i春秋python_i春秋CTF web题(1)

原创

weixin_40001245 于 2021-01-14 11:18:29 发布 229 收藏
文章标签： i春秋python
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/weixin_40001245/article/details/112936309
版权

之前边看writeup，边做实验吧的web题，多多少少有些收获。但是知识点都已记不清。所以这次借助i春秋这个平台边做题，就当记笔记一样写写writeup(其实都大部分还是借鉴其他人的writeup)。

本人小白一枚，于是从低分题(简单题)边学边做

这篇随笔会写4道题

0x01：爆破-1

0x02：爆破-2

0x03：爆破-3

0x04：upload

0x01：爆破-1

打开链接，发现一段PHP代码

明确我们的flag在flag.php这个文件里面以注释或者不外显的形式存在。

hello这个变量是我们可控的，并且只能是全是字符，如果有其他则结束。

"$$a"，这里有2个$符号，$a是我们传过去的变量，再加上个$号则又是个变量，于是这里就用到$GLOBALS这个全局变量来访问flag.php里面的变量

顺手贴一下php官方文档对该变量的定义

于是构造url

http://97104ae4f3174765a9e2f59dc028fc4553582fd8eeb54f81.game.ichunqiu.com/?hello=GLOBALS

回显：

发现flag(话说题目提示6位，GLOBALS不应该7位吗？)

0x02:爆破-2

点进去也是一段PHP代码

var_dump函数是会将变量内容输出来并加上变量的类型

因为外围有个eval()函数，说明可以我们变量内容如果是一个语句的话是可以执行的

因此我们要控制hello里面的值，用它来读出flag.php文件

构造url：

http://62c123bf4f8a456a870a0b3a3841acde07a12dce89ee48a3.game.ichunqiu.com/?hello=file_get_contents('flag.php')

回显：

string(83)，是回显了了个83长度的字符串，但是这里并不完全，查看源码：

发现flag

0x03：爆破-3

打开链接，又是一段php代码.....

这段代码意思是创建一个会话内容，并存在120秒，初始值 whoami = 'ea'; num = 0

在num = 10的情况打印出我们的flag

那么num++的条件是参数value的前2个字符和whoami的内容匹配，然后whoami又会随机生成2个数并输出

后面一个substr(md5($value), 5, 4) == 0 这个好办，因为md5()这个函数参数如果为数组就会返回false，也就是满足 == 0

我们手动打入vlaue[]=ea

这里要写到python脚本，(其实120秒内10个也可以一个一个试出来)

importrequests

url= 'http://2db8577cbeff436c92a5a69276b7f5aba502655072244904.game.ichunqiu.com/?value[]='s=requests.Session()

payload= 'ea';

r= s.get(url+payload)printr.text

i=0for i in range(10):

payload= r.text[0:2]

r= s.get(url +payload)print r.text

最先写的时候直接用r = requests.get(url + payload)来发送请求，但是它只有第一次回显了2个随机字母之后没有回显。

然后我稍加思考，难道是session有什么特别的回显方式吗？

最后是这样的，在我们一次session会话中，如果中途关闭这个页面，再打开不管你还没到120秒，都会重新创建新的会话，然后初始值为ea和num为0

所以在开头 s = requests.Seesion()里面一定要保证，这次payload传输是在一次会话(不关闭页面)进行的，通过对s进行get操作，就可以保证每次都是在s这个session中完成的。

最后我们在第10次显示后发现flag。

0x04:upload

打开链接，发现是个上传页面

丢个php的一句话木马上去

回显成功

访问我们的木马：

http://53c3f44f7ae4492fa1a2b13462bc12ae1e458361aa104f95.game.ichunqiu.com/hack.php

回显404！！！说明路径不在该web的根目录下

那么上传目录在哪？我重新构造url

http://53c3f44f7ae4492fa1a2b13462bc12ae1e458361aa104f95.game.ichunqiu.com/upload/hack.php

也是返回404，冷静下。。。。。

回到上传页面看看源码，发现上传的路径是

这时候重新构造url

http://53c3f44f7ae4492fa1a2b13462bc12ae1e458361aa104f95.game.ichunqiu.com/u/hack.php

回显

估计<?php 是被过滤掉了，百度下php是否能用其他的标签

于是可以写成

访问没有回显，我们试着发点数据过去

但是没有回显，这个地方php也被过滤了，改成大写即可绕过

重写我们的木马

上传后，用菜刀一连，找到html目录下的flag.php

发现flag。

本人的一点小唠叨：18年初才开始接触信息安全，学了几个月膨胀了。然而6月1日的比赛被打自闭了后，和毕业后的学长交流，学长建议学习的时候多做做笔记，写写博客之类的。这也是我第一次写writeup，我想将我遇到的问题和解决办法详详细细的记录下来。写这4题的writeup的时候，我是前一天都看着别人writeup做好的，然而在今天写writeup的时候，还是在第三和第四题之间卡住了。第三题，我其实不会用python，在调用requests中遇到了些麻烦，但是我希望自己writeup尽可能详细，不要出现模棱两可的情况，于是终于完全弄懂这个session的问题。第四题我记得是用script language和大写绕过，但是在自己做的时候language少了一个字母，搞了半天。script language = "phP" 在phP上没加 " " 又搞了半天，还以为eval函数被过滤掉了，再者不知道为啥hackbar也有点问题。最后终于解决这些小毛病。其实自己看着别人writeup做一遍，和自己写writeup又是两种感觉，自己写writeup的时候发现自己还是有许许多多的细节毛病，这四道题真的都不难，看writeup写的时候，1个小时不到就做完了，但是自己写writeup，写了接近3小时了。通过这些写writeip真的又学习到了很多。以后我都会记录自己做的有意义的题的writeup。