

# 第一周环境准备任务

---

## 个人资料

---

个人在知识星球中的ID: 1210

常用名: sharp

联系方式: qq: 418428916

目前职业: 实习生(大三)

所在地区: 上海

熟悉的编程语言: php/python

自我介绍: 了解基础的Web安全, 熟悉常见的安全问题, 会使用常见工具sqlmap,burpsuit,msf等, 对于python脚本还是有点心得的, 希望可以用一年的时间好好沉淀一下自己, 再好好的补充一下基础知识, 牢固的基础是最重要的, 希望找到一群志同道合, 热爱网安的人。

github:<https://github.com/wwfft>

附上自己的星球名片



## 操作系统：ubuntu虚拟机

### 1.搭建linux+nginx+php-fpm+mysql环境

文章参考

[https://blog.csdn.net/qq\\_34039018/article/details/94437355](https://blog.csdn.net/qq_34039018/article/details/94437355)

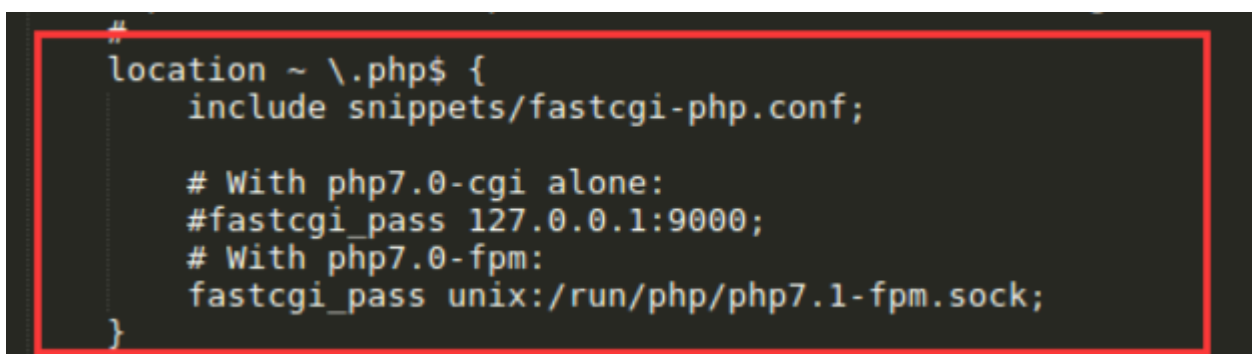
<https://www.cnblogs.com/xbxxf/p/9122920.html>

以前都是直接用集成好的xampp，当自己重新一步一步搭环境的时候出现了好多问题...

安装nginx，安装php，安装mysql按部就班

按照上面第一个链接就可以搭好，当时我首先是用的第二个链接方法，可是搭到nginx解析php文件时出现了问题，每次访问都提示下载文件，在群里也看到了许多人也出现了这个问题，上面所写的配置文件和我ubuntu的配置文件不一样，所以后来又找到了第一个链接。

这两篇文章最大的不同，最大的坑就是



```
#
location ~ /\.php$ {
    include snippets/fastcgi-php.conf;

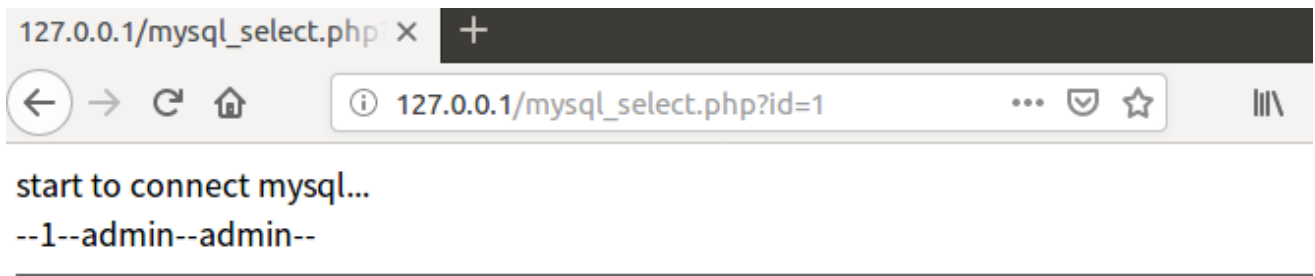
    # With php7.0-cgi alone:
    #fastcgi_pass 127.0.0.1:9000;
    # With php7.0-fpm:
    fastcgi_pass unix:/run/php/php7.1-fpm.sock;
}
```

