# Holynix

## 信息收集

1. sudo arp-scan -l 收集开放的主机
2. 收集到目标主机开放端口80，且漏洞扫描可能存在sql注入

## Sql注入

注入点是用户登录的密码，构造万能密码即可，不过万能密码是在passwd位置

## 越权

发现可以上传文件，但是上传提示用户不允许，

看看cookie，发现cookie是1，可以修改，将UID=2,登录页面显示出新的用户，

可以上传文件，但是不知道文件上传路径

## 文件包含

在安全一栏，发现url可以构造文件包含，包含了ssl目录下无权访问的transfer.php，发现用户上传文件只能是.tar.gz才能解压为可以允许执行的文件，

## 提权

Mv 和tar root权限且不需要密码，

用mv将目录下的su命令切换为/bin/tar命令,tar修改掉，sudo su即可执行成功