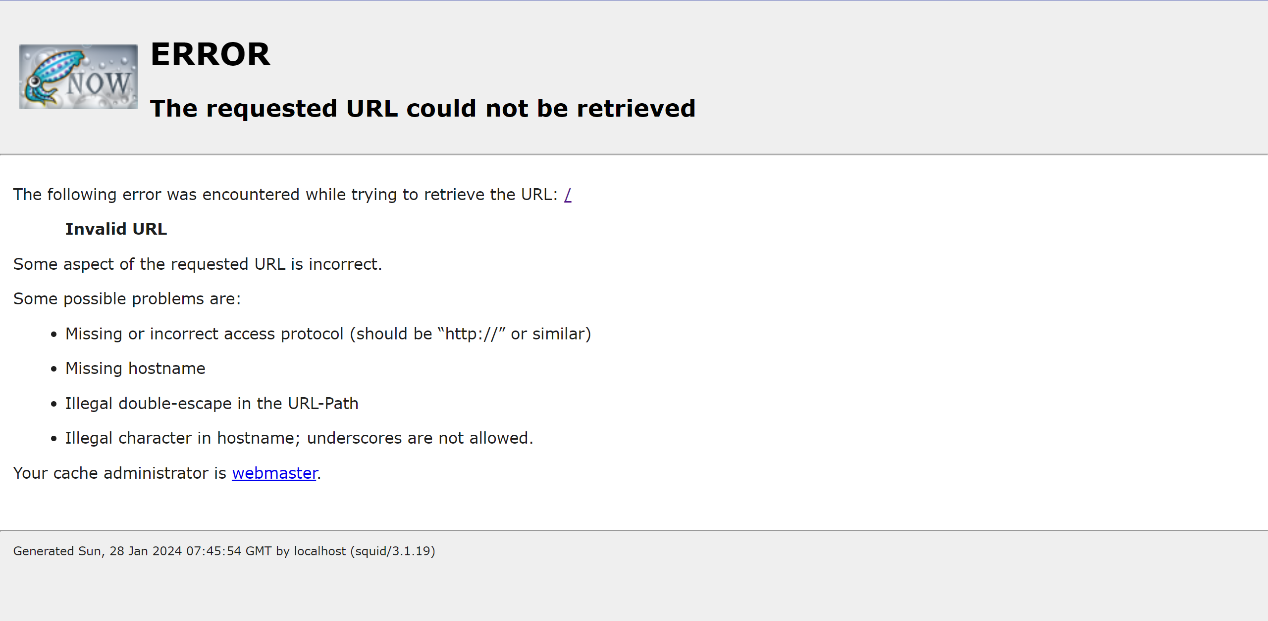
# 一.信息收集

nmap 扫描到目标开放22,8080,3128端口

默认脚本漏洞扫描没有获取到有效信息

# 二.web渗透

查看网页，没有有效信息，http://192.168.153.128:3128

显示请求url不被允许，猜测是开了代理

更具收集到的信息，也显示很多proxy字样，猜测3128作为代理端口，设置浏览器代理

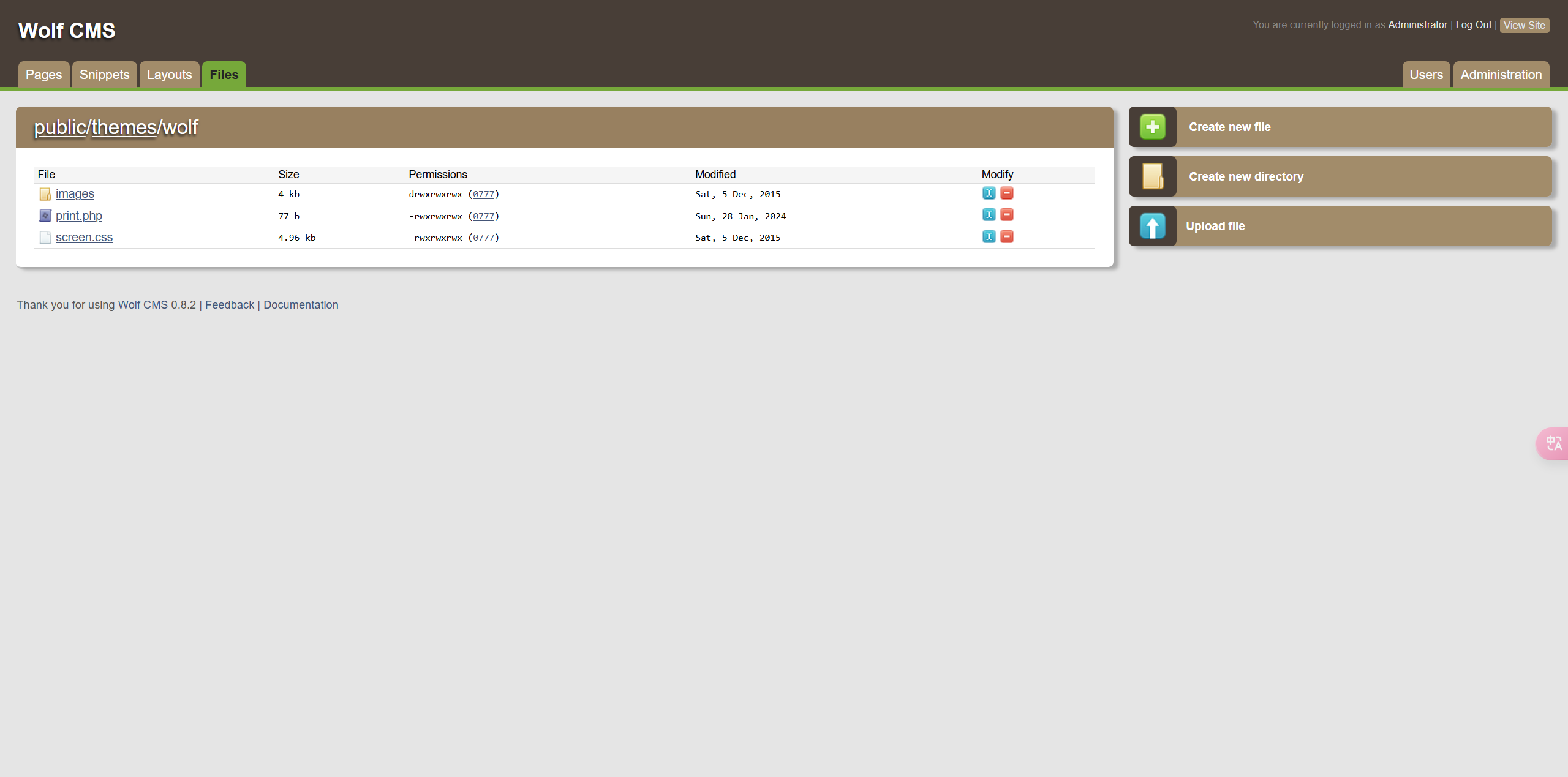
## 路径爆破

爆破出来路径robots.txt,显示有wolfcms路径

对方网站极有可能是wolfcms，信息查询到wolfcms的后台登录路径为/wolfcms/?admin

登录，尝试弱密码登录admin admin登录成功

## 获取初始权限



文件权限为777，修改文件内容为php一句话反弹shell，并且将文件名后缀更改为.php，并开启监听，获取到目标权限。

# 提权

查看到目标config.php文件暴露出信息，数据库root用户密码为john@123

猜测密码复用性，获取root密码为，尝试root登录，但是密码不对

查看/etc/passwd看看可能存在的用户，发现sickos，登录尝试成功

Sudo -l 显示权限为所有