Keywords

Data Validation, Data Sanitisation, Authentication, Maintainability, Comments, Indentation

Robust Programs

Defensive Design Consideration

Starter

Objectives

BEGINNER:
Understand the elements of defensive program design.

ADVANCED:
Know how comments and indentation can support maintainability.

EXPERT:
Describe the role of testing, including how to identify errors and select appropriate test data.

What caused the **SONY** hack?
What are the outcomes of this hack?
How could **SONY** have prevented the attack?
How might **SONY** alter their programs to prevent this kind of attack in the future?

C O M P U T E R   S C I E N C E

Input Validation

Objectives

BEGINNER: Define the term key stakeholder.

ADVANCED: Understand how key stakeholders are affected by technology.

EXPERT: Recognise and discuss issues related to Environmental, Cultural, Morals & Ethics.

Validation is a check made by a computer to ensure that the data entered is sensible or reasonable.
It cannot check that it is correct because a user may lie or make a mistake.
It attempts to ensure that it is within certain limits or rules.
For example, a user is asked to enter a mobile phone number but only enters 9 digits.
A standard UK mobile number is 11 digits.
A length check validation can be used to ensure that 11 digits are entered.

Validation

CARR MANOR
COMMUNITY SCHOOL

VALIDATION TYPE	DEFINITION	EXAMPLE
Check digit	the last one or two digits in a code are used to check the other digits are correct	bar code readers in supermarkets use check digits
Format check	checks the data is in the right format	a National Insurance number is in the form LL 99 99 99 L where L is any letter and 9 is any number
Length check	checks the data isn't too short or too long	a password which needs to be six letters long
Lookup table	looks up acceptable values in a table	there are only seven possible days of the week
Presence check	checks that data has been entered into a field	in most databases a key field cannot be left blank
Range check	checks that a value falls within the specified range	number of hours worked must be less than 50 and more than 0
Spell check	looks up words in a dictionary	MS Word uses red lines to underline misspelt words

C O M P U T E R   S C I E N C E

Input Sanitisation

Objectives

BEGINNER: Define the term key stakeholder.

ADVANCED: Understand how key stakeholders are affected by technology.

EXPERT: Recognise and discuss issues related to Environmental, Cultural, Morals & Ethics.

Another method for validating data and stopping attacks is to clean up the data that is inputted so that it is ready for the application to use.

Some users may add additional data to try and access the program or provide clues on how to access the program.

Data sanitisation trims or strips strings, removing unwanted characters from strings

For example, Dave not dav%e, the % would be removed

This ensures that the input is correct and contains only the permitted characters, letters and symbols.

Input Sanitisation

Objectives

BEGINNER:
Define the term key stakeholder.

ADVANCED:
Understand how key stakeholders are affected by technology.

EXPERT:
Recognise and discuss issues related to Environmental, Cultural, Morals & Ethics.

Look at the data below and identify the issues
1. Dav3
2. Sarah@#gmail.com
3. Name: claire swainsworth
4. £546.56.67
5. O1982 56O635

1. Dav**3**
2. Sarah@**#**gmail.com
3. Name: **c**laire **s**wainsworth
4. £546**.**56**.**67 (two options here)
5. **O**1982 56**O**635

Anticipating Misuse

Objectives

BEGINNER:
Define the term key stakeholder.

ADVANCED:
Understand how key stakeholders are affected by technology.

EXPERT:
Recognise and discuss issues related to Environmental, Cultural, Morals & Ethics.

Defensive program design will consider and anticipate misuse.
Misuse may be in the form of a brute force attack on the program.
Many programs and systems only allow a user to enter a password three or four times before it locks out the system.
The program should be able to identify when a user keeps inputting the same data.
Consider Twitter which allows you to send the same tweet only once.
If you send the same Tweet twice the program identifies this and removes the tweet, sending you an error message.

Planning for contingencies

Objectives

BEGINNER:
Define the term key stakeholder.

ADVANCED:
Understand how key stakeholders are affected by technology.

EXPERT:
Recognise and discuss issues related to Environmental, Cultural, Morals & Ethics.

Once a programmer has anticipated the misuse they can then plan for the these issues.
For example:
Limiting the number of logon attempts
Ensuring the code is robust in validating the data entered.
Another method used is authentication.

What is authentication?

Authentication

CARR MANOR
COMMUNITY SCHOOL

Authentication is a coding method to check that a user is who they say they are and allowed to accesses the program.
This can be as simple as the user entering a user name and password which is compared against a stored user name and password.
If they match then the user is authenticated.
Authentication can also be physical.
New software often requires a key code which is generated by an app on the users phone and then entered.
Online banking requires a user to enter credentials into a webpage and then a number is generated which is entered into a key device.
This returns a number code which is entered into the webpage as well.
Without the second part of the code the user is not authenticated.

Authentication

Objectives

BEGINNER:
Define the term key stakeholder.

ADVANCED:
Understand how key stakeholders are affected by technology.

EXPERT:
Recognise and discuss issues related to Environmental, Cultural, Morals & Ethics.

Authentication methods vary from passwords to patterns and even image scanners.
Authentication also occurs when you access a website, you request access to the server which hosts the page.
A summary of basic web authentication goes like this:
You make for a request for a webpage by typing in the URL
The server responds with an error, requesting authentication
Your device retries request - with authentication details encoded in request
Again the server checks the details and sends the page requested, or another error.

Can you define maintainability, indenting and comments?

Maintainability, Indenting and Comments

Objectives

BEGINNER:
Define the term key stakeholder.

ADVANCED:
Understand how key stakeholders are affected by technology.

EXPERT:
Recognise and discuss issues related to Environmental, Cultural, Morals & Ethics.

MAINTAINABILITY
If a program is to be defensive against attacks then it has to be maintained and up to date.
API and code changes, which means that programs will need to adapt to complement new requirements.
Comments and indentation are two methods to provide information for future users or programmers that may be required to maintain the code.

INDENTATION
Code is indented for a number of reasons.
To group together a function
The code does not use a { syntax and indentation is used instead
If altering a function in the future it can be easily found.

COMMENTS
Comments in programs serve a number of purposes
To inform them reader of a bug or issues
To explain the code and its function in more detail
To stop a line of section of code from executing