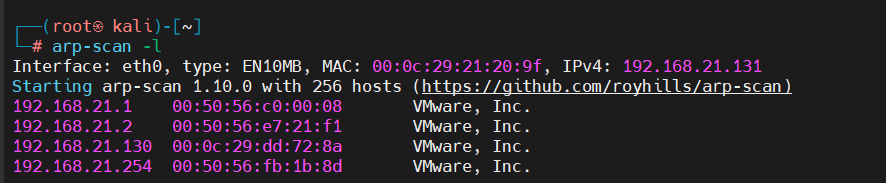
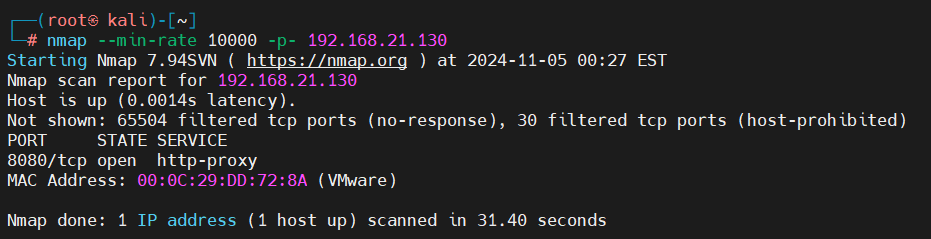
靶机地址：<https://www.vulnhub.com/entry/hackxor-1,19/>

