BAYSN DEPARTMENT OF CYBERSECURITY

Netplayz@programmer.net ✉

Date :
9, September, 2025

The audit focused on testing for potential security vulnerabilities in Baysn, including:

1. Access to the .env file
2. Access to the source code
3. Access to user data
4. Password cracking attempts on the database

Of the four areas tested, three did not reveal any issues. However, user data was successfully accessed. This discovery was made by the Chief Information Security Officer, NetByte, who identified the data originating from Baysn's AI chat feature implementation.

The method used to uncover this data involved an advanced password-cracking technique, the specifics of which will remain confidential for security reasons. Upon discovery, NetByte promptly reported the findings to WizzyWusky to ensure timely mitigation and review.

Screenshots of database can be found in the same folder as this PDF.

Signed,

NetByte

Baysn
Built to outperform every other automod.