这个fastcgi\_pass 127.0.0.1:9000 一个是注释掉的 另一个是开启的

上网查了很多资料，都说要开启这个fastcgi\_pass，可是每次开启都会报错，有的人说是端口问题更改端口，有的人说是端口没有开启，各种办法都试过还是报错，最后直接注释掉就ok了

这里还是有些问题，记录一下，有时间请教一下大佬

贴一张搭好环境的图



附上代码

```
1  <?php
2  $servername = "127.0.0.1";
3  $username = " ";
4  $password = " ";
5  $db_name = "test";
6  echo 'start to connect mysql...<br>';
7  $conn = mysqli_connect($servername,$username,$password,$db_name);
8
9  if (!$conn){
10     die("连接失败: ".mysql_error());
11 }
12 $id = $_GET['id'];
13
14 $sql = "select * from user where id=?";
15 $stmt = $conn->prepare($sql);
16 $stmt->bind_param('i',$id);
17 $stmt->bind_result($id,$username,$password);
18 $stmt->execute();
19 #$result = mysqli_query($conn,$sql);
20 // if(!$result){
21 //     echo "fail";
22 // }
23
24 // while($row = mysqli_fetch_array($result)){
25 //     echo $row['id'];
26 //     echo $row['username']."<br>";
27 // }
28 while($stmt->fetch()){
29     echo "--$id--$username--$password--<br>";
30 }
31 $stmt->free_result();
32 $stmt->close();
33 $conn->close();
34 ?>
```

预编译防止sql注入

强调一下:

开发模式下要添加php报错信息回显

<https://blog.csdn.net/coderjiang/article/details/27526789>

反正我本机最开始是没有回显的... 之前少打了一个;

页面一直显示空白，找了好久才发现...

## ubuntu加固

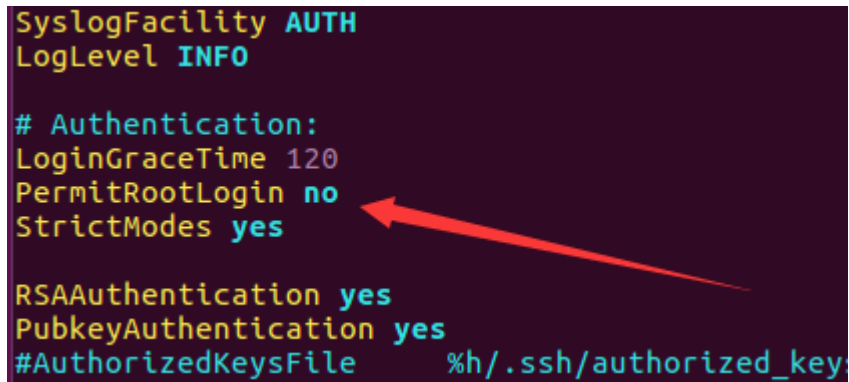
文章参考

<https://www.jianshu.com/p/a76202ae8eef>

[https://blog.csdn.net/qq\\_36119192/article/details/82906799](https://blog.csdn.net/qq_36119192/article/details/82906799)

