

Nursing Electronic Forms Application

Development and Security Testing

By Benjamin Atkins

1809782

1809782@student.uwtsd.ac.uk

Abstract

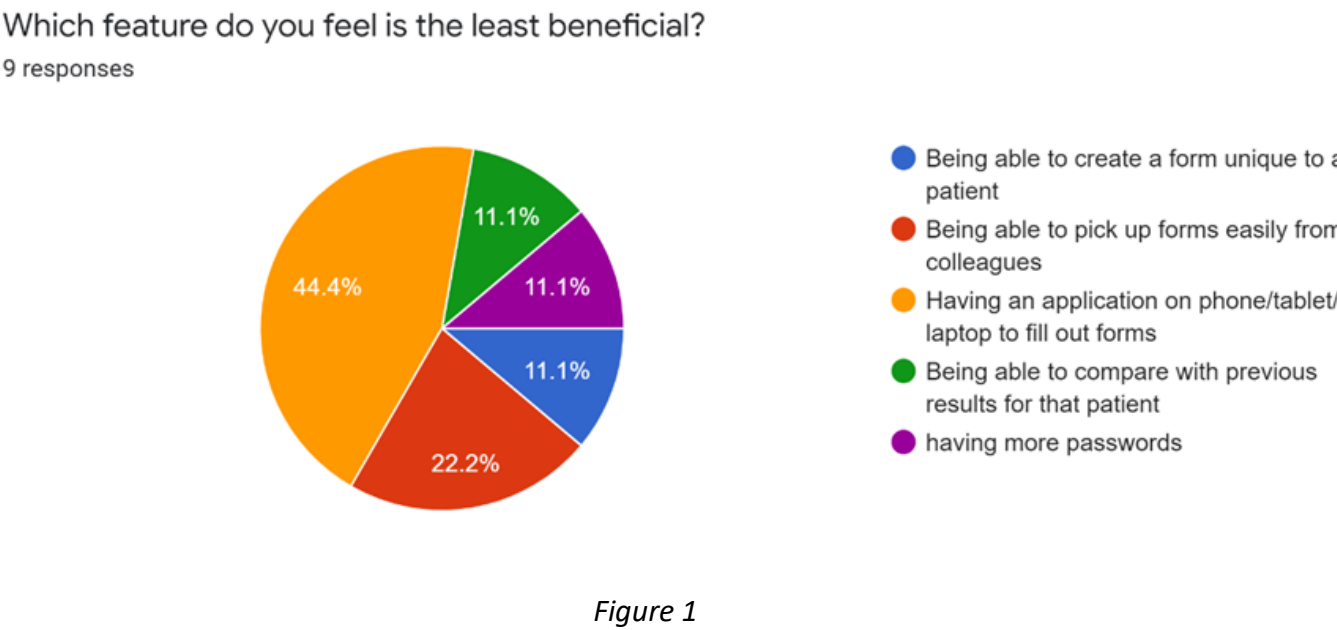
An Electronic forms design application, this was found as an application left in development limbo within the NHS. Was proposed to be a way to allow community nurses to create custom forms per patient to provide a more patient-centered approach to care. As this would eventually contain patient data this also covers the security testing on the web application to measure its security and how vulnerable it would be to attack. The application was developed with ADO.NET entity framework with a T-SQL database and a website front-end and security testing completed using a number of researched, industry-standard tools to verify if the application could uphold data’s Confidentiality, Integrity and Availability.

Research

Top Threats to web-apps:[1]

- XSS
- SQL Injection
- DoS & DDoS
- Broken Access Control
- Cryptographic Failures

Questionnaire issued to Community Nurses:



Other Summaries:

- Healthcare Data found to be nearly 20 times more valuable than financial data [2]
- .NET Researched and found to be the most suitable technology for use-case
- Encryption methods like AES-256 at DB level can help to mitigate security threats [3]

Testing

- SQLmap scan ran revealed no susceptibility to SQL injection attacks.
- Zed Attack Proxy Scan launched again revealed 3 XSS vulnerabilities but were subsequently mitigated.
- User Hands-on session with community nurse confirmed app was fit for purpose and gave recommendations.
- Most attacks launched against the application were unsuccessful due to the separation of the database and client tier with a service layer abstraction.

