实验吧CTF web刷题

转载

小 白 渣 于 2020-07-13 16:08:08 发布 978 收藏 8
分类专栏： 实验吧CTF web刷题 文章标签： 网络安全
原文链接：https://blog.csdn.net/Eastmount/article/details/98529597

最近开始学习网络安全相关知识，接触了好多新术语，感觉自己要学习的东西太多，真是学无止境，也发现了好几个默默无闻写着博客、做着开源的大神。接下来系统分享一些网络安全的自学笔记，希望读者们喜欢。
上一篇文章分享了解BurpSuite工具的安装配置、Proxy基础用法，并分享一个简单的暴库案例；本篇文章分享实验吧CFT实战的题目，涉及WEB渗透和隐写术常见题型，包括“这是什么”、“天网管理系统”、“忘记密码”、“false”、“天下武功唯快不破”和“隐写术之水果、小苹果”。非常有意思的文章，作为在线笔记，希望对入门的博友们有帮助，大神请飘过，谢谢各位看官！

下载地址：https://github.com/eastmountyxz/NetworkSecuritySelf-study
百度网盘：https://pan.baidu.com/s/1dsunH8EmOB_tlHYXXguOeA 提取码：izeb

PS：作为初学者，这些题目自己只能完成很少部分，更多是学习别人的知识慢慢成长，未来希望自己能真正独立完成更多CTF夺旗题目。

前文学习：
[网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例
[网络安全自学篇] 二.Chrome浏览器保留密码功能渗透解析及登录加密入门笔记
[网络安全自学篇] 三.Burp Suite工具安装配置、Proxy基础用法及暴库示例

前文欣赏：
[渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入
[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法
[渗透&攻防] 三.数据库之差异备份及Caidao利器
[渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

补充学习资料：
TK13大神Windows PE专栏 https://blog.csdn.net/u013761036/article/category/6401236
TK13大神Windows对抗专栏 https://blog.csdn.net/u013761036/article/category/6365454
鬼手56大神六个专栏 https://blog.csdn.net/qq_38474570/article/details/87707942
whatiwhere大神逆向工程专栏 https://blog.csdn.net/whatiwhere/article/category/7586534

文章目录

一.WEB之这是什么

题目地址： http://www.shiyanbar.com/ctf/56
解题链接： http://ctf5.shiyanbar.com/DUTCTF/1.html
题目描述：

打开链接如下图所示，确实是什么鬼东西。

题目解析：

1.它们其实是Jother编码，它是一种运用于Javascript语言中利用少量字符构造精简的匿名函数方法对于字符串进行的编码方式，其中少量字符包括"["，"]"，"{"，"}"，"("，")"，"!"，"+"。这些字符就能完成对任意字符串的编码，本质上是一种Javascript的编码，其优点是代码字符就那么几个，比较好记，缺点是编码极其冗长和复杂。
这种编码一般现在只会出现在CTF比赛中，实际开发中用的到就很少了。

2.打开Chrome浏览器，按F12键选择控制台Console，将代码复制过去回车即可得到flag值。

3.得到该题的密码：lhatejs。

正确答案：lhatejs

参考链接： https://www.writeup.top/391.html

二.隐写术之水果

隐写术是一门关于信息隐藏的技巧与科学，所谓信息隐藏指的是不让除预期的接收者之外的任何人知晓信息的传递事件或者信息的内容。隐写术的英文叫做Steganography，来源于特里特米乌斯的一本讲述密码学与隐写术的著作Steganographia，该书书名源于希腊语，意为“隐秘书写”。在CTF题目中，图片隐写题属于杂项的一部分，题目较为简单。

题目地址： http://www.shiyanbar.com/ctf/1903
解题链接： http://ctf5.shiyanbar.com/stega/pic.png
题目描述：

打开网页如下图所示，显示一张水果的图片，flag就隐藏在图片中。作者第一反应是查看源代码，哈哈~原谅我这个小白第一次学习。

题目解析：

1.将图片另存为本地。

2.从CSDN下载Stegsolve工具，它是用于图像解析的工具，然后导入本地图片，按方向键右键不断切换，直到出现下图的二维码。

如下图所示：

3.使用手机扫描二维码，得到一串数字，我们根据数值可以分析，这是十进制的ASCII码。

4.将数字转换为ASCII，45对应“-”、46对应“.”、32对应空格。

```
45 46 45 46 32        -.-.
45 32                 -
46 46 45 46 32        ..-.
46 45 46 46 32        .-..
46 46 46 32           ...
45 46 46 46 32        -...
46 46 45 45 46 45 32  ..--.-
45 46 46 46 32        -...
46 46 46 32           ...
46 45 46 46 32        .-..
```

