

# Evaluating The Impact of Development Practises on Web Application Security: An Analysis of Application, Infrastructure, And API Security

Owen Evans - 2121421

Digital Health and Care Wales (DHCW)



## Research Context

Workplace related – currently working within Penetration Testing.

Firsthand experience of applications with different development time and maintenance levels.

Hoping to improve knowledge and understanding of both secure development and vulnerabilities.



# Research Problem

Inadequate maintenance and rushed development cycles by service teams lead to vulnerabilities in web applications, infrastructure, and APIs.



# Research Aim & Objectives

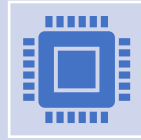
**Aim:** To evaluate the impact of development practises, including the thoroughness and duration of the development cycle, on the security of web applications, their supporting infrastructure, and associated APIs, using security testing tools and providing recommendations for enhancing secure development practises.

## **Objectives:**

- To review and analyse a range of penetration testing tools and vulnerability management solutions applicable to web applications, infrastructure, and APIs.
- To conduct a comparative security assessment of web applications, including their infrastructure and APIs, based on variations of development time and thoroughness.
- To identify common security vulnerabilities associated with rushed development and insufficient testing across applications, infrastructure, and APIs.
- To provide actionable recommendations for improving security practises in the software development lifecycle, emphasising the importance of adequate development time, regular maintenance, and thorough security testing.

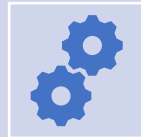


# Literature Review



Web applications were the top attack vector of 2023

80% of incidents  
60% of breaches



Misconfigurations and outdated components were the most targeted areas [1].



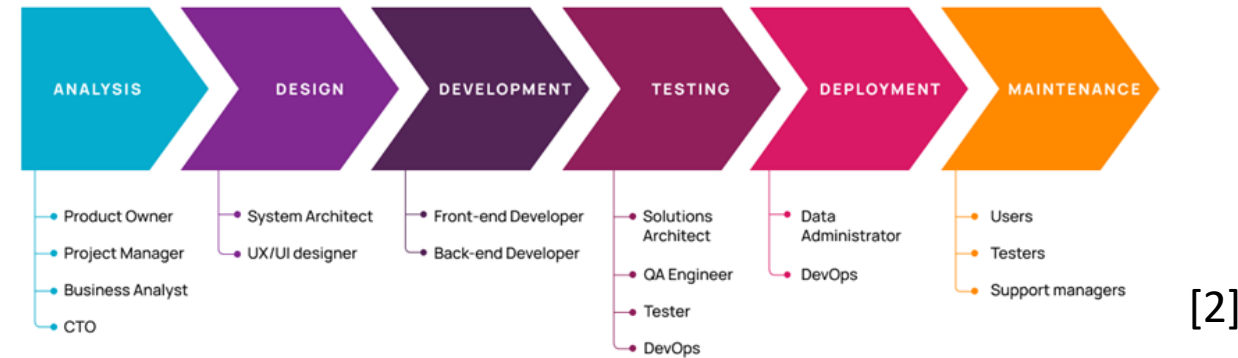
Mainly researched organisations and standards bodies.



Gaps in literature – couldn't find anything specifically for rushed development and inadequate maintenance of applications.



## 6 Phases of the Software Development Life Cycle



- Repeatabe developer framework for the full process of creating and maintaining software [3].
- Waterfall and Spiral Models [4].

# Software Development Life Cycle (SDLC)



# Secure Coding

Attackers often target the source code [5].

Automated security monitoring, logging, and alerting.

Scan code for issues so they can be mitigated/remediated.

Ensure encryption and protection against Cross Site Scripting (XSS) attacks.

Validate any external data sources [6].



# Security Testing Methodologies

## Penetration Testing

- Authorised test of applications that look for security weakness.
- Use same tools and techniques as an attacker.
- Annual tests or as needed [7].
- Can test all elements of an application [8].

## Automated Scanning Tools

- Tenable Nessus VMS – Infrastructure scanning.
  - Tenable cloud and web application scanning also possible [9].
- Qualys Web Application and API scanning.
  - Uses OWASP top 10 [10].





Standard awareness detailing most critical security risks.

