#5 Make a screen capture showing the exposed XSS vulnerability

Graphical user interface, text

Description automatically generated

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.

Briefly describe the results of steps 4-6.

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

Make a screen capture showing the user information.

Graphical user interface, text, application

Description automatically generated

Make a screen capture showing the hash information

Graphical user interface, text, application

Description automatically generated

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.

Make a screen capture showing the contents of the yourname\_S2.txt file

Text

Description automatically generated

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.

Section 3

Part 1. What is a UNION based SQL injection attack and why would you use it to exploit a database?

When an application is vulnerable to SQL injection attacker will gain the information from the table.

UNION based sql injection means attacker will UNION to get information from more tables.

We use UNION based SQL injection attack to get the data from more than one table from the database.

To perform this attack, it both tables should have same selected columns and they must be same