For updating Apache to the newer version, firstly download the apache files from Apache lounge.

Rename the existing apache folder in xampp installation and keep it.

Paste the new downloaded apache folder in the xampp folder.

Replace the httpd.conf file with the older one.

Replace all the conf folder if required.

For updating openssl version, download the newer version of openssl compatible with your OS architecture.

Take a backup of OpenSSL files in bin directory of apache, and paste OpenSSL.exe, libcrypto and libssl files.

Paste the libcrypto and libssl in the php folder too.

For updating PHP, download the latest from php website.

Rename the existing php folder and paste the downloaded one.

Replace the php.ini present in the pasted php folder with the previous version.

After doing this restart the server.

If you need to test the version of openssl, in command prompt type in bin location of apache, type “openssl version”.

Inorder to check the syntax errors in apache, type httpd -t

If you get any errors related to openssl configuration regarding the security level in the test environment, place “SSLCipherSuite DEFAULT@SECLEVEL=0” or “SSLCipherSuite DEFAULT@SECLEVEL=1” just below the heading SSL Protocol. When it comes to production environment, regenerate the public keys to 2048 bit.

For knowing the version of moment, type moment.version in console.

For knowing the version of jquery, type $.fn.jQuery in the cosole.

For knowing the version of data tables, type dataTable.version in console.

For finding TRACE method is enabled or disabled, use the below code in the console

Fetch(“https://inventory.vimta.com”, {method:”TRACE”}).then(response=>console.log(response)).catch(error=>console.error(“Trace method in my website is disabled”))

Clickjacking

Add x-frame options in httpd.conf file.

To check if clickjacking is enabled, open the developer tools, open the website and go to network tab, click on the url, on the right side click on the headers, under headers check response headers and check for x-frame, if you find it as SAMEORIGIN or DENY, clickjacking is enabled.

Disable http headers or x-poweredby options

To check this, follow the same process of clickjacking, and in response headers search for x-poweredby or x-content-type-options, if not found, they are disabled.

Cookie without secure and samesite, withonly http

Same process of clickjacking, open application tab and click on cookie, search for the tick mark on http, secure and samesite. To enable or disable, edit the config file and for samesite CI3 wont be supporting, create a special hook condition.