Computing

Lesson 4: Fighting Fire with Fire

KS4 Security

Ben Garside

[1] *Materials from the Teach Computing Curriculum created by the National Centre for Computing Education*

Task 1 - SQL simulation

Follow the steps in the interactive simulator below to help you understand how SQL injection attacks are carried out:

SQL simulation (oaknat.uk/comp-SQLsimulation)

Please ask your parent or carer before completing this task. Oak National Academy are not responsible for any third party content.

Task 2 - Encryption practice

Using either a cipher wheel or the Caesar cipher decoder website, decode this message:

Nzxafepc Dntpynp td xj qlgzfctep dfmupne

- oaknat.uk/comp-cipherdecoder
- oaknat.uk/comp-cipherdecoder

Please ask your parent or carer before completing this task. Oak National Academy are not responsible for any third party content.

Task 2 - Encryption practice

Nzxafepc Dntpynp td xj qlgzfctep dfmupne

What did the message decode to?	
What was shift was used? (i.e 1,2,3?)	
Do you think this is easy to decode?	
How could you make it more complicated and therefore less easy to decode?	

Task 3 – software security case studies

The following slides have six brief case studies in which companies have each used one means of securing their software. Identify the name of each technique from the following list and then explain how it protects the software:

- Encryption
- Automatic software updates/securing operating systems
- Input sanitisation
- Code reviews to remove code vulnerabilities in programming languages and bad programming practices
- Modular testing
- The use of passwords

Task 3 – software security case studies

Case Study	Method	Description
Case study 1: Data sent around a network in an insurance company is disguised and can only be recognised with a key.		
Case study 2: An app design company ensures that after unit testing is complete, they check individual subprograms, subroutines, classes, and procedures in a program.		
Case study 3: A financial software company regularly reviews its existing programs.		

Task 3 – software security case studies

Case Study	Method	Description
Case study 4: ensures that all its staff have to identify themselves individually using a secret word or code when logging on to its secure databases.		
Case study 5: When reviewing security options, the IT department of a publishing company commits to ensuring that the most up-to-date version of software is used.		
Case study 6: A website designer ensures that all input is cleaned up to prevent unauthorised access.		