Programmers are not perfect.

Unvalidated input –

Incomplete mediation or unvalidated input –

It might be difficult for number of us to get to grips with what we are talking about simply because we are used to graphical user interfaces.

So Alan needs to make something clear about this.

Programs could indeed be perfect and they’d probably be wonderful if they were totally segregated things ,if they kept to themselves ,if we started them and let them run and they finished.

They seldom are, as we need to interact with our programs.

At some point presumably a user(or another machine ) will be able to put input into the program to steer what later happens.

Idea is we are getting program to change what it’s doing depending on pushing buttons or something like that.

Even if your GUI only has menus or buttons, I hope you can imagine that a bad programmer could create problems by allowing you to do illogical things – like save a file without doing anything.

Programs that have to deal with typed input or other kinds of streamed data ,that can be more of a problem.

Input validation – making sure all input that is coming to the program will not spoil what the programming is trying to do.

In cross site scripting I was sending things to the website that was getting reflected back to me. That reflection was causing problems.

If the website had validated the input and made sure there were no HTML codes with scripts, it could have stripped the code of the JavaScript and what came back would have been harmless.

We have now got possibility to realize that cross site scripting is subclass of this unvalidated input.

On server side they are sending data to every kind of user and assuming that user will not manipulate it.poor programming

SQL injection

Here in the picture you see that what’s represented here is what’s happening on your browser.

You come to a web page where you see this. This might be that you’re logging into my application for students so students can see what their results are.

Login through the webpage as we used to with dsv systems , and the like.

This is part of what will be happening on the server side. I will be evaluating a piece of code

This is kind of code we are used to accessing DB’s with (SQL code)

Will show you first what happens and then explain more about what that piece of code does. So first thing I’m likely to do ,is to type in user id and password.

Goal with login form – use it in a way that gives us access to underlying DB.

When you try to login to website ,when u hit enter website will run a search on an underlying DB to see if your username and password are there in DB , if there u login successfully

Username-admin

Password – s3cret123

SELECT \* FROM USERS WHERE username=’ admin’ AND password=’s3cret123’

When string of characters between single quotes -string

What will tell us if website is vulnerable to SQL injection

Username – admin’

Password – password123

We know we can insert extra stuff besides string

Syntax error

SELECT \* FROM USERS WHERE username=’admin’’ AND password='password123’

If both true it will evaluate to true – we get successful login

What if we can make SQL statement always evaluate to true no matter what we put in

OR payload - admin’ or ‘1’=’1’

SQL injection actually affects the server side database but not Cross site scripting.

Buffer overflow