



LAB MANUAL ON BUG & BOUNTY



**ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY
TRAINING TO TECHNICAL TEACHERS**

**DEPARTMENT OF INFORMATION MANAGEMENT AND COORDINATION
SPONSORED BY MINISTRY OF ELECTRONICS AND INFORMATION
TECHNOLOGY**

GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Ms. Purnima Mohanty (Project Assistant)

Table of Contents

Introduction to Bug & Bounty	3
Security Bug	3
What is Bug Bounty?	4
History of Bug Bounty	4
Graphical Report	6
Sample of Bug Bounty XSS found in Mail.....	6
Installation of Visual Studio.....	9
Installation and completion	12
Introduction to Wamp Server.....	13
To activate WAMP.....	22
Introduction to Xtreme Vulnerable Web Application	23

Introduction to Bug & Bounty

Security Bug

A security bug or security defect is a software bug that can be exploited to gain unauthorized access or privileges on a computer system. Security bugs introduce security vulnerabilities by compromising one or more of Authentication of users and other entities. Security bugs introduce security vulnerabilities by compromising one or more of:

- Authentication of users and other entities
- Authorization of access rights and privileges
- Data confidentiality
- Data integrity

On September 9, 1947, a team of computer scientists and engineers reported the world's first computer bug. A bug is a flaw or glitch in a system. Thomas Edison reported "bugs" in his designs as early as the 1800s, but this was the first bug identified in a computer. First case of bug being found," one of the team members wrote in the logbook. The team at Harvard University in Cambridge, Massachusetts, found that their computer, the Mark II, was delivering consistent errors. The first report of bug was delivered by Grace Hopper.

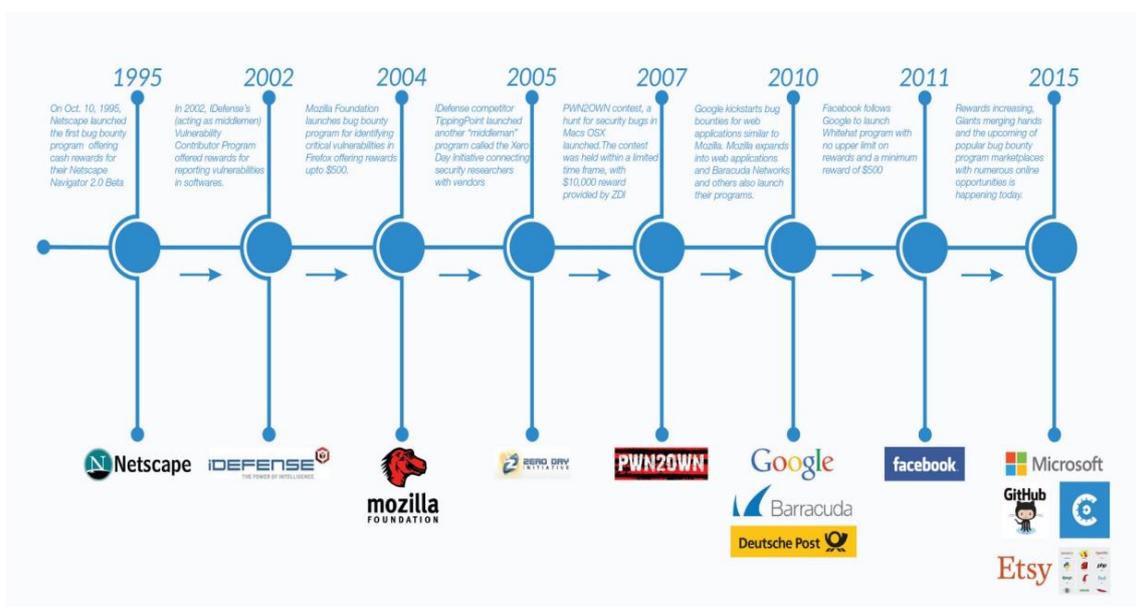
What is Bug Bounty?

A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities. These programs allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse. Bug bounty programs have been implemented by a large number of organizations. A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

History of Bug Bounty

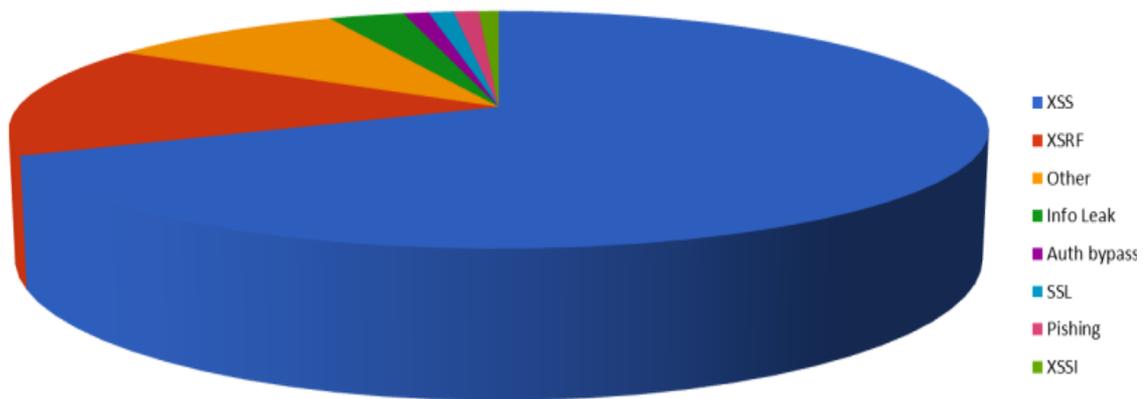
Three years back when Ola was hacked, compromising the data of millions of users, they created India's first full-fledged bug bounty program to encourage independent security researchers to help them create a safe platform. The company now offers up to 3,00,000 INR for security loopholes such as injections, server-side issues, client-side issues, and other valid security vulnerabilities. Ola has seen success with its program. Security research bloggers from Fallible say Ola awarded them with \$1000 in bounty and some electronic goodies for reporting vulnerabilities in one of their apps. The researchers also

claim Ola took around 2 months to fix their reported bug. McDonalds India (West and South) runs a bug bounty program in India for its web and mobile apps for McDelivery. In 2017, researchers from Fallible discovered a huge vulnerability in their app. They found it was possible for hackers to dump the data of 2.2 million users by exploiting a flaw. Paytm is another company running a bug bounty program in India. Avinash Jain, an independent security researcher found a vulnerability in Paytm’s electricity bill payment service. Sandeep reveals bug bounty hunting allows you to be your own boss, and work with freedom and flexibility. From 2016, nullcon has started a BountyCraft Track. It is a platform where the Bug Bounty Program offering companies (Microsoft, Apple, Google) & crowdsourced security platforms (Bugcrowd, Hackerone, NCC Group, Crowdfense) interact directly with Bug



Graphical Report

What types of bugs do they find?



Sample of Bug Bounty XSS found in Mail

+Nils E-Mail Kalender Text & Tabellen Fotos Reader Web Mehr -



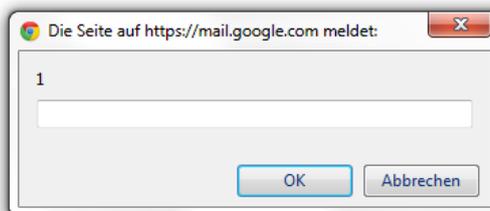
An:

Cc/Bcc

Betreff: Fwd:

----- Weitergeleitete Nachricht -----
Von: Nils Juenemann
Datum: Freitag, 1. Juli 2011
Betreff: <x>
An: Nils Juenemann

XSS

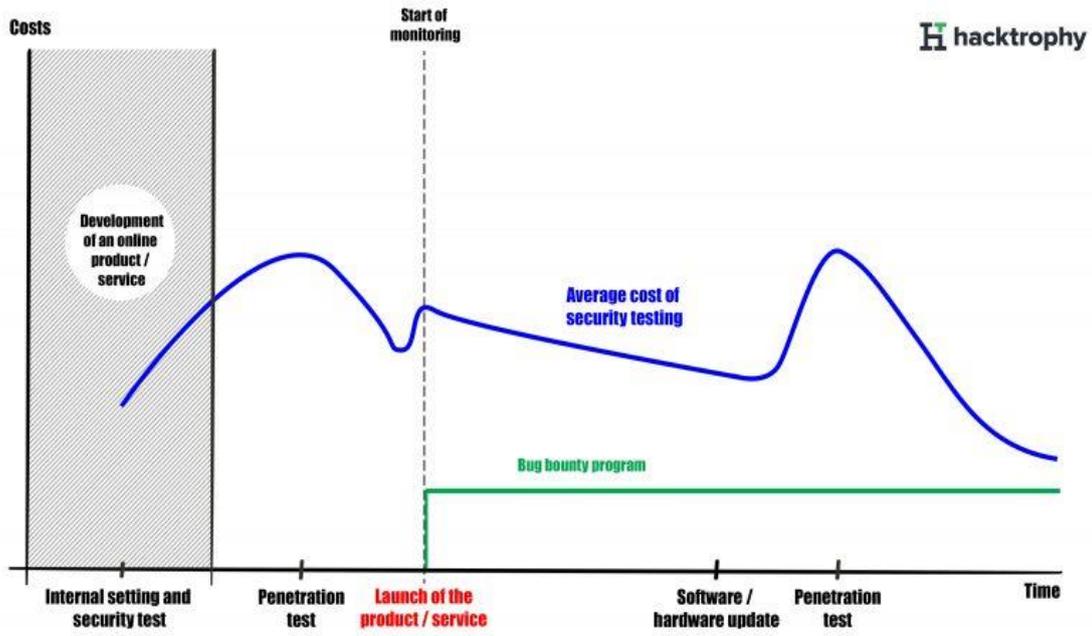


[Feedback senden](#)

Google Mail anzeigen in: [Mobil](#) | [Ältere Version](#) | [Desktop](#)

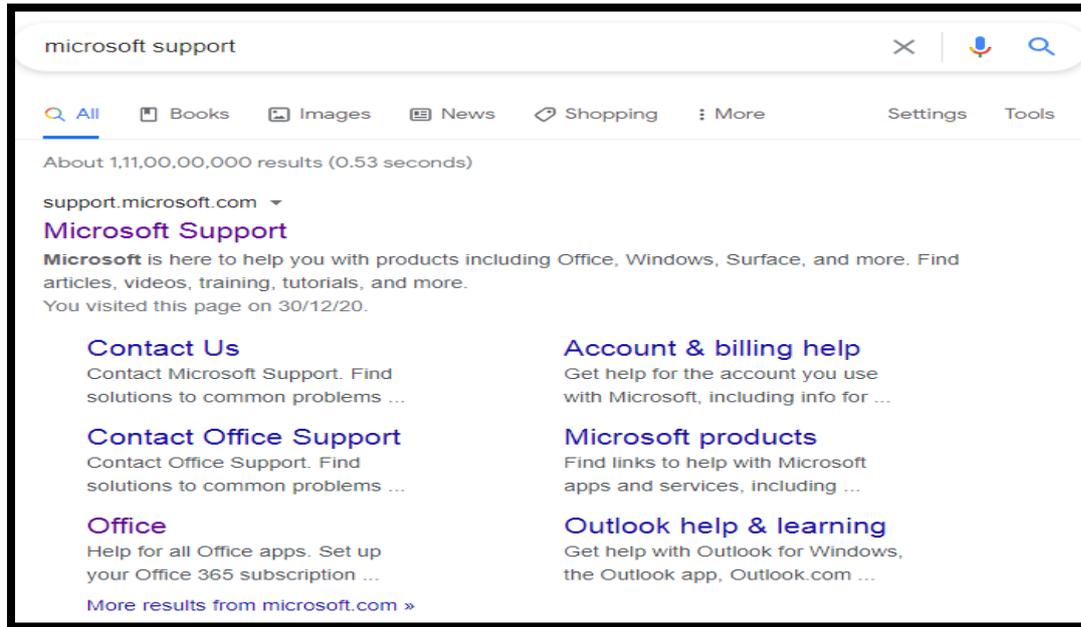
©2011 Google

The objective is to search for organizations that announce and provide a professional and transparent ecosystem for carrying out security testing, reporting and payments, while indemnifying the tester from any legal or other action. Permission will be obtained from the organization that has announced the program. At the very least, a record of start date, end date and access times will be maintained and may be shared with the organization if needed. Vulnerability will be exploited only for the purpose of getting a screenshot of the extent of penetration into the organization's infrastructure. All testing will be non-destructive. Making changes in source code of programs running on the organization infrastructure or in documents stored on the systems to which access has been obtained. No data or documents will be copied from any of the vulnerable systems on which access has been obtained during the course of searching for bugs and vulnerabilities. No testing will be done for "information" or "knowledge enhancement" purposes as this is a professional activity and one expects to earn from the same. Payments as per the payout norms of the organizing company will be accepted without dispute. Any bug / vulnerability / issue that is reported under a bug bounty program will be released in public only after it has been repaired by the affected organization.

