

5> Compare following

a) GET & POST method

b) Client side scripting and server side scripting

a) GET & POST

	GET	POST
i> Parameters & history	Parameters are part of the URL, hence remain in the browser history	Parameters are not saved in browser history
ii> Exposure	Easier to hack	More difficult to hack
iii> Resubmit behaviour	GET requests are re-executed but may not be re-submitted to server if the HTML is stored in browser cache	The browser usually alerts the user that data will need to be re-submitted
iv> Bookmark	Can be bookmarked	cannot be bookmarked.
v> Parameter limit	Parameter data is limited to what we can stuff into the request line. Safest to use less than 2000 parameters	Can send parameters including uploading files to the server also. There is no limit on parameters in POST
vi> Usability	GET method should not be used when sending passwords or other sensitive information.	POST method is used when sending sensitive information as it is more secure.
vii> Visibility	GET URL is visible to everyone	POST method variables are not displayed
viii> Caching	Can be cached	cannot be cached.

b) Client side scripting & server side scripting

	Client side scripting	Server side scripting
i> Basic	Works at the front end and the script are visible among users.	Works in the back end which is invisible at the client side
ii> Languages involved	HTML, CSS, bootstrap, Javascript	PHP, ASP.net, Ruby on Rails, Python
iii> Affect	Can reduce the load to the server	Could effectively customise the web pages and provide dynamic websites
iv> Security	Insecure as scripts are visible	Secure relatively
v> Processing	Requires no server side interaction	Requires server interactions.
vi> Running environment	Client side environment used to run scripts is usually a browser	Server side environment that runs a script is a web server.