主机发现

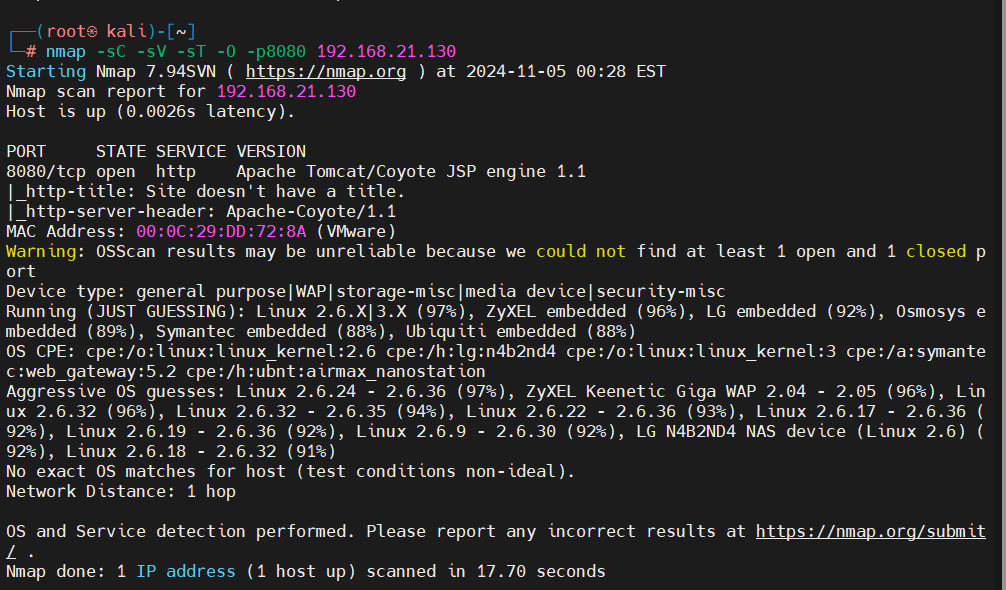


130是靶机

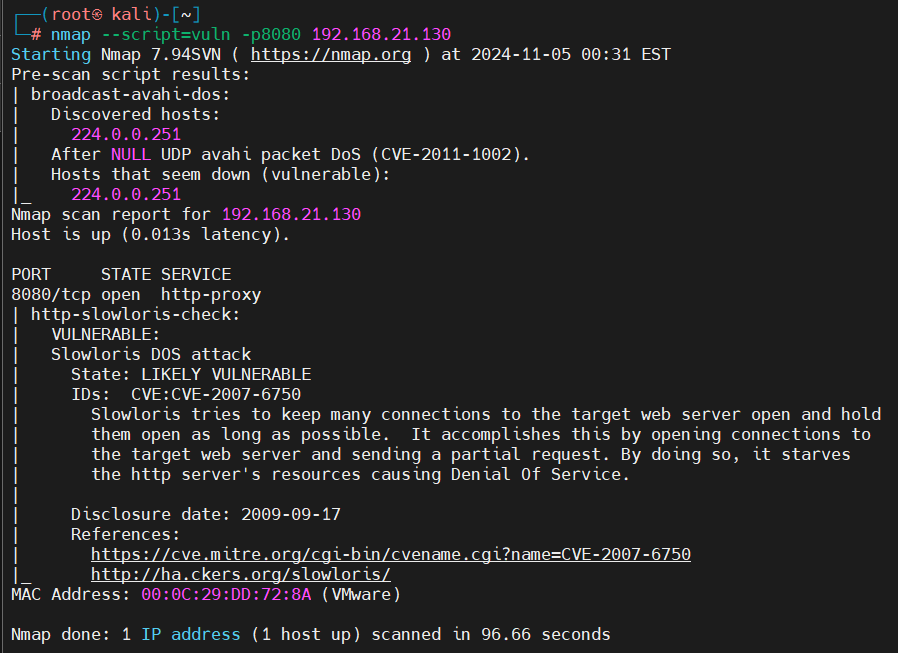
端口扫描



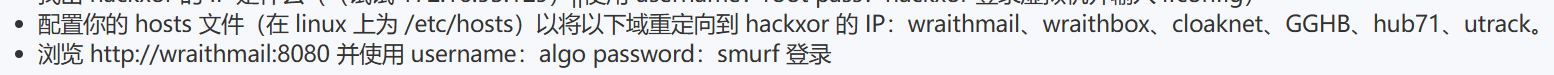
服务扫描

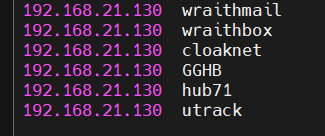


漏洞扫描



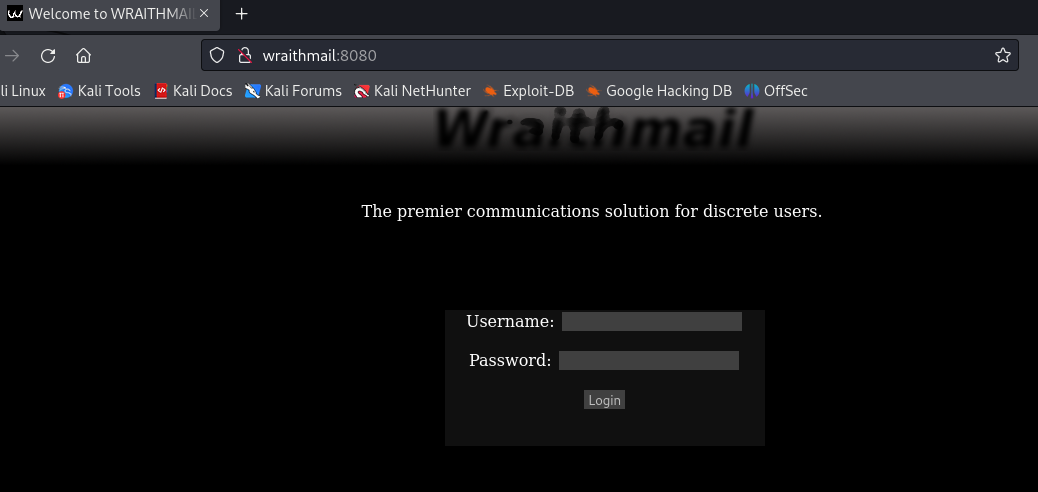
Hosts配置（这个是需要在网上找的，这个是靶机的缘故搭建不完全所以需要自己写hosts）

