LAB

Easy Chat Server & Get Simple CMS

v.1.0

Ni’am Habibiy Sahid

Detail Dokumen

Judul Dokumen	: Instalasi Lab untuk Praktikal Mandiri
Tujuan Dokumen	: Universitas Amikom Purwokerto
Tanggal	: 19 Juni 2023
Tipe Dokumen	: Lab Manual
Klasifikasi	: Publik

Disclaimer :

Dokumen ini diberikan sedemikian adanya, untuk menjadi bahan belajar membuat Lab pada lokal PC / Laptop / Virtual Machine bagi teman teman semua.

Instalasi lab dilakukan dan dapat berjalan dengan baik pada device milik penulis dengan spesifikasi RAM diatas 8 GB. Penulis tidak bertanggung jawab terhadap eror atau kerusakan yang terjadi selama pembuatan lab. Silahkan lakukan dengan tanggung jawab terhadap gawai milik masing masing.

Instalasi lab di lokal pribadi :

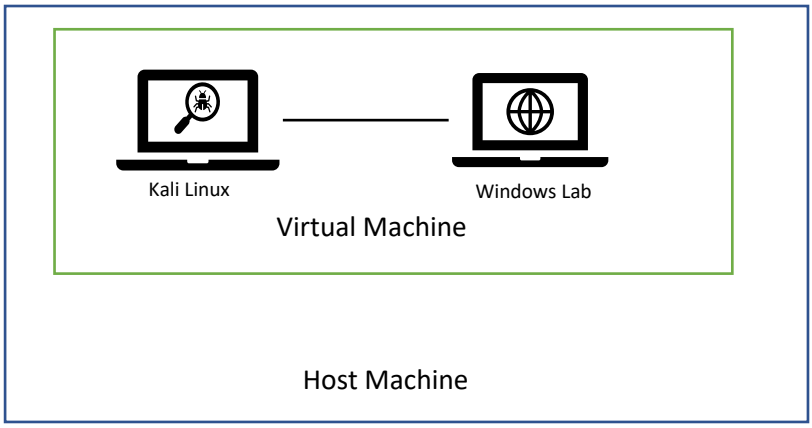
Prequisite :

XAMPP (tidak akan dibahas disini, asumsinya semua sudah bisa)

Windows terinstall di laptop/PC/vmware/virtualbox

Ada dua aplikasi yang akan digunakan untuk test yaitu Easy Chat Server, yang mempunyai kerentanan berupa Directory Traversal dan Arbitraty File Read, dan Get-Simple CMS.

Asumsi dari Lab yang akan dibuat pada dokumen ini adalah attacker akan menggunakan mesin Kali Linux yang berada satu jaringan dengan mesin Windows Lab yang menjalankan service berupa web apps yang memiliki kerentanan. Untuk membuat hal tersebut, kita dapat menjalankan dua VM pada virtualbox/vmware.



Berikut IP Address milik penulis :

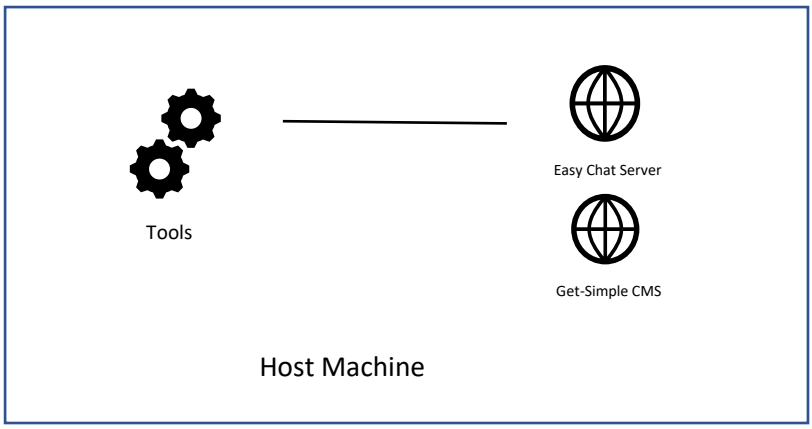
- Kali Linux : 192.168.112.136
- Windows 10 : 192.168.112.132

Perlu di perhatikan bahwa lab ini tidak mensyaratkan untuk dijalankan pada VM, apabila memori RAM laptop anda kurang dari 8GB, lebih baik jika :

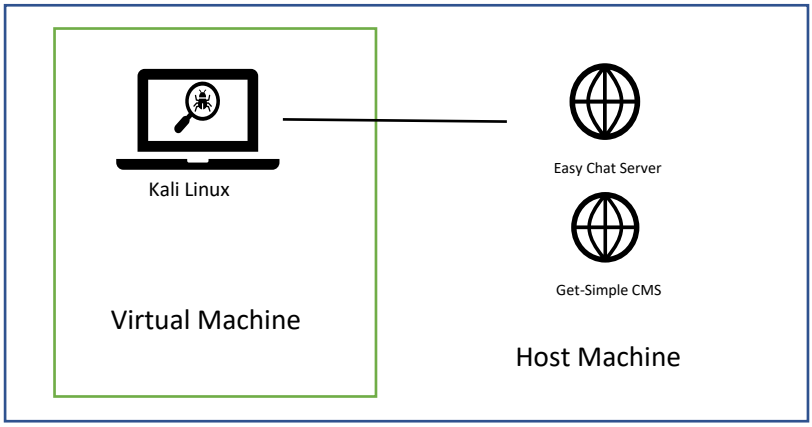
1. Aplikasi di install di lokal laptop saja. Tool untuk melakukan serangan juga di install pada lokal laptop/pc.
2. Atau bisa juga kali linux vm dijalankan dari virtual sedangkan aplikasi di install pada laptop windows.
3. Atau Windows dijalankan di VM sedangkan penyerang menggunakan Host machine sebagai mesin penyerang.

Feel free untuk melakukan penyesuaian lab sesuai keinginan.

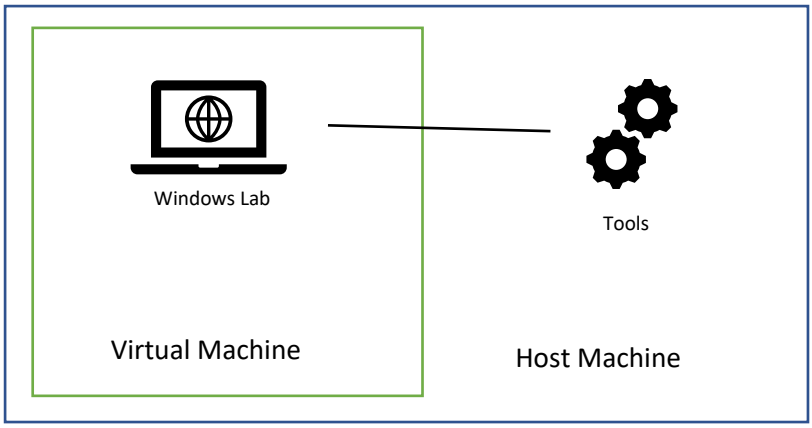
1. Tools untuk menyerang, Aplikasi Easy Chat Server & get Simple CMS di install di Laptop/PC



2. Kali Linux di letakkan pada VM sedangkan Easy Chat Server & Gest-Simple CMS di install di Host Machine.



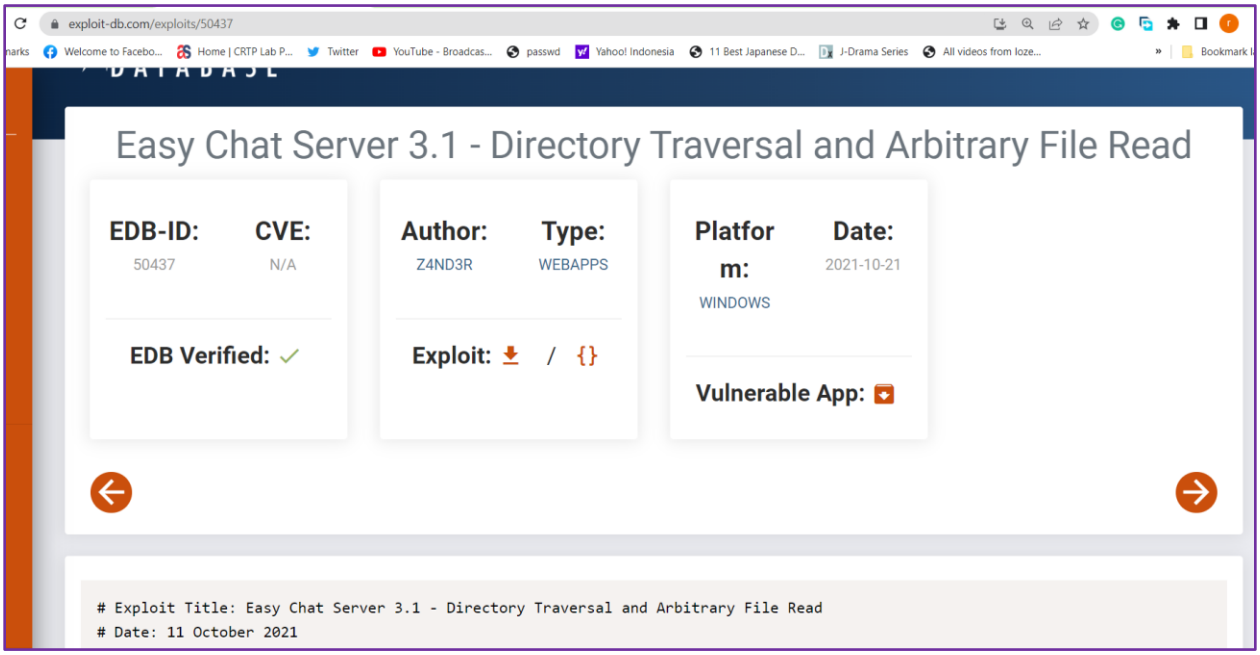
3. Windows Lab berisi Easy Chat Sever & Get-Simple CMS di letakkan pada VM sedangkan tool untuk menyerang di install pada Host Machine.


