

CTF实践

原创

楊雨欣同學 于 2020-12-24 20:46:39 发布 98 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/Yangyuxin0228/article/details/111655428>

版权

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

实验原理：

1、什么是CTF

CTF (Capture The Flag) 中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

1.1 CTF竞赛模式

(1) 解题模式 (Jeopardy) 在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

(2) 攻防模式 (Attack-Defense) 在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续48小时及以上），同时也比团队之间的分工配合与合作。

(3) 混合模式 (Mix) 结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。

1.2 CTF各大题型简介

MISC (安全杂项)

全称Miscellaneous。题目涉及流量分析、电子取证、人肉搜索、数据分析、大数据统计等等，覆盖面比较广。我们平时看到的社工类题目；给你一个流量包让你分析的题目；取证分析题目，都属于这类题目。主要考查参赛选手的各种基础综合知识，考察范围比较广。

PPC (编程类)

全称Professionally Program Coder。题目涉及到程序编写、编程算法实现。算法的逆向编写，批量处理等，有时候用编程去处理问题，会方便的多。当然PPC相比ACM来说，还是较为容易的。至于编程语言嘛，推荐使用Python来尝试。这部分主要考查选手的快速编程能力。

CRYPTO (密码学)

全称Cryptography。题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术。这样的题目汇集的最多。这部分主要考查参赛选手密码学相关知识点。

REVERSE (逆向)

题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译扎实功底。需要掌握汇编，堆栈、寄存器方面的知识。有好的逻辑思维能力。主要考查参赛选手的逆向分析能力。此类题目也是线下比赛的考察重点。

STEGA (隐写)

全称Steganography。题目的Flag会隐藏到图片、音频、视频等各类数据载体中供参赛选手获取。载体就是图片、音频、视频等，可能是修改了这些载体来隐藏flag，也可能将flag隐藏在这些载体的二进制空白位置。有时候需要你侦探精神足够的强，才能发现。此类题目主要考查参赛选手的对各种隐写工具、隐写算法的熟悉程度。

PWN（溢出）

PWN在黑客俚语中代表着攻破，取得权限，在CTF比赛中它代表着溢出类的题目，其中常见类型溢出漏洞有栈溢出、堆溢出。在CTF比赛中，线上比赛会有，但是比例不会太重，进入线下比赛，逆向和溢出则是战队实力的关键。主要考察参赛选手漏洞挖掘和利用能力。

WEB（web类）

WEB应用在今天越来越广泛，也是CTF夺旗竞赛中的主要题型，题目涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码审计、上传等漏洞。这些题目都不是简单的注入、上传题目，至少会有一层的安全过滤，需要选手想办法绕过。且Web题目是国内比较多也是大家比较喜欢的题目。因为大多数人开始安全都是从web*站开始的。

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。

先查kali的网关地址，nmcli device show eth0

```
kali@kali:~$ nmcli device show eth0
GENERAL.DEVICE:           eth0
GENERAL.TYPE:             ethernet
GENERAL.HWADDR:          00:0C:29:D1:50:47
GENERAL.MTU:             1500
GENERAL.STATE:           100 (connected)
GENERAL.CONNECTION:      Wired connection 1
GENERAL.CON-PATH:        /org/freedesktop/NetworkManager/ActiveConnection/5
WIRED-PROPERTIES.CARRIER: on
IP4.ADDRESS[1]:          192.168.204.128/24
IP4.GATEWAY:              192.168.204.2
IP4.ROUTE[1]:            dst = 0.0.0.0/0, nh = 192.168.204.2, mt = 100
IP4.ROUTE[2]:            dst = 192.168.204.0/24, nh = 0.0.0.0, mt = 100
IP4.DNS[1]:              192.168.204.2
IP4.DOMAIN[1]:            localdomain
IP6.ADDRESS[1]:          fe80::20c:29ff:fed1:5047/64
IP6.GATEWAY:              --
IP6.ROUTE[1]:            dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:            dst = ff00::/8, nh = ::, mt = 255
```

192.168.204.2

```
Nmap scan report for 192.168.204.126 [host down]
Nmap scan report for 192.168.204.127 [host down]
Nmap scan report for 192.168.204.128
Host is up (0.000099s latency).
Nmap scan report for 192.168.204.129 [host down]
Nmap scan report for 192.168.204.130 [host down]
Nmap scan report for 192.168.204.131 [host down]
Nmap scan report for 192.168.204.132
Host is up (0.0024s latency).
```