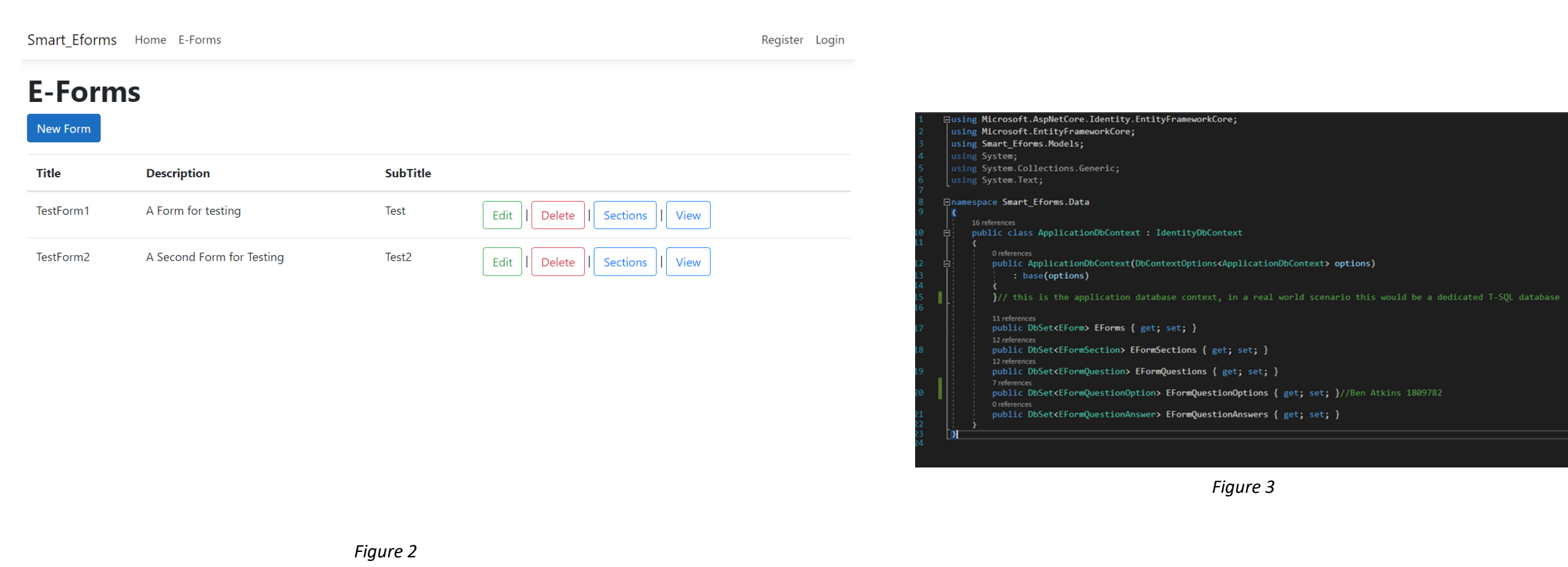
Aims & Objectives

Aim to develop a high quality and resilient E-Forms application that does not compromise security for functionality.

Objectives:

- Research current cyber security threats within application development, specifically relating to databases, web apps and mobile app.
- Construct an application able to meet the requirements set out in design phase and specification
- Utilise knowledge from research and from app dev to perform critical cyber security testing on application and attempt to
- Highlight any weaknesses for CSI (Continual service improvement)
- Gain user feedback by way of small-scale trials and user hands-on

Design and Implementation



Application successfully developed with .Net technologies, T-SQL database was converted to application defined database as there were issues with local databases being used. Most features specified were implemented, able to perform CRUD operations on forms. Forms, sections and questions can be created in the forms for use within nursing.

Conclusions & Recommendations

Development was successfully and yielded a functioning application with observed and advised benefits to community nursing by way of user trials. Subsequent security testing displayed that it did not pose an elevated level of threat.

Recommendations:

Continue with development in same manner, add unfinished features and start small scale testing once completed. Next things to be added should be dedicated database with database or column level encryption. Following further security testing mitigation of any identified threats should be completed prior to working on additional features.

References:

- [1] - OWASP, “OWASP Top Ten,” *OWASP*, 2021. [Online]. Available: <https://owasp.org/www-project-top-ten/>.
- [2] - L. Ponemon, “Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data conducted by Ponemon Institute LLC,” *Ponemon Inst.*, vol. 6th, 2016.
- [3] - “Types of Database Encryption Methods,” *MyDaimo*, 2014. [Online]. Available: <https://mydiamo.com/types-of-database-encryption-methods/>.

Table of Figures:

- 1— Excerpt from questionnaire issued to community nurse
- 2— Screenshot of application in current state
- 3— Excerpt from application code—application DB context