### 1.禁止root用户登录ssh，指定普通用户才能登录

修改/etc/init.d/sshd\_config文件，找到



```
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

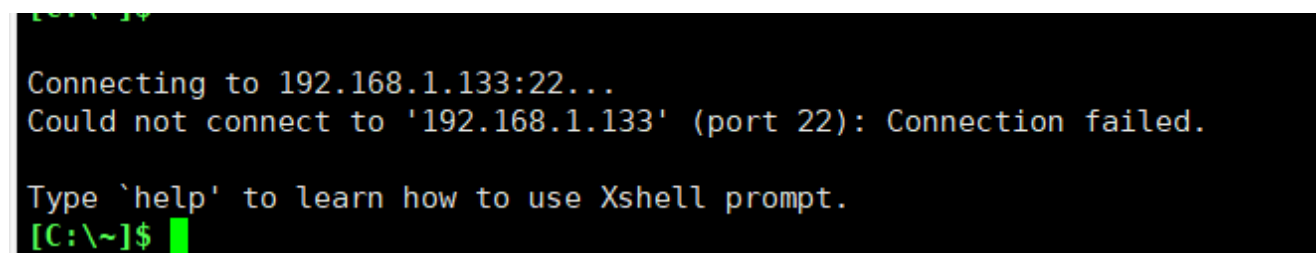
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile      %h/.ssh/authorized_keys
```

将其改为no，然后重启一下ssh服务/etc/init.d/ssh restart，这里踩了点小坑，之前设置为yes尝试用root来登录，没有重启ssh服务，ssh一直连不上，导致我一直以为root密码不对....

加固原因：设置完以后就无法使用ssh来连接root用户，保证了黑客获取了你的root密码远程登录搞破坏。

### 2.修改ssh登录端口

修改/etc/init.d/sshd\_config文件，找到Port 22所在行，就在文件首部位置，更改为其他端口例如2222，再使用ssh连接如下图



```
[C:\~]$ ssh 192.168.1.133
Connecting to 192.168.1.133:22...
Could not connect to '192.168.1.133' (port 22): Connection failed.

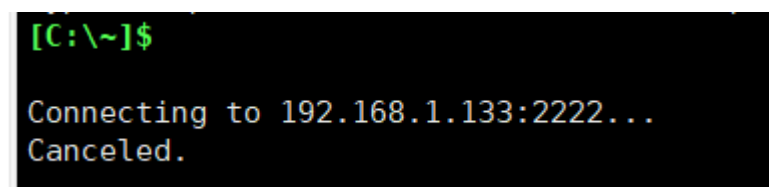
Type 'help' to learn how to use Xshell prompt.
[C:\~]$
```

加固原因：防止黑客使用常用端口进行登录爆破，修改端口提升了系统的隐蔽性

### 3.开启ufw防火墙

ubuntu自带ufw防火墙

ufw enable 开启防火墙，即使重启仍然处于开始状态，默认拒绝任意端口的请求



```
[C:\~]$ ssh 192.168.1.133
Connecting to 192.168.1.133:2222...
Canceled.
```

为ssh端口2222添加一个允许规则：ufw allow 2222/tcp

```

Connecting to 192.168.1.133:2222...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-55-generic x86_64)

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

```

加固原因：开始ufw防火墙防止不允许的端口对系统进行访问，控制端口白名单。

#### 4.设置密码复杂度

修改 /etc/login.defs

```

PASS_MAX_DAYS      90
PASS_MIN_DAYS      0
PASS_WARN_AGE      7
PASS_MIN_LEN        8
#

```

将最小长度修改为8，可以会有一个问题

```

密码：
配置错误 - 未知项目“PASS_MIN_LEN”(请通知管理员)
zhangsan@wft-virtual-machine:/home/wft$ passwd
更改 zhangsan 的密码。
(当前) UNIX 密码：
输入新的 UNIX 密码：
重新输入新的 UNIX 密码：
必须选择更长的密码
输入新的 UNIX 密码：
重新输入新的 UNIX 密码：
passwd: 已成功更新密码
zhangsan@wft-virtual-machine:/home/wft$ vim /etc/login.defs
zhangsan@wft-virtual-machine:/home/wft$

```

进入其他已有账号时会提示配置错误，不知道怎么修改，但是更改密码时长度不超过8会提示以上错误

```

password optional pam_gnome_keyring.so
# end of pam-auth-update config
password requisite pam_pwquality.so try_first_pass local_users_o
nly retry=3 authtok_type= difok=1 minlen=8 lcredit=-1
~
~
~

