桂林电子科技大学 2022-2023 学年 第 1 学期

网络渗透测试实验报告

实验名称	**实验四 CTF 实践**		
院　　系	**计算机与信息安全学院**	专业	**信息安全**
学　　号	**2100300124**	姓名	**马驰**
同 作 者			
实验日期	**2022** 年 **11** 月 **16** 日		

辅导教师意见：

成绩　　教师签名：

1. 实验目的和要求

实验目的：通过对目标靶机的渗透过程，了解 CTF 竞赛模式，理解 CTF 涵盖的知识范围，如 MISC、PPC、WEB 等，通过实践，加强团队协作能力，掌握初步 CTF 实战能力及信息收集能力。熟悉网络扫描、探测 HTTP web 服务、目录枚举、提权、图像信息提取、密码破解等相关工具的使用。

系统环境：Kali Linux 2、WebDeveloper 靶机来源：https://www.vulnhub.com/

实验工具：不限

2. 实验步骤

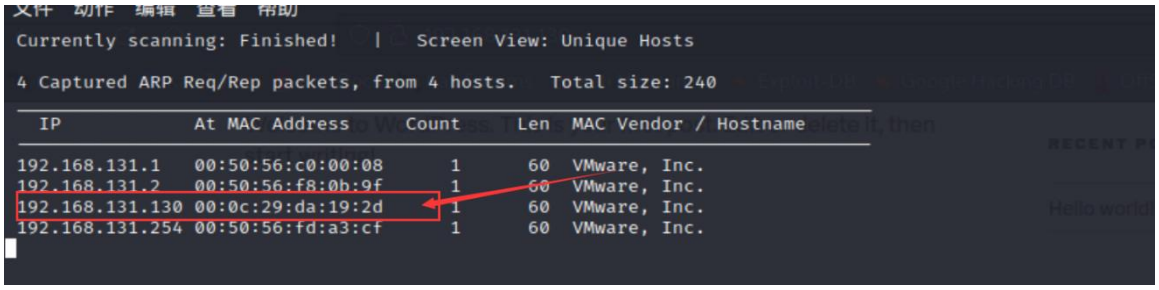
实验步骤和内容：

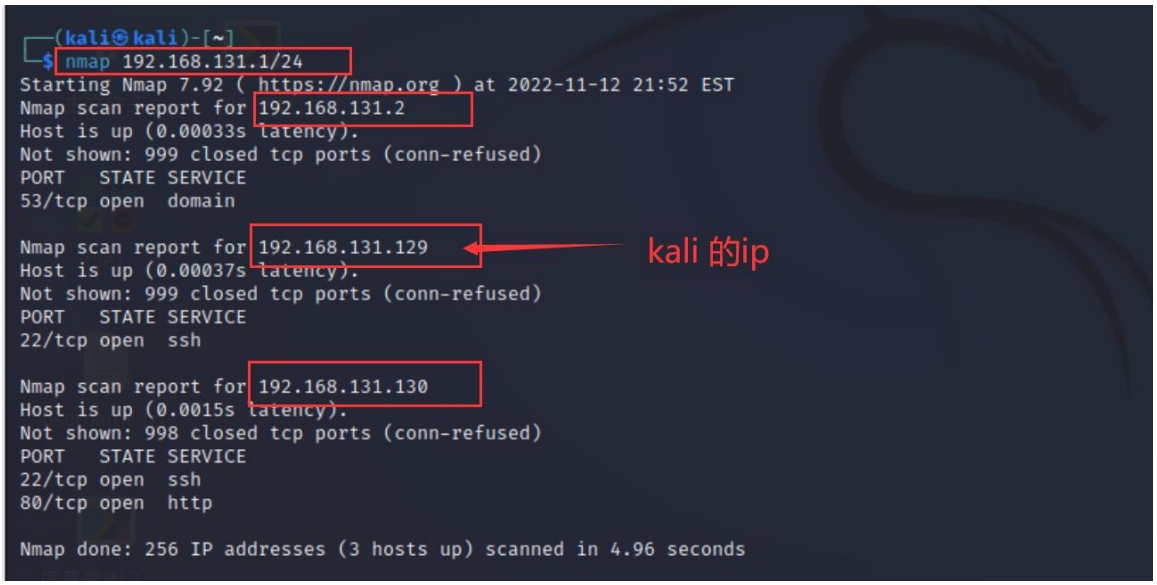
目的：获取靶机 Web Developer 文件/root/flag.txt 中 flag。