Windows Lab
Tools
Virtual Machine
Host Machine

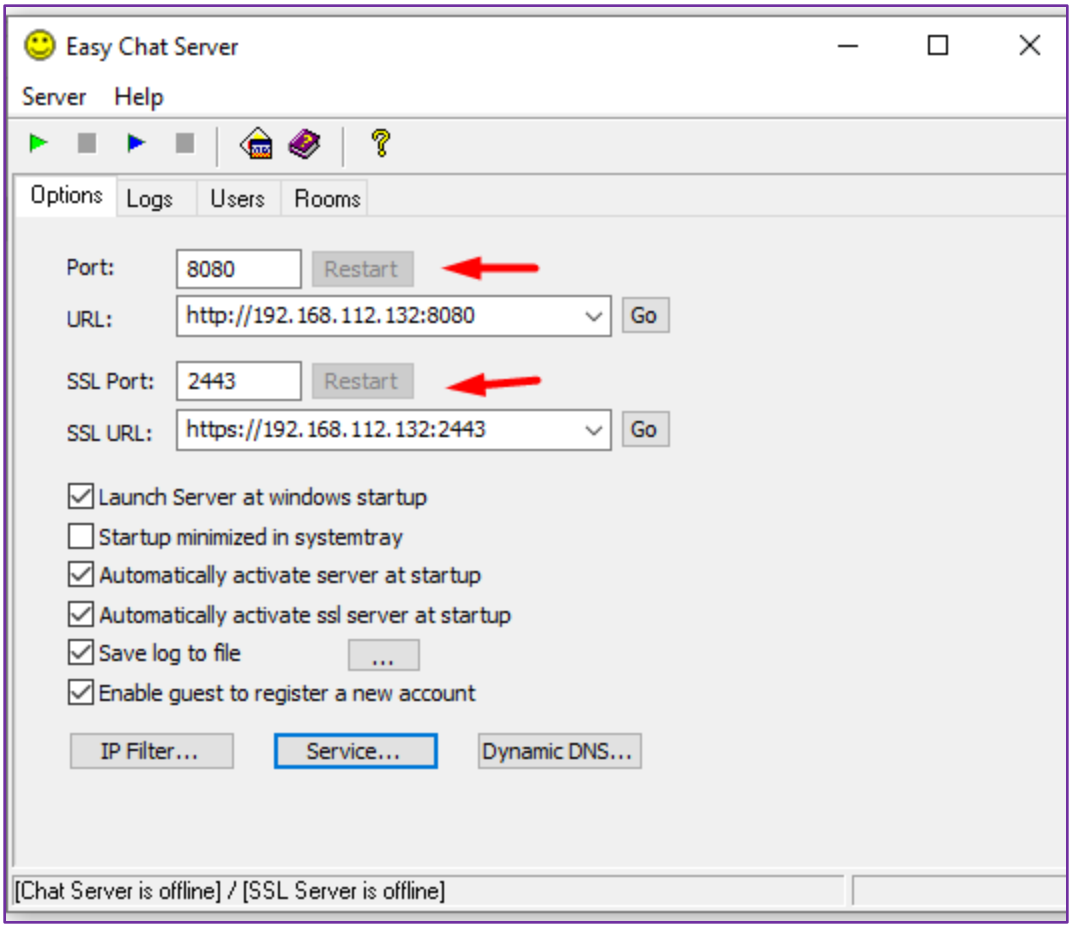
A. Instalasi Easychat server

Untuk mendownload versi vulnerable kita bisa mendapatkannya dari exploit-db

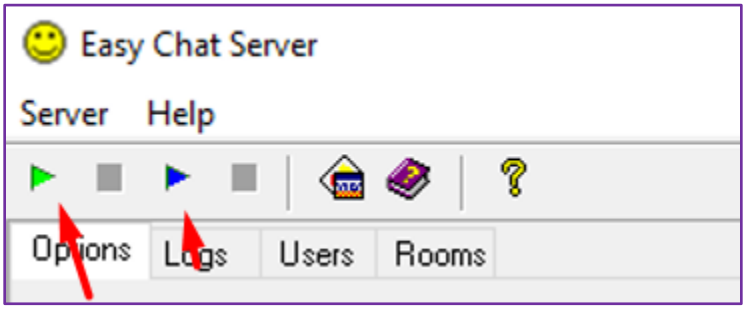
https://www.exploit-db.com/exploits/50437

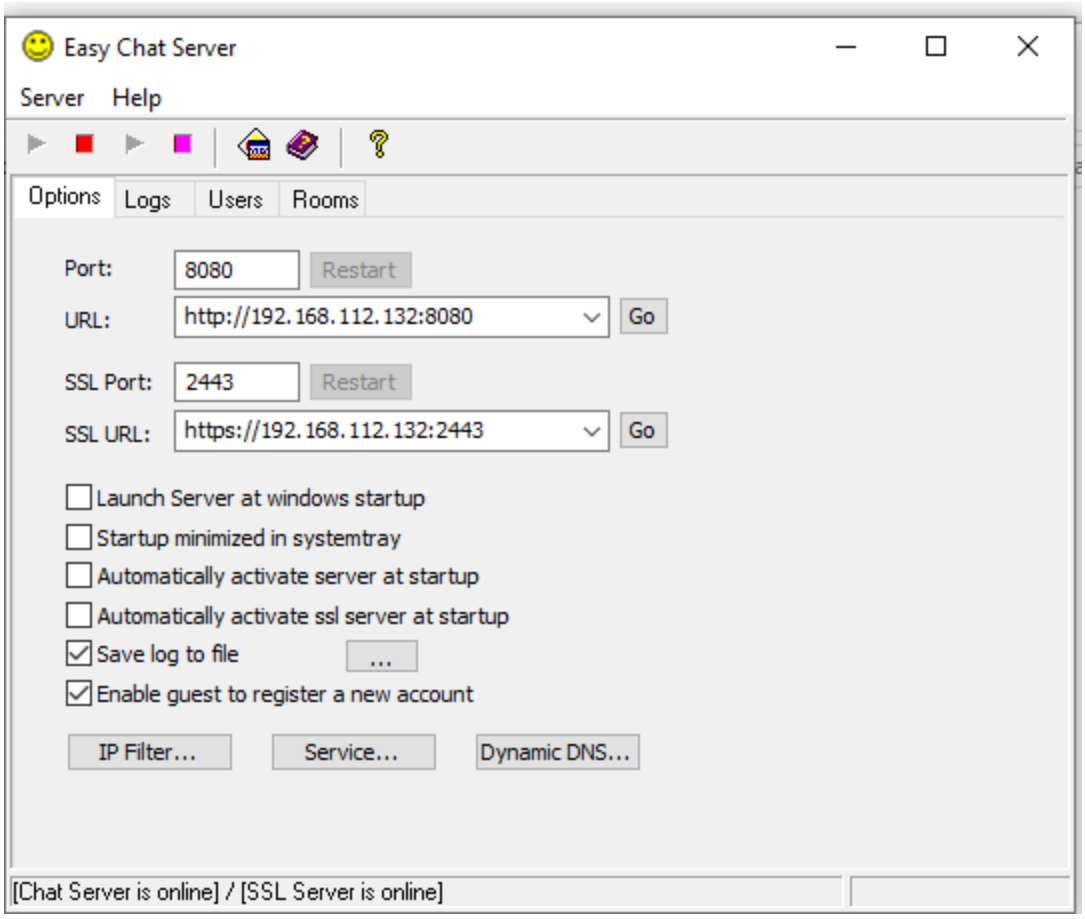


1. Download file yang vulnerable dengan mengklik tombol unduh pada bagian Vulnerable App.
2. Jalankan easy server, kemudian pilih trial
3. Ubah port http nya ke 8080 dan port https nya ke 2443



4. Pastikan untuk mencentang checkbox pada “Launch Server at windows Startup” apabila ingin Easy Chat Server berjalan otomatis ketika windows startup. Namun tidak diperlukan untuk lab ini.
5. Klik tombol “start the server” dan “start the ssl server”





6. Buka cmd kemudian perhatikan apakah port 8080 dan 2443 sudah berjalan dengan command *netstat -ano*

```
C:\Users\murid.sariya>netstat -nao

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       996
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:2443           0.0.0.0:0              LISTENING       212
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       1092
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       212
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       836
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       756
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1076
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1036
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       708
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       836
  TCP    0.0.0.0:49690          0.0.0.0:0              LISTENING       828
  TCP    192.168.112.132:139    0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       996
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       836
  TCP    [::]:49665             [::]:0                 LISTENING       756
```