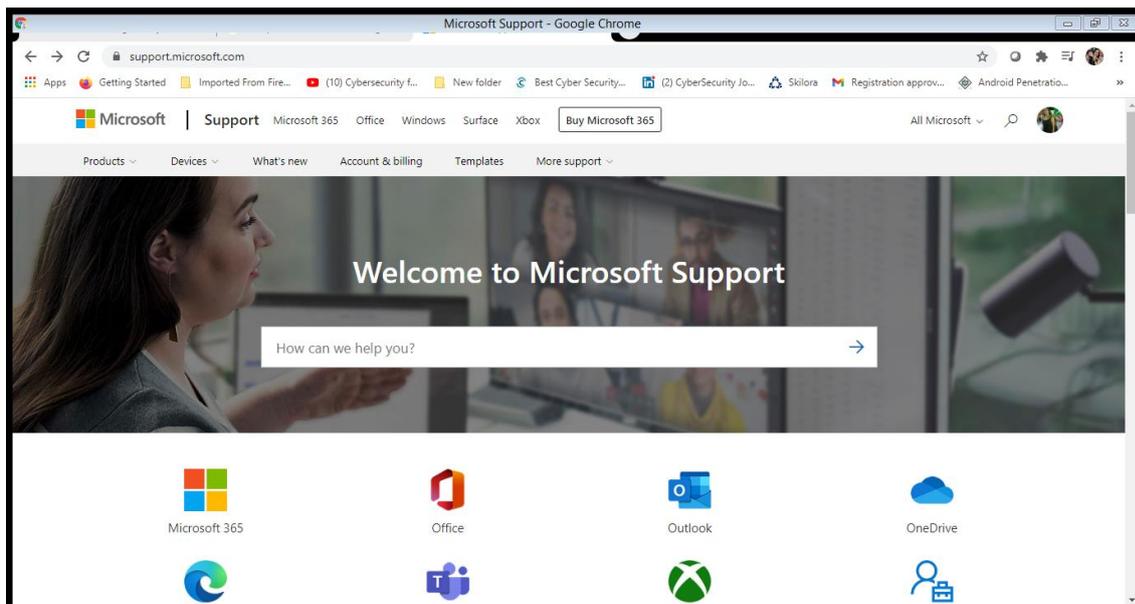


Installation of Visual Studio

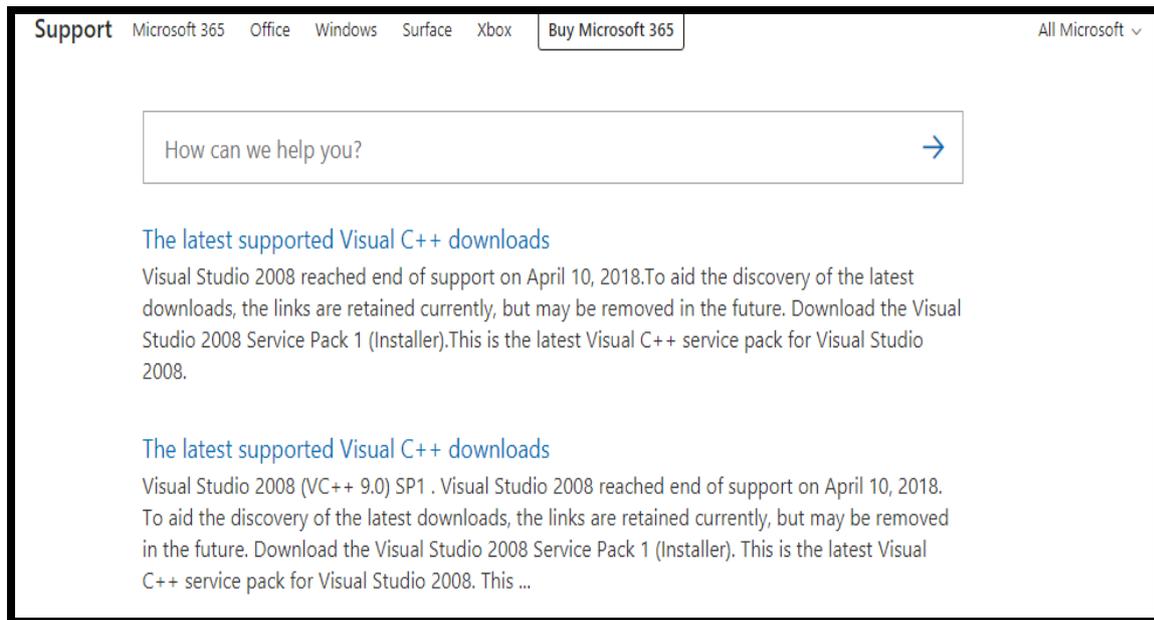
Step 1:- Open google website and type “Microsoft support”



Step 2:- After getting the page type visual studio in search

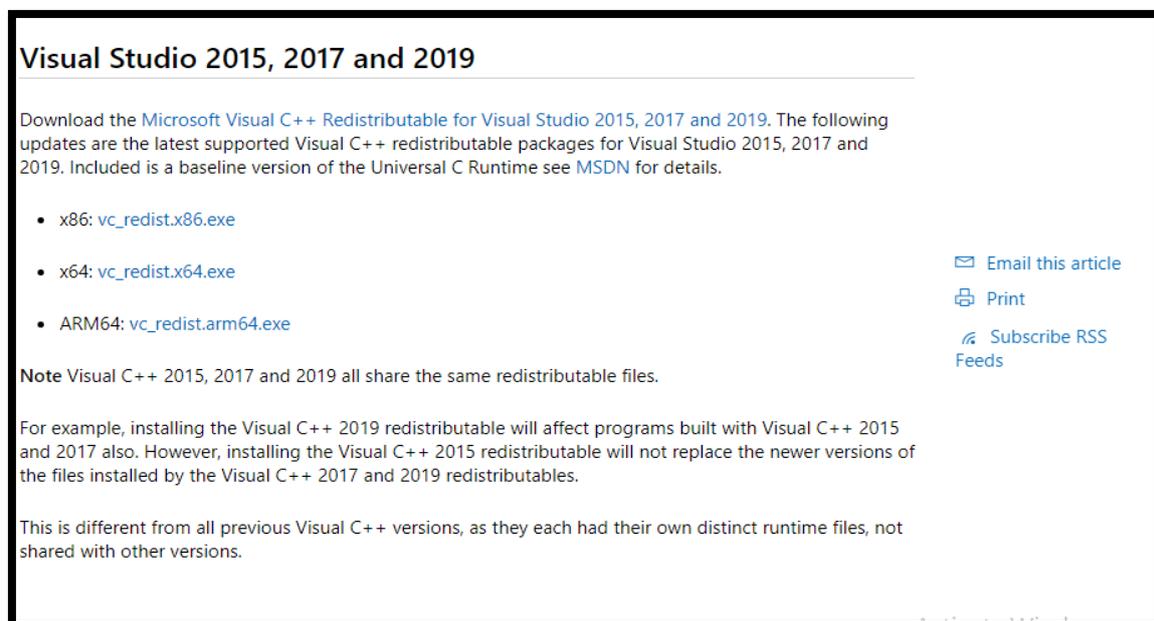


Step 3:- click on latest download



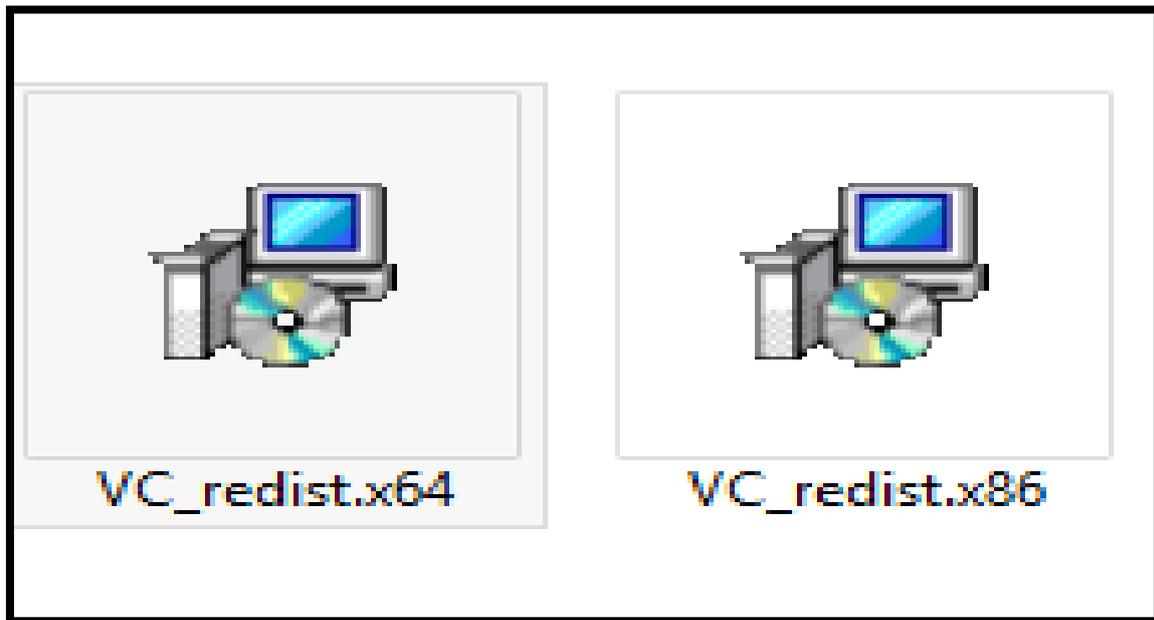
The screenshot shows the Microsoft Support website. At the top, there is a navigation bar with links for 'Support', 'Microsoft 365', 'Office', 'Windows', 'Surface', 'Xbox', and 'Buy Microsoft 365'. A search bar contains the text 'How can we help you?' with a right-pointing arrow. Below the search bar, there are two sections of text. The first section is titled 'The latest supported Visual C++ downloads' and discusses the end of support for Visual Studio 2008 on April 10, 2018, and provides information about downloading the Visual Studio 2008 Service Pack 1 (Installer). The second section is also titled 'The latest supported Visual C++ downloads' and provides similar information for Visual Studio 2008 (VC++ 9.0) SP1.

Step 4:- download all support set up

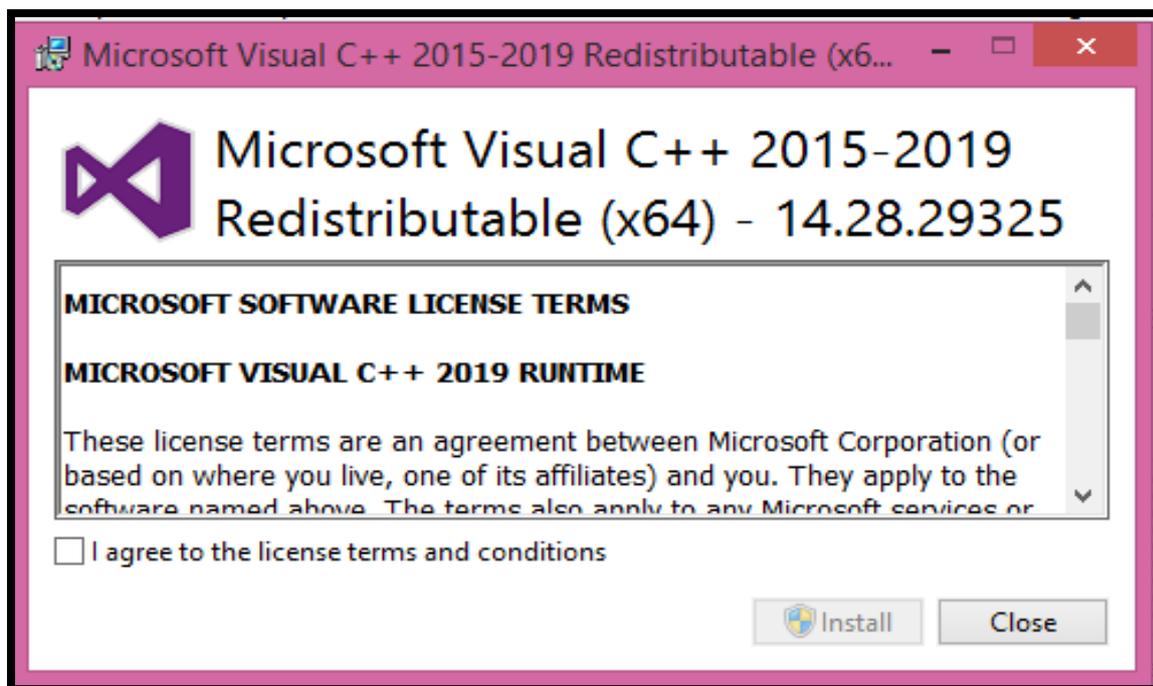


The screenshot shows a Microsoft article titled 'Visual Studio 2015, 2017 and 2019'. The article text states: 'Download the Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. The following updates are the latest supported Visual C++ redistributable packages for Visual Studio 2015, 2017 and 2019. Included is a baseline version of the Universal C Runtime see MSDN for details.' Below this text is a bulleted list of three files: 'x86: vc_redist.x86.exe', 'x64: vc_redist.x64.exe', and 'ARM64: vc_redist.arm64.exe'. To the right of the list are three icons with corresponding text: 'Email this article', 'Print', and 'Subscribe RSS Feeds'. Below the list, there is a 'Note' section stating: 'Visual C++ 2015, 2017 and 2019 all share the same redistributable files.' Another paragraph explains: 'For example, installing the Visual C++ 2019 redistributable will affect programs built with Visual C++ 2015 and 2017 also. However, installing the Visual C++ 2015 redistributable will not replace the newer versions of the files installed by the Visual C++ 2017 and 2019 redistributables.' A final paragraph states: 'This is different from all previous Visual C++ versions, as they each had their own distinct runtime files, not shared with other versions.'