可以看出WebDeveloper的ip是192.168.204.132

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

```
kali@kali:~$ nmap 192.168.204.132
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-06 02:36 EST
Nmap scan report for 192.168.204.132
Host is up (0.00078s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

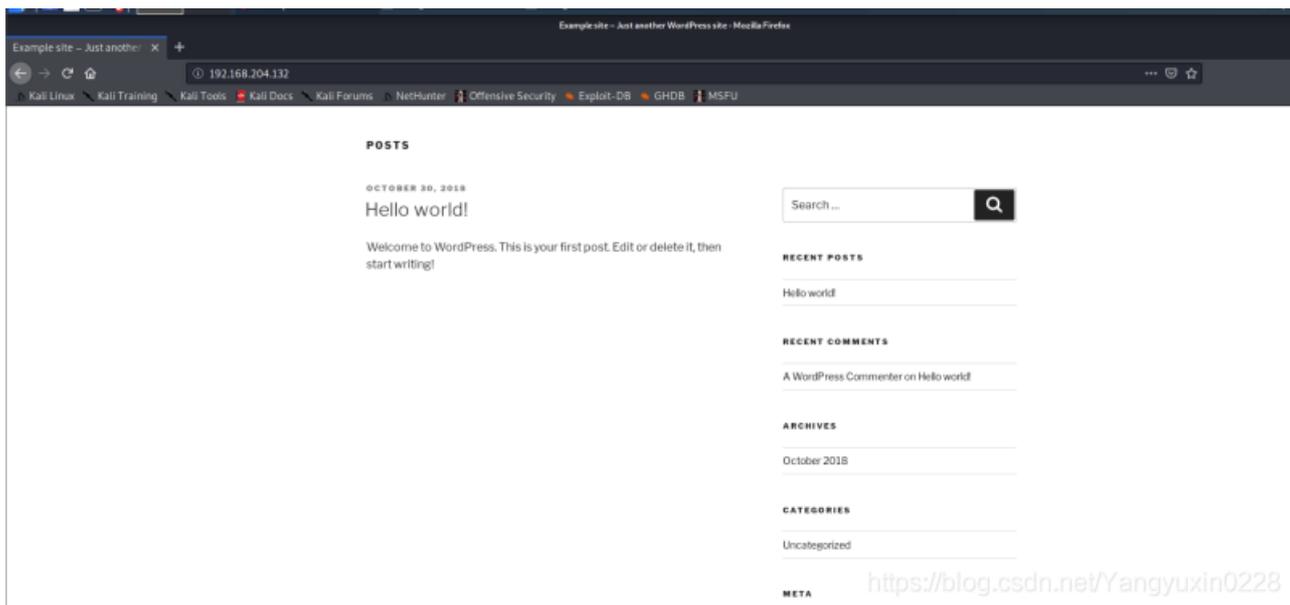
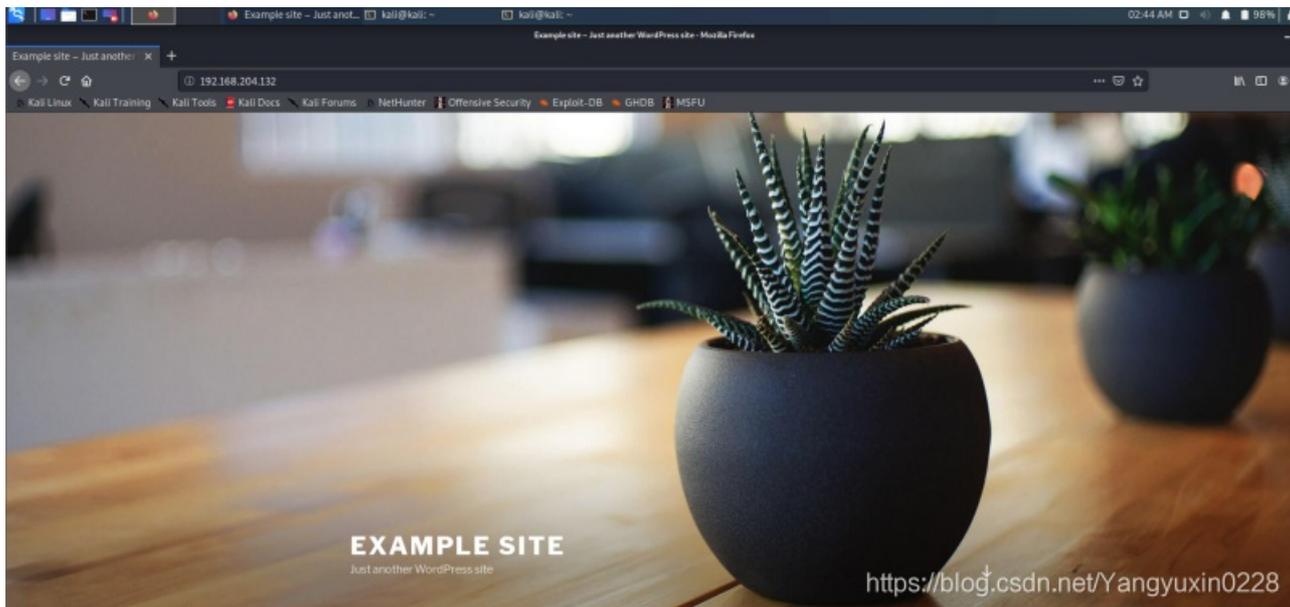
```
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

```
kali@kali:~$
```