基本思路：本网段 IP 地址存活扫描(netdiscover)；网络扫描(Nmap)；浏览 HTTP 服务；网站目录枚举(Dirb)；发现数据包文件 “cap”；分析 “cap” 文件，找到网站管理后台账号密码；插件利用（有漏洞）；利用漏洞获得服务器账号密码；SSH 远程登录服务器；tcpdump 另类应用。

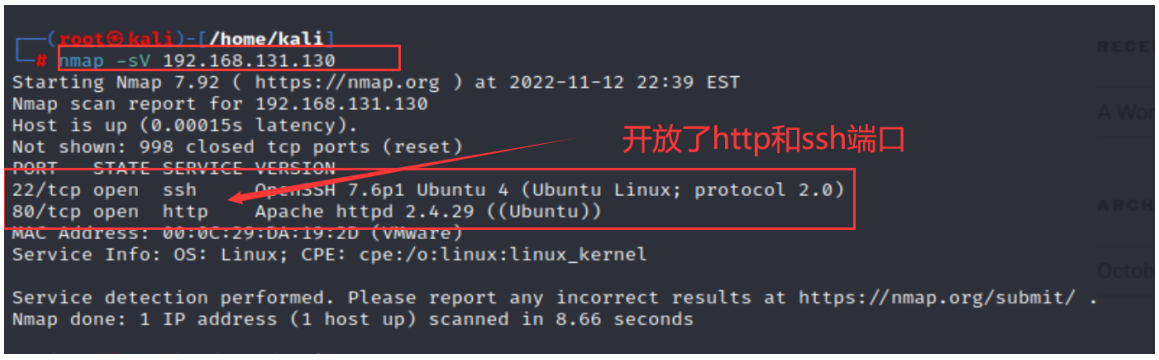
实施细节如下：

1、发现目标 (netdiscover)，找到 WebDeveloper 的 IP 地址。截图。

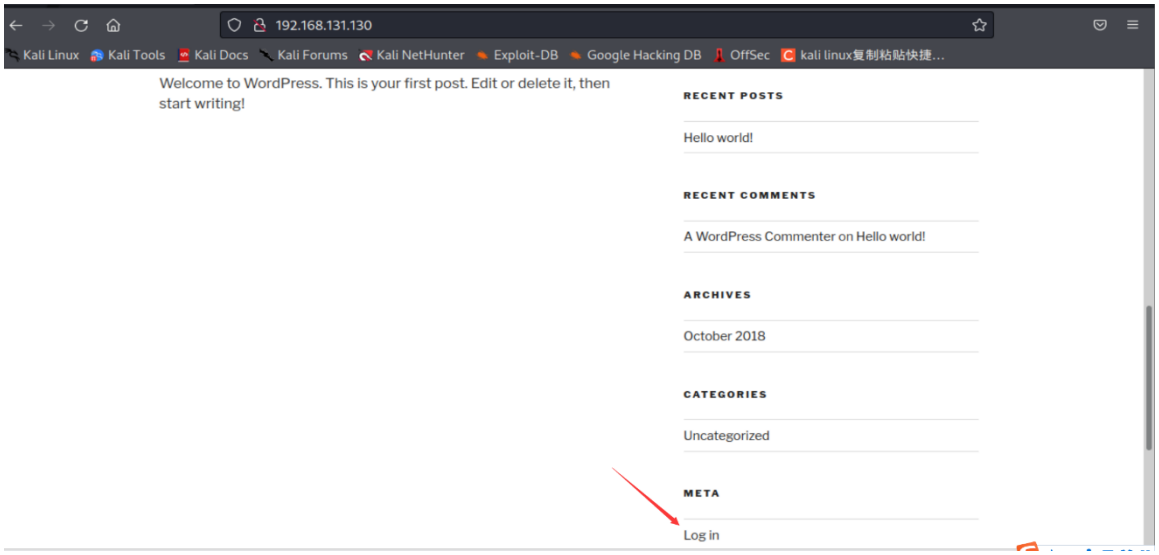




2、:利用 NMAP 扫描目标主机，发现目标主机端口开放、服务情况，截图并说明目标提供的服务有哪些？（利用第一次实验知识点）



3、若目标主机提供了 HTTP 服务，尝试利用浏览器访问目标网站。截图。是否有可用信息？



4、利用 whatweb 探测目标网站使用的 CMS 模板。截图。分析使用的 CMS 是什么？

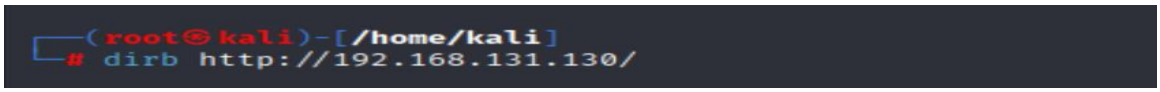
```
┌──(root㉿kali)-[/home/kali]
└─# whatweb 192.168.131.130