```

对于文章中密码强度的设定，可能不是一个系统，我将这段话加到配置文件中会报错，找了很多文章也没有和我配置文件一样的

这里还是有些问题，记录一下，有时间请教一下大佬

#### nginx加固

参考资料

<https://www.cnblogs.com/cnjava/archive/2013/07/16/3193757.html>

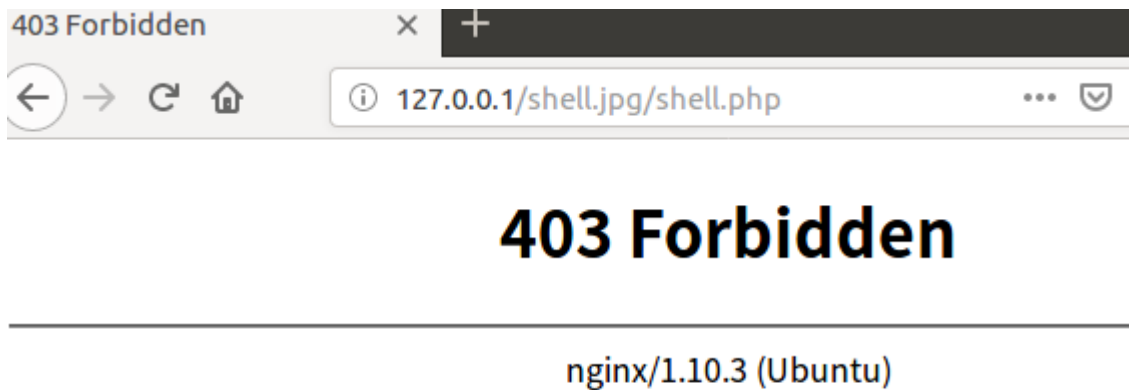
## 1.nginx解析漏洞

上传一个1.jpg，访问1.jpg/1.php时会把1.jpg当做php脚本运行 vim /etc/nginx/sites-available/default

添加下面代码

```
}  
if ( $fastcgi_script_name ~ \..*\/*.php ) {  
    return 403;  
}  
# pass the PHP scripts to FastCGI server listen
```

当触发规则后会报403错误



可是我本机没有加固配置时会报404错误... 并没有出现解析漏洞，我猜应该是nginx版本问题

加固原因：防止利用解析漏洞上传图片马

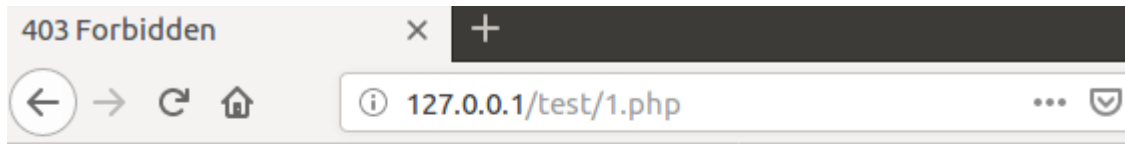
## 2.禁止特定目录解析php脚本

vim /etc/nginx/sites-available/default

添加下面代码

```
location ~ /test/.*.(php|php5)?$ {  
    deny all;  
}
```

就会变成这样



# 403 Forbidden

nginx/1.10.3 (Ubuntu)

加固原因：可以用在一起上传目录，禁止php脚本执行

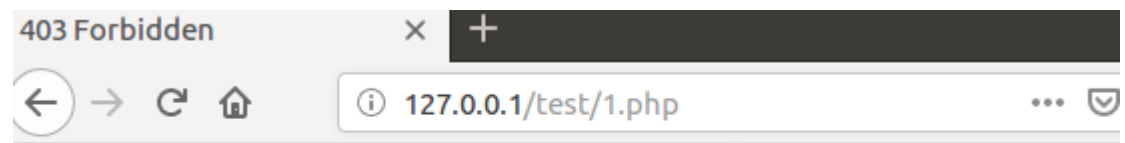
### 3.隐藏版本信息

vim /etc/nginx/nginx.conf

添加代码 server\_tokens off;

```
server_tokens off;
```

隐藏掉了版本信息



# 403 Forbidden

nginx

加固原因：可以避免黑客根据版本信息查找相应漏洞