Part 2: #5 Make a screen capture showing the exposed XSS vulnerability

Graphical user interface, application

Description automatically generated

9. Briefly describe what the new results tell you about how the form now handles cross-site scripting attacks in the High setting:

The new results have limited characters displayed where when the settings where on low they gave a complete message and made it very clear to see.

10. briefly describe the results of steps 7-9.

I only received output from the a' ORDER BY 3; # command and it entailed (Unknown column '3’ in ‘order clause’.

19. Make a screen capture showing the user account information

Graphical user interface, text

Description automatically generated

21. Make a screen capture showing the hash informationGraphical user interface, text

Description automatically generated

Part 3 22. Describe the purpose of hashing in a database.

Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms.

Part 4 3. Make a screen capture showing the contents of the yourname\_S1.txt file

Graphical user interface, text

Description automatically generated

Part 4 5. Briefly describe the security countermeasures you recommend to mitigate the risk from compromise and exploitation. To counter SQL injection attacks: Your application should constrain and sanitize input data before using it in SQL queries. Use type safe SQL parameters for data access. These can be used with stored procedures or dynamically constructed SQL command strings. Using SQL parameters ensures that input data is subject to type and length checks and also that injected code is treated as literal data, not as executable statements in the database. Use a SQL Server login that has restricted permissions in the database. Ideally, you should grant execute permissions only to selected stored procedures in the database and provide no direct table access.