Step5:- Install the Setup

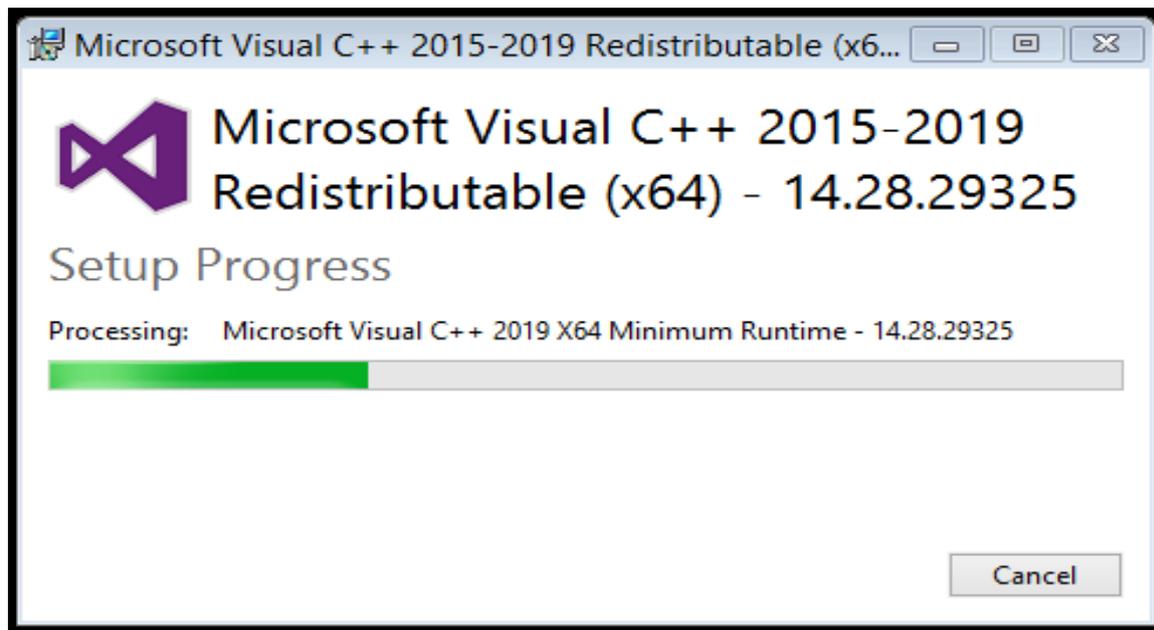


Step: 6:- agreement to policy and condition

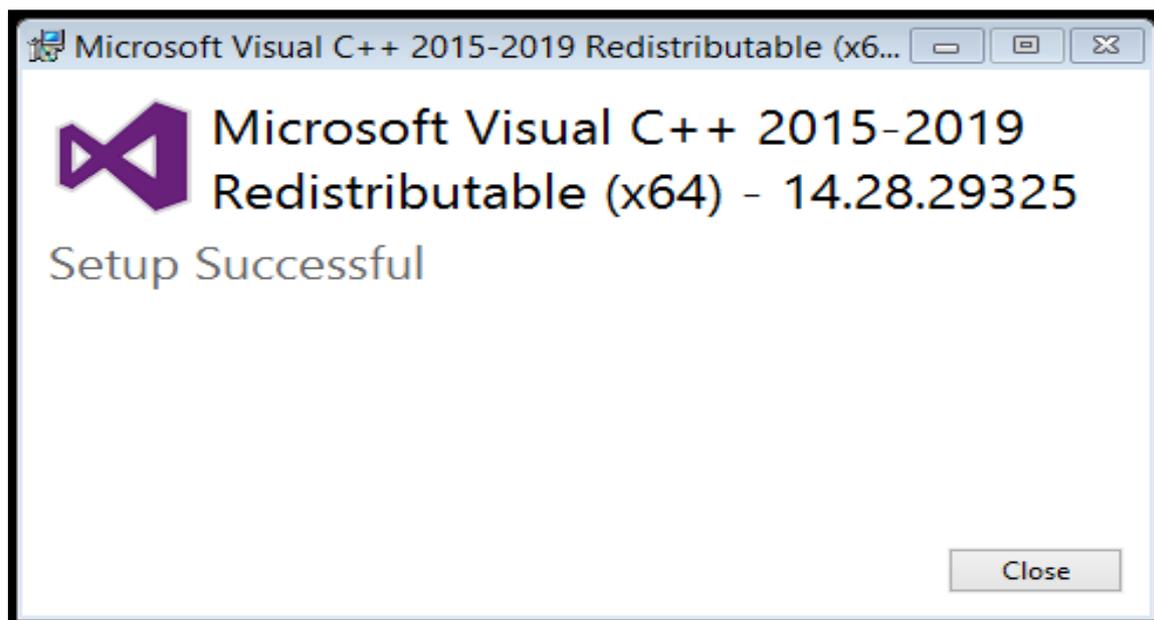


Installation and completion

Step 1:- Install Microsoft Visual



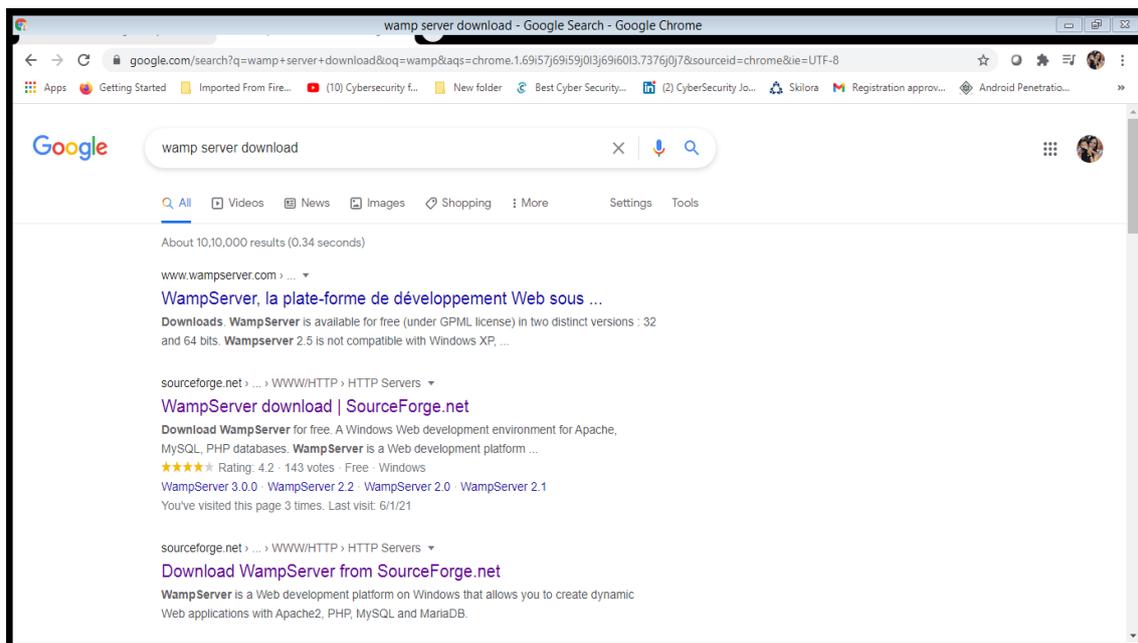
Step 1:- Setup Successful



Introduction to Wamp Server

Wamp Server refers to a solution stack for the Microsoft Windows operating system, created by Romain Bourdon and consisting of the Apache web server, Open SSL for SSL support, MySQL database and PHP programming language. Stands for "Windows, Apache, MySQL, and PHP." WAMP is a variation of LAMP for Windows systems and is often installed as a software bundle (Apache, MySQL, and PHP). It is often used for web development and internal testing but may also be used to serve live websites.

Step 1:- Download Wamp Server



Step 2:- Download Wamp From Given Site

sourceforge.net > ... > WWW/HTTP > HTTP Servers ▾

WampServer download | SourceForge.net

Download WampServer for free. A Windows Web development environment for Apache, MySQL, PHP databases. **WampServer** is a Web development platform ...

★★★★★ Rating: 4.2 · 143 votes · Free · Windows

[WampServer 3.0.0](#) · [WampServer 2.2](#) · [WampServer 2.0](#) · [WampServer 2.1](#)

You've visited this page 3 times. Last visit: 6/1/21

sourceforge.net > ... > WWW/HTTP > HTTP Servers ▾

Step 3:- click on download

Advertisement - Report

Home / Browse / Development / WWW/HTTP / HTTP Servers / WampServer



WampServer

A Windows Web development environment for Apache, MySQL, PHP databases
Brought to you by: [alterway](#), [herveleclerc](#), [otomatic](#)

★★★★★ 143 Reviews Downloads: 49,432 This Week Last Update: 2 days ago

[Download](#) [Get Updates](#) [Share This](#)

Windows

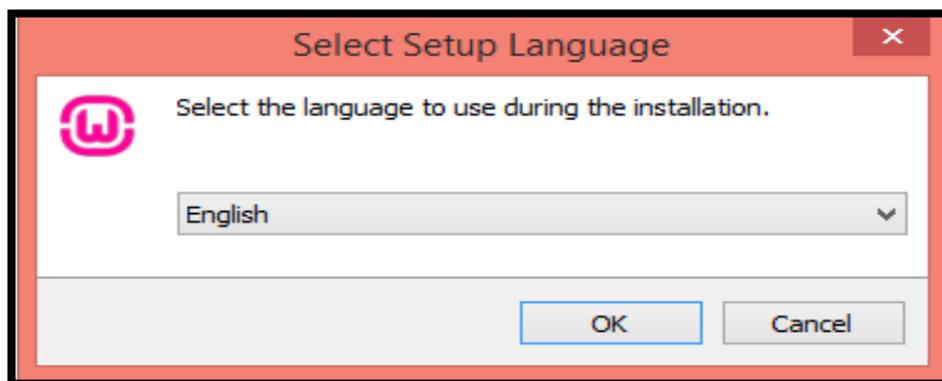
Summary	Files	Reviews	Support	Wiki	Tickets ▾	News
-------------------------	-----------------------	-------------------------	-------------------------	----------------------	---------------------------	----------------------

WampServer is a Web development platform on Windows that allows you to create dynamic Web applications with Apache2, PHP, MySQL and MariaDB. WampServer automatically installs everything you need to intuitively develop Web applications. You will be able to tune your server

