Assignment 2:

Objective: To learn programming practices and importantly keep in mind all the time "Do what required only - not less not more".

Role: Developer/Architect

Problem Description:

In the user authentication, programmer takes user name and password as input and validates against database. If user is authenticated successfully, the process moves on accordingly. i.e. Land on the user dashboard. If user has not entered correct credentials, he shall get appropriate message on the screen avoiding security breach.

Two programmer implements requirement in two different ways (pseudo code):

Programmer: B	Programmer: I

Read currentUserName
Read currentPassword
 	
try
{
select actualPassword
from usertable
where actualUserName=currentUserName;
 	
if(actualPassword.Equals(currentPassword))
{
syso("Welcome");
}
else
{
syso("Wrong password");
}
}
catch(Exception e)
{
syso("User is not present");
}
	Read currentUserName
	Read currentPassword
	
	try
	{
	select actualUserName
	from usertable
	where actualUserName=currentUserName
	and
	actualPassword=decode(currentUserPassword);
	
	syso("Welcome");
	
	}
	catch(Exception e)
	{
	syso("Either User or password is not correct.");
	}

Analyze programmer B and I approach. Comment on technical loop faults from both logic.

Estimated Time: 10 minutes

Model Solution:

Following are the area of improvement:

- Programmer 'B' retrieves actual password from table for no reason whereas he could just fire query to match both username and password together.

  This is a security breach. Because, program now has correct password from db into local variable whereas the currentPassword entered by user may be incorrect.

  Programmer 'I' clearly avoids this glitch.

- Programmer B is not using any encoding/decoding scheme for storing and retrieving actualPassword is visible from the query.

- Programmer 'B' is showing the message “User is not present” in the catch block, which is actually informative. More than needed information for the random user. Hackers can take benefit of this.

  Whereas programmer 'I' smartly shows the same message on whether user is not present or password is not matching. This does not leave a hint to hacker about the user database.

Summary of the assignment: Here, It can be derived that programmer 'B' is 'Beginner' while Programmer 'I' is 'Intermediate'. As, there are always chances of improvement and hence those who follow proven process can adhere expertise.

“Do what is needed not less not more – that is programming skill.”

Documented By: Jigar M. Pandya (jigarpandya.ce@ddu.ac.in)
09/01/2015