Task A

1. What is a SQL injection?

|  |
| --- |
| A SQL injection is a type of cyber-attack in which a hacker uses a piece of SQL (Structured Query Language) code to manipulate a database and gain access to potentially valuable information. |

1. How does SQL injection work?

|  |
| --- |
| Hackers will enter malicious code into a website and use SQL commands to login and gain unauthorised access to an account with the intentions of stealing, modifying or deleting the data stored inside of the database. |

1. What measures can be put in place to ensure that users don’t become a victim of a SQL injection attack?

|  |
| --- |
| * Validation on user input to check what has been input into a box does not contain SQL statements / disallowed characters * Escaping input strings to indicate that characters are to be ignored for processing * Penetration testing so someone tests for vulnerabilities and reports back. * Prepared statements / parameterised queries / stored procedures in an attempt to restrict what SQL can be executed. |

1. Look at the screenshot below and read the following headline.



1. What is meant by credential stuffing?

|  |
| --- |
| Credential stuffing takes advantage of people reusing username and password combinations. Attackers fraudulently obtain valid combinations for one site and then use them across others to try and gain access to accounts. |

1. How is credential stuffing different from a brute force attack?

|  |
| --- |
| Hackers will use SQL injection to find valid login credentials for one site and use them across other sites to gain access to accounts. Brute force attack is different because that involves the random generation of password guesses using a trial and error method. |

1. How does this sort of attack impact a user?

|  |
| --- |
| Leaking of sensitive data such as name, address, phone number, credit card/bank details.  Locked out of accounts for failed login attempts (not done by the user) |

1. What measures can be put in place to stop credential stuffing?

|  |
| --- |
| Use different passwords for different websites that require you to log in. Make sure that each password is strong.  From an organisation point of view, they might employ an ethical hacker to test vulnerabilities within the system because no matter how strong a user’s password is, if the organisations security system is vulnerable then the hackers will still be able to get access to these accounts. |