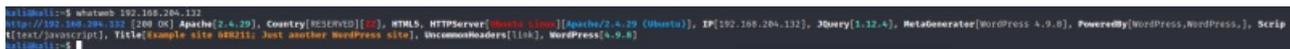
<https://blog.csdn.net/Yangyuxin0228>

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？



该网站的CMS为WordPress

5、网络搜索wpscan，简要说明其功能。

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 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）。

dirb http://192.168.204.132

```
kali@kali:~$ dirb http://192.168.204.132
-----
Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Sun Dec 6 02:59:57 2020
URL_BASE: http://192.168.204.132/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612

--- Scanning URL: http://192.168.204.132/ ---
+ http://192.168.204.132/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.204.132/ipdata/
+ http://192.168.204.132/server-status (CODE:403|SIZE:303)
=> DIRECTORY: http://192.168.204.132/wp-admin/
=> DIRECTORY: http://192.168.204.132/wp-content/
=> DIRECTORY: http://192.168.204.132/wp-includes/
+ http://192.168.204.132/xmlrpc.php (CODE:405|SIZE:42)

--- Entering directory: http://192.168.204.132/ipdata/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.204.132/wp-admin/ ---
+ http://192.168.204.132/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.204.132/wp-admin/css/
=> DIRECTORY: http://192.168.204.132/wp-admin/images/
=> DIRECTORY: http://192.168.204.132/wp-admin/includes/
+ http://192.168.204.132/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.204.132/wp-admin/js/
=> DIRECTORY: http://192.168.204.132/wp-admin/maint/
=> DIRECTORY: http://192.168.204.132/wp-admin/network/
=> DIRECTORY: http://192.168.204.132/wp-admin/user/

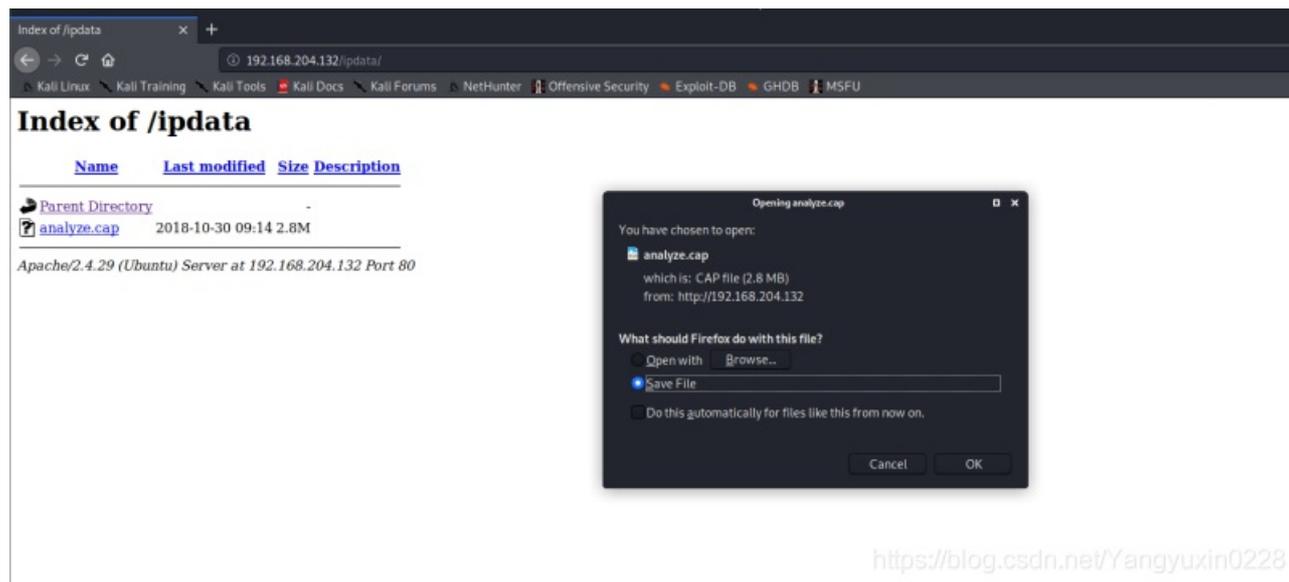
--- Entering directory: http://192.168.204.132/wp-content/ ---
+ http://192.168.204.132/wp-content/index.php (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.204.132/wp-content/plugins/
=> DIRECTORY: http://192.168.204.132/wp-content/themes/
=> DIRECTORY: http://192.168.204.132/wp-content/uploads/

--- Entering directory: http://192.168.204.132/wp-includes/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
```

