There are certain things which should be kept in mind :-

* SQL injection is a very big threat. We need to protect our form fields and stuff like it which contains input and is open to public. Doing checks both on client side and on server side would do the task I think. On Client side using js or jquery and using regex, by not allowing special characters on input and also not allowing special keywords of sql , special combination of special chars like ‘;-- this is usually used to insert sql query , since putting ;-- will comment the remaining of the query. Verifying the input before putting in sql query is a must, we don’t want to give away all the data in injection.
* Cross site scripting, well, one word its bad.
* CSRF token using for well not to have attack of csrf.
* For storing passwords, use salted hash and not just hash. And for salt don’t use username, use some random string which would be unique for user. What I think best is using a small simple hash for the password that comes and then appending that hash to password and then hash it with a proper hash, Bigger than sha1 and off course not md5.