http://192.168.131.130 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[192.168.131.130], JQuery[1.12.4], MetaGenerator[WordPress 4.9.8], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[Example site &#8211; Just another WordPress site], UncommonHeaders[link], WordPress[4.9.8]
```

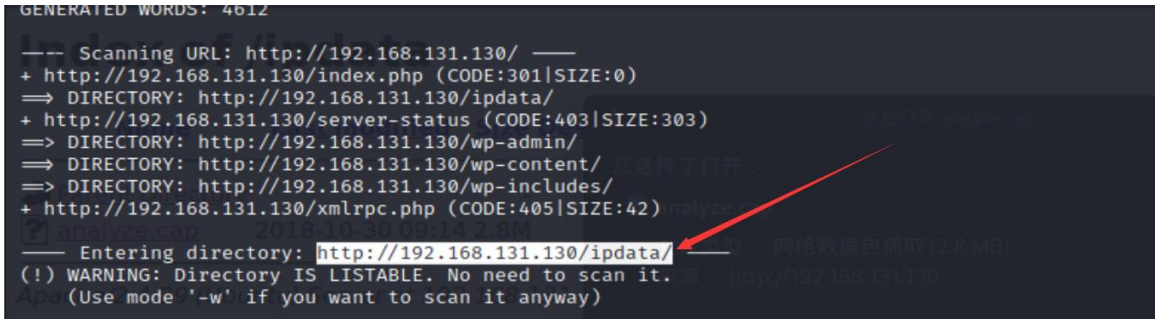
5、网络搜索 wpscan，简要说明其功能。

- WordPress 是全球流行的博客网站，全球有上百万人使用它来搭建博客。他使用 PHP 脚本和 Mysql 数据库来搭建网站。
- Wordpress 作为三大建站模板之一，在全世界范围内有大量的用户，这也导致白帽子都会去跟踪 WordPress 的安全漏洞，Wordpress 自诞生起也出现了很多漏洞。Wordpress 还可以使用插件、主题。于是 Wordpress 本身很难挖掘什么安全问题的时候，安全研究者开始研究其插件、主题的漏洞。通过插件，主题的漏洞去渗透 Wordpress 站点，于是 WPScan 应运而生，收集 Wordpress 的各种漏洞，形成一个 Wordpress 专用扫描器