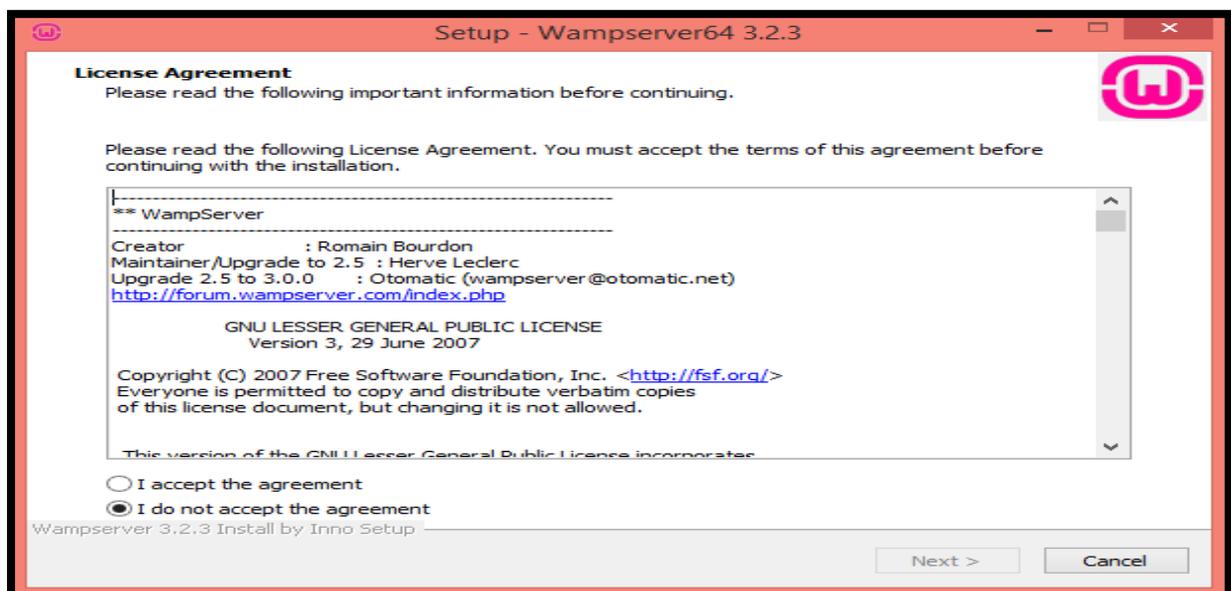
Now it is downloaded in our system



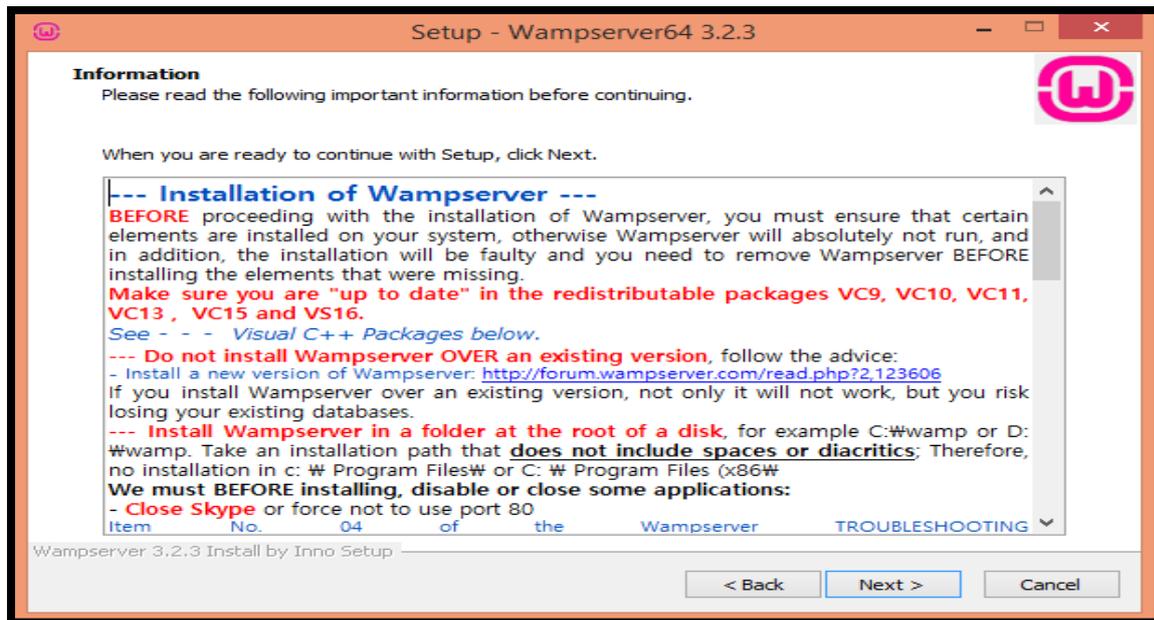
Step 4:- click on language and ok



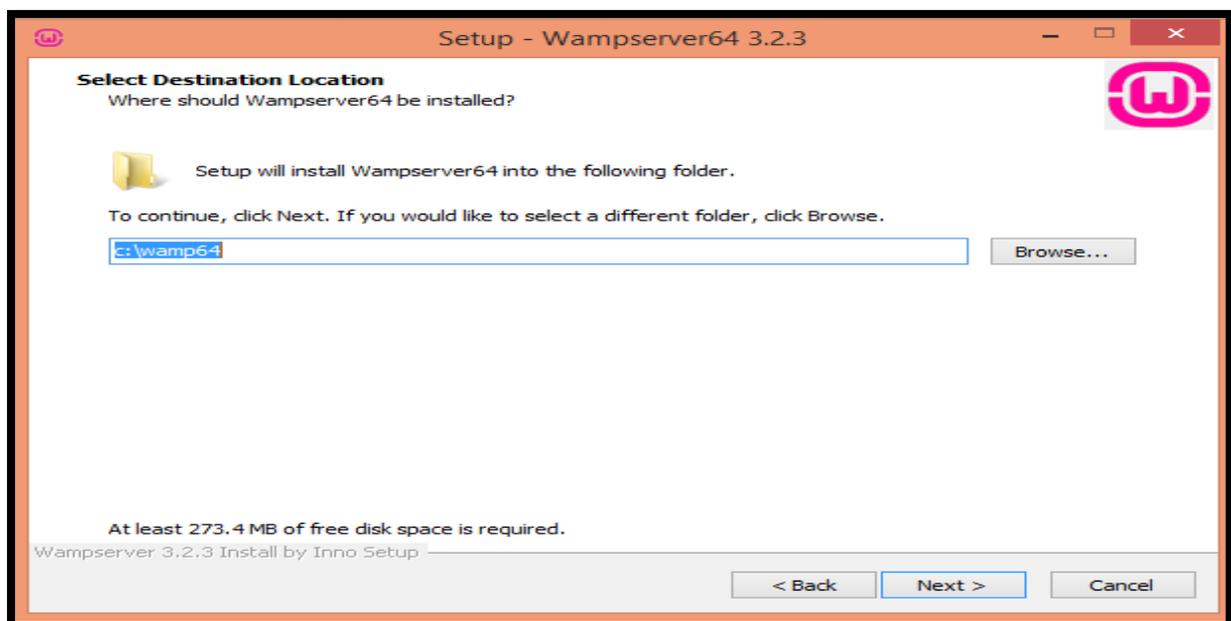
Step 5:- click on I accept



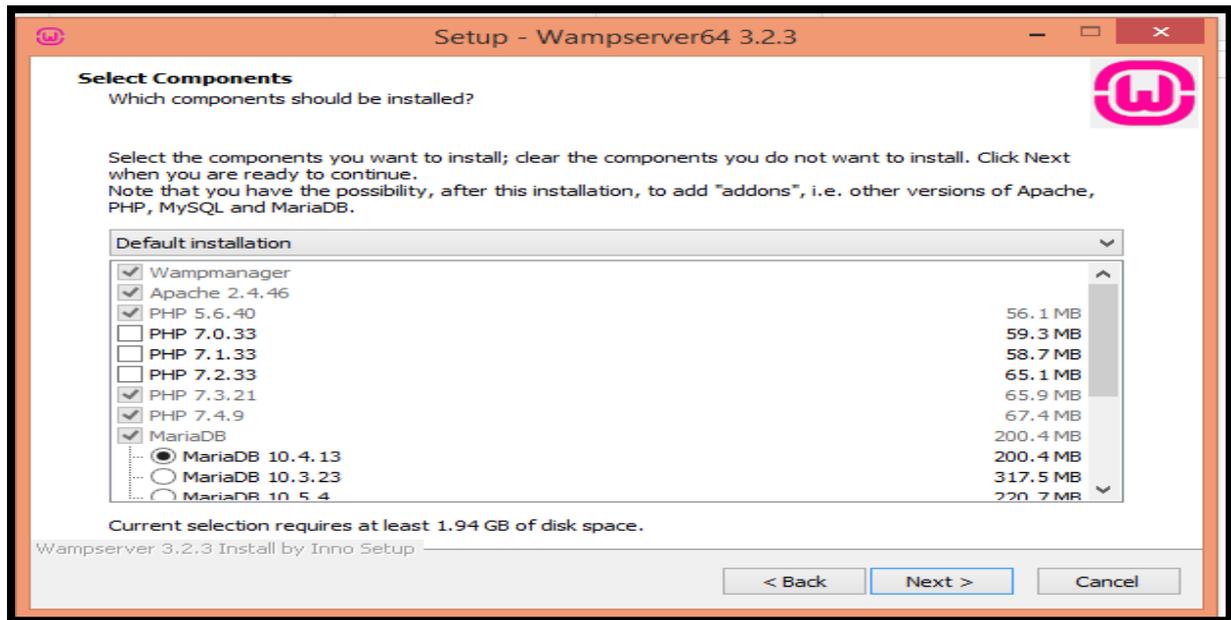
Step 6:- On Information Wizard Click On Next



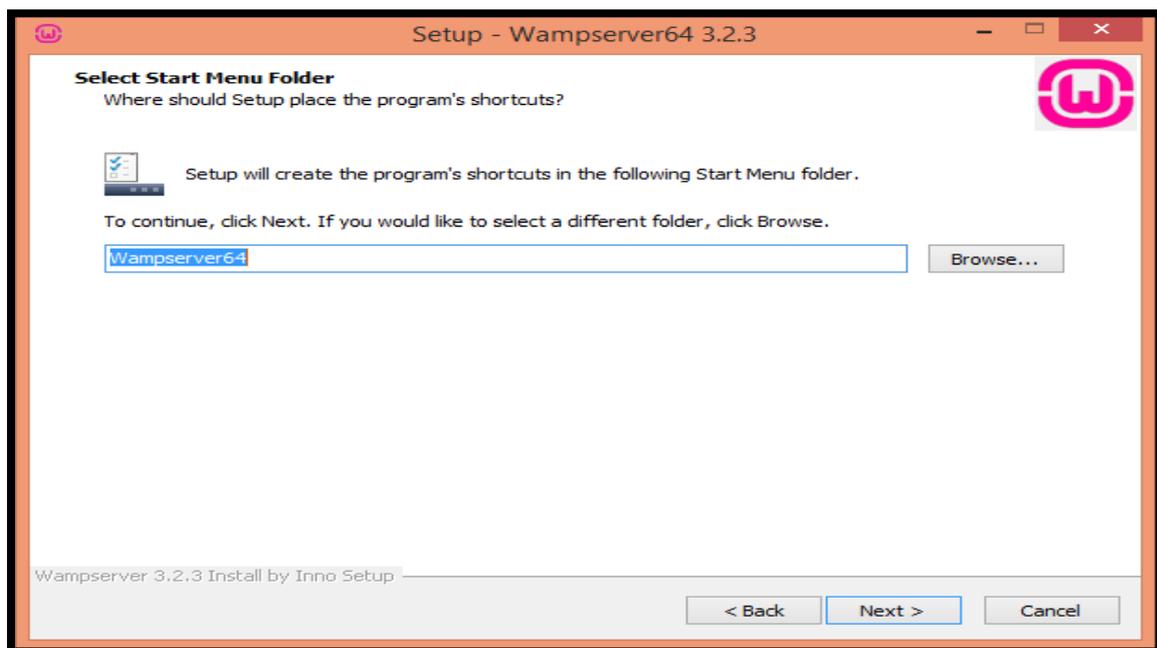
Step 7:- Select the destination click on next



