论剑场部分web题的writeup

原创

m0_45118974 于 2019-11-16 23:03:03 发布 136 收藏

文章标签： web安全

本文链接：https://blog.csdn.net/m0_45118974/article/details/103098490

论剑场部分web题的writeup

论剑场

web1

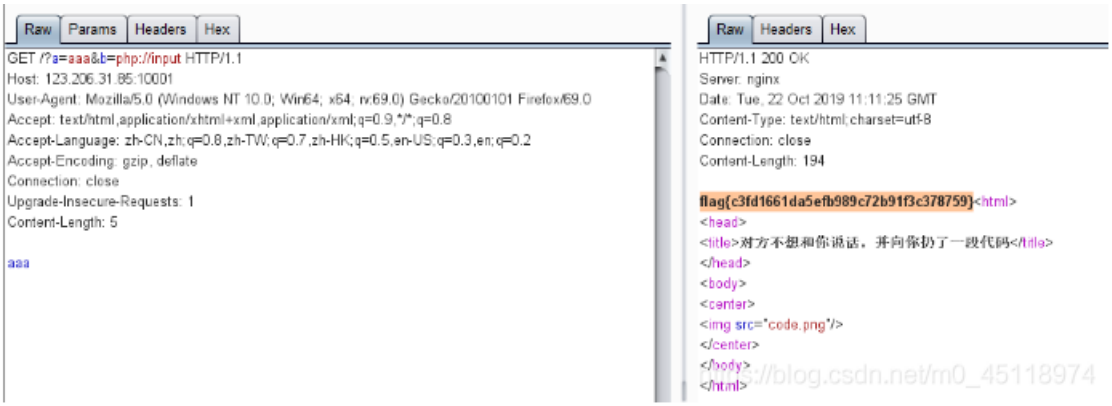
变量覆盖漏洞—extract()函数

extract()函数使用数组键名作为变量名，使用数组键值作为变量值。但是当变量中有同名的元素时，该函数默认将原有的值给覆盖掉。这就造成了变量覆盖漏洞。

file_get_contents()函数是将文件读入一个字符串中，但是b是一个字符串，所以读出来应该是空，if条件判断a不能是空，所以用php://input来绕过file_get_contents()函数，