5.它们就是传说中的摩斯密码。根据下面的对照表，其结果为：CTFLSB_BSL

> 摩尔斯电码（又译为摩斯密码，Morse code）是一种时通时断的信号代码，通过不同的排列顺序来表达不同的英文字母、数字和标点符号。它发明于1837年，发明者有争议，是美国人塞缪尔·莫尔斯或者艾尔菲德·维尔。 摩尔斯电码是一种早期的数字化通信形式，但是它不同于现代只使用零和一两种状态的二进制代码，它的代码包括五种： 点、划、点和划之间的停顿、每个字符之间短的停顿、每个词之间中等的停顿以及句子之间长的停顿。

正确答案：CTF{lsb_bsl}

参考链接：
https://blog.csdn.net/miko2018/article/details/81627130
https://www.cnblogs.com/nul1/p/9594387.html
https://blog.csdn.net/u012486730/article/details/82016706

三.隐写术之小苹果

题目原理和上一题一样。

题目地址： http://www.shiyanbar.com/ctf/1928
解题链接： http://ctf5.shiyanbar.com/stega/apple.png
题目描述：

题目打开也是一张图片，中国结。

题目解析：

1.下载图片至本地并打开，得到如下二维码：

2.二维码包含如下数字。

```
\u7f8a\u7531\u5927\u4e95\u592b\u5927\u4eba\u738b\u4e2d\u5de5
```

这是unicode编码的方式，让我们在相关网站（搜索“unicode解码即可”）中进行解码，得到中文“羊由大井夫大人王中工”，这是一种从未见过的加密方式。

3.通过百度了解到该加密为当铺密码，曾在CTF题目中出现过，我们按照编码规则进行解码，得到数字：9158753624。

> 当铺密码是一种将中文和数字进行转化的密码，算法相当简单:当前汉字有多少笔画出头，就是转化成数字几。
> “羊由大井夫大人王中工”对应的数字为“9158753624”

4.再回头分析图片可知，里面包含了一个压缩文件，我们通过修改扩展名为.ZIP并解压，得到了apple.mp3的音频文件。

5.使用mp3隐写术工具MP3Stego的Decode.exe对其进行解码，密码就是我们刚刚得到的那串数字9158753624。解码后得到字串Q1RGe3hpYW9fcGluZ19ndW99。

6.通过尝试，在base64解码中得到了正确的结果：CTF{xiao_ping_guo}。

正确答案：CTF{xiao_ping_guo}

四.WEB之天网管理系统

题目地址： http://www.shiyanbar.com/ctf/1810
解题链接： http://ctf5.shiyanbar.com/10/web1/index.php
题目描述：

题目显示如下图所示，需要输入正确的用户名和密码获取flag。

考点：PHP弱类型

题目解析：

1.查看网页源代码如下所示，注意注释的提示。

```
<!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->
```

2.需要用户名传入一个字符串，并且它经过md5加密后要等于0。
注意，PHP某些情况会把类数值数据（如含有数字的字符串等）转换成数值处理。在使用“= =” 运算符对两个字符串进行比较时，PHP会把类数值的字符串转换为数值进行比较，如果参数是字符串，则返回字符串中第一个不是数字的字符之前的数字串所代表的整数值。比如: ‘3’ == '3ascasd’结果为true。

因此只要找到一个字串加密后第一个字符为0即可，这里提供几个：240610708、aabg7XSs

3.用户名输入“aabg7XSs”，此时返回的提示信息如下图所示。
http://ctf5.shiyanbar.com/10/web1/user.php?fame=hjkleffifer

4.访问该页面显示内容如下图所示：
函数serialize()是对输入的数据进行序列化转换，把变量和它们的值编码成文本形式。
函数unserialize()是还原已经序列化的对象，对单一的已序列化的变量进行操作，将其转换回反序列化 PHP 的值。

```
$unserialize_str = $_POST['password'];
$data_unserialize = unserialize($unserialize_str);
if($data_unserialize['user'] == '???' && $data_unserialize['pass']=='???') {
    print_r($flag);
}
```

这段代码是将Post提交的密码值经过unserialize()函数 反序列化处理，得到一个数组，要求数组里的user和pass都等于值“???”，此时输出flag。那么，这个“???”又是什么内容呢？