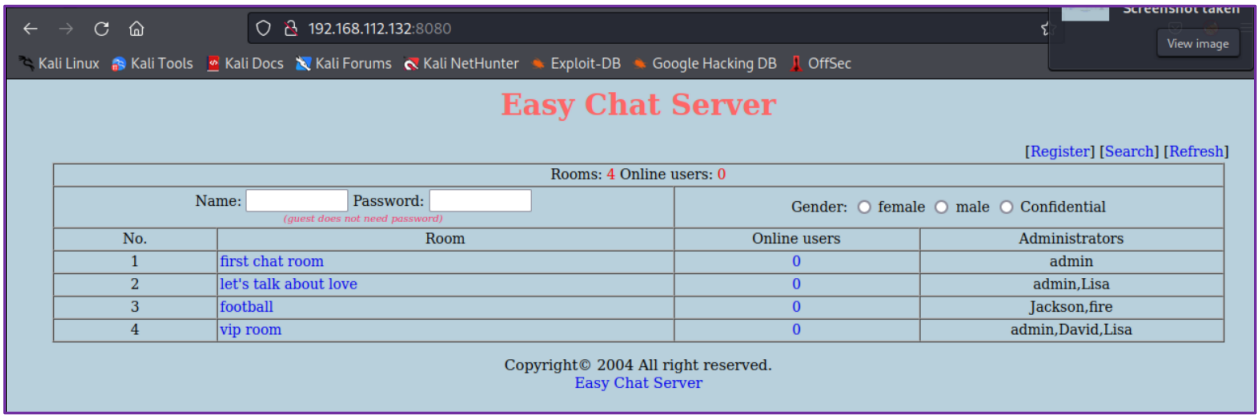
7. Coba scan menggunakan nmap atau dengan membuka http://ip-lab:8080,

Mengecek dari localhost :

http://localhost:8080 atau http://127.0.0.1:8080/

Mengecek dari IP address lain : http://192.168.112.132:8080

Yang perlu diperhatikan, karena kita hanya menggunakan versi trial, easy chat server dibatasi hanya dapat berjalan selama 30 menit kemudian port akan mati namun aplikasi easychat masih bejalan. Karena port sudah mati dan service untuk easychat server sudah di hentikan, kita tidak akan bisa membuka web Easy Chat pada port 8080. Untuk dapat kembali berjalan, kita harus mematikan aplikasi kemudian menjalankan ulang.



Selamat Easy Chat Server sudah berjalan, kita bisa mencoba melakukan exploitasi.

PS : Tambahan saja, setelah 30 menit berjalan port Easy Chat Server mati, namun proses EasyChat masih berjalan. Apabila ingin mematikan aplikasi secara otomatis setelah 30 menit, kemudian otomatis menjalankannya kembali, teman teman bisa membuat scriptnya menggunakan powershell. Berikut referensi yang bisa di cek dan mungkin bisa membantu pembuatan scriptnya.

Untuk mematikan proses :

https://dzhavat.github.io/2020/04/09/powershell-script-to-kill-a-process-on-windows.html

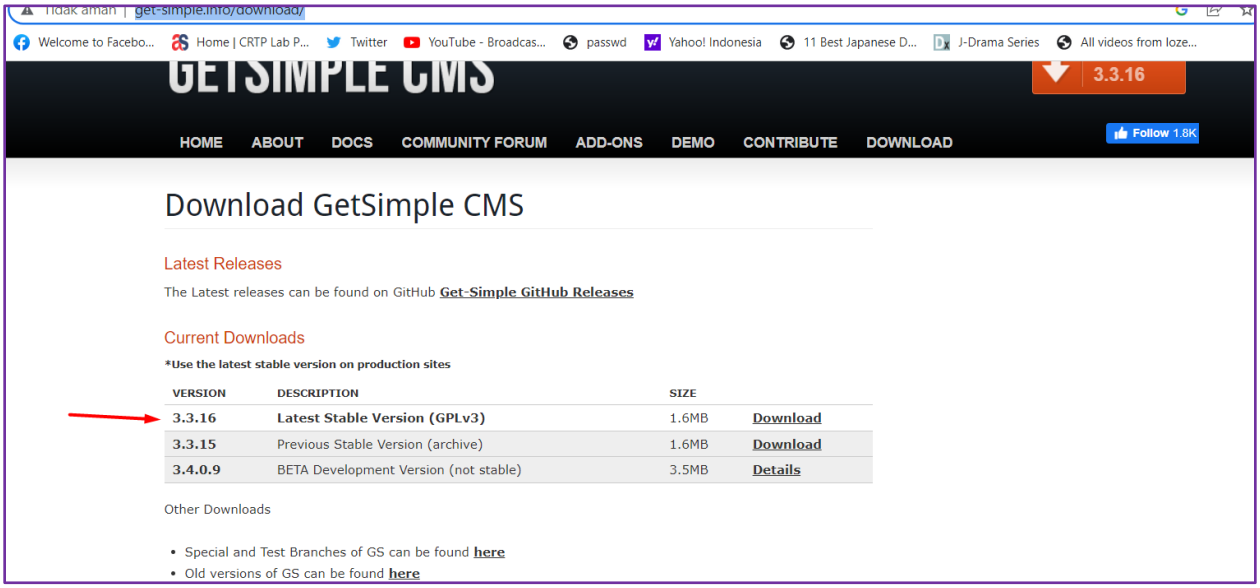
Untuk menyalakan otomatis menggunakan powershell (click button pada aplikasi) :

https://stackoverflow.com/questions/38225874/mouse-click-automation-with-powershell-or-other-non-external-software

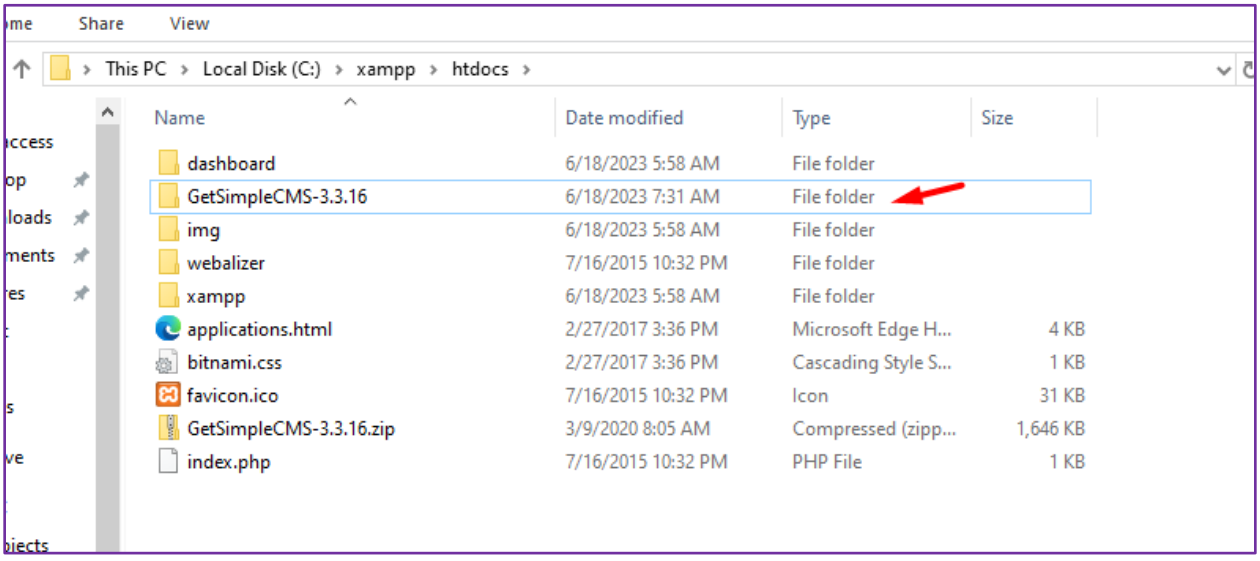
B. Instalasi Get-Simple CMS

Kerentanan yang ada pada Get-Simple CMS, ada pada versi 3.3.16, pada saat dokumen ini dibuat, 18 juni 2023, versi 3.3.16 adalah versi yang paling baru sehingga kita bisa mendownload versi yang rentan dengan mudah karena merupakan last version.