payload：http://123.206.31.85:10001/?a=aaa&b=php://input

抓包，在请求主体下加aaa。



web9

提示：put me a message bugku

Bp抓包，改包的一串base64编码，解码的flag

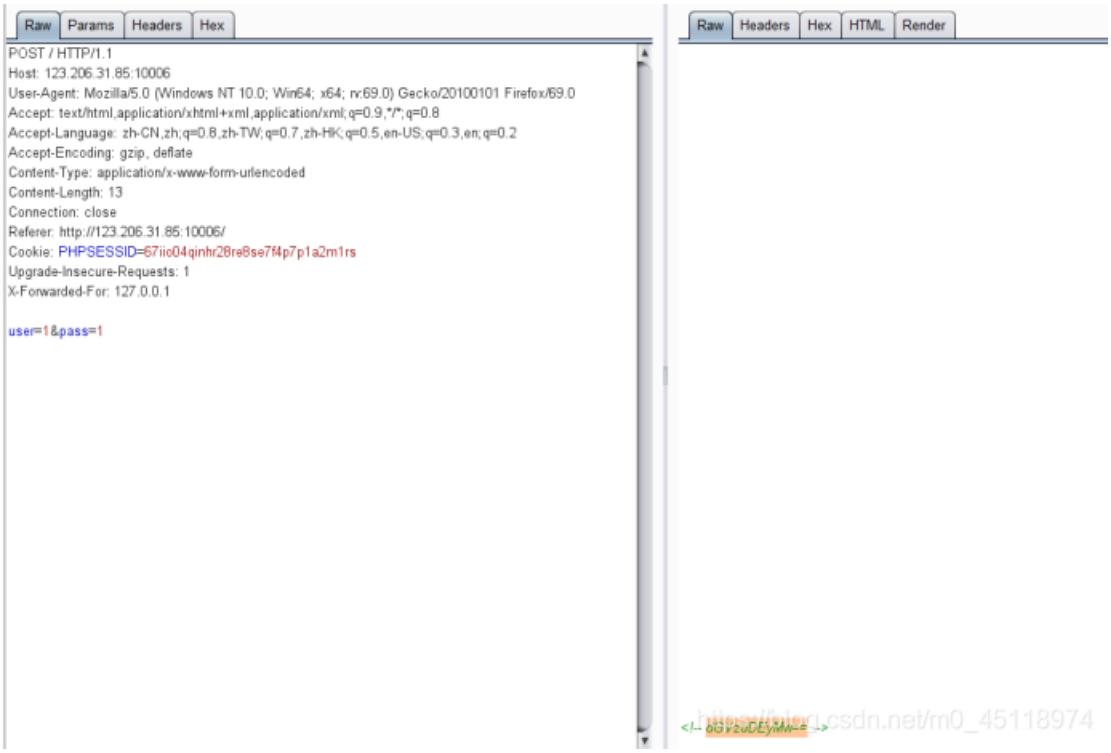
流量分析

没有wireshark……

web2

web6

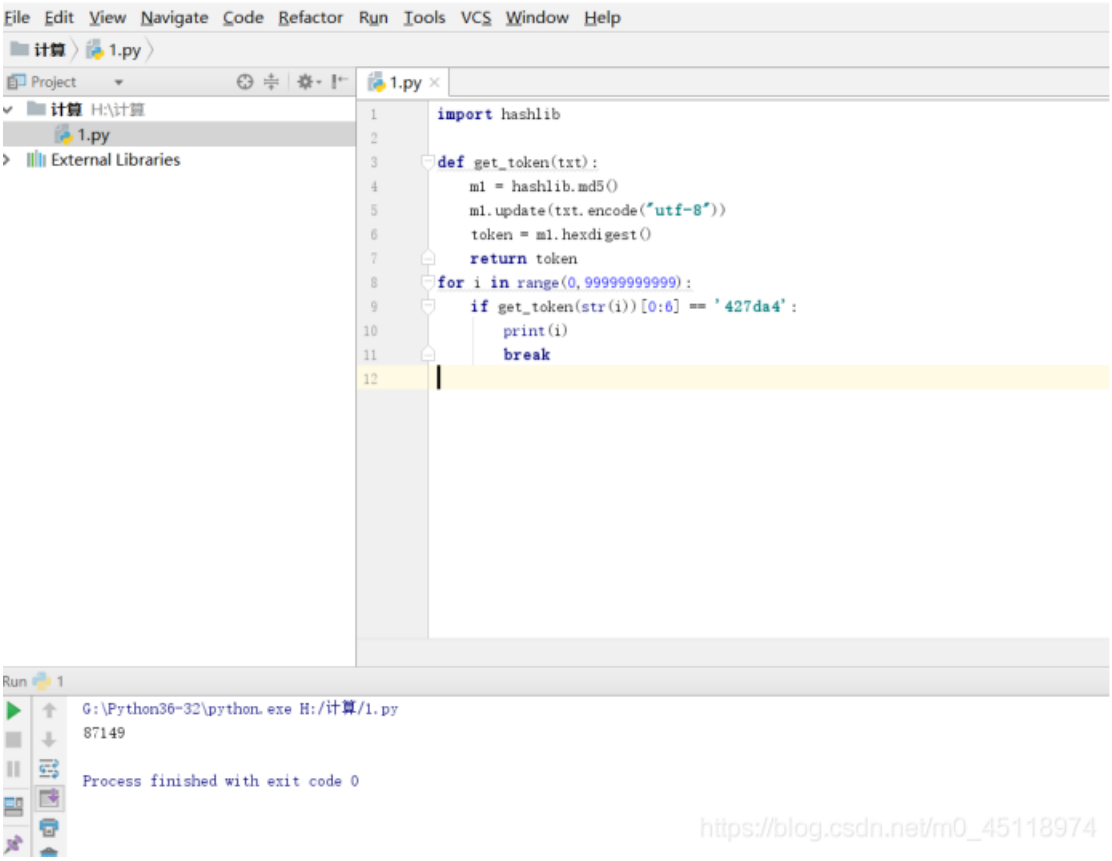
猜一下用户名admin 密码123456访问，提示ip禁止访问，请联系本地管理员登录；bp抓包改请求头X-Forwarded-For: 127.0.0.1；访问，抓包，看到最后有一段被注释的base64编码，在线解码得test123，猜是密码，用户名admin，访问得flag



