编码掉，而绝大部分的网站也只是简简单单地对这两个符号进行转移或过滤

3.utf-7 bom 目前知道的有4个：+/v8 | +/v9 | +/v+ | +/v

2.题目：

请输入密码

对不起，密码错误！！！错误！！！错误！！！

解题链接： http://ctf1.shiyanbar.com/basic/js/

解答：

查看源代码

```
document.oncontextmenu=function(){return false};

var a,b,c,d,e,f,g;
a = 3.14;
b = a * 2;
c = a + b;
d = c / b + a;
e = c - d * b + a;
f = e + d /c -b * a;
g = f * e - d + c * b + a;
a = g * g;
a = Math.floor(a);

function check(){
    if(document.getElementById("txt").value==a){
        return true;
    }else{
        alert("密码错误");
        return false;
    }
}
```


可知a的值即为密码
将这一段直接复制到console中，得出结果

输入424178，拿到key

3.题目：

猫抓老鼠

catch！catch！catch！嘿嘿，不多说了，再说剧透了

解题链接： http://ctf1.shiyanbar.com/basic/catch/

解答：

查看响应头

将MTQ3NTk0MDEyMA==输入得到KEY

相关：

1.base64加密特点

1>base64只有64个字符，英文大小写、数字和+、/，用作后缀等号

2>base64是把3个字节变成4个可打印字符，base64编码后的字符串一定能被4整除（包括用作后缀的等号）

3>等号一定用作后缀，且数目一定是0个、1个或2个。因为如果原文长度不能被3整除，base64要在后面添加\0凑齐3n位。为了正确还原，添加了几个\0就加上几个等号。显然添加等号的数目只能是0、1或2

4>严格来说base64不能算是一种加密，只能说是编码转换。使用base64的初衷。是为了方便把含有不可见字符串的信息用可见字符串表示出来，以便复制粘贴

4.题目：

Forbidden

不要相信此题有提示描述哦！

解题链接：http://ctf1.shiyanbar.com/basic/header/

解答：

显示说要在HongKong

抓包后，将Accept-Language改为zh-HK,发现不行，改成zh-hk,小写对了，得到KEY:123JustUserAGent

5.题目：

头有点大

解题链接： http://ctf8.shiyanbar.com/sHeader/

提示都这么多了，再提示就没意思了。

解答：

根据提示，需要修改.net framework 9.9，England ，browsing this site with IE三处，抓包修改

将Accept-Language改为en-gb（搜索语言代码表可以找到，这里需要小写。。。）,User-Agent要添加IE和.NET CLR 9.9

The key is:HTTpH34der

6.题目：

进来就给你想要的

想当年老孙降妖除魔，九九八十一难都过去了，更何况找它

解题链接：http://ctf1.shiyanbar.com/web/1/

解答：

一开始想着把id改改，试了几个后发现问题不在这；
又改成admin.asp试试，出现：“不猜猜文件夹就先猜文件吗？:)"的提示，于是尝试的改为admin，在源代码中发现

这就知道方向应该对了，改成system再看源代码即可找到KEY: "!!!WellDoneBrother!"

7.题目：

程序员的问题

以后写代码要注意了

解题链接： **http://ctf1.shiyanbar.com/web/4/index.php**

解答：

在username中随意输入字符，提示You are not admin!

在index.txt中，查看这一段

```
$row = mysql_fetch_array($query, MYSQL_ASSOC);
//echo $row["pw"];
  if($row['user']=="admin") {
    echo "<p>Logged in! Key: ********** </p>";
  }

  if($row['user'] != "admin") {
    echo("<p>You are not admin!</p>");
  }
}
```


sql语句：$sql = "select user from php where (user='$user') and (pw='$pass')";

改为$sql = "select user from php where (user='admin')#') and (pw='$pass')";

于是用户名输入admin')#,密码随意输，即得Key: WWW_SIMPLEXUE_COM

8.题目：

what a fuck!这是什么鬼东西?

解题链接： **http://ctf5.shiyanbar.com/DUTCTF/1.html**

解答：

之前做过类似的题目，知道js代码是可以转化为[]()!这种字符的，于是直接把字符复制到console，回车，即得结果Ihatejs

9.题目：

这个看起来有点简单 很明显。过年过节不送礼，送礼就送这个，格式：解题链接： http://ctf5.shiyanbar.com/8/index.php?id=1

解答：

当前库my_db—>表thiskey—>字段k0y—>暴字段k0y得whatiMyD91dump，不过目前题目貌似有点问题，这个答案提交上去显示错误(⊙o⊙)…，过段时间再看看吧

10.题目：

不多说，去看题目吧。

解题链接： http://ctf5.shiyanbar.com/phpaudit/

解答：

点击View the source code —>代码显示IP为1.1.1.1即可得到KEY—>使用modify header伪造IP—>Great! Key is SimCTF{daima_shengji}

很蓝瘦KEY提交不对，以前的KEY是http_client，老答案提交是对的，晕+_+,咳咳。。。我这方法是没毛病的

相关：

modify header我也是第一次用，下面附上相关说明：

1>在firefox中打开https://addons.mozilla.org/en-US/firefox/addon/modify-headers/

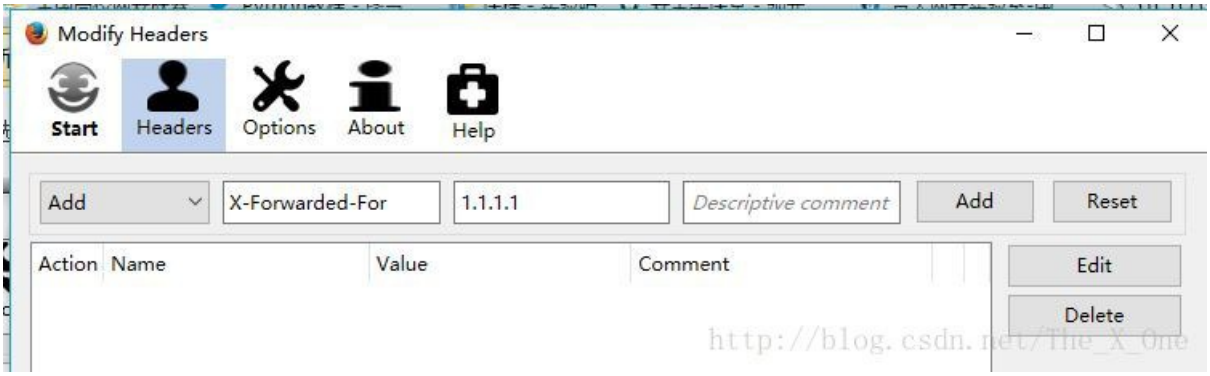
2>点击Add to Firefox

3>安装后重启浏览器

4>点击 

，选择Open ModifyHeaders

5>如图，选择Add—>输入X-Forwarded—>输入IP，这里是1.1.1.1



6>点击Add—>点击Start，此时已伪造IP成功，用完再Stop就好

11.题目

PHP大法

注意备份文件

解题链接： http://ctf5.shiyanbar.com/DUTCTF/index.php

解答：

依据提示，打开http://ctf5.shiyanbar.com/DUTCTF/index.php.txt，看到这段代码

```
<?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?
```

由于在浏览器输入url后会进行一次decode，这段代码中又进行一次decode，所以应对hackerDJ进行两次encode

```
Access granted!

flag: DUTCTF{PHP_is_the_best_program_language}


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