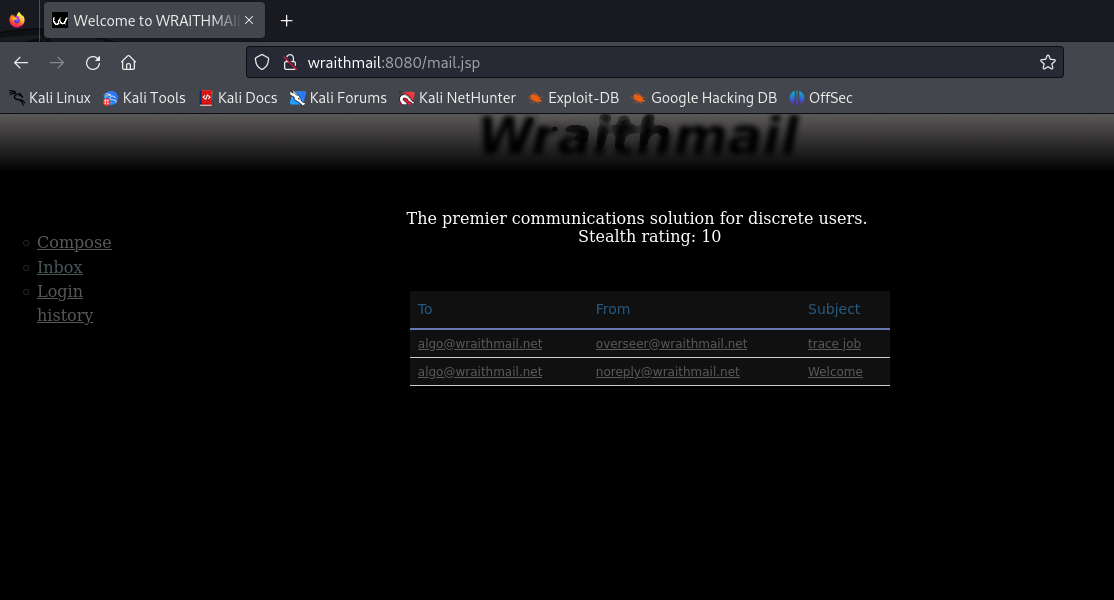


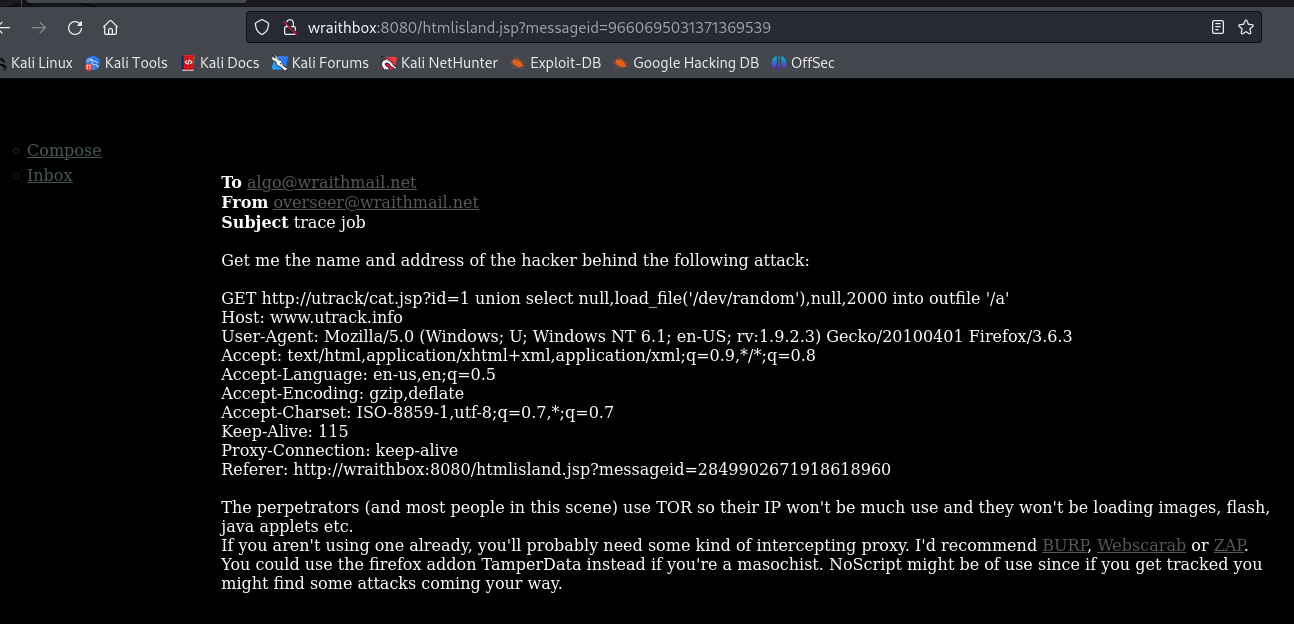




访问wraithmail:8080







数据包



GET http://utrack/cat.jsp?id=1 union select null,load\_file('/dev/random'),null,2000 into outfile '/a'