5.此时“成也布尔，败也布尔”提醒我们。
bool类型的true跟任意字符串可以弱类型相等。 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。（a代表array，s代表string，b代表bool，而数字代表个数/长度）

```
<?php
error_reporting(0);
$test='';
$test=array("user"=>1,"pass"=>1);
echo var_dump($test);
echo var_dump(serialize($test));
```

test1

找个在线PHP网站进行测试，输出如下图所示：string(36) “a:2:{s:4:“user”;i:1;s:4:“pass”;i:1;}”

6.构造password值为： a:2:{s:4:“user”;b:1;s:4:“pass”;b:1;}，输出最后的flag。

正确结果：ctf{dwduwkhduw5465}

参考链接：
https://blog.csdn.net/dongyanwen6036/article/details/77650921
https://www.cnblogs.com/ssooking/p/5877086.html

五.WEB之忘记密码

题目地址： http://www.shiyanbar.com/ctf/1808
解题链接： http://ctf5.shiyanbar.com/10/upload/step1.php
题目描述：

题目显示如下图所示，需要输入正确的邮箱找回密码。

考点：vim备份文件泄露

题目解析：

1.首先我们随便输入一个密码，如“123456”看返回结果。

返回如下图所示，注意“step2.php”页面。

2.查看源代码，发现提醒用户名为admin，输入邮箱为“admin@simplexue.com”。

输入该邮箱发现Scripts提醒变成了“邮箱已送到管理员邮箱了，你看不到”，真是逗~

3.这里有个细节，Step2.php页面跳转了一下，然后又跳转回step1，说明step2里面有猫腻！页面跳转这么快，那我们该怎么去看这个页面呢？这时候要用到一个名叫Burp Suite的神器，抓包拦截。

Step2.php显示立刻跳转：

方法一：在Target查看目录树发现有个“submit.php”文件。

方法二：使用Repeater，查看响应Response。

将GET方法的网址修改为step2.php，然后响应表单提交为“submit.php”。

4.赶紧查看该网页，结果提醒“you are not an admin”，有权限访问该页面，但不是管理员不透露信息。有意思~

5.再回到最初step1.php的源代码，这里有个非常重要的提示信息——编辑器采用的是VIM。

> VIM备份文件（参考Sp4rkW大神）
> 默认情况下使用VIM编程，在修改文件后系统会自动生成一个带 ~ 的备份文件，某些情况下可以对其下载进行查看。例如，index.php普遍意义上的首页，它的备份文件则为index.php~。
> VIM中的swp即swap文件，在编辑文件时产生，它是隐藏文件，如果原文件名是submit，则它的临时文件“.submit.swp”。如果文件正常退出，则此文件自动删除。

这个题目叫备份文件泄露，我们知道这个VIM编辑器可以存放临时文件，而临时文件会存放信息，咱们可以尝试一下访问临时文件，格式如下：

```
ctf5.shiyanbar.com/10/upload/.submit.php.swp
```

PS：因为vim备份文件是隐藏文件，所以需要加上一个点“.submit.php.swp”。

6.尝试打开.submit.php.swp文件。

重点是后面的if判断语句，这个条件必须要满足token的长度必须等于10，并且token的值为0，咱们可以构造十个0试试。

```
.....这一行是省略的代码.....

if(!empty(KaTeX parse error: Expected 'EOF', got '&' at position 82: …oken operator">&amp;&amp;</span… emailAddress)){
if(strlen(
token< /span> <
```

7.最终构造的结果如下：

```
http://ctf5.shiyanbar.com/10/upload/submit.php?emailAddress=admin@simplexue.com&token=0000000000
```

然后访问得到如下结果：

正确答案：flag is SimCTF{huachuan_TdsWX}

参考链接：

https://www.cnblogs.com/ECJTUACM-873284962/p/7860788.html

https://blog.csdn.net/wy_97/article/details/76559354

六.WEB之false

题目地址： http://www.shiyanbar.com/ctf/1787

解题链接： http://ctf5.shiyanbar.com/web/false.php

题目描述：

题目显示如下图所示。

考点：PHP代码审计（PHP Code Audit）

题目解析：

1.首先随便输入内容，点击“Login”按钮。

```
http://ctf5.shiyanbar.com/web/false.php?name=1&password=2
```

2.点击“View the source code”获取源代码如下所示。

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

它的含义是GET获取name和password，然后进行判断。
（1）if ($ _GET[‘name’] == $ _GET[‘password’])，用户名和密码相等，提示如下。