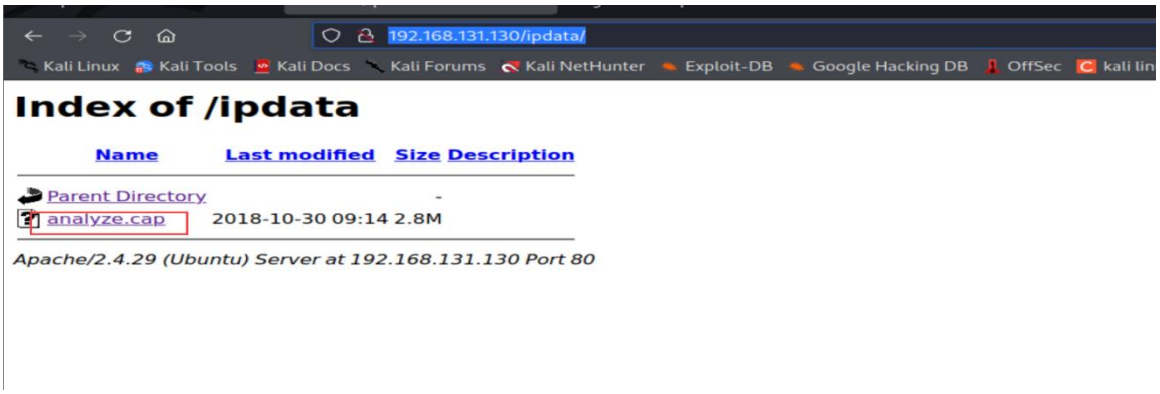
- WPScan 是一个扫描 WordPress 漏洞的黑盒子扫描器，它可以为所有 Web 开发人员扫描 WordPress 漏洞并在他们开发前找到并解决问题。我们还使用了 Nikto ，它是一款非常棒的 Web 服务器评估工具，我们认为这个工具应该成为所有针对 WordPress 网站进行的渗透测试的一部分
- WPScan 是 Kali Linux 默认自带的一款漏洞扫描工具，它采用 Ruby 编写，能够扫描 WordPress 网站中的多种安全漏洞，其中包括 WordPress 本身的漏洞、插件漏洞和主题漏洞。最新版本 WPScan 的数据库中包含超过 18000 种插件漏洞和 2600 种主题漏洞，并且支持最新版本的 WordPress。值得注意的是，它不仅能够扫描类似 robots.txt 这样的敏感文件，而且还能够检测当前已启用的插件和其他功能
- 该扫描器可以实现获取站点用户名，获取安装的所有插件、主题，以及存在漏洞的插件、主题，并提供漏洞信息。同时还可以实现对未加防护的 Wordpress 站点暴力破解用户名密码。

6、使用 Dirb 爆破网站目录。（Dirb 是一个专门用于爆破目录的工具，在 Kali 中默认已经安装，类似工具还有国外的 patator，dirsearch，DirBuster， 国内的御剑）截图。找到一个似乎和网络流量有关的目录（路径）。