web11

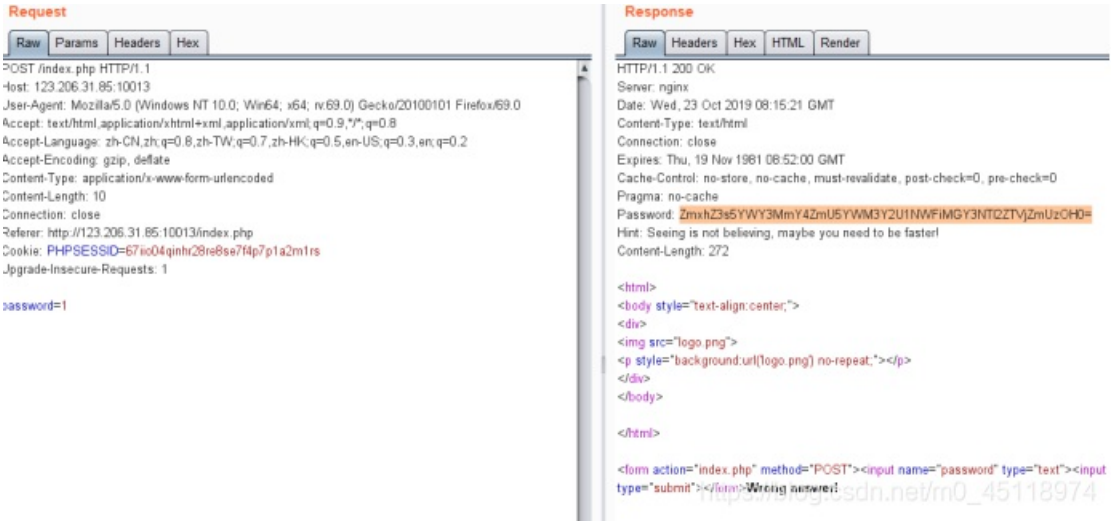
看到提示robots，访问robots.txt;看到shell.php，访问shell.php;看到要求某个值得md5值前六位为427da4，写个python脚本

