CTF——实验吧（web总结1.1）

原创

gyt478922579 于 2016-10-19 23:08:32 发布 14641 收藏 9

分类专栏： ctf 文章标签： ctf

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/gyt478922579/article/details/52863757

版权

ctf 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

地址：http://www.shiyanbar.com/ctf/practice

一、你能跨过去吗

题目：？，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/

思路：

1、发现所给字串中有%+数字，怀疑使用escape加密了url，使用站长工具http://tool.chinaz.com/Tools/Escape.aspx进行解（unescape），得到字符串如下：http://www.test.com/NodeMore.jsp?id=672613&page=2&pageCounter=32&undefined&callback=+/v+

+ADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGsAZQB5ADoALwAlAG4AcwBmAG8AYwB1AHMAWABTAFMAdABlAHMAdAAlAC8AIgApADwALwBzAGMAcgBpAHAAdAA+AC0-&_=1302746925413

2、其中我们观察

到：`+/v++ADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGsAZQB5ADoALwAlAG4AcwBmAG8AYwB1AHMAWABTAFMAdABlAHMAdAAlAC8AIgApADwALwBzAGMAcgBpAHAAdAA+AC0-&_`这一段比较特殊。我们知道+/v++代表为utf-7编码，这种编码方式使其他的字元被编码成 UTF-16 然后转换为修改的 Base64。这些区块的开头会以 + 符号来标示，结尾则以任何不在 Base64 里定义的字元来标示。

3、因此我们使用base64

对`ADwAcwBjAHIAaQBwAHQAPgBhAGwAZQByAHQAKAAiAGsAZQB5ADoALwAlAG4AcwBmAG8AYwB1AHMAWABTAFMAdABlAHMAdAAlAC8AIgApADwALwBzAGMAcgBpAHAAdAA+`进行解码，得到夹杂不可见字符的一段js语句，去除不可见字符后得到key，提交到所给页面，得到最终flag

二、进来就给你想要的

题目：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/

思路：

1、观察urlhttp://ctf1.shiyanbar.com/web/1/index.asp?id=1`，怀疑是文件包含。

2、用御剑跑一下发现以下页面：

扫描信息：http://ctf1.shiyanbar.com/web/1/a%5c.aspx　　扫描线程：20　　扫描速度：92/秒

ID	地址	HTTP响应
1	http://ctf1.shiyanbar.com/web/1/login.htm	200
2	http://ctf1.shiyanbar.com/web/1/admin/index.htm	200
3	http://ctf1.shiyanbar.com/web/1/login.html	200
4	http://ctf1.shiyanbar.com/web/1/admin_login.asp	200
5	http://ctf1.shiyanbar.com/web/1/admin.asp	200
6	http://ctf1.shiyanbar.com/web/1/Admin_Login.asp	200
7	http://ctf1.shiyanbar.com/web/1/Admin.asp	200

点击发现提示：不猜猜文件夹就先猜文件吗？:)

3、尝试进入文件夹页面：`http://ctf1.shiyanbar.com/web/1/admin/
，查看源代码发现提示：Error....呵呵，思路是对的哈，但是不在这儿。想想谁的权利最大

4、猜测是想让我们进入system权限的文件夹，访问view-source:http://ctf1.shiyanbar.com/web/1/system/ 发现KEY。

补充：Windows系统权限介绍
1、 普通权限
默认情况下，系统为用户分了6个组，并给每个组赋予不同的操作权限，依次为:管理员组(Administrators)、高权限用户组(Power Users)
、普通用户组(Users)、备份操作组(Backup Operators)、文件复制组(Replicator)、来宾用户组(Guests)

2、特殊权限
系统还存在一些特殊权限成员，SYSTEM(系统)、Everyone(所有人)、CREATOR OWNER(创建者)

三、请输入密码

题目：对不起，密码错误！！！错误！！！错误！！！
解题链接： http://ctf1.shiyanbar.com/basic/js/

思路：
1、查看器查看源代码发现js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;
    }
}
```

、

2、计算得到a值，提交通过

四、猫抓老鼠

题目：catch！catch！catch！嘿嘿，不多说了，再说剧透了
解题链接： http://ctf1.shiyanbar.com/basic/catch/

思路：
1、查看页面提交的响应头，发现可疑字串：`Content-Row:"MTQ3Njg3ODc2NA=="`

2、提交后通过

五、Forbidden

题目：不要相信此题有提示描述哦！
解题链接： http://ctf1.shiyanbar.com/basic/header/

思路：
1、查看题目，提示需要我们在香港才能访问该页面

2、尝试修改响应头Accept-Language字段，将`zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3`改为`zh-hk,zh;q=0.8,en-US;q=0.5,en;q=0.3`

3、重新发送请求，获得key值

六、貌似有点难

题目：不多说，去看题目吧。
解题链接： http://ctf8.shiyanbar.com/phpaudit/

思路：
1、查看所给php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！";
}
?>
```