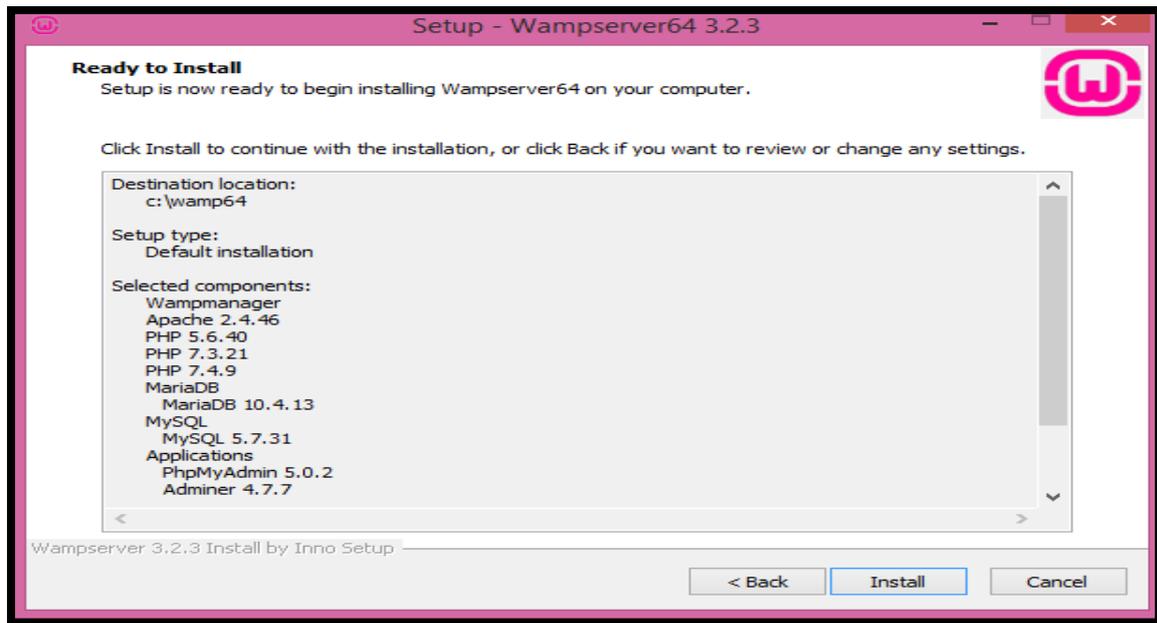
Step 8:- Select components



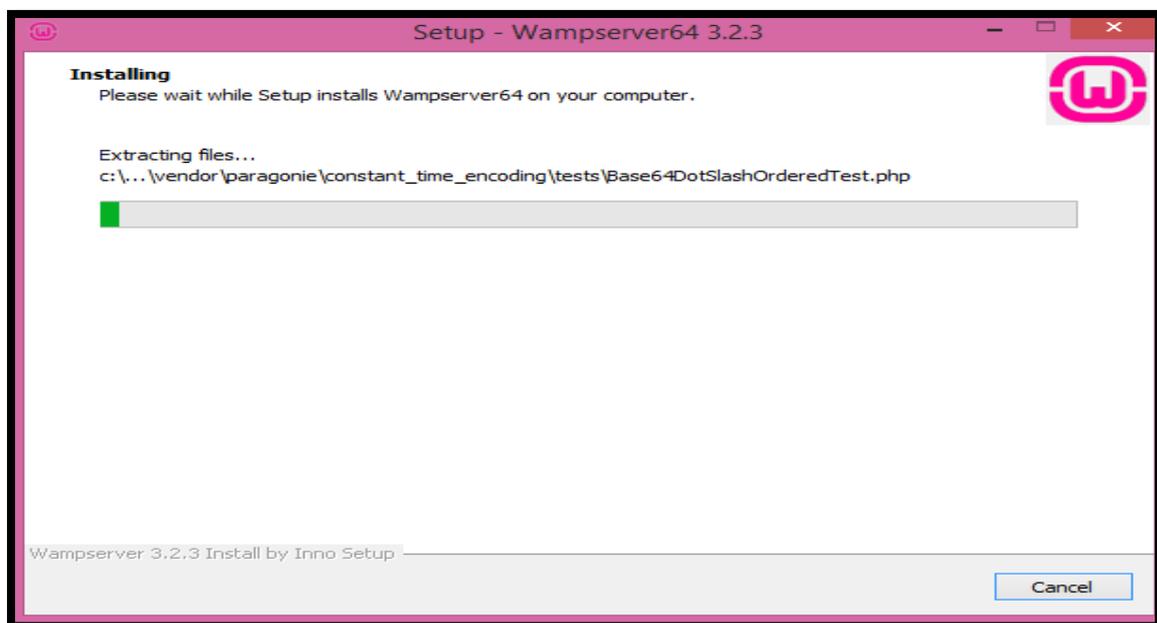
Step 9:- We can edit the name



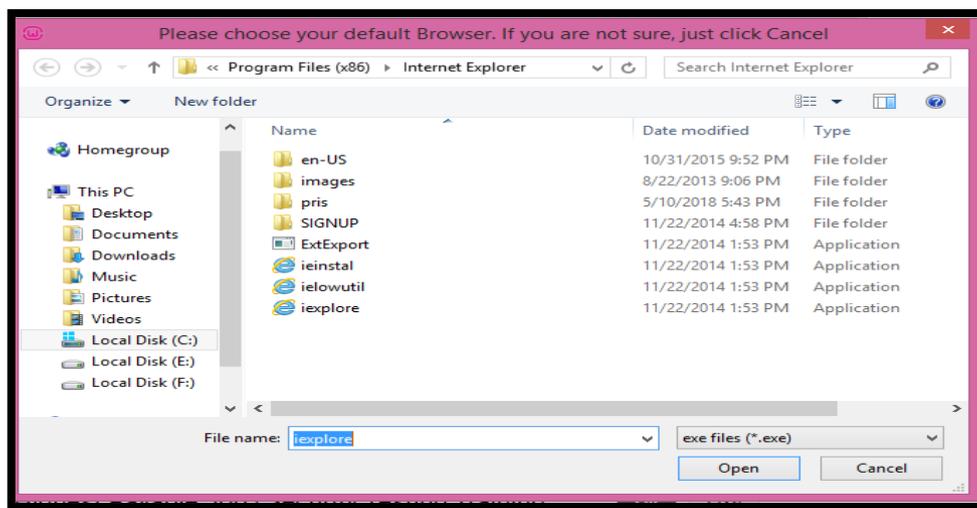
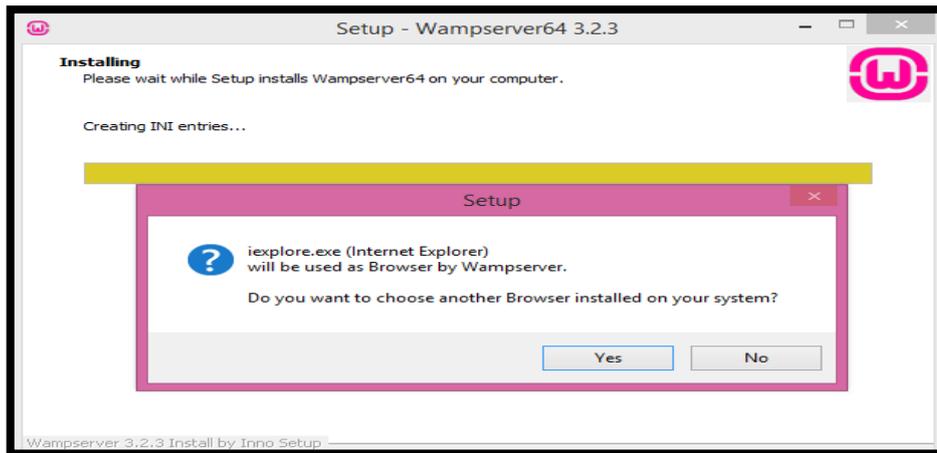
Step 10:- Showing the installation is ready



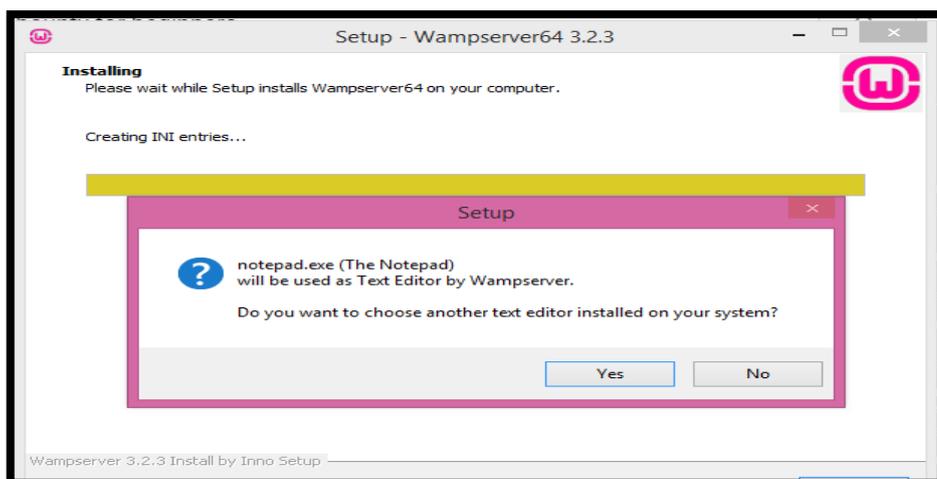
Step 11:- Installation process is going on



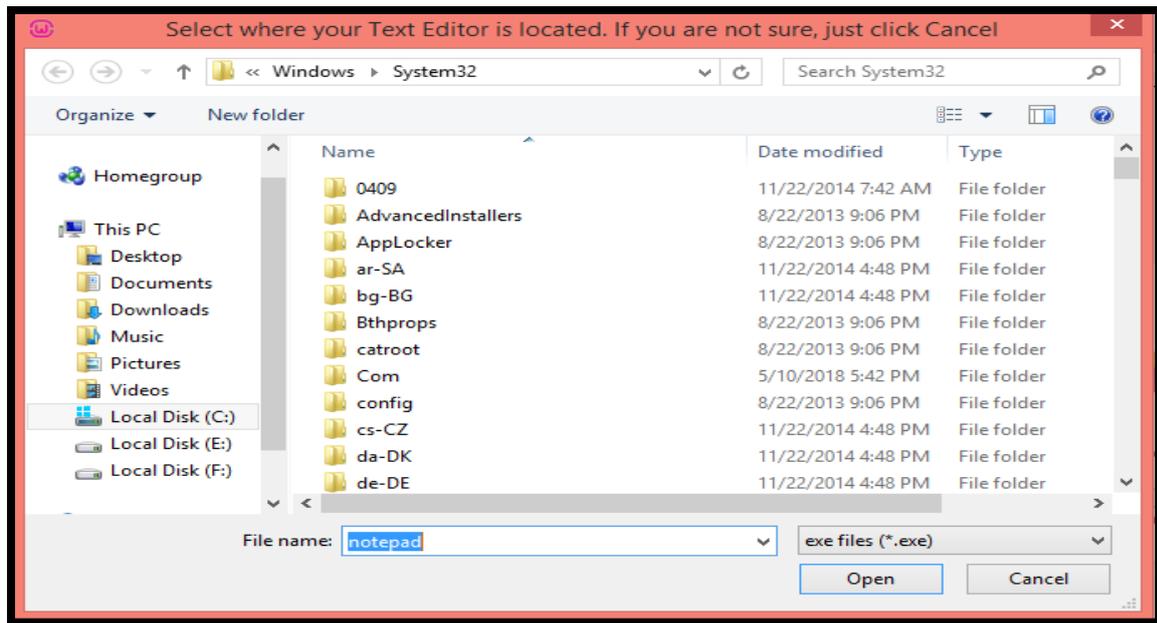
Step 12:-Click on yes for linking to web browser



