

CRITICAL ANALYSIS OF PENETRATION TEST ON NHS SYSTEM X TEST ENVIRONMENT BY ASHLEY REES - 2009258

INTRODUCTION

In a time where digital technologies dominate nearly every aspect of our lives, ensuring the security and integrity of our data is essential. This is especially true within the Nation Health Service, where confidentiality and privacy of patient information is essential.

The study identifies key vulnerabilities found on an NHS system, aligns them with the open web application security project, give recommendations on how to mitigate these vulnerabilities and test the recommendations within a virtual environment to ensure they work.



[This Photo](#) by Unknown Author is licensed under [CC BY-ND](#)

CONCLUSION

This study highlights critical vulnerabilities within the NHS system, aligning them with the OWASP top 10. Implementing recommended security measures have proven successful in a controlled environment, demonstrating the potential for significantly enhanced system security and sensitive data protection.

As IBM states [1]

Enhancing security measures is crucial in today's digital landscape as organizations face increasingly sophisticated cyber threats. Failing to do so can result in severe consequences, including data breaches, financial loss, and damage to reputation.

AIMS AND OBJECTIVES

Aims

- Analyse results of a penetration test conducted on the NHS system, to identify and categorise these vulnerabilities
- Conduct a comprehensive assessment
- Give actionable recommendations for improving the security

Objectives

- Review and analyse the penetration report
- Identify and categorise vulnerabilities
- Evaluate the effectiveness of tools and methodologies
- Propose recommendations for enhancements
- Ensure compliance with OWASP standards

RESULTS

the penetration test conducted by a third party identified the following key vulnerabilities.

- Client-side control weaknesses
- Outdated/ unsupported software
- TLS Session cookie without a secure flag set
- Single-factor authentication
- Weak password policy

recommendations

- Client-side controls – the decision was to implement server-side validation in addition to existing client-side controls.
- Outdated/ unsupported software – the decision was made to upgrade/ update all outdated and unsupported software components
- Single-factor authentication – to address this vulnerability, the design incorporated multi-factor authentication (MFA).
- Weak password policy – the decisions included a revised password policy that incorporates strong, complex passwords, regular password changes, and the use of password management tools

References

- [1] I. security, "Cost of a Data Breach," IBM, 2024.