通达OA前台任意用户伪造登录漏洞复现

原创shiyi Timeline Sec
2020-05-12原文

收录于话题
#漏洞复现文章合集
70个

点击上方蓝色字体关注我们，一起学安全！

本文作者：shiyi（团队正式成员）

本文字数：544

阅读时长：2~3min

声明：请勿用作违法用途，否则后果自负

0x01 简介

通达OA采用基于WEB的企业计算，主HTTP服务器采用了世界上最先进的Apache服务器，性能稳定可靠。数据存取集中控制，避免了数据泄漏的可能。提供数据备份工具，保护系统数据安全。多级的权限控制，完善的密码验证与登录验证机制更加强了系统安全性。

0x02 漏洞概述

该漏洞类型为任意用户伪造，未经授权的远程攻击者可以通过精心构造的请求包进行任意用户伪造登录。

0x03 影响版本

通达OA < 11.5.200417 版本

0x04 环境搭建

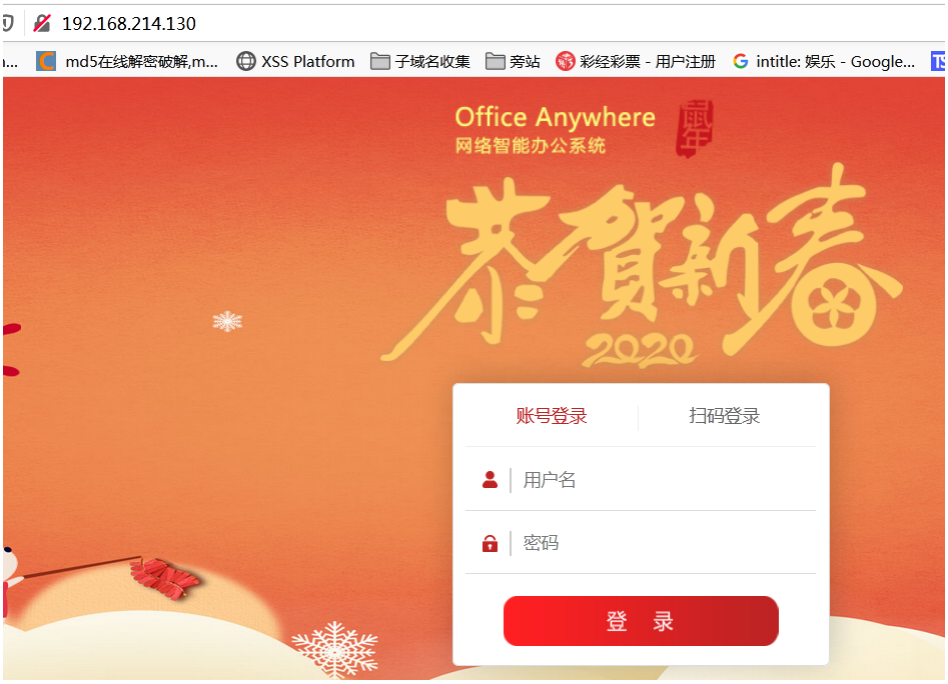
公众号内回复“通达OA环境”获取
使用解密工具对文件解密可获得所有解密代码

解密工具下载链接：
https://paper.seebug.org/203/

用于分析，解密后的部分代码
将通达V11下载后直接运行EXE文件安装，访问localhost即可

0x05 漏洞复现

1、访问通达登录口



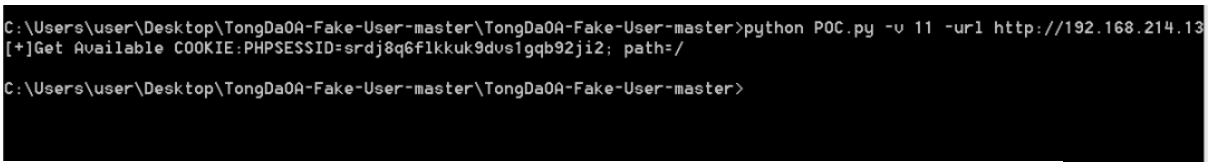
2、POC生成cookie

poc下载地址：

```
https://github.com/NS-Sp4ce/TongDaOA-Fake-User
```

生成cookie命令：

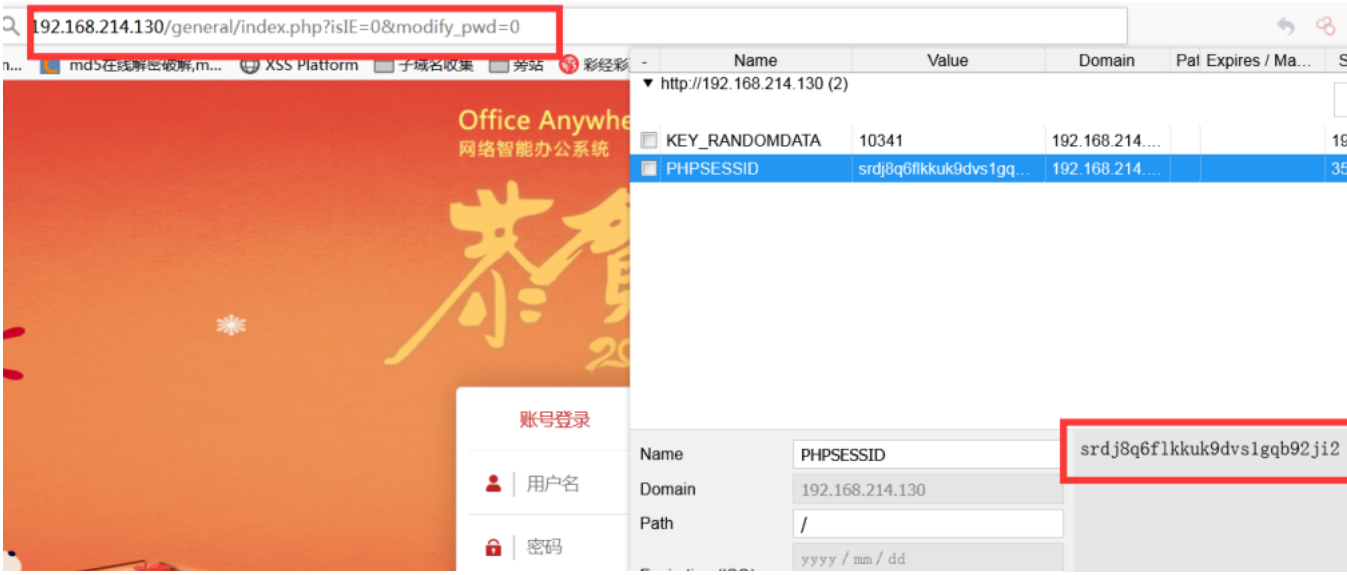
```
python poc.py -v 11 -url target_url
```



3、替换cookie

通过cookie修改插件，替换cookie之后，访问登录后得页面就可以绕过登录了

```
http://192.168.214.130/general/index.php?isIE=0&modify_pwd=0
```



替换cookie后

0x06 修复方式

官方补丁修复或升级最新版本

https://www.tongda2000.com/download/sp2019.php

参 考 链 接 :

https://github.com/NS-Sp4ce/TongDaOA-Fake-User

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

阅读全文