得到结果为87149，提交查询得flag

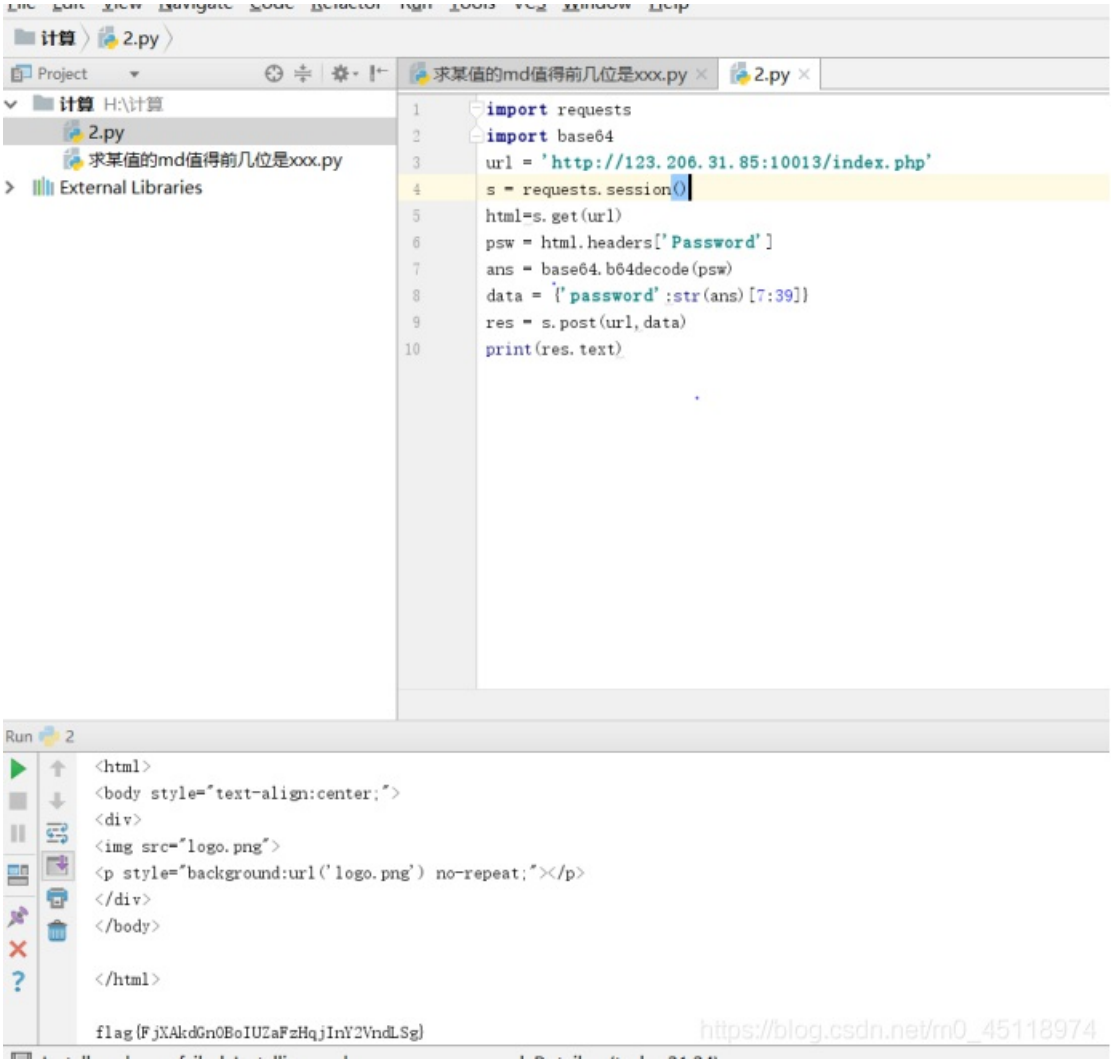


web13

随便输入提交查询，没用；bp抓包，看到响应头里有个passward字段，是base64编码，在线解码得flag



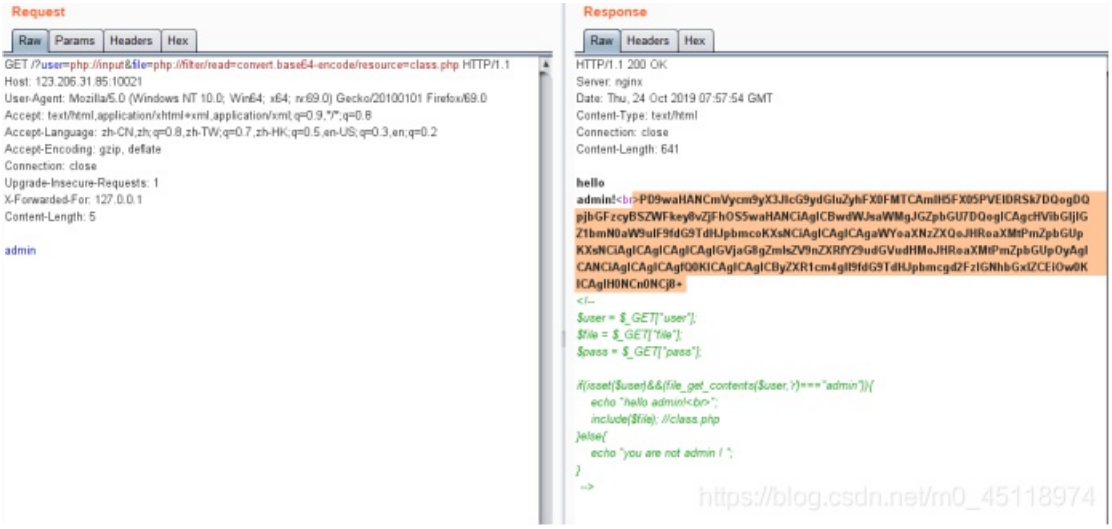
但是提交flag发现不对，把flag{}去掉后提交到输入框中得到：Can you do it faster,让我们快一点，那就用python写个脚本提交



得到flag

web25
什么题目…我的dirsearch实在太慢了，告辞
web3
打开还以为是文件上传漏洞，一句话木马都写好了，怎么绕过都上传不了，看人家的writeup，说是文件包含漏洞，why！！！Payload：php://filter/read=convert.base64-encode/resource=flag

Web21
F12看源码，file_get_contents函数绕过，include（$file）提示class.php，php伪协议读class.php



Base64解码得

堆叠注入
BUUCTF
随便注
堆叠注入定义
Stacked injections(堆叠注入)从名词的含义就可以看到应该是一堆 sql 语句(多条)一起执行。而在真实的运用中也是这样的, 我们知道在 mysql 中, 主要是命令行中, 每一条语句结尾加; 表示语句结束。这样我们就想到了是不是可以多句一起使用。这个叫做 stacked injection。
堆叠注入原理：在sql中，分号是用来表示一条sql语句的结束，试想一下我们在分号结束一个语句后继续构造下一条语句，会不会一起执行？因此这个想法也就早就了堆叠注入，而union injection（联合注入）也是将两条语句合并在一起，两者之间有什么区别？区别就在于union或者union all执行的语句类型是有限的，可以用来执行查询语句，而堆叠注入可以执行的是任意的语句。