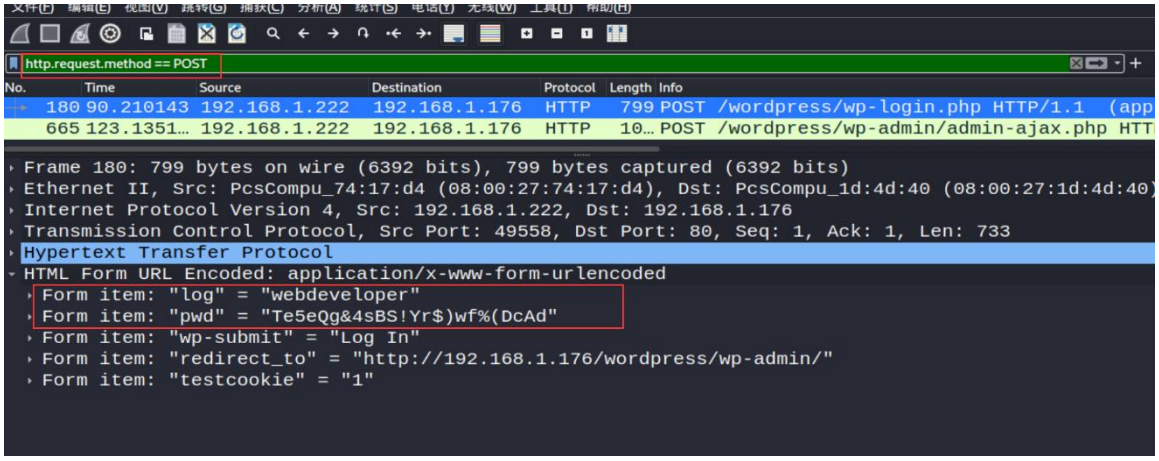




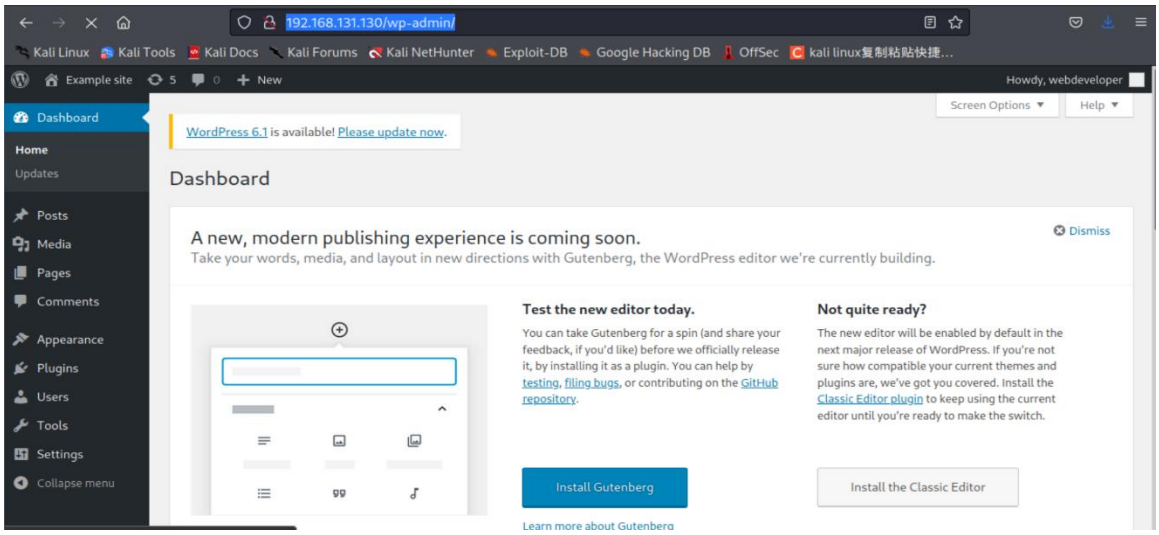
7、浏览器访问该目录（路径），发现一个 cap 文件。截图。



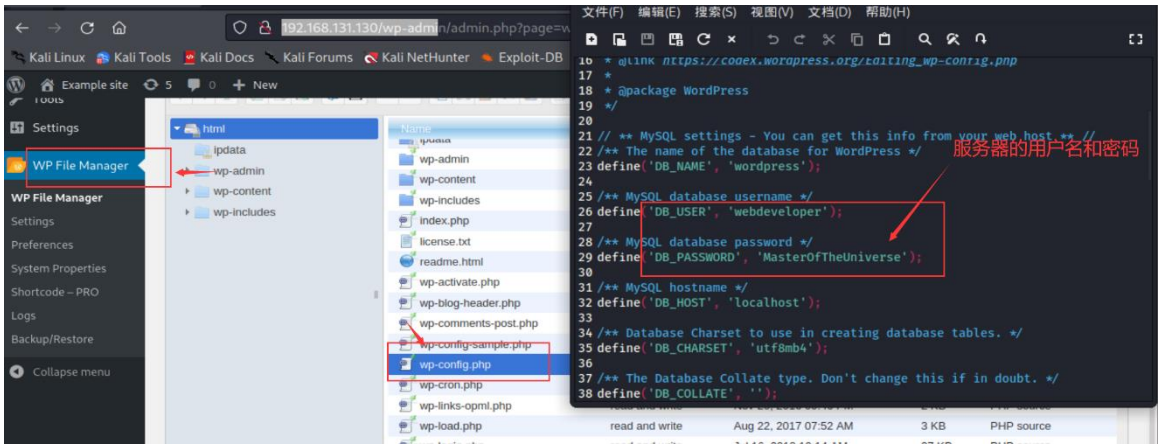
8、利用 Wireshark 分析该数据包，分析 TCP 数据流。找到什么有用的信息？截图。