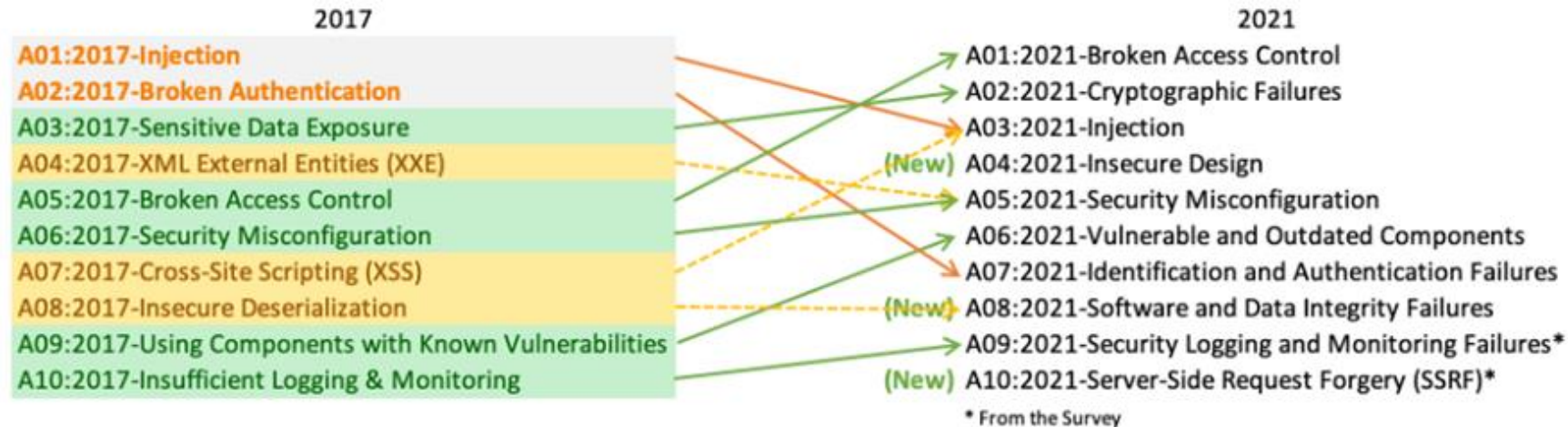


Covers various areas, including web applications and APIs.



Similarities between results:

Access control  
Broken authentication  
Security misconfigurations



[11] [12]

# Standards, Guidance and Frameworks - OWASP



# Standards, Guidance and Frameworks – NIST & ISO

## NIST

- Cybersecurity framework for managing risks.
- 6 core functions [13].

## ISO 27001

- Defined standard for ISMS [14].



# Research Philosophy and Approach

## Mixed method approaches

## Philosophy

- Positivism – facts through observation.
- Interpretivism – contextual factors to be considered [14][15][16].

## Abductive Approach

- Deductive – specific hypothesis.
- Inductive – existing data and individual instances used [17]



# Research Strategies

## Literature Review

Existing literature covering relevant areas.

## Case Study

Specific instances already known to be compared.  
Instances of applications with varying development and maintenance.

## Survey

Gain insights into development experiences.



# Risks, Limitations and Ethical Issues



## Risks

Sensitive data involved.



## Limitations

Approval of  
documentation usage.  
Approval of  
survey/interview.



## Ethical considerations

Anonymity of data,  
individuals, and services.  
Gaining approval.  
Potential bias.  
Alternative data sources.



# Validity, Reliability and Generalisability

## Validity

- Research methods relevant to achieving aim.

## Reliability

- Consistent data collection.
- All sources treated with the same anonymity and respect. No bias.

## Generalisability

- Mainly valid for similar projects.
- Useful to show importance of development, maintenance and security practises.



# Data Evaluation

## Collection

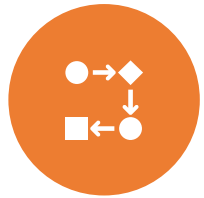
- Quantitative – vulnerability severity and frequency.
- Qualitative – vulnerability data and interviews/surveys

## Evaluation

- Most common vulnerabilities and severity.
- Themes and insights.



# Research Development Methodology



Agile development methodology – understanding that challenges may emerge.



Collaboration and feedback are important.



Overall goal to create a workplace policy for secure development and security testing.



# Resources/Materials



## Hardware

Work laptop  
Personal Laptop



## Software

Web Browser  
Tenable VMS  
Microsoft SharePoint  
Work Document storage solution  
Office packages (word, excel and outlook)