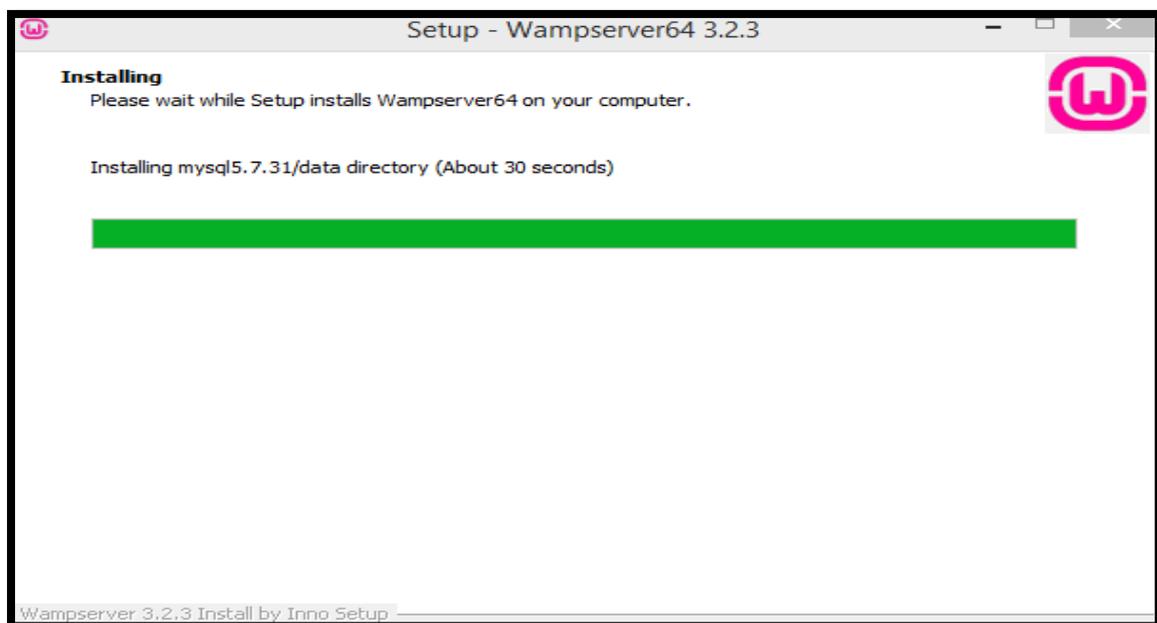
Step13:- Linking notepad

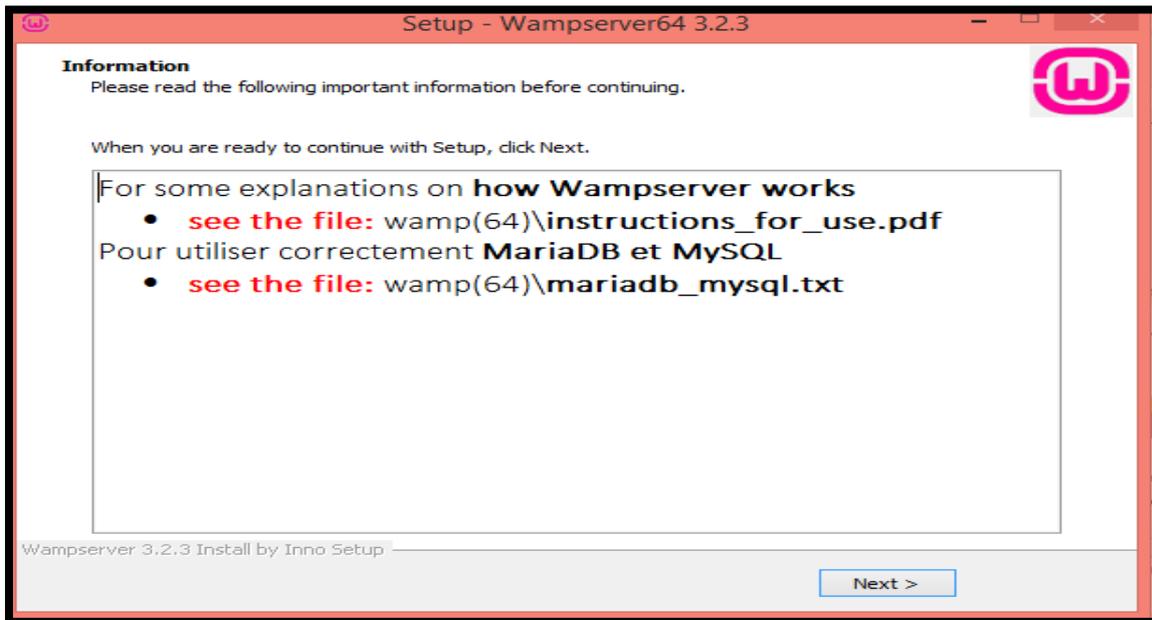


Step 14:- Select destination location

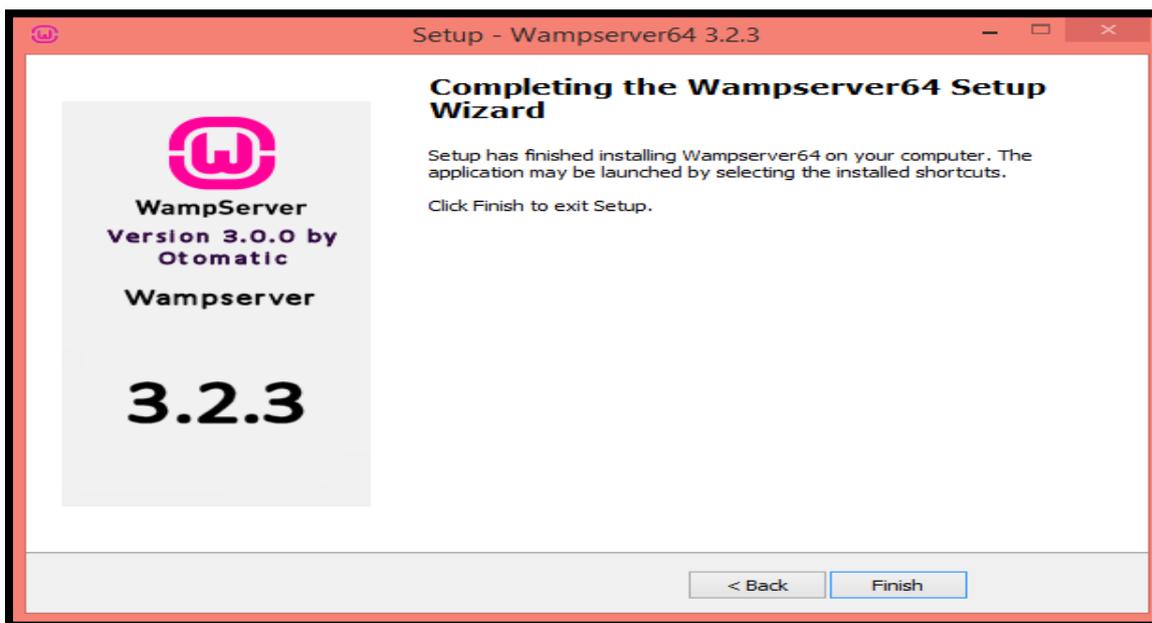


Step 15:- Installation and Warning

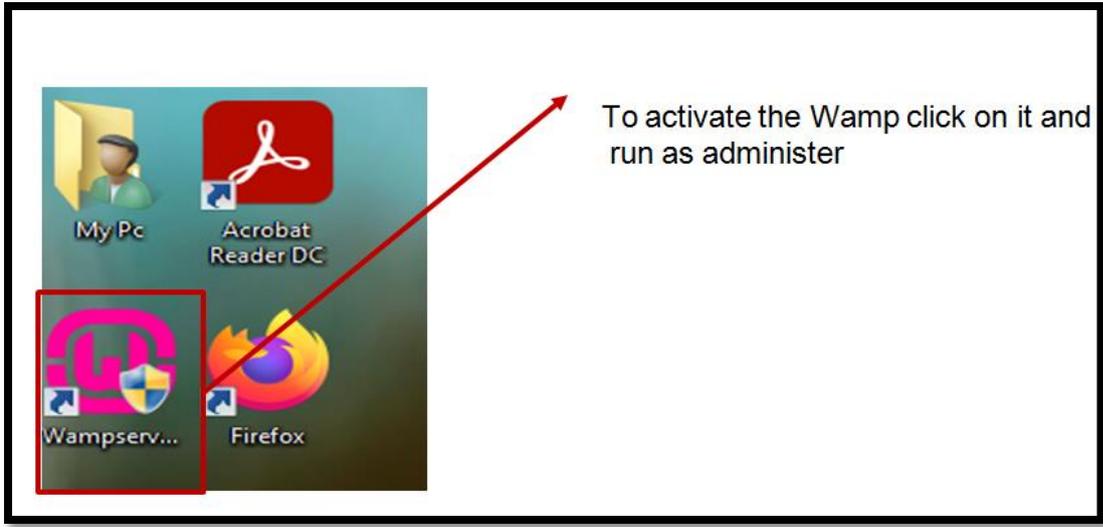




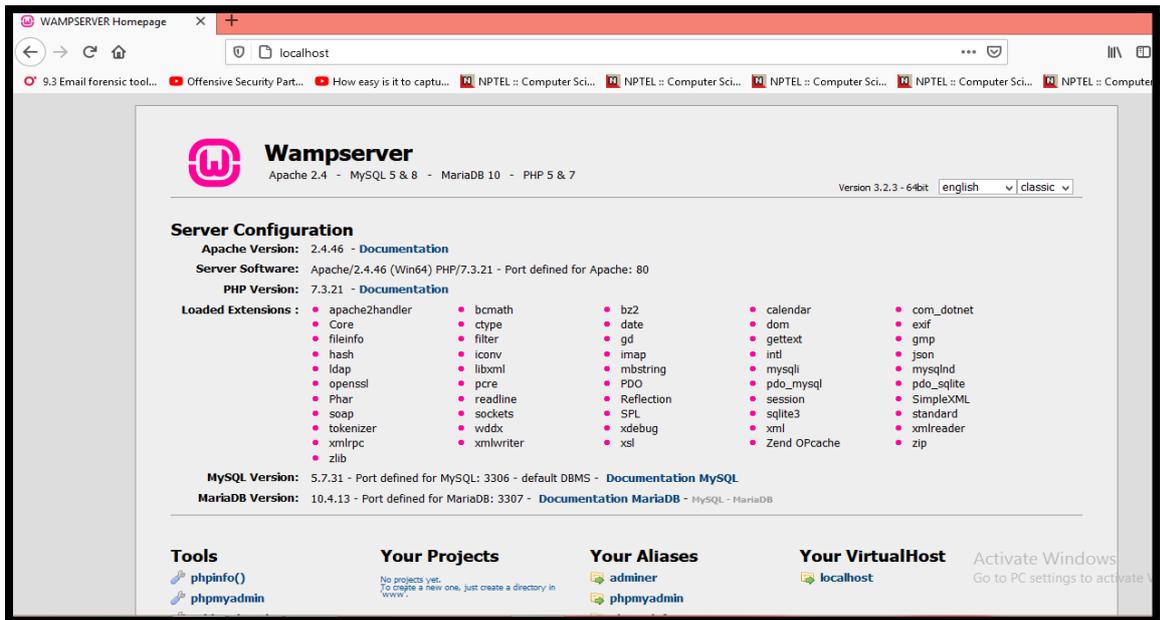
Step 16:- Click on finish



To activate WAMP



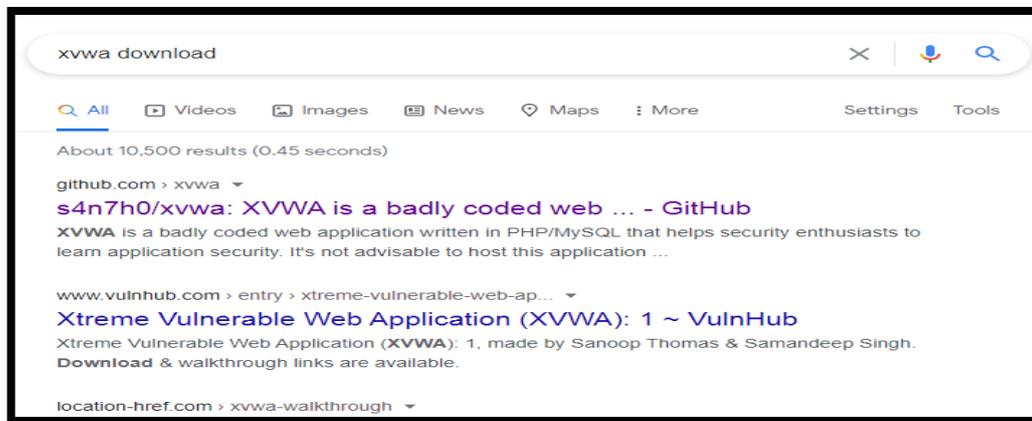
In Firefox write local host



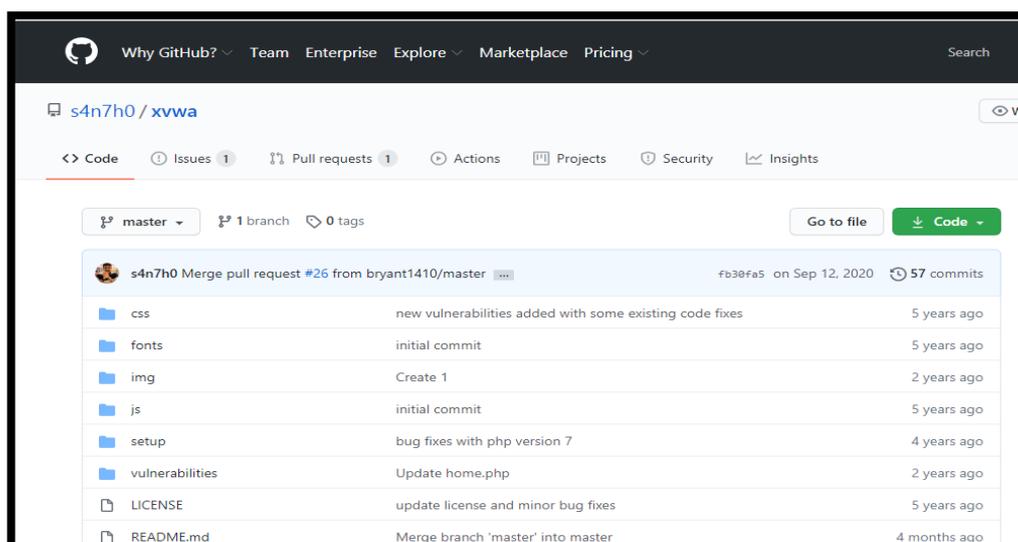
Introduction to Xtreme Vulnerable Web Application

Xtreme Vulnerable Web Application (XVMA) is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security.

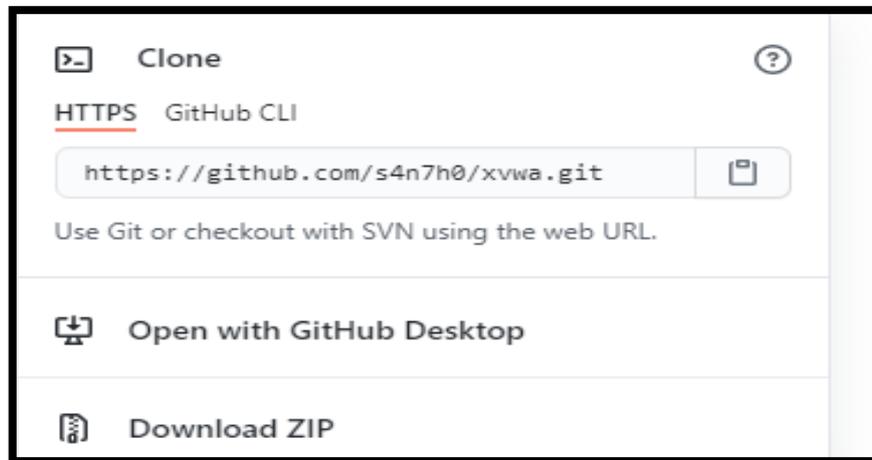
Step1: Type XVWA download in the dialogue box



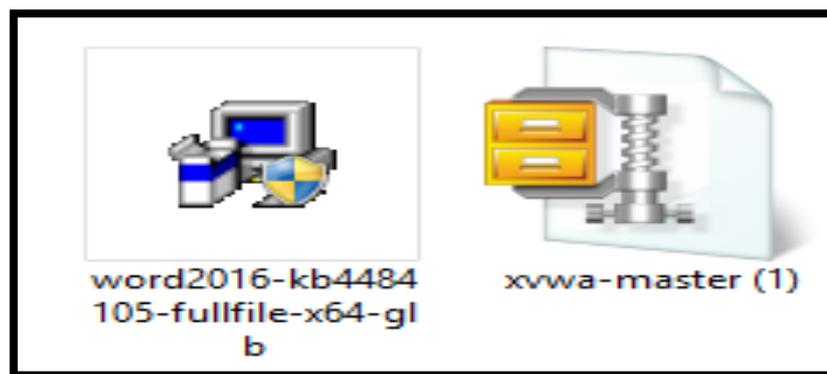
Step 2: After getting XVWA in search



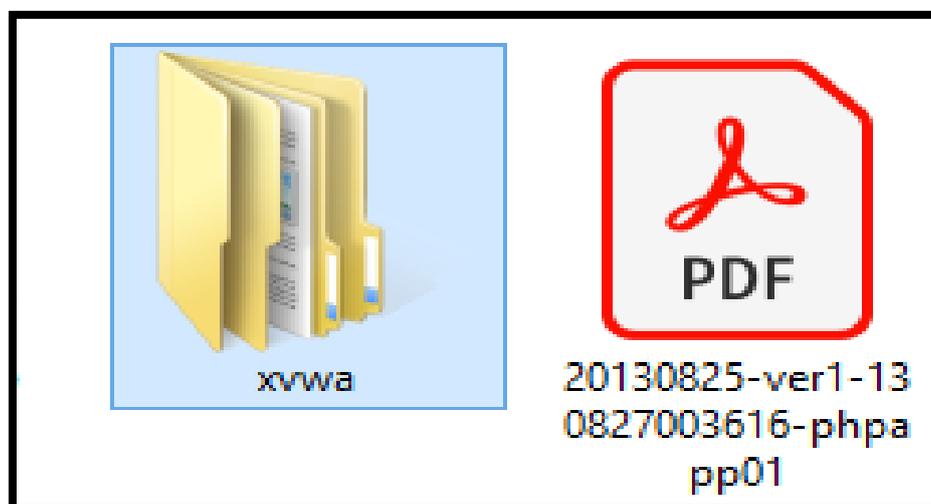
Step 3: Open the website Github



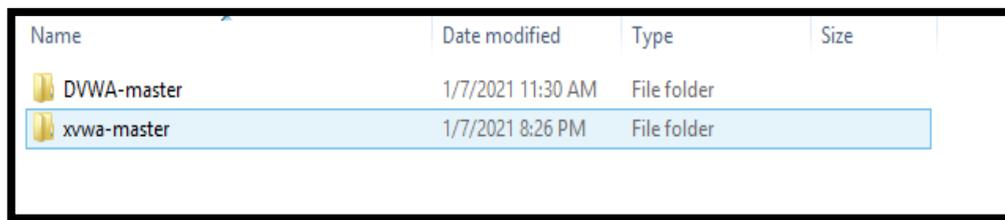
Step 4: Download the ZIP file



Step 5: Save the folder XVWA

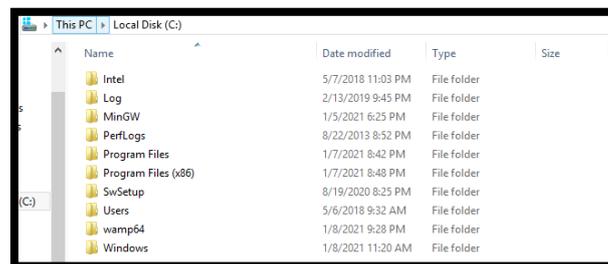


Step 6: Open XVWA-Master folder



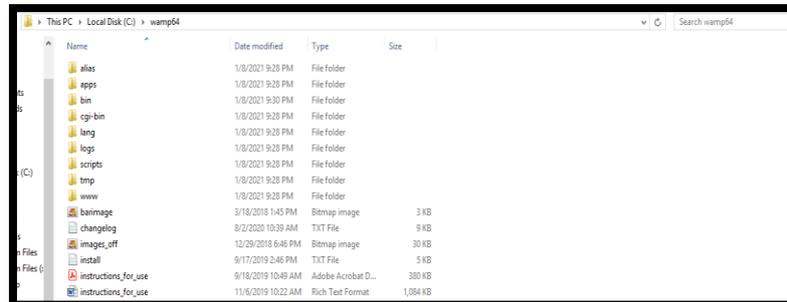
Name	Date modified	Type	Size
DVWA-master	1/7/2021 11:30 AM	File folder	
xvwa-master	1/7/2021 8:26 PM	File folder	