发现$GetIPs==”1.1.1.1”时才输出key值

2、尝试伪造php消息请求头，在请求头中添加字段：Client-Ip: 1.1.1.1

3、重新提交获得key值

补充：

HTTP_CLIENT_IP：可通过http头伪造
HTTP_X_FORWARDED_FOR：可通过http头伪造
REMOTE_ADDR：可能是用户真实IP也可能是代理IP

七、PHP大法

题目：注意备份文件
解题链接： http://ctf5.shiyanbar.com/DUTCTF/index.php

思路：
1、访问页面发现提示：Can you authenticate to this website? index.php.txt

2、访问：http://ctf5.shiyanbar.com/DUTCTF/index.php.txt

3、发现php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?
```

4、阅读php代码，发现是将传过来的字符串多进行了一次urldecode，那我们可以在提交时进行两次urlencode

5、提交通过

八、what a fuck!这是什么鬼东西？

题目：what a fuck!这是什么鬼东西?
解题链接： http://ctf5.shiyanbar.com/DUTCTF/1.html

思路：
1、打开代码，发现是BrainFuck编码

2、直接复制粘贴在控制台跑一下

3、获得key值

补充：
BrainFuck：一种极度精简的计算机语言
字符 含义

```
        指针加一
```

< 指针减一
+ 指针指向的字节的值加一
- 指针指向的字节的值减一
. 输出指针指向的单元内容（ASCⅡ码）
, 输入内容到指针指向的单元（ASCⅡ码）
[如果指针指向的单元值为零，向后跳转到对应的]指令的次一指令处
] 如果指针指向的单元值不为零，向前跳转到对应的[指令的次一指令处

九、FALSE

题目：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： http://ctf4.shiyanbar.com/web/false.php

思路：
1、点击查看php代码

```
<?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>';
?>
```

2、注意：
===是恒等计算符：同时检查表达式的值与类型
==是比较运算符号：不会检查条件式的表达式的类型
所以，===会比较类型，比如bool。

3、php为弱类型语言，其中sha1()函数和md5()函数存在着漏洞，sha1（）函数默认的传入参数类型是字符串型，若给它传入数组会返回错误，也就是返回false，这样一来===运算符就可以发挥作用了，所以，这道题需要构造username和password既不相等，又同样是数组类型。

4、构造url：http://ctf4.shiyanbar.com/web/false.php?name[]=a&password[]=b
，获取key值

十、 思路很重要（好难，啊啊啊没思路Google的，羞羞）

题目： 源
格式：ctf{}
解题链接： http://ctf4.shiyanbar.com/web/9

思路：
1、进入页面发现右键无法查看源代码，那我们按f12打开控制台查看源代码

2、发现有一段js代码，仔细阅读感觉只是限制了右键阅读代码，此时我们注意文字提示“ 粗心的程序员，写完代码也不删。”

3、推测出题者是想让我们查看备份文件（.bak），访问http://ctf4.shiyanbar.com/web/9/index.php.bak
得到源代码

```
$flag='xxx'; extract($_GET); if(isset($shiyan)){ $content=trim(file_get_contents($flag)); if($shiyan==$
```

4、可以是 *shiyanba*和

5、获得加密后的flag，经过凯撒密码移位后取得key值

十一、 天下武功唯快不破

题目： 看看响应头
格式：CTF{}
解题链接： http://ctf4.shiyanbar.com/web/10.php

思路：
1、查看消息头，发现可疑字段： FLAG:”UDBTVF9USEITX1QwX0NlNE5HRV9GTDRHOktHY2pOWHAwTg==”，base64解密，得到字符串：P0ST_THIS_T0_CH4NGE_FL4G:KGcjNXp0N，但是刷新页面发现后面的字符串会变化，所以我们考虑写爬虫将页面爬取下来后将相应FLAG提交到指定页面

2、使用Python2.7的requests模块和base64模块编写：

```
import base64
import requests

url=”https://ctfd.a101e.lab/backend/url_fopen.php”
flag=requests.get(url).headers[“FLAG”]
post={“key”:base64.decodestring(flag).split(“:”)[1]}
print requests.post(url,data=post).text
```

3、运行获取flag

补充：
requests.get(url).headers[“FLAG”]
requests.post(url,data).text