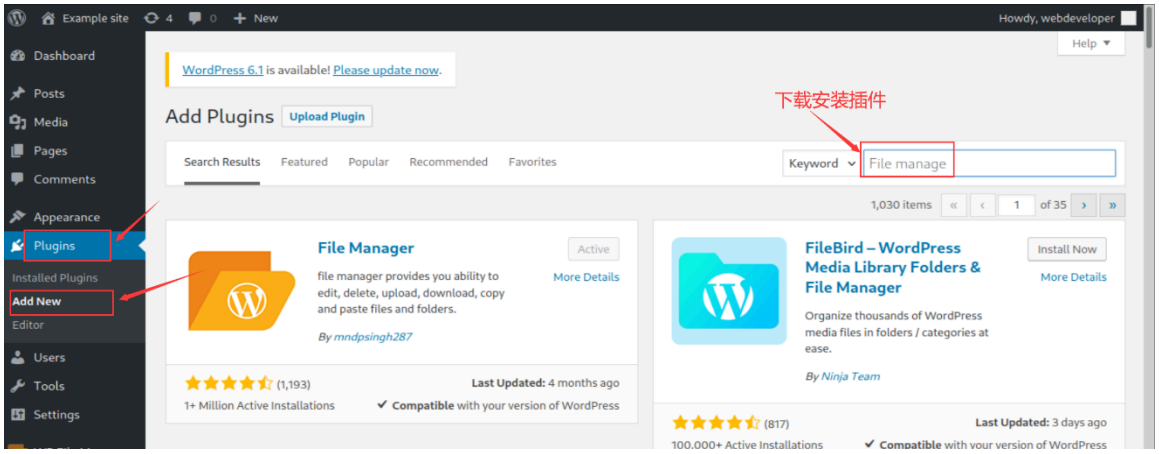


9、利用上一步得到的信息进入网站后台。截图。



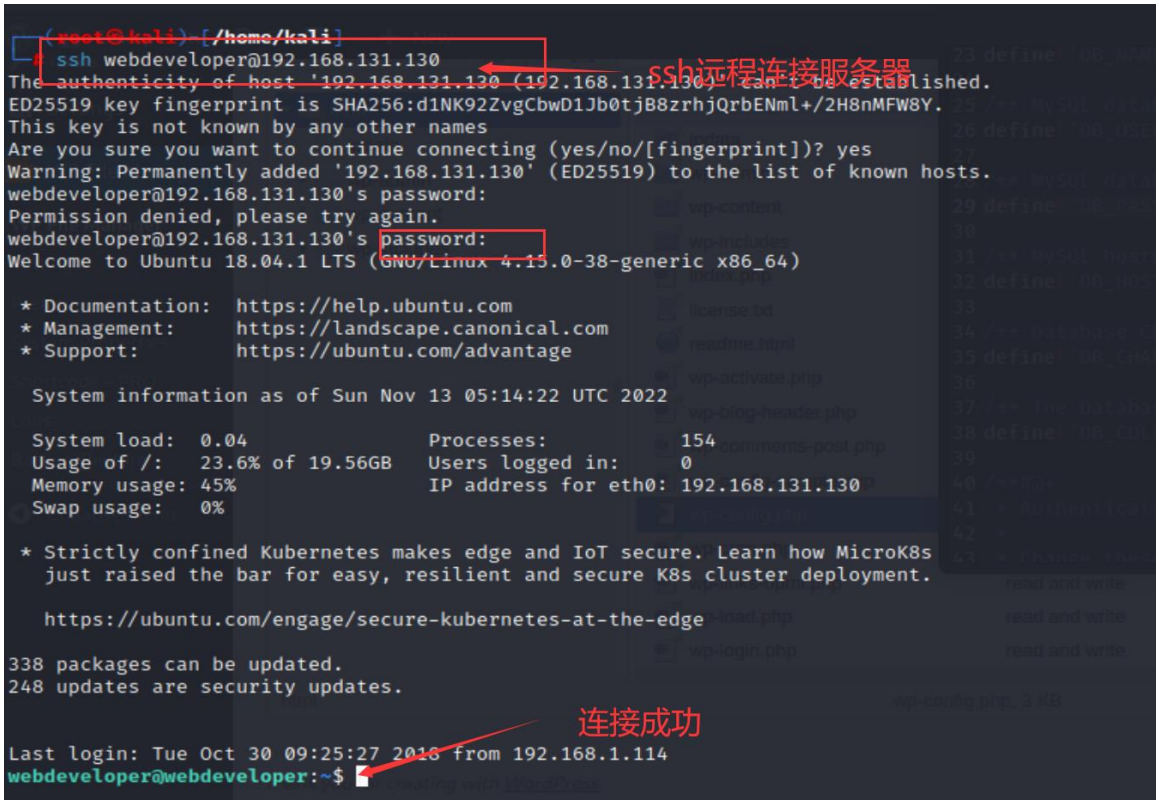
10、利用该 CMS 存在的（插件 Plugin）漏洞。



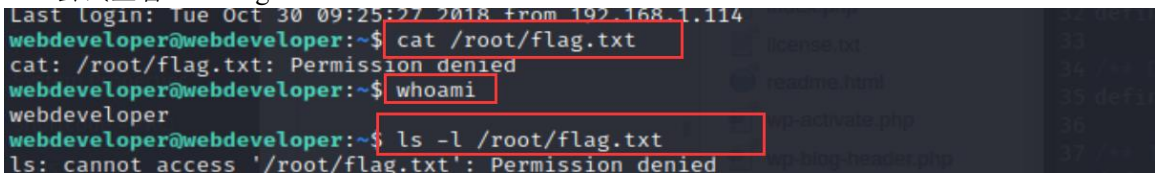


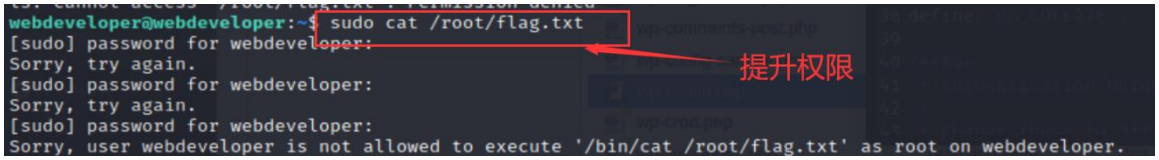
11、利用该插件漏洞提权。

尝试利用上一步获得的访问数据库的用户名和密码连接远程服务器。截图。



1、尝试查看/root/flag.txt





均无法查看。

2、使用 tcpdump 执行任意命令（当 tcpdump 捕获到数据包后会执行指定的命令。）

查看当前身份可执行的命令

发现可以 root 权限执行 tcpdump 命令

3.创建攻击文件->写入 shellcode->赋予可执行权限->利用 tcpdump 执行任意命令

3. 实验小结