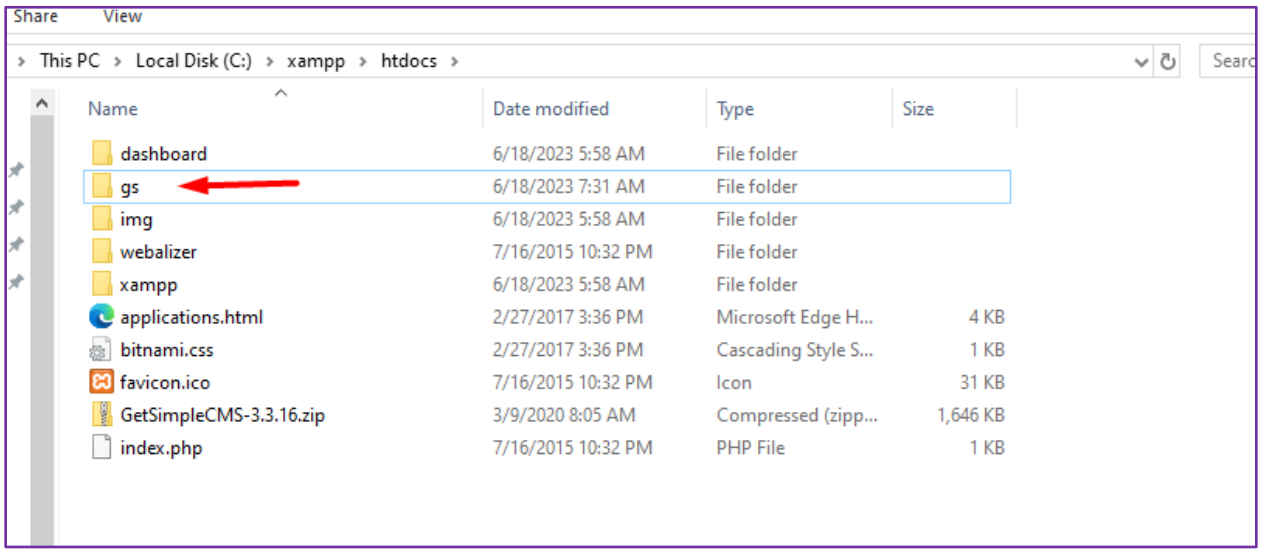
Link Download : http://get-simple.info/download/



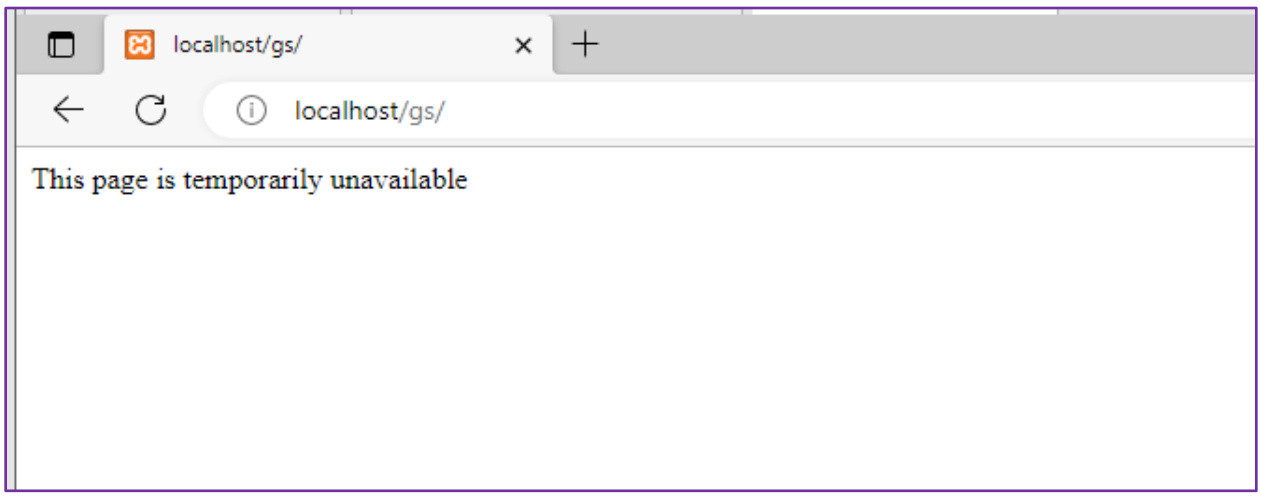
1. Download versi yang rentan
2. Jalankan XAMPP
3. Taruh file GetSimple.zip di folder htdocs pada XAMPP kemudian extract.



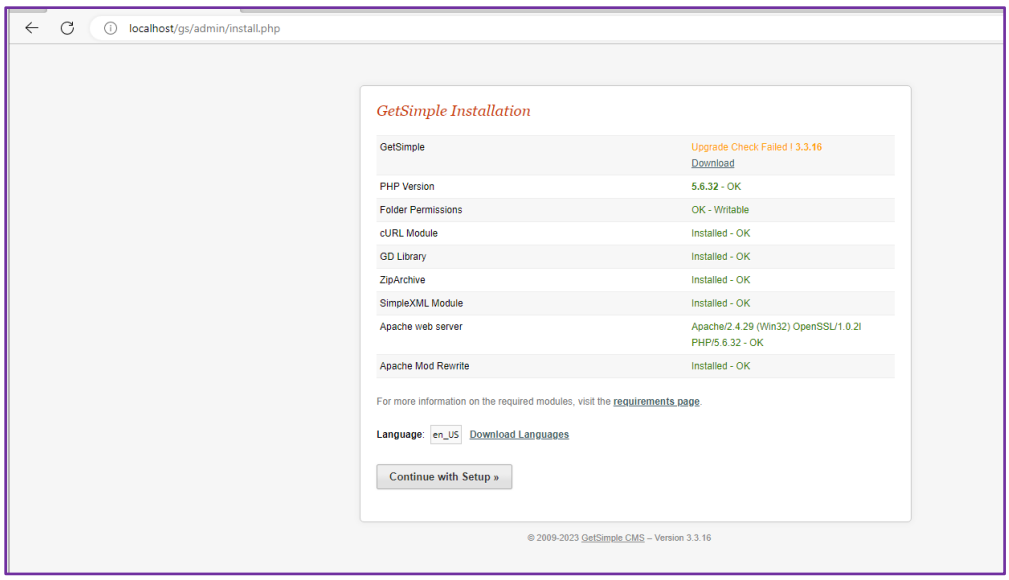
4. Untuk mempermudah, dan juga tidak menunjukkan versi pada nama direktori, ganti nama folder GetSimpleCMS menjadi gs



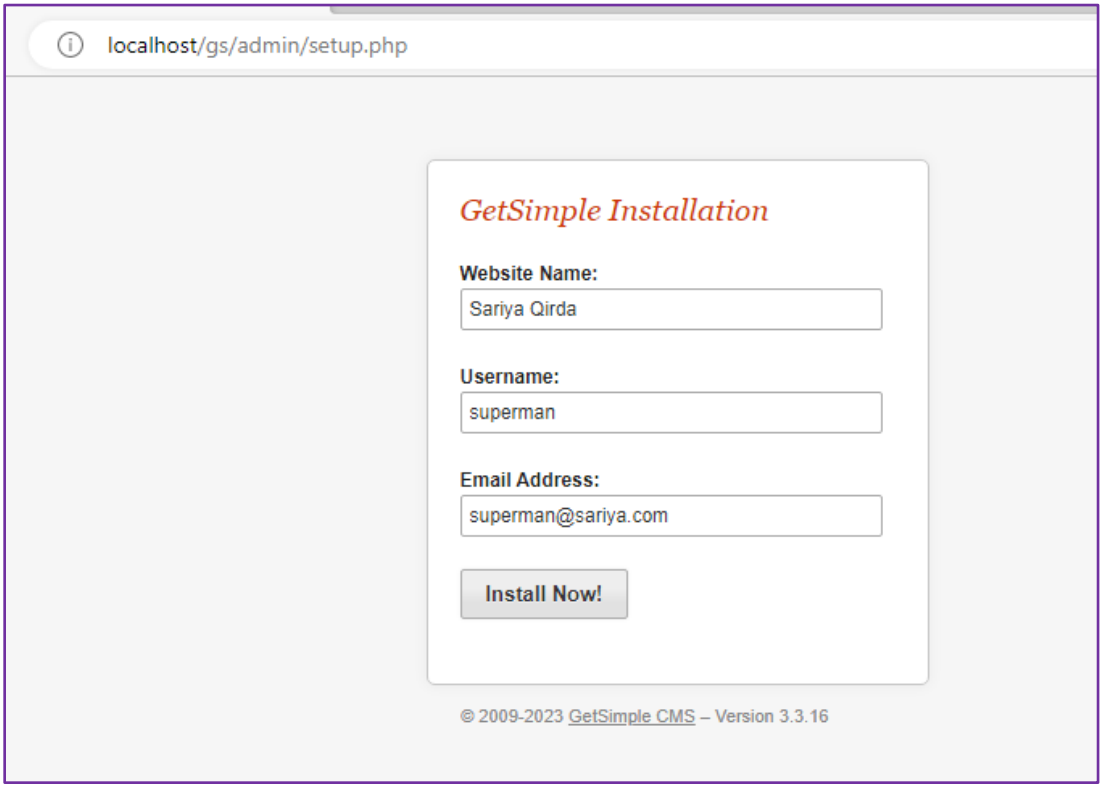
5. Kunjungi pada http://localhost/gs
6. Kita akan menemukan halaman tidak available, karena GetSimple CMS belum terinstall.