Step 7: Search for wamp64 folder



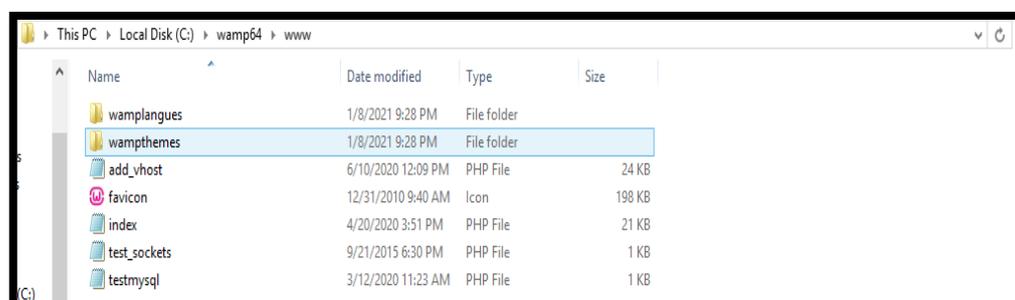
Name	Date modified	Type	Size
Intel	5/7/2018 11:03 PM	File folder	
Log	2/13/2019 9:45 PM	File folder	
MinGW	1/5/2021 6:25 PM	File folder	
PerlLogs	8/22/2013 8:52 PM	File folder	
Program Files	1/7/2021 8:42 PM	File folder	
Program Files (x86)	1/7/2021 8:48 PM	File folder	
SwSetup	8/19/2020 8:25 PM	File folder	
Users	5/6/2018 9:32 AM	File folder	
wamp64	1/8/2021 9:28 PM	File folder	
Windows	1/8/2021 11:20 AM	File folder	

Step 8: Open wamp64 folder



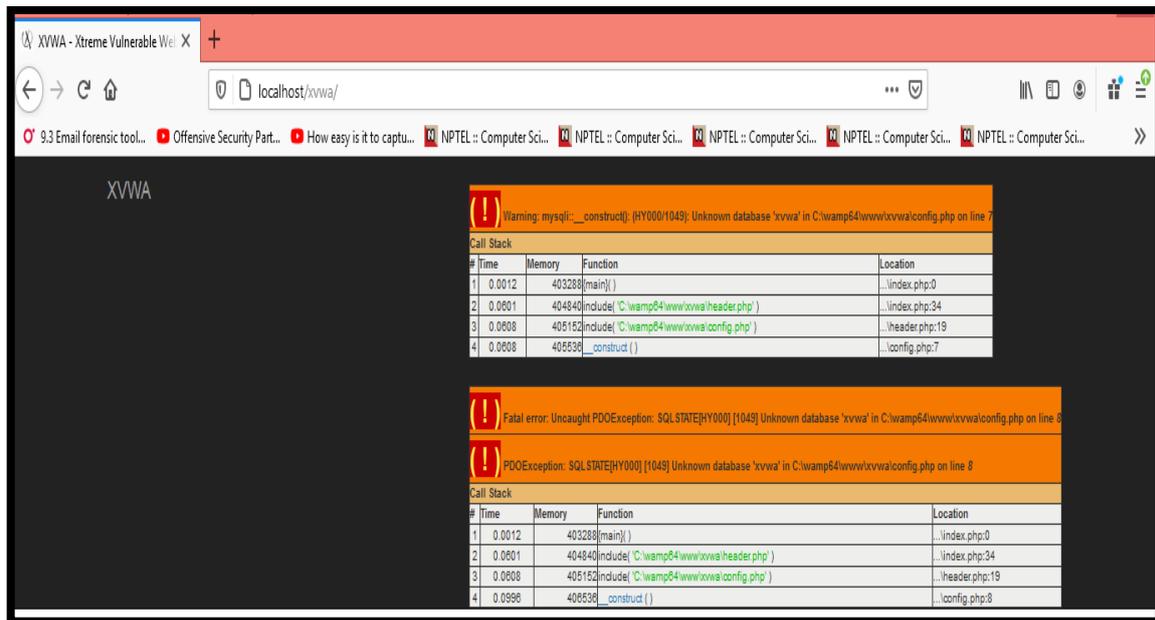
Name	Date modified	Type	Size
alias	1/8/2021 9:28 PM	File folder	
apps	1/8/2021 9:28 PM	File folder	
bin	1/8/2021 9:30 PM	File folder	
cgi-bin	1/8/2021 9:28 PM	File folder	
lang	1/8/2021 9:28 PM	File folder	
logs	1/8/2021 9:28 PM	File folder	
scripts	1/8/2021 9:28 PM	File folder	
tmp	1/8/2021 9:28 PM	File folder	
www	1/8/2021 9:28 PM	File folder	
banimage	3/18/2018 1:45 PM	Bitmap image	3 KB
changelog	8/2/2020 10:39 AM	TXT File	9 KB
images_off	12/29/2018 6:46 PM	Bitmap image	30 KB
install	9/17/2019 2:46 PM	TXT File	5 KB
instructions_for_use	9/18/2019 10:49 AM	Adobe Acrobat D...	380 KB
instructions_for_use	11/8/2019 10:22 AM	Rich Text Format	1,084 KB

Step 9: Then Open wampthemes folder

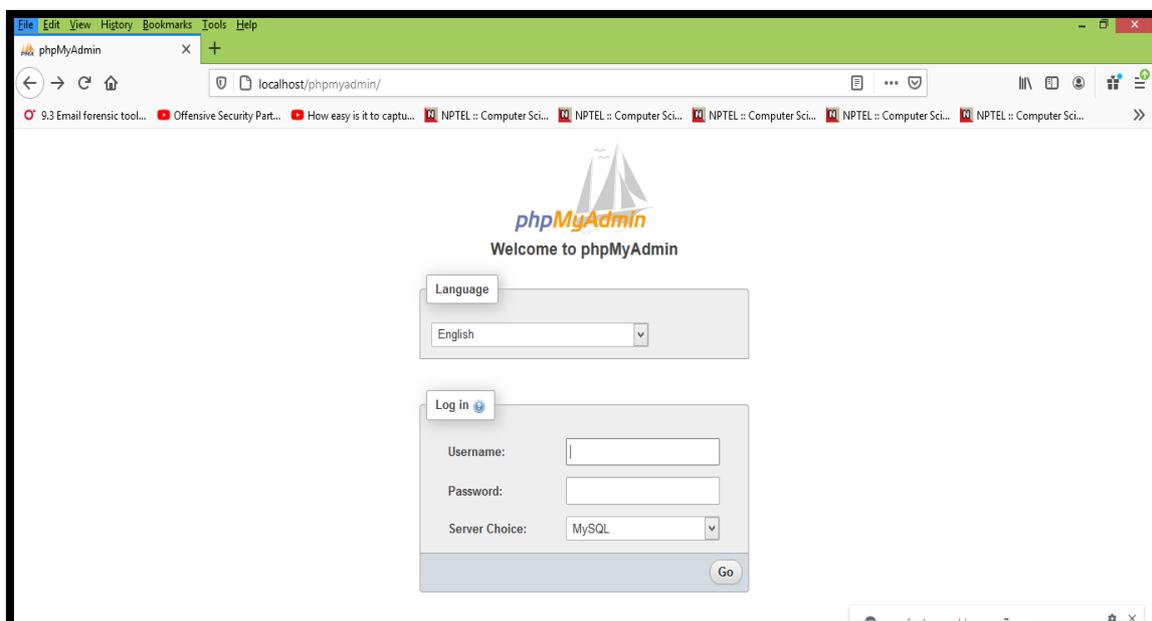


Name	Date modified	Type	Size
wamplanguages	1/8/2021 9:28 PM	File folder	
wampthemes	1/8/2021 9:28 PM	File folder	
add_yhost	6/10/2020 12:09 PM	PHP File	24 KB
favicon	12/31/2010 9:40 AM	Icon	198 KB
index	4/20/2020 3:51 PM	PHP File	21 KB
test_sockets	9/21/2015 6:30 PM	PHP File	1 KB
testmysql	3/12/2020 11:23 AM	PHP File	1 KB