Host: www.utrack.info

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

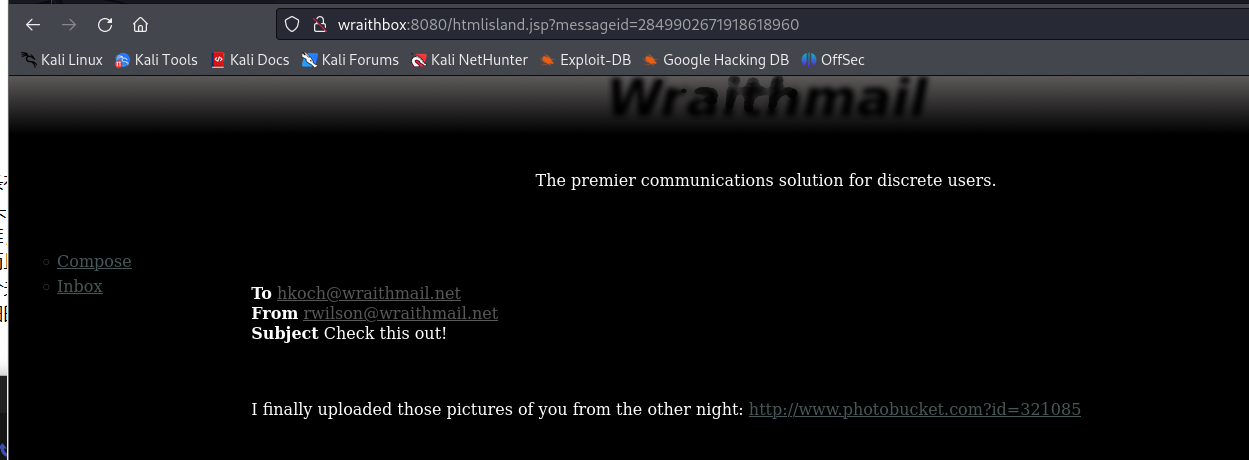
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7