7. Kunjungi halaman http://localhost/gs/admin untuk melakukan instalasi.

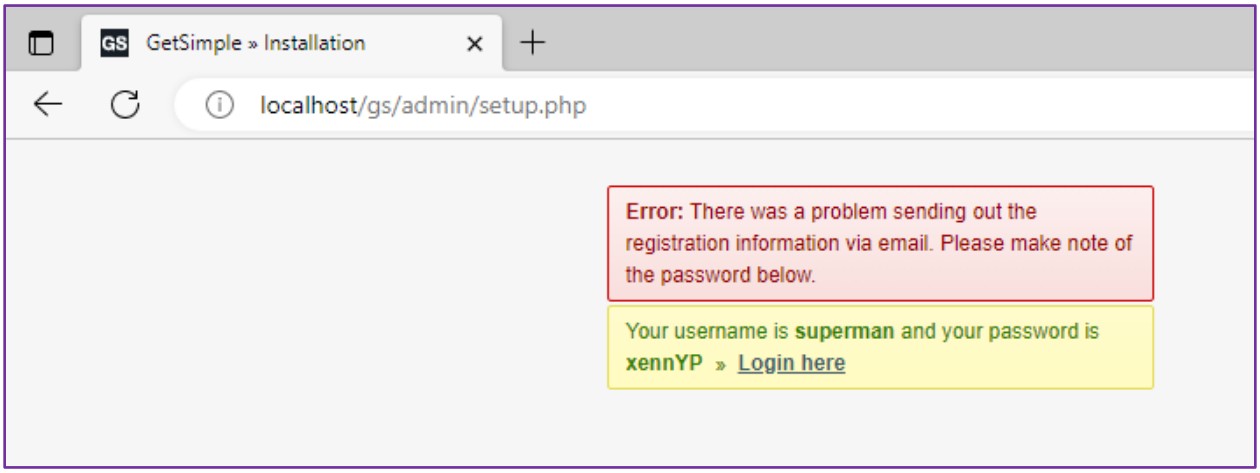


8. Klik tombol “Continue with Setup” kemudian halaman setup akan ditampilkan.
9. Isikan Nama website, username, dan email address nya. Semisal data berikut :
   - Nama Website : Sariya Qirda
   - Username : superman
   - Alamat Email : superman@sariya.com



10. Klik tombol “Install Now!”

11. Pada dasarnya GetSimple akan melakukan pengiriman password melalui email, dimana password akan dikirimkan ke alamat email yang sudah di masukkan. Namun karena kita menggunakan lab lokal dengan nama email yang tidak ada, sebaiknya kita simpan password yang di tampilkan pada halaman instalasi.



Berikut informasi kredensial yang kita miliki :

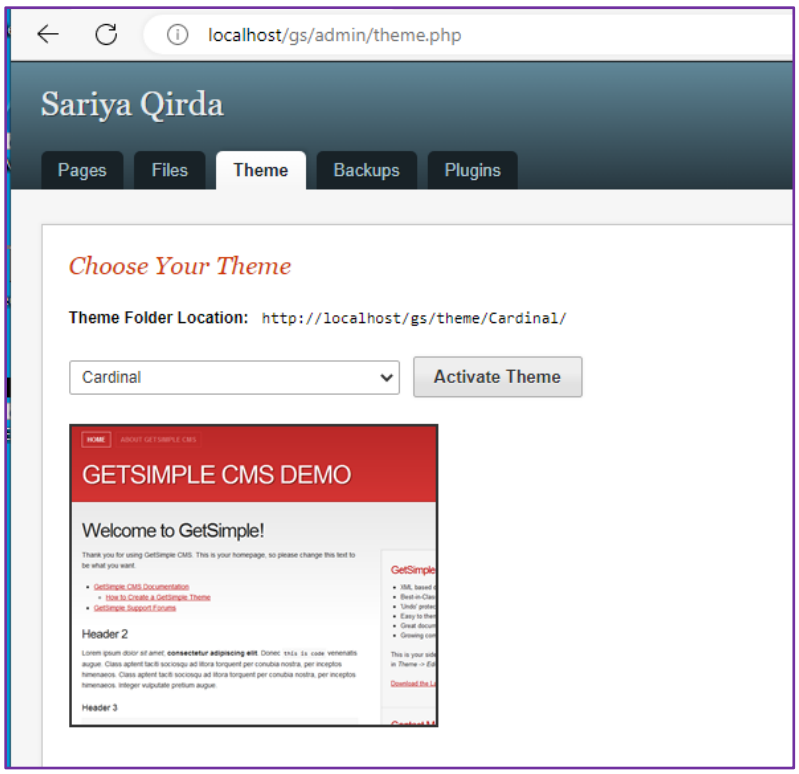
Username : superman

Password : xennYP

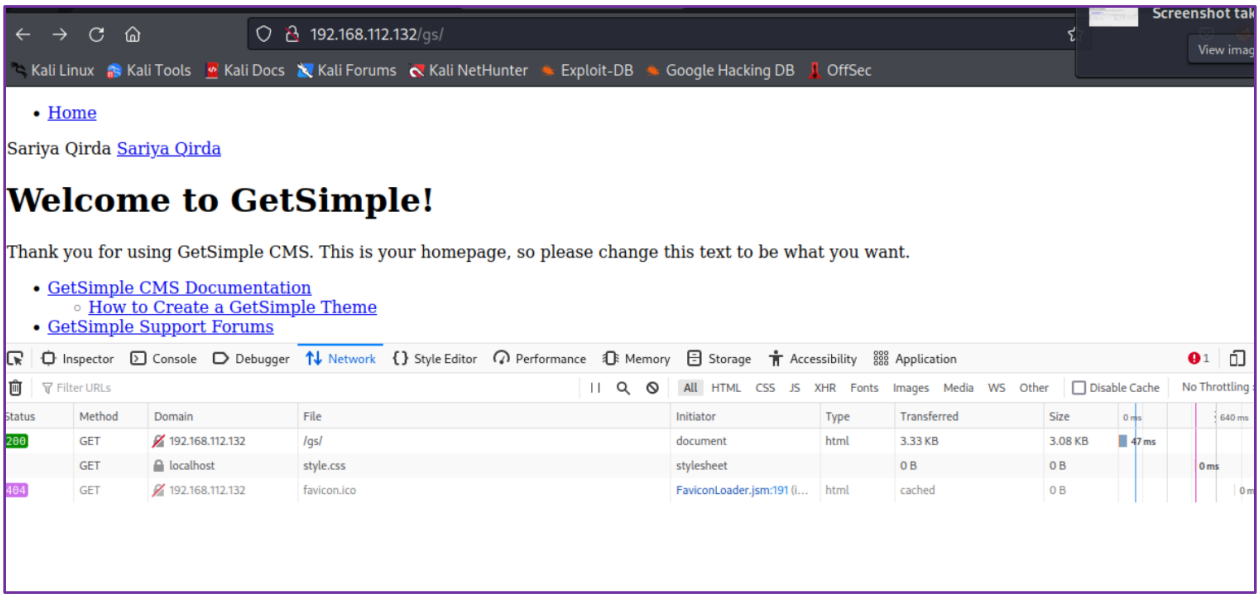
12. Klik “Login here”, dan kita akan di arahkan ke halaman dashboard. Apabila tidak diarahkan ke dashboard, kunjungi http://localhost/gs/admin dan login menggunakan kredensial yang di dapatkan.
13. Ganti passwordnya menjadi yang lebih rumit dan sesuai dengan standard keamanan :
    - Karakter minimum 8
    - Ada huruf kapital
    - Ada karakter khusus seperti &@#!

    Untuk contoh pada lab ini kita menggunakan kredensial superman : Superman@123 yang mana merupakan praktik password yang kurang kuat.

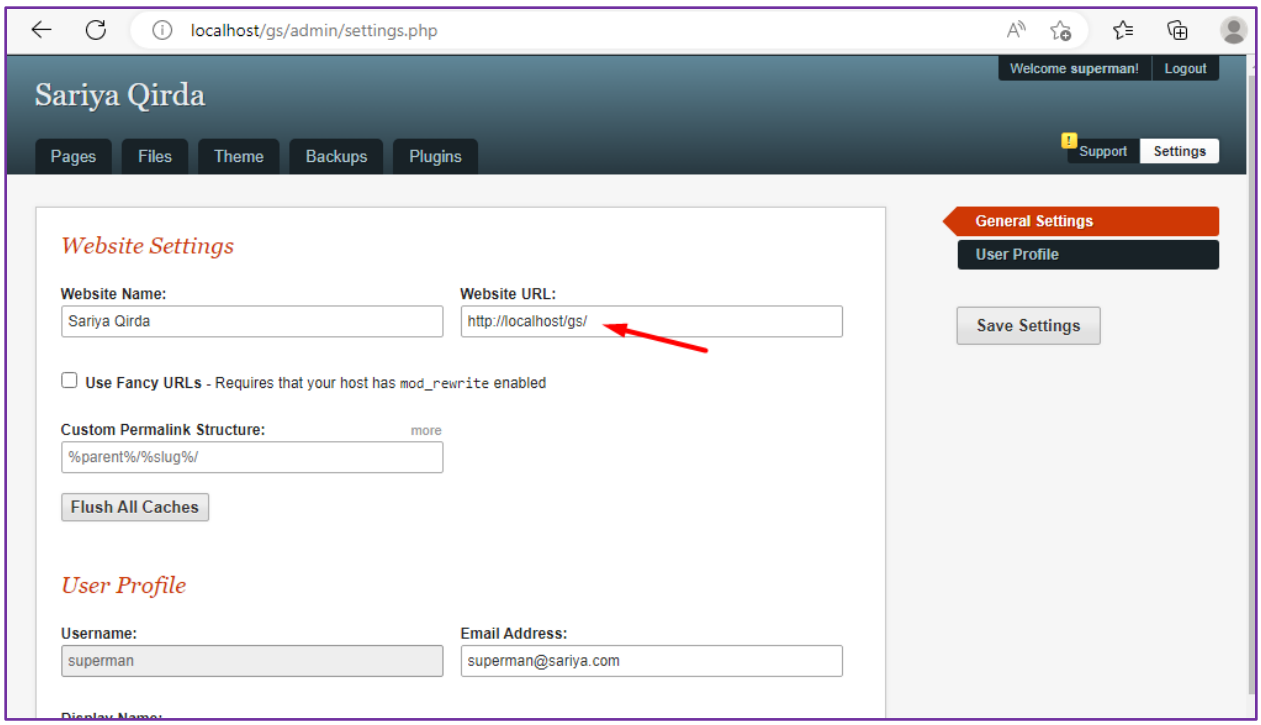
14. Kita kemudian dapat merubah theme website, misal menggunakan cardinal theme.