<https://blog.csdn.net/Yangyuxin0228>

http: //192.168.204.132/ipdata/

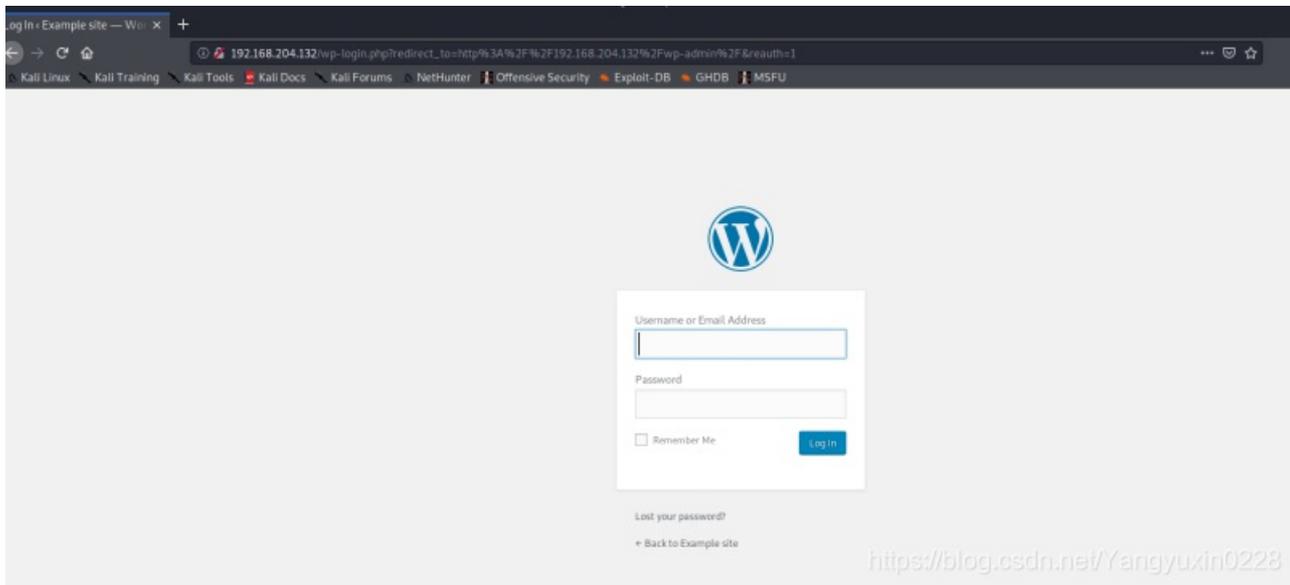
5、浏览器访问该目录（路径），发现一个cap文件。截图。![在这里插入图片描述](https://img-blog.csdnimg.cn/20201224204321633.



