**Bludit 3.9.2 Directory Traversal漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

远程用户可以滥用图像上载功能中的uuid参数，以将恶意有效负载保存到服务器上的任何位置，然后使用自定义.htaccess文件绕过文件扩展名检查，以最终获得远程代码执行。

# 二、机理分析

## 1、RCE漏洞

**影响版本：** 3.9.2

**漏洞编号：CVE-2019-16113**

1. 创建一个包含PHP payload的png文件，然后将png文件上传到/bl-content/tmp目录下。需要管理员账户以便访问/bl-content/tmp目录。

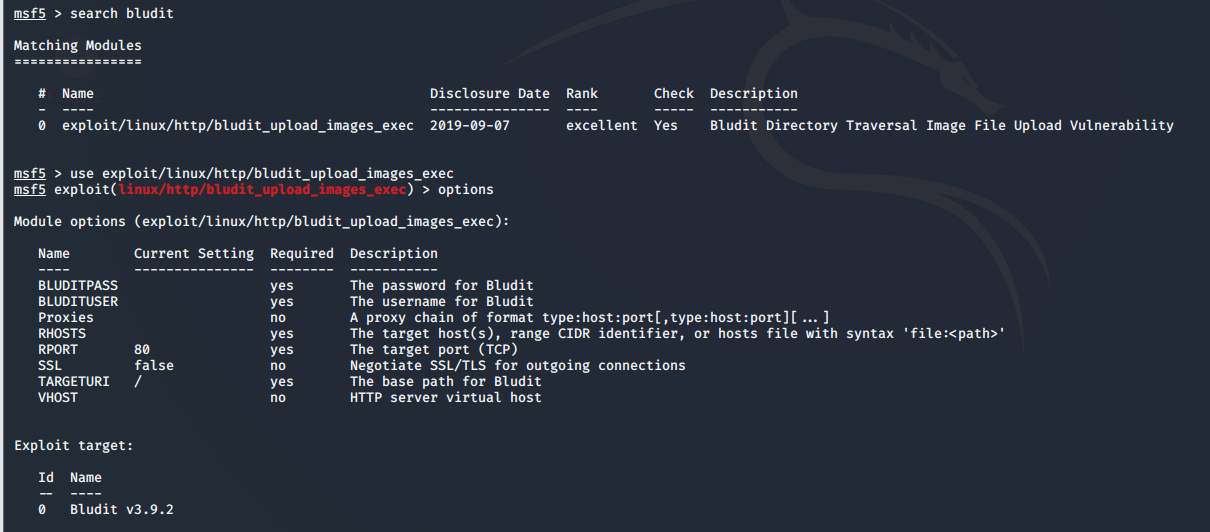
2. 创建可以将png解析为php的.htaccess文件，然后将.htaccess上传到/bl-content/tmp目录，这样/bl-content/tmp目录下png文件相当于php文件来解析，同样可以执行png文件中的php代码。

3. 访问png路径执行php代码。

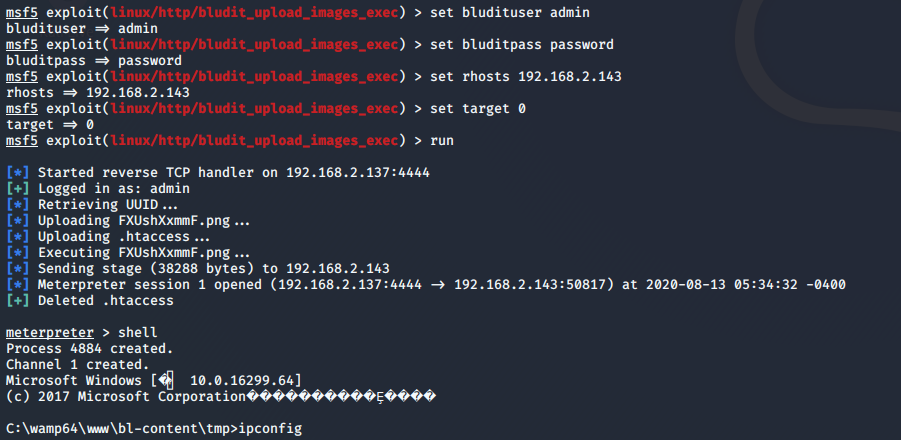
# 三、攻击路径

Metasploit中已有响应EXP，可以方便测试。

使用模块exploit/linux/http/bludit\_upload\_images\_exec



设置好参数执行即可获得反弹shell



# 四、防御方案

升级版本