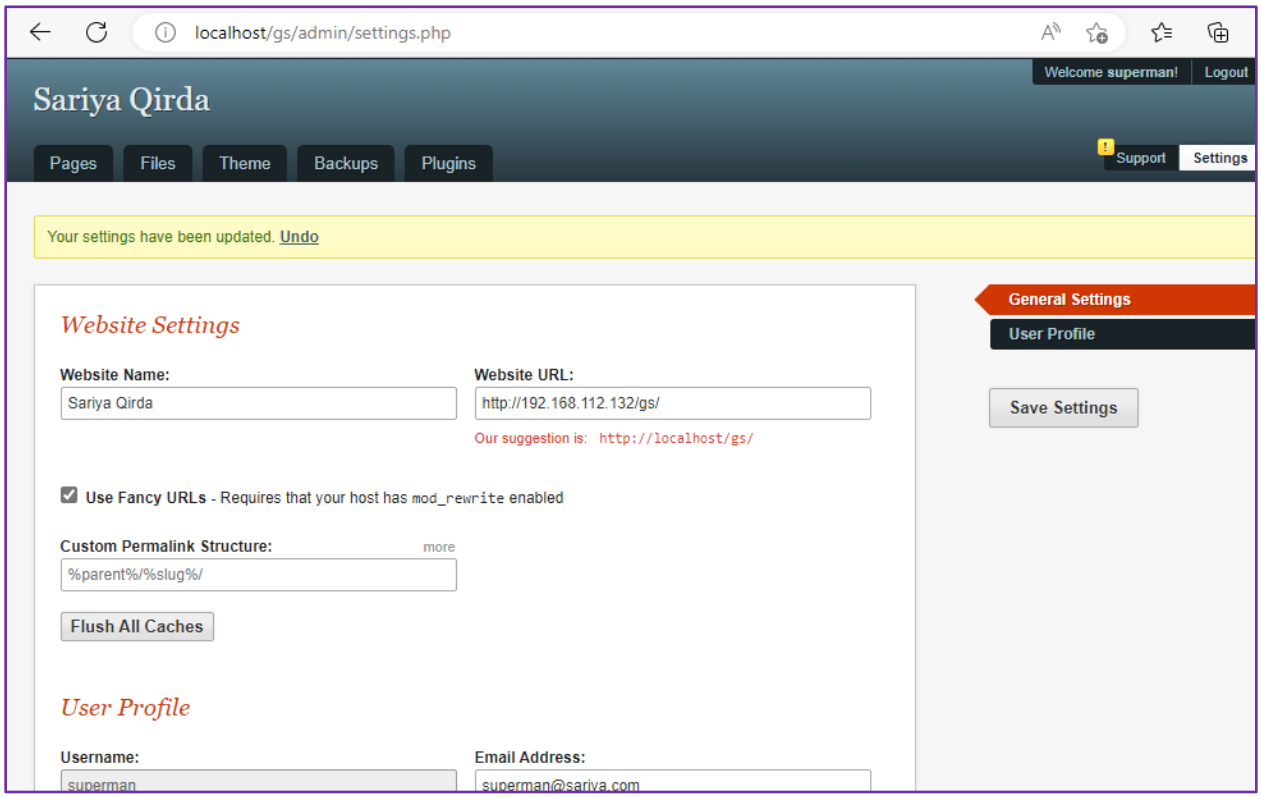
15. Ketika dikunjungi via localhost, tampilan akan terlihat normal, akan tetapi ketika dikunjungi oleh IP Address lain, tampilan dari halaman website nya jadi eror.



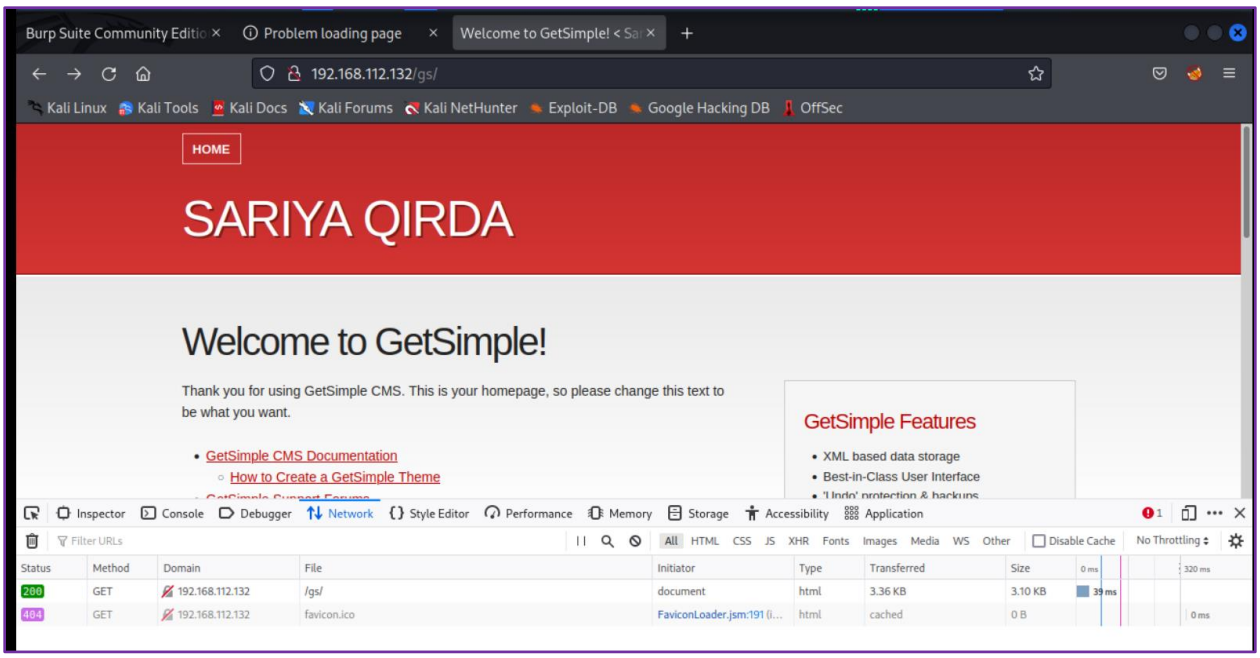
16. Ini dapat dilihat menggunakan developer tools, apabila di perhatikan style.css masih di set oleh aplikasi untuk dipanggil via localhost.
17. Menggunakan user admin (superman), kita bisa pergi ke pengaturan dan melihat jika website url masih tertulis localhost. Kita akan ubah menjadi ip address lab windows kita.



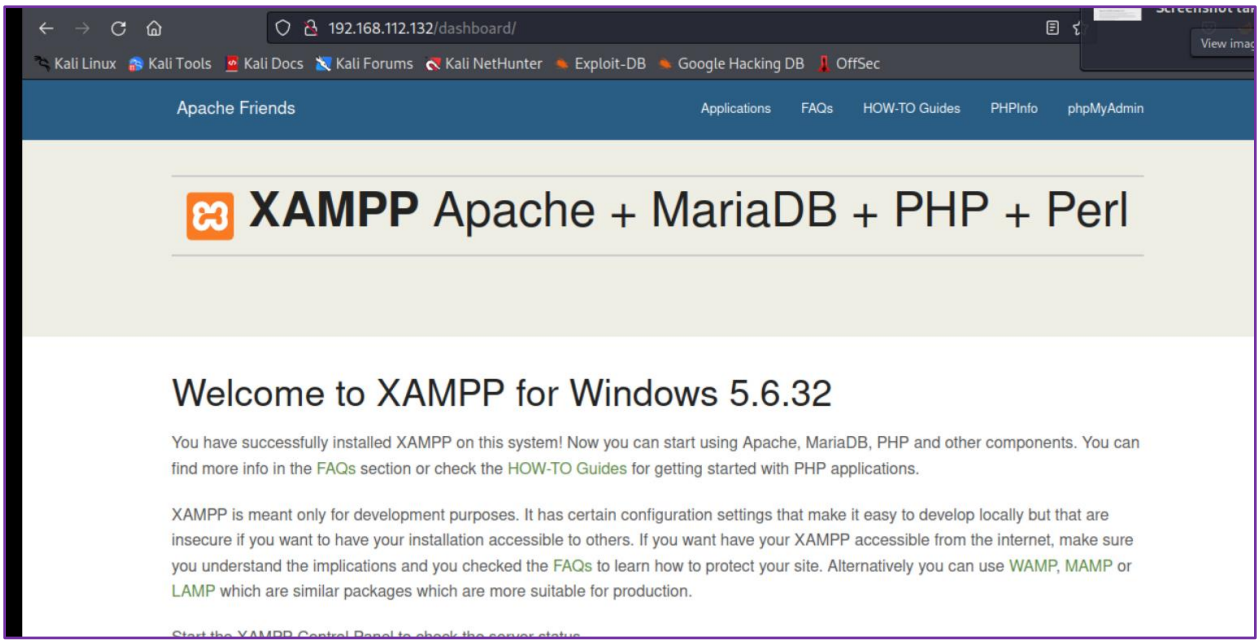
18. Ubah sesuai dengan IP Address Lab kita.