6、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。

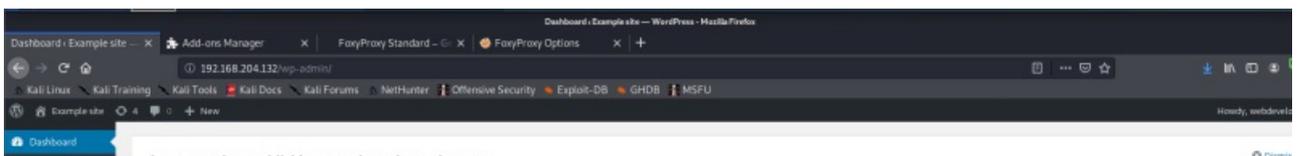
No.	Time	Source	Destination	Protocol	Length	Info
73	9.273898	192.168.1.176	192.168.1.222	HTTP	1680	HTTP/1.1 200 OK (text/css)
82	9.279987	192.168.1.176	192.168.1.222	HTTP	5226	HTTP/1.1 200 OK (application/javascript)
85	9.302054	192.168.1.222	192.168.1.176	HTTP	389	GET /wordpress/wp-includes/js/wp-emoji-release.min.js?ver=4.9.8 HTTP/1.1
86	9.303116	192.168.1.176	192.168.1.222	HTTP	4799	HTTP/1.1 200 OK (application/javascript)
89	9.532956	192.168.1.222	192.168.1.176	HTTP	399	GET /wordpress/wp-content/themes/twentyseventeen/assets/images/header.jpg HTTP/1.1
101	9.534033	192.168.1.176	192.168.1.222	HTTP	15298	HTTP/1.1 200 OK (JPEG JFIF image)
127	18.454239	192.168.1.222	192.168.1.176	HTTP	397	GET /wordpress/wp-admin/ HTTP/1.1
129	18.454604	192.168.1.176	192.168.1.222	HTTP	670	HTTP/1.1 301 Moved Permanently (text/html)
131	18.459295	192.168.1.222	192.168.1.176	HTTP	398	GET /wordpress/wp-admin/ HTTP/1.1
132	18.472292	192.168.1.176	192.168.1.222	HTTP	473	HTTP/1.1 302 Found
133	18.475930	192.168.1.222	192.168.1.176	HTTP	475	GET /wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.1.176%2Fwp-admin%2F&reauth=1 HTTP/1.1
134	18.488682	192.168.1.176	192.168.1.222	HTTP	3771	HTTP/1.1 200 OK (text/html)
136	18.535692	192.168.1.222	192.168.1.176	HTTP	581	GET /wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,110n,login&ver=4.9.8 HTTP/1.1
146	18.541084	192.168.1.176	192.168.1.222	HTTP	12463	HTTP/1.1 200 OK (text/css)
148	18.575040	192.168.1.222	192.168.1.176	HTTP	527	GET /wordpress/wp-admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1
149	18.577324	192.168.1.176	192.168.1.222	HTTP/X.	1876	HTTP/1.1 200 OK
180	90.210143	192.168.1.222	192.168.1.176	HTTP	799	POST /wordpress/wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
182	90.232018	192.168.1.176	192.168.1.222	HTTP	1200	HTTP/1.1 302 Found