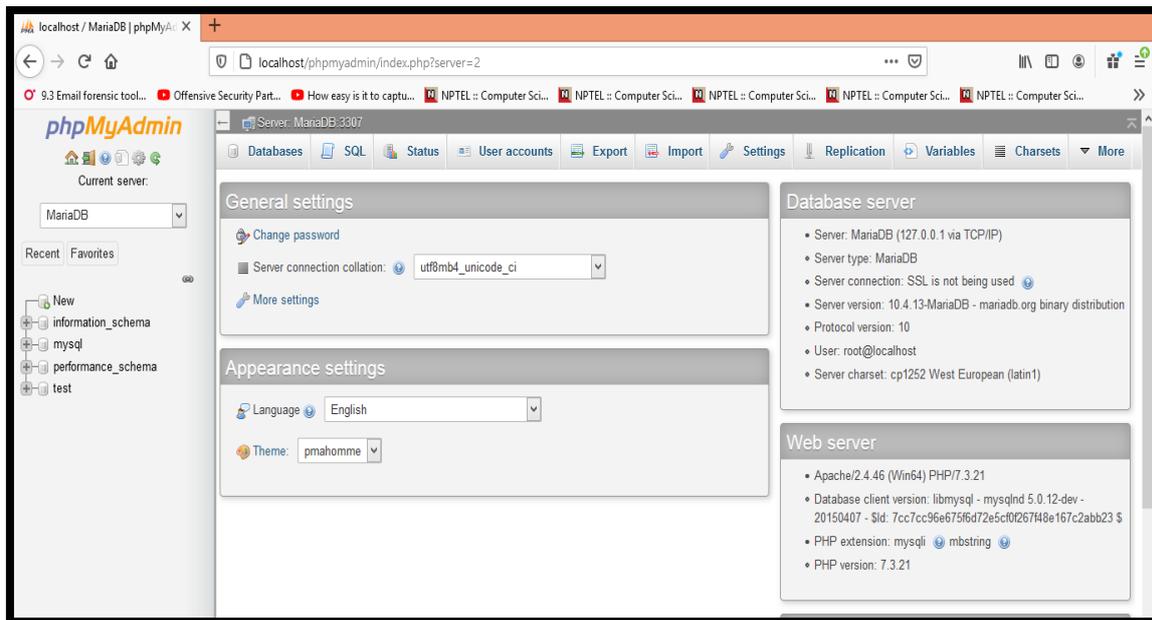
Step 10: Run xvwa in local server



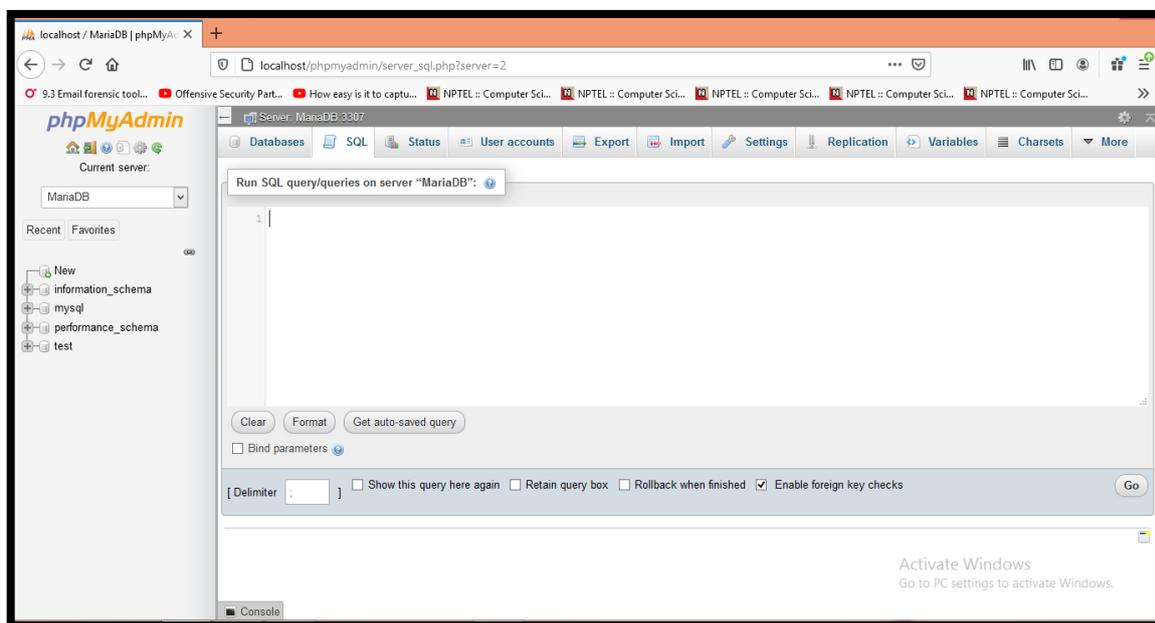
Step 11: Fill login credentials



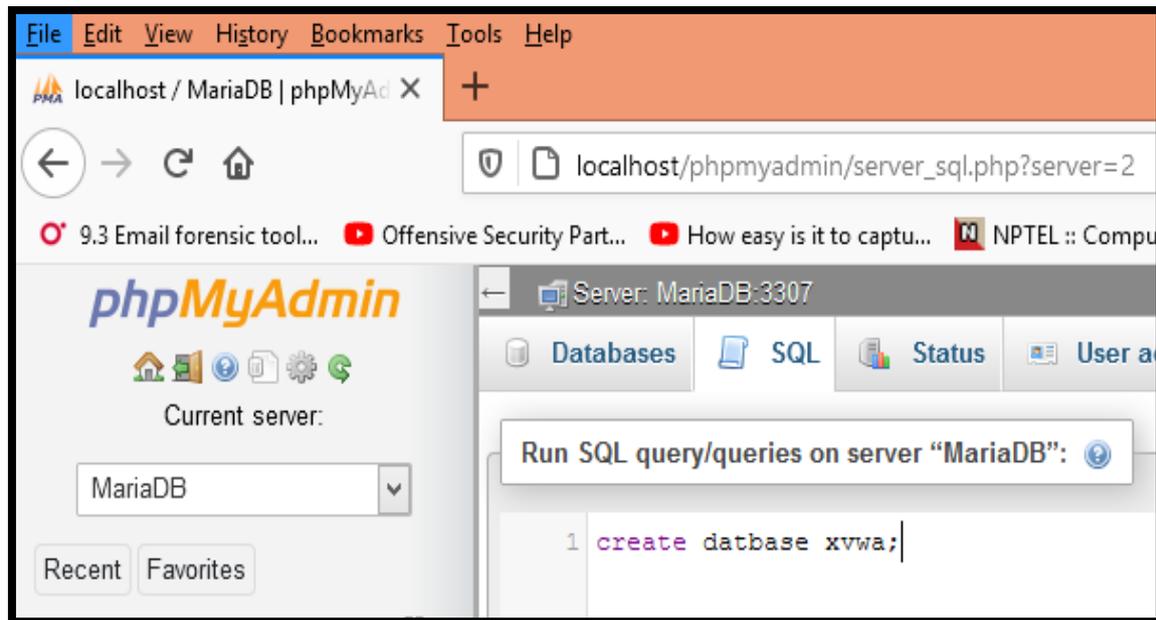
Step 12: Here it is showing the General setting



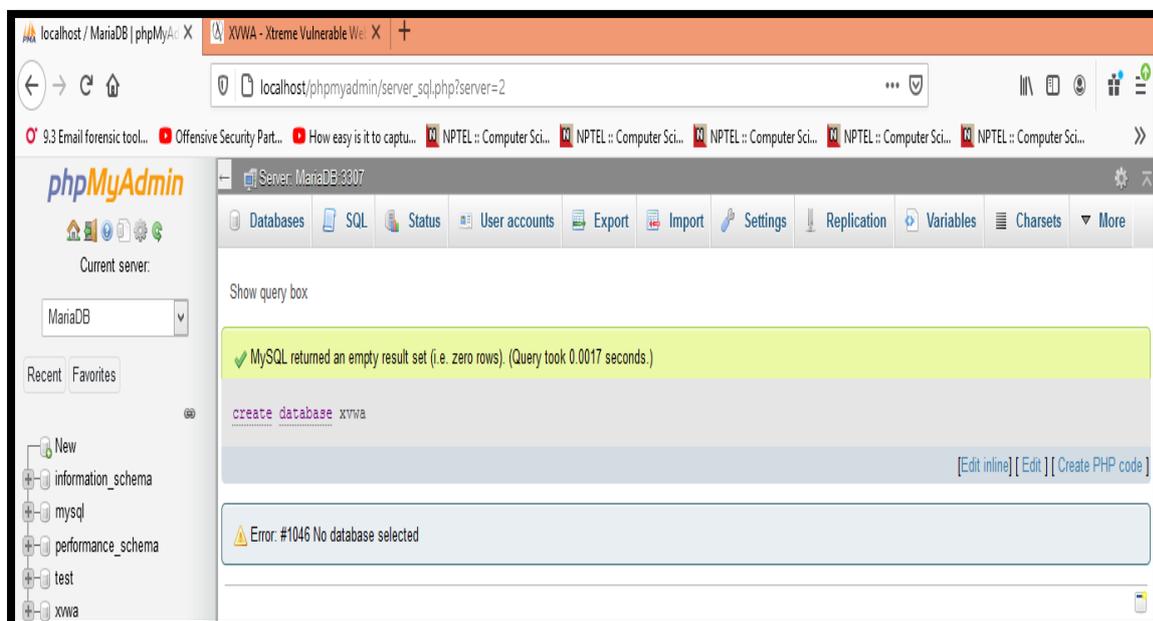
Step 13: Run SQL query/queries



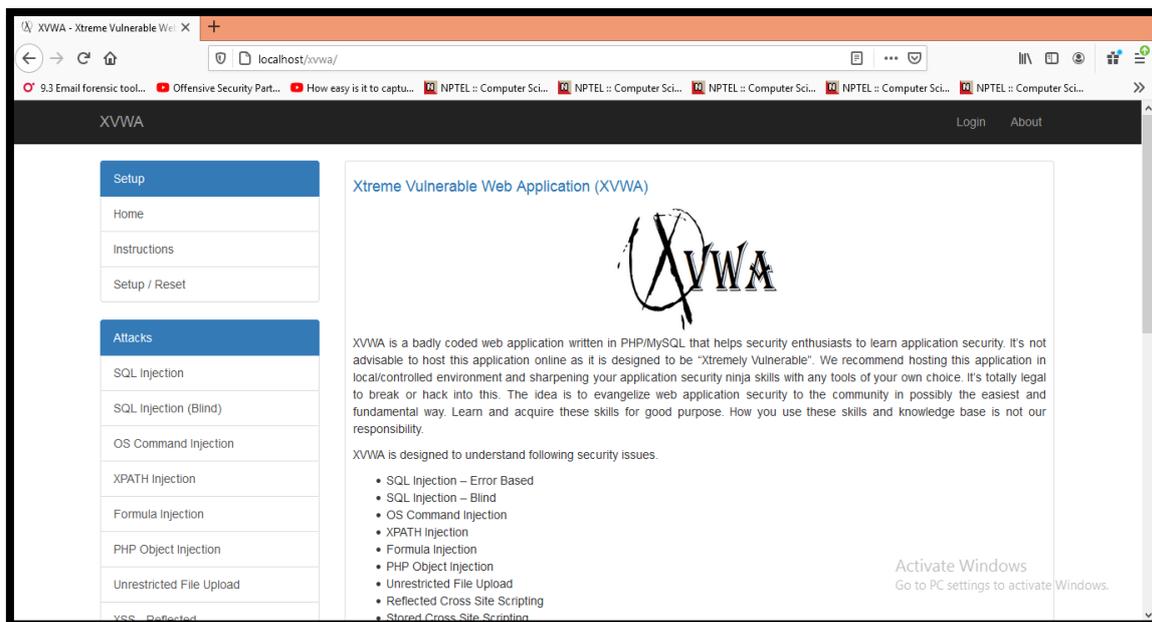
Step 14: Click on SQL > then run query.



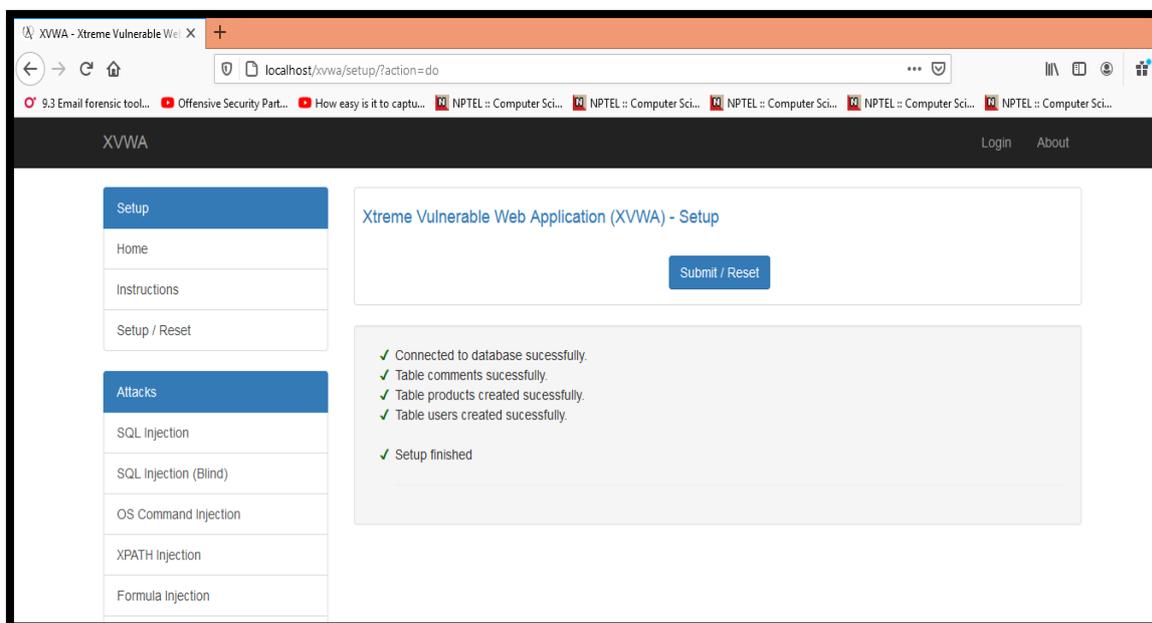
Step 15: MySQL returned an Empty result



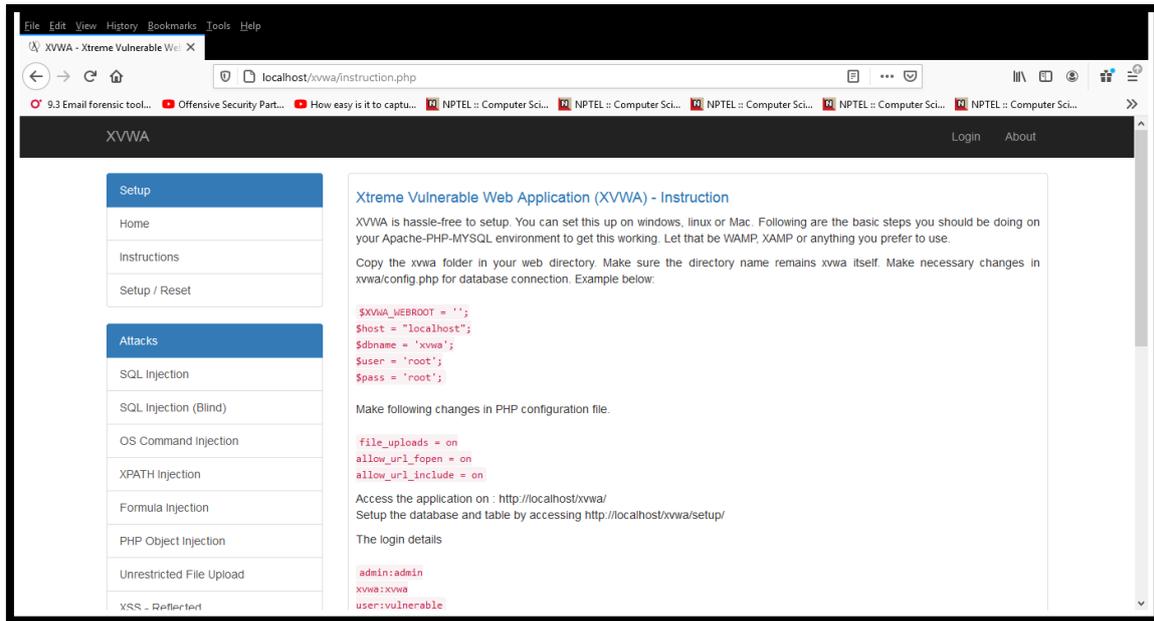
Step 16: Run XVWA in local server



Step 17: Setup Settings



Step 18: XVWA Instruction



Step 19: Fill Credentials to login.