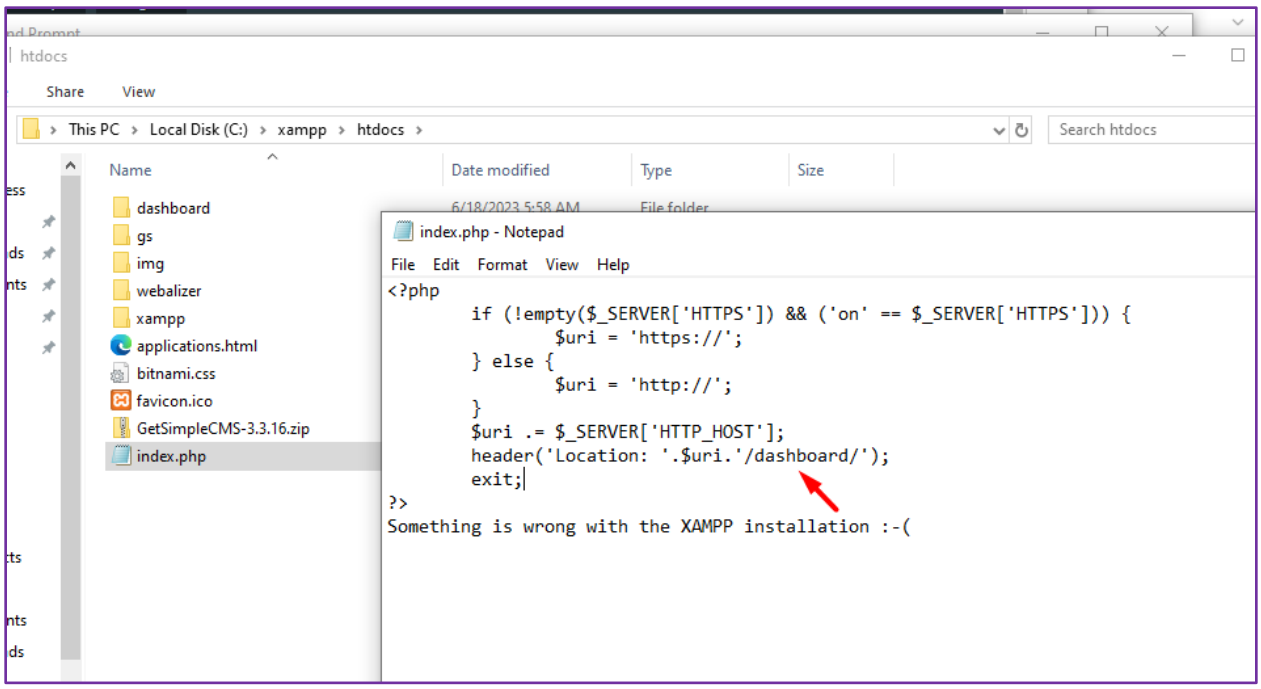


19. Ketika dibuka dari mesin lain, sekarang website sudah terlihat normal.

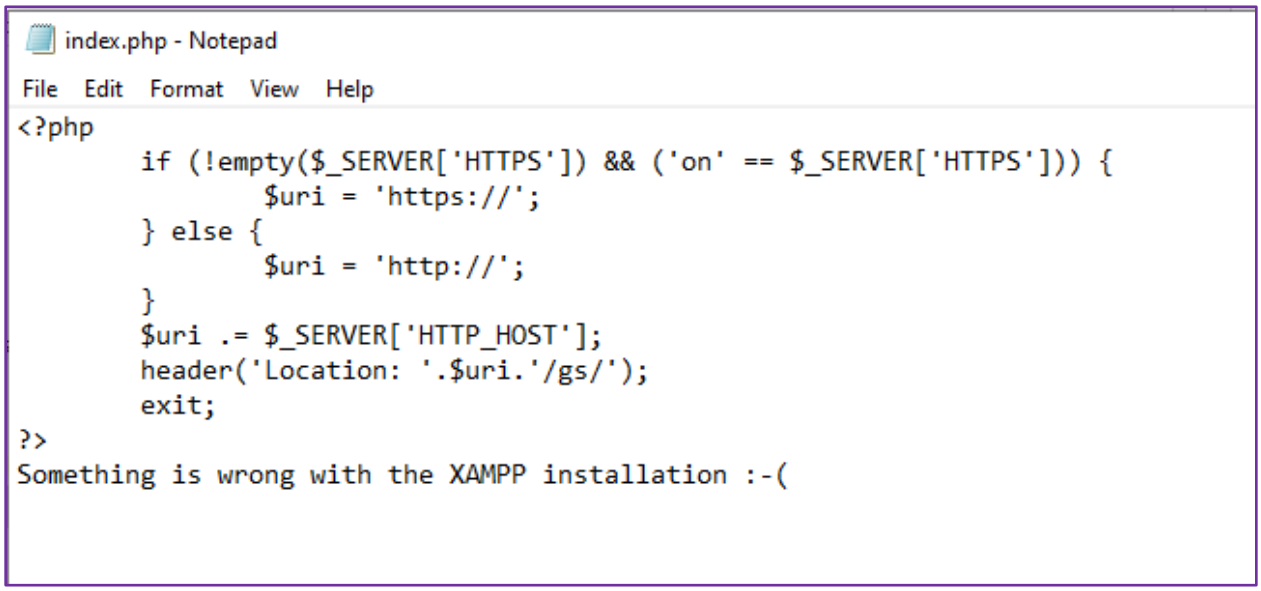


20. Website sudah siap berjalan dengan baik.
21. Apabila kita mengunjungi IP lab saja : http://192.168.112.132 maka mesin lain akan dapat melihat jika kita menggunakan XAMPP, karena secara default file index.php pada halaman utama htdocs akan meredirect ke /dashboard.





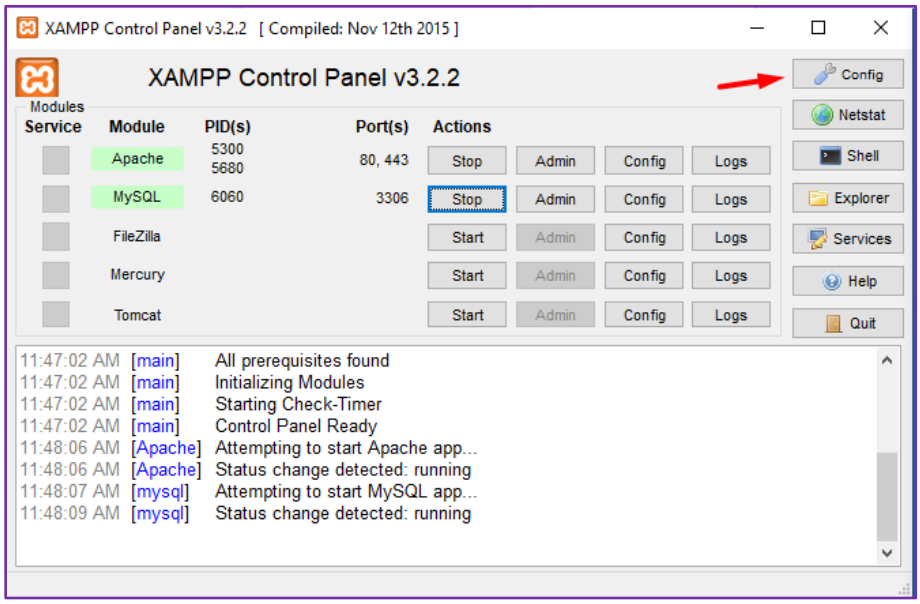
22. Ubah redirect index.php pada htdocs agar mengarah pada /gs