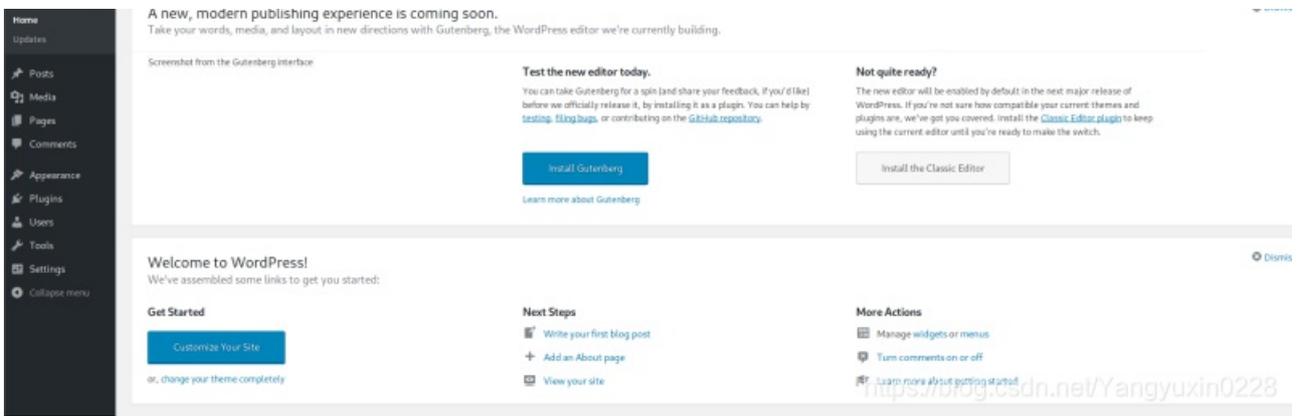
7、利用上一步得到的信息进入网站后台。截图。



随便提交一个账号密码

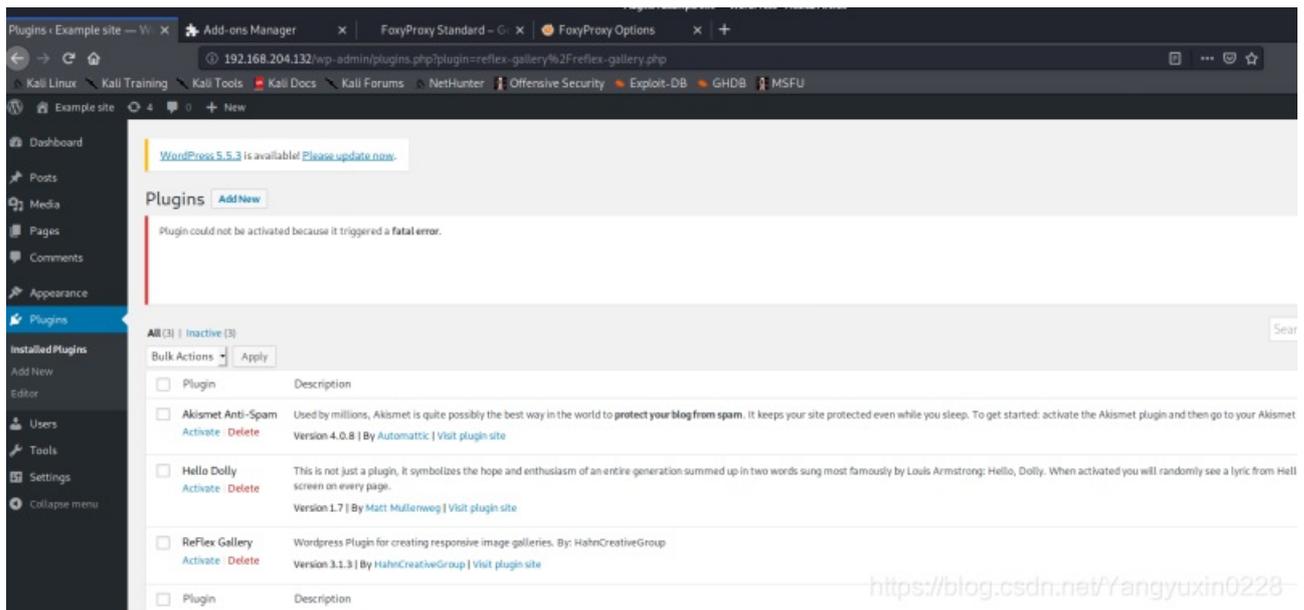
No.	Time	Source	Destination	Protocol	Length	Info
177	90.209811	192.168.1.222	192.168.1.176	TCP	74	49558 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=54456099 TSecr=0 WS=128
178	90.209858	192.168.1.176	192.168.1.222	TCP	74	80 → 49558 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1478185263 TSecr=54456099 WS=128
179	90.209969	192.168.1.222	192.168.1.176	TCP	66	49558 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=54456099 TSecr=1478185263
180	90.210143	192.168.1.222	192.168.1.176	HTTP	799	POST /wordpress/wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
181	90.210171	192.168.1.176	192.168.1.222	TCP	66	80 → 49558 [ACK] Seq=1 Ack=734 Win=30464 Len=0 TSval=1478185264 TSecr=54456099
182	90.232018	192.168.1.176	192.168.1.222	HTTP	1209	HTTP/1.1 302 Found
183	90.232225	192.168.1.222	192.168.1.176	TCP	66	49558 → 80 [ACK] Seq=734 Ack=1135 Win=32128 Len=0 TSval=54456121 TSecr=1478185285
184	90.236559	192.168.1.222	192.168.1.176	HTTP	949	GET /wordpress/wp-admin/ HTTP/1.1
187	90.278053	192.168.1.176	192.168.1.222	TCP	66	80 → 49558 [ACK] Seq=1135 Ack=1617 Win=32256 Len=0 TSval=1478185331 TSecr=54456125
209	91.520747	192.168.1.176	192.168.1.222	TCP	7306	80 → 49558 [ACK] Seq=1135 Ack=1617 Win=32256 Len=7240 TSval=1478186573 TSecr=54456125 [TCP segment of a reassembled PDU]
219	91.520924	192.168.1.176	192.168.1.222	TCP	7306	80 → 49558 [ACK] Seq=8375 Ack=1617 Win=32256 Len=7240 TSval=1478186573 TSecr=54456125 [TCP segment of a reassembled PDU]
211	91.521120	192.168.1.222	192.168.1.176	TCP	66	49558 → 80 [ACK] Seq=1617 Ack=8375 Win=46592 Len=0 TSval=54457409 TSecr=1478186573
212	91.521133	192.168.1.176	192.168.1.222	HTTP	1420	HTTP/1.1 200 OK (text/html)
213	91.521455	192.168.1.222	192.168.1.176	TCP	66	49558 → 80 [ACK] Seq=1617 Ack=15615 Win=61056 Len=0 TSval=54457409 TSecr=1478186573
214	91.557657	192.168.1.222	192.168.1.176	HTTP	1054	GET /wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=dashicons,admin-bar,common,forms,admin-menu,dashboard,11st-tables
215	91.557698	192.168.1.176	192.168.1.222	TCP	66	80 → 49558 [ACK] Seq=16969 Ack=2605 Win=34176 Len=0 TSval=1478186610 TSecr=54457446
236	91.574945	192.168.1.176	192.168.1.222	TCP	8531	80 → 49558 [PSH, ACK] Seq=16969 Ack=2605 Win=34176 Len=8465 TSval=1478186627 TSecr=54457446 [TCP segment of a reassembled PDU]
237	91.575081	192.168.1.176	192.168.1.222	TCP	8170	80 → 49558 [PSH, ACK] Seq=25434 Ack=2605 Win=34176 Len=8104 TSval=1478186628 TSecr=54457446 [TCP segment of a reassembled PDU]