Keep-Alive: 115

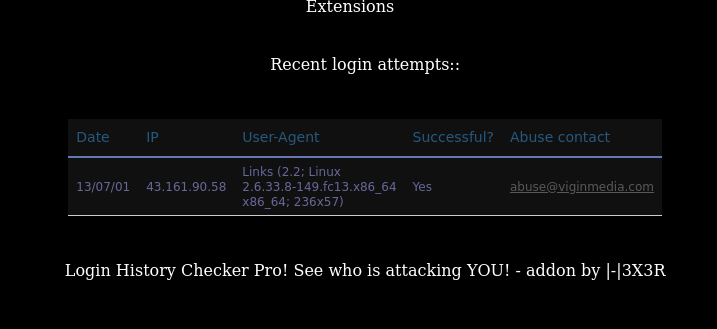
Proxy-Connection: keep-alive

Referer: <http://wraithbox:8080/htmlisland.jsp?messageid=2849902671918618960>

数据包如上，注意referer



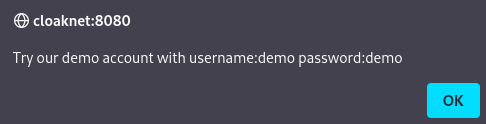




Ip 43.161.90.58

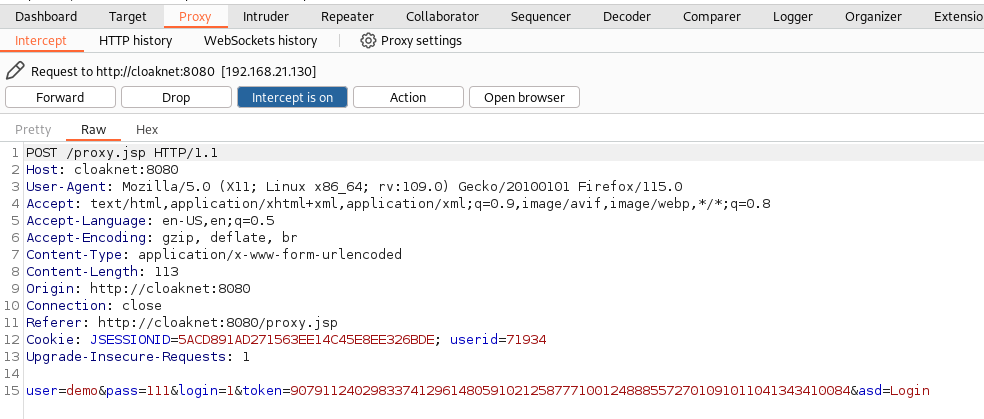
下一关

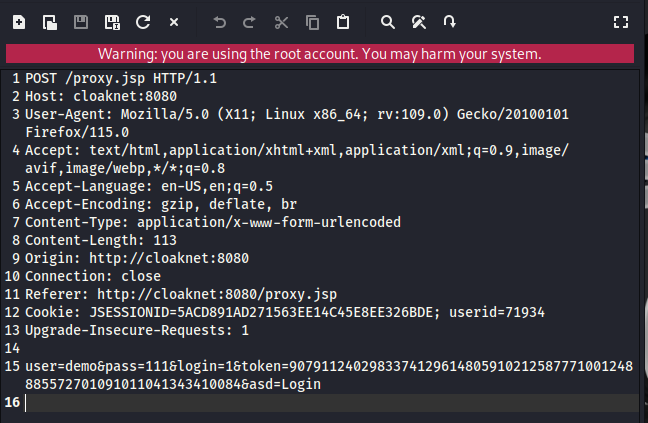
访问http://cloaknet:8080/



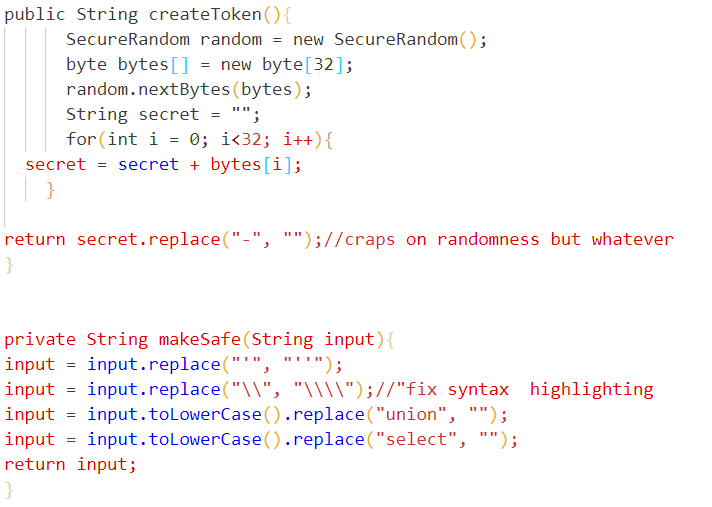


应该是sql注入





https://download.vulnhub.com/hackxor/hackxorSource.7z



替换单引号 转义符union select

你们自己测吧

[**GGHB系列**](http://gghb:8080/)

* 您可能需要使用 wraithmail 发送一些消息。
* 一个电子邮件地址是公开的，另一个可以从用户名中猜出。您可以使用信息泄漏来检查电子邮件地址是否存在
* 受害者不会点击链接，但您可以在消息中输入 javascript......
* 如果您的攻击是基于时间/顺序的，请记住 TOR 速度慢且不可靠。
* 有时偷饼干并不能解决问题。
* 管理面板可能在哪里？

**[集线器71](http://hub71:8080/)**

* 开发人员了解一点安全性，只信任 .txt，但除此之外是一个糟糕的程序员。
* 尝试理解本网站使用的 CSRF 辩护。
* 有时你必须做一些非常不合逻辑的事情才能成功。
* 我保证，这个水平并非不可能。

剩下的两关提示