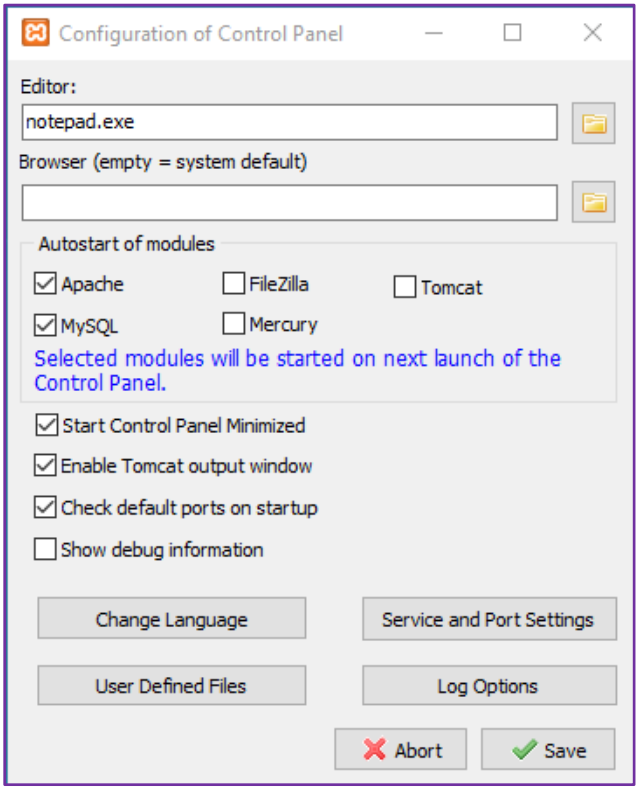
23. Sekarang apabila kita mengunjungi IP Address Lab http://192.168.112.132 maka akan langsung di redirect ke halaman getsimple.

C. Jadikan xampp auto start ketika windows startup

1. Klik config di xampp control panel

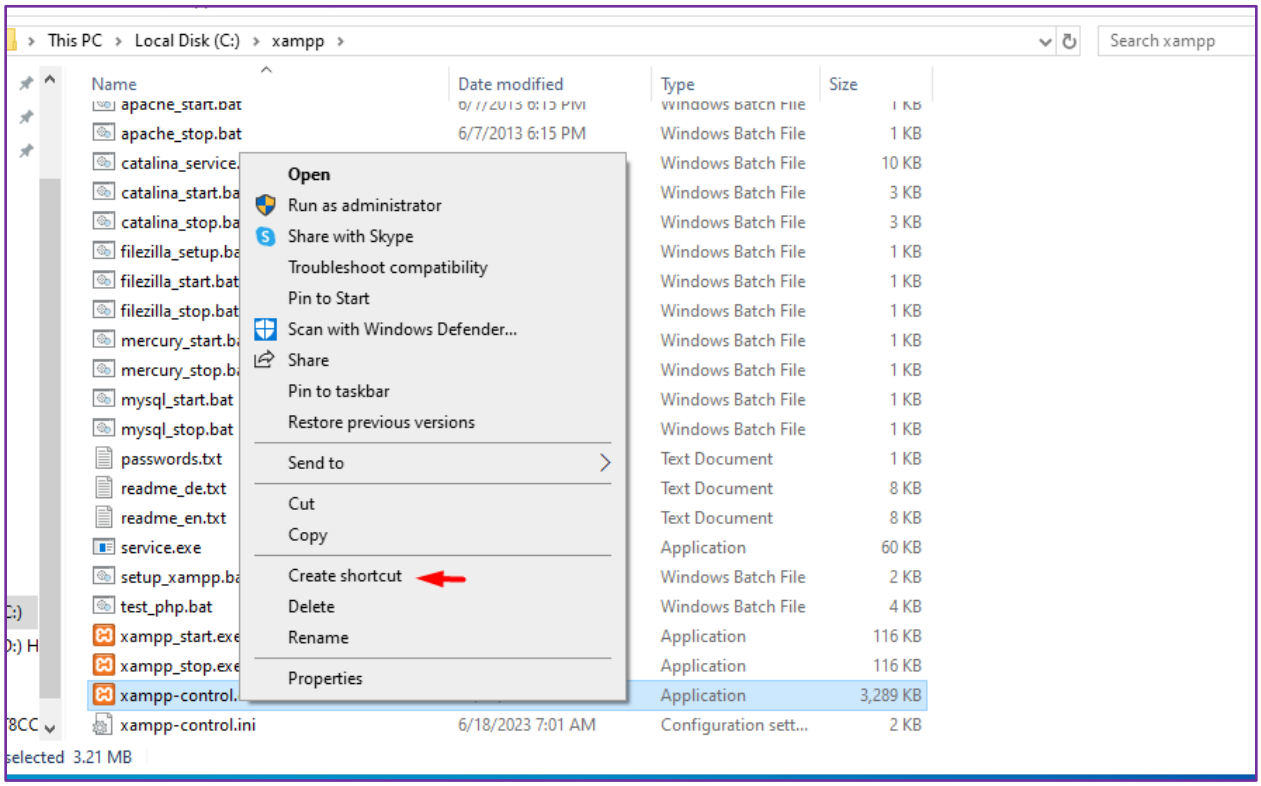


2. Centang pada menu “Autostart of module” pada bagian Apache dan MySQL.
3. Centang juga bagian “Start Control Panel Minimized”

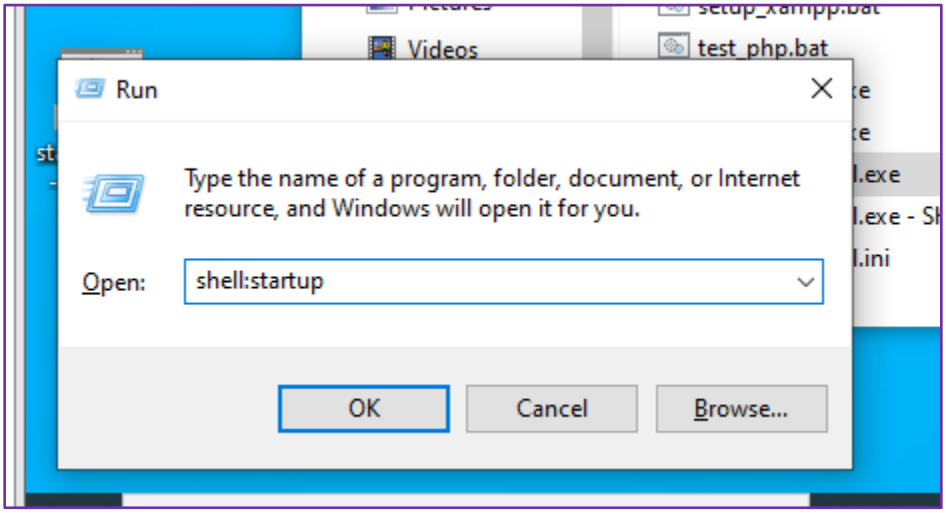


4. Klik Save

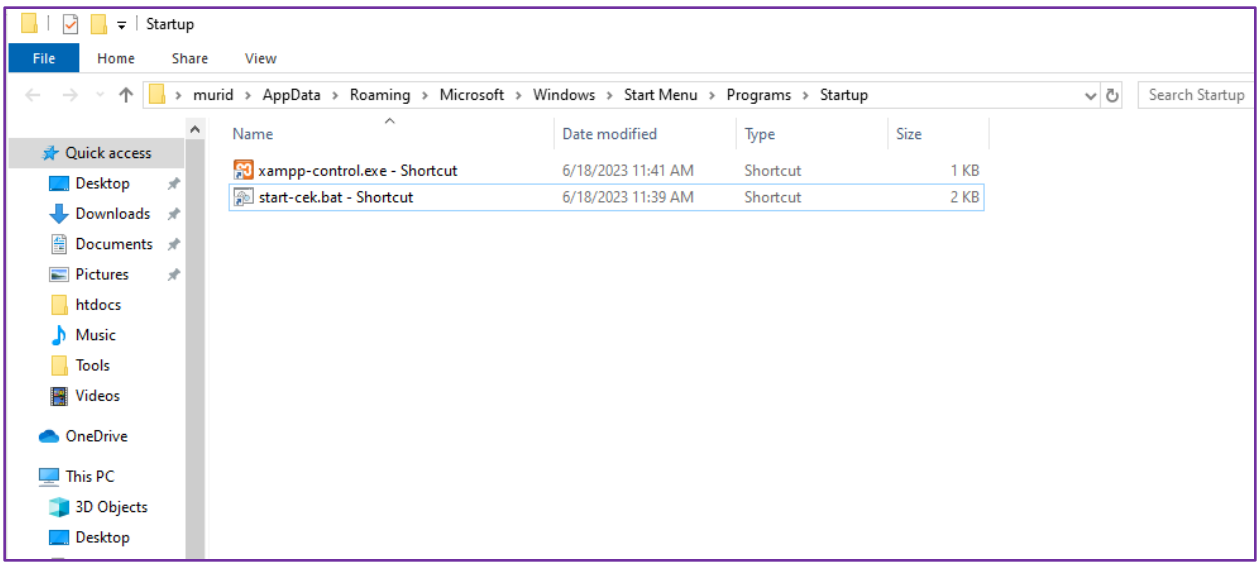
5. Ke folder xampp : C:\xampp
6. Buat shortcut dari xampp-control.exe



7. Buka folder startup dengan cara **windows + r**
8. Kemudian isikan *shell:startup*



9. Kopikan shortcut xampp-control.exe ke folder startup



10. Restart VM