首先，利用网络扫描工具扫描同一子网下的主机，根据 ip 的对比和开放端口的数量发现目标主机。其次，扫描目标主机的开放的端口，发现其 80 端口是开放的，从而它提供 http 服务。紧接着在浏览器中访问它，发现有登录的模块。但此时并不知道用户和密码，然后利用爆破工具对网站的目录进行爆破，通过观察寻找，发现一个似乎与网络流量有关的目录（ipdata），猜测这个流量中可能有登录网站后台的账户和密码（可能是“工作人员”登录时发送的报文）。在浏览器中访问这个目录，发现其中有一个 cap 文件，根据 wireshark 使用经验，它是一个数据包。那么用其默认的 wireshak 打开它，利用登录服务器时发送的 http 请求进行过滤，猜想即可获得验证，发现登录网站后台

的用户名和密码。果断登录网站，在插件安装界面安装带有漏洞的插件 file mangage，在其的配置文件 wp_config.php 发现可以登录网站数据库的账户密码。最后远程登录网站数据库，测试在其数据库中是否能直接发现 flag 文件，显然不行，但是发现可以用 root 权限执行 tcpdump 命令的细节。通过查看 tcpdump 工具的使用方法，先创建一个打开 flag 文件的脚本(赋予它可执行权限)，用 tcpdump 执行该脚本，最后得到 flag 对应的字符串。