例如以下这个例子，用户输入：1；DELETE FROM products服务器端生成的sql语句为：（因未对输入的参数进行过滤）Select *from products where productid=1;DELETE FROM products当执行查询后，第一条显示查询信息，第二条则将整个表进行删除。
堆叠注入这种方法可以在select等重要关键字被过滤时考虑使用。
1';show tables;#
1';show columns from `words`;#
1';show columns from `1919810931114514`;#
看到有flag但是select被过滤了，

> 这里是引用

而show命令又不能查看值。这就比较头疼了，不过如果仔细观察的话，一开始过滤的并没有alert 和 rename，我们已经知道了words是用来回显内容的，能不能我们把1919810931114514这个表更改名字为words,并增加相应的字段，使之回显原1919810931114514这个表的内容那，当然是可以的，这种思路。。。大师傅tql
现在常规方法基本就结束了，要想获得flag就必须来点骚姿势了

因为这里有两张表，会县内容肯定是从word这张表中回显的，那我们怎么才能让它回显flag所在的表呢

内部查询语句类似 : select id, data from word where id =

(这里从上面的对word列的查询可以看到它是有两列，id和data)

然后1919810931114514只有一个flag字段

这时候虽然有强大的正则过滤，但没有过滤alert和rename关键字

这时候我们就可以已下面的骚姿势进行注入：

1.将words表改名为word1或其它任意名字

2.1919810931114514改名为words

3.将新的word表插入一列，列名为id

4.将flag列改名为data

> 这里是引用