用burp

8、利用该CMS存在的（插件Plugin）漏洞。



先安装插件

10、SSH登录服务器

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 以下操作得到的结果截图替代以下截图。

```
webdeveloper@webdeveloper:~$ cat /root/flag.txt
cat: /root/flag.txt: Permission denied
webdeveloper@webdeveloper:~$ whoami
webdeveloper
webdeveloper@webdeveloper:~$ ls -l /root/flag.txt
ls: cannot access '/root/flag.txt': Permission denied
webdeveloper@webdeveloper:~$ sudo cat /root/flag.txt
[sudo] password for webdeveloper:
Sorry, user webdeveloper is not allowed to execute '/bin/cat /root/flag.txt' as root on webdeveloper
webdeveloper@webdeveloper:~$
```

均无法查看。

10、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。

```
webdeveloper@webdeveloper:~$ sudo -l
[sudo] password for webdeveloper:
Matching Defaults entries for webdeveloper on webdeveloper:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
  (root) /usr/sbin/tcpdump
```

```
webdeveloper@webdeveloper:~$ cat /root/flag.txt
cat: /root/flag.txt: Permission denied
webdeveloper@webdeveloper:~$ whoami
webdeveloper
webdeveloper@webdeveloper:~$ ls -l /root/flag.txt
ls: cannot access '/root/flag.txt': Permission denied
webdeveloper@webdeveloper:~$ sudo cat /root/flag.txt
[sudo] password for webdeveloper:
Sorry, user webdeveloper is not allowed to execute '/bin/cat /root/flag.txt' as root on webdeveloper
webdeveloper@webdeveloper:~$ █
```

tcpdump命令详解:

- i eth0 从指定网卡捕获数据包
- w /dev/null 将捕获到的数据包输出到空设备（不输出数据包结果）
- z [command] 运行指定的命令
- Z [user] 指定用户执行命令
- G [rotate_seconds] 每rotate_seconds秒一次的频率执行-w指定的转储
- W [num] 指定抓包数量