ctf php 流量分析题,CTF平台hackit题目分析与解答

转载

小芋头君 于 2021-03-09 19:34:01 发布 110 收藏
文章标签： ctf php 流量分析题

之前在网上经常看到很多的CTF的练习平台，在加上搞CTF比赛的学弟推荐了这个 CTF平台 。当时在网上看了一下，这个平台推荐的人还是很多的。这个平台是由一个白帽子个人开发的一个平台。趁着这个平台还没有关闭的时候，我抓紧时间来练习一下，找找做CTF比赛的感觉，同时也提升我的渗透能力。当我千辛万苦地做完了之后，发现网上还没有人写这个练习平台的writeup,于是我决定记录下我的做题过程。一方面是为了能够帮助做题遇到困难的同学们，另一方面也是记录我的成长过程。

第一关

第一关很简单，根据题目的提示key藏在页面中。做CTF比赛的题目，第一步就是要查看网页的源代码，查看源代码就可以发现key。

第二关

第二关的提示是：

有时候网页源码并不是唯一可以隐藏信息的。

除了看源代码之后，很多时候还要看题目与分服务器之间发送的网路请求包。这道题目中，key就藏在了网页的响应包中。 Key:SDUH@HEADER

这道题目要求对HTTP协议有一个基本的了解和认识。知道HTTP的请求报文和响应报文的格式，以及每个字段所代表的含义，哪些字段是必须的等等知识。

使用PHP来设置header也是十分地简单

header("Key:SDUH@HEADER");

第三关

第三关的提示是：

right,但还是有地方可以隐藏信息

这道题目就需要使用到burpsuite这个白帽子都很熟悉的工具了。

从上图中可以看到，Cookie中的值为give_me_key的值为no，将其改为yes,然后转发。在页面中就可以看到了key。 $('#key').val("0fC00k13@sc")

这个题目同样是需要看请求包的，不同的是这个题目需要看的是cookie。同时这个题目还告诉我们，在浏览器和服务器进行通信的过程中，我们还可以使用各种拦截工具，如burosuite，fiddle，firefox插件Tamper Data来进行修改。

第四关

第四关中给出了网页的源代码。

if (isset ($_GET['getkey'])) { if (@ereg ("^[1-9]+$", $_GET['getkey']) === FALSE) echo '必须输入数字才行'; else if (strpos ($_GET['getkey'], 'givemekey') !== FALSE) die('Flag: '.$flag); else echo 'getkey姿势不对啊';}

这段代码中有2个函数。

@ereg(string pattern, string string):以patttern的规则来解析字符串string，如果解析成功返回True否则返回FALSE；

strpos(str1,str2)：查找str2在str1的位置，如果找到返回True否则FALSE；

从代码中我们知道，这道题目要求输入getkey，但是这个值首先必须要是数字，然后这个值又必须含有givemeky这个字符串。这道题目需要用到 ereg()函数的%00字符串截断漏洞 。具体就是当ereg读取字符串string时，如果遇到了%00,后面的字符串就不会被解析。那么我们输入的字符串为: getkey=1%00givemekey 。这样就可以绕过验证，拿到key。 Flag: m4g1c@ppp

第五关

第五关给了一张图片。

遇到这样的题目，一般都是信息隐藏。需要查看图片中隐藏的信息。我们使用UltraEdit打开图片，发现图片后面有一句话。 Hero's Name Add 666 。key为 LeBlanc6666

第六关

这关给的是一个压缩包。提示如下：

压缩密码很短也很简单，秒秒钟破，不过你知道key可以藏在图片的哪里吗？

这个题目说了密码很短，找一个rar的密码爆破软件，得到解压密码是0oO。解压之后同样得到的是一个这样的图片。之前已经说过了，遇到了图片的题目一般都是信息隐藏的题目。要么是在图片中隐藏了信息，要么是在图片中包含了其他的文件。在这个题目上，我之前的思路受到了限制。第五题中已经在图片中包含了信息，那么我认为这题应该是在图片了包含了文件。最后我使用了 binwalk 来对图片进行分析，发现其中确实是包含了文件，但是始终找不出key。后来询问作者才知道，这道题目的key其实很简单，就隐藏在了图片的exif信息中。

在版权信息中，有 65 83 77 68 68 64 49 48 ，转换为字母是 ASMDD@10 ，这个就是key。

第七关

第七题给出的题目的形式如下： http://3.hackit.sinaapp.com/index.php?file=flag.php

提示是：

Key就在这个页面，不是headers也不是cookie,如果你知道如何读取这个php的源码，key就是你的了

这道题目就是一个典型的文件包含的题目，而且这道题目还需要读取文件的源代码。这篇 php文件包含漏洞 中的题目和本题的题目大致相同。那么我们就使用使用下面的代码来显示页面的源代码。

http://3.hackit.sinaapp.com/index.php?file=php://filter/read=convert.base64-encode/resource=flag.php

网页返回的源代码base64编码代码如下：

PD9waHAKLy9LZXk6QTg5c2FkU0QKPz4KPGgzPktleeWwseWcqOi/meS4qumhtemdou+8jOS4jeaYr2hlYWRlc

解码之后得到key为 Key:A89sadSD

第八关

将文件下载之后发现一个C#编写的exe程序，那么就是一个简单的逆向的题目。使用C#编写的程序，就可以直接使用 IISpy 来看源代码。找出其中的关键代码如下：

string text = string.Empty;for (int i = 0; i <= this.username.TextLength; i++){string arg_A5_0 = text;short num = (short)Encoding.ASCII.GetBytes(this.password.Text[i].ToString())[0];text = arg_A5_0 + num.ToString();}if (text.Equals("837450777811510050")){MessageBox.Show("right!the password is flag!");}else{MessageBox.Show("Error! Try Again");}

其中关键的就在于 (short)Encoding.ASCII.GetBytes(this.password.Text[i].ToString()) 。这段代码就是去除password中的每一个字符，然后获得字符的ACSII码，看最后的ASCII码为 837450777811510050 ，我们得到对应的password为SJ2MNsd2。这个就是key了。

最后，就进入了最后的 闯关成功页面

当自己一路走来，最终到达了这个页面的时候，我还是比较兴奋的，就像是玩游戏最后通关的感觉一样。虽然总体说来这个上面的题目不是很难，其实比较适合刚刚入门CTF比赛的新手，我感觉这个平台上面的题目我也恰好比较适合，在这个平台上面我也学到了很多，尤其是图片的隐写技术。做完了这个平台上面之后，我后来做WHCTF(可以看这篇文章)上面的题目时遇到的图片题目，我还是能够动手的。一段旅途走完了之后，总会有新的收获的。通过这个平台，我学习了很多，我也意识到我需要学习和了解的内容还有很多。路漫漫其修远兮。

最后非常感觉作者提供了一个这样好的平台，让我这样的菜鸟有一个好的练习的地方。最后附上作者的blog地址。 sco4x0’s blog