（2）else if (sha1($ _GET[‘name’]) === sha1($ _GET[‘password’]))，用户名名和密码的sha1加密散列值相等，执行die函数。

（3）以上都不是返回“Invalid password”。

（4）未输入用户名和密码，提示“Login first”。

3.函数说明：

- die()函数：停止程序运行，输出内容
- sha1()函数：计算字符串 “Hello” 的 SHA-1 散列。默认的传入参数类型是字符串型
- isset()函数：检测变量是否已设置并且非 NULL。
- 若变量不存在则返回 FALSE， 若变量存在且其值为NULL，也返回 FALSE ，若变量存在且值不为NULL，则返回 TURE。同时检查多个变量时，每个单项都符合上一条要求时才返回 TRUE，否则结果为 FALSE。

参考官网：https://www.php.net/manual/zh/function.isset.php

```
<?php
$a = array ('test' => 1, 'hello' => NULL, 'pie' => array('a' => 'apple'));

var_dump(isset(
```

```
a< /span> ,
```

```
// 键 ‘hello’ 的值等于 NULL，所以被认为是未置值的。
// 如果想检测 NULL 键值，可以试试下边的方法。
var_dump(array_key_exists(‘hello’, $a)); // TRUE

// Checking deeper array values
var_dump(isset(
```

```
a< /span> ,
```

4.这里需要执行“if (sha1($ _GET[‘name’]) === sha1($ _GET[‘password’]))”语句。

重点：sha1()函数默认的传入参数类型是字符串型，也可以传入其他类型，使其返回值为false，如数组类型。再加上题目标题false，可以想到构造FALSE===FALSE拿到flag。

> = =：比较运算符号 不会检查条件式的表达式的类型
> ===：恒等计算符 , 同时检查表达式的值与类型。

构造网址：

```
http://ctf4.shiyanbar.com/web/false.php?name[]=1&password[]=2
```

5.name和password为数组，并且值不相等，提交即可获得flag。

正确结果：Flag: CTF{t3st_th3_Sha1}

七.WEB之天下武功唯快不破

题目地址： http://www.shiyanbar.com/ctf/1854
解题链接： http://ctf5.shiyanbar.com/web/10/10.php
题目描述：

题目显示如下图所示，提醒“You must do it as fast as you can!”。

考点：Python脚本

题目解析：

1.尝试SQL注入都无反应，接着查看源代码，发现一个提示信息：

```
<!-- please post what you find with parameter:key -->
```

2.根据题目内容，试图将网页链接速度放慢，这里可以采Burp Suite抓包，Proxy的intercept载入网页，并将抓到的信息发到repeater中Go一下，会发现一个FLAG值。另一种方法，Chrome浏览器审查网络状态。

3.在响应头中发现了FLAG，看起来像是一个Base64编码，尝试在线解码。

但是该值每次生成的值是随机的。

FLAG: UDBTVF9USEITX1QwX0NlNE5HRV9GTDRHOnZhbmRmQXp1Zg==
解码：P0ST_THIS_T0_CH4NGE_FL4G:vandfAzuf

FLAG: UDBTVF9USEITX1QwX0NlNE5HRV9GTDRHOktsSVBLWmVkOQ==
解码：P0ST_THIS_T0_CH4NGE_FL4G:KlIPKZed9

4.回想之前的注释（please post what you find with parameter:key）以及解密后的FLAG值，需要快速提交POST，故采用Python脚本实现。哈哈，又回到熟悉的语言。

```
# -*- coding: utf8 -*-
import requests
import base64

url = 'http://ctf5.shiyanbar.com/web/10/10.php'
s = requests.session()
response = s.get(url)

#获取FLAG值
#FLAG: UDBTVF9USEITX1QwX0NlNE5HRV9GTDRHOnZhbmRmQXp1Zg==
head = response.headers
flag = base64.b64decode(head['FLAG']).split(':')[1]
print(flag)
```

```
#设置POST请求
pdata = {'key': flag}
result = s.post(url=url, data=pdata)
print(result.text) #响应
```

5.运行得到如下结果。

正确答案：CTF{Y0U_4R3_1NCR3D1BL3_F4ST!}

参考链接：

https://www.jianshu.com/p/11b5c1bd62d0
https://blog.csdn.net/miko2018/article/details/83314088
https://blog.csdn.net/dongyanwen6036/article/details/77358693