## Information

Publicly accessible –  
books, journals, reports  
Private documents from  
work

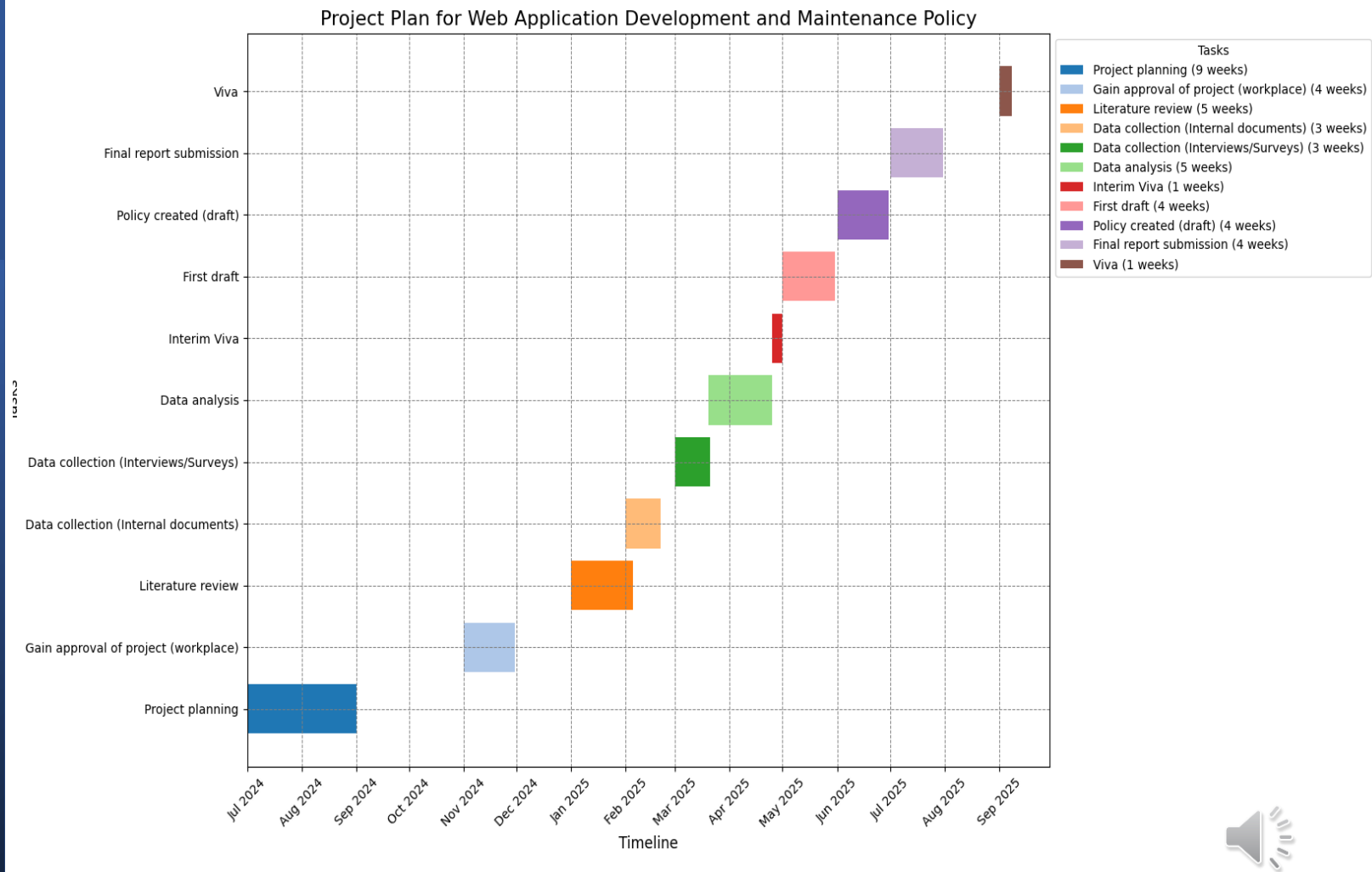


## Human

Application Developers  
Security Professionals



# Project Plan



# References

- [1] T. Richabadas, “Threat Spotlight: How attackers are targeting your web applications right now,” Barracuda, 2024. [Online]. Available: <https://blog.barracuda.com/2024/02/07/threat-spotlight-attackers-targeting-web-applications-right-now>. [Accessed 10 09 2024].
- [2] Y. Glamazdina, “A Guide to the Agile Software Development Life Cycle (SDLC),” 2021. [Online]. Available: <https://brocoders.com/blog/agile-software-development-life-cycle/>. [Accessed 10 09 2024].
- [3] R. Murch, “The Software Development Lifecycle - A Complete Guide,” 2012, pp. 13-14.
- [4] S. Pargaonkar, A Guide to Software Quality Engineering, CRC Press, 2024.
- [5] A. Hoffman, “Web Application Security: Exploitation and Countermeasures for Modern Web Applications,” United States, O'Reilly Media, 2020, pp. 17-27.
- [6] CheckPoint, “What is Secure Coding?,” [Online]. Available: <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-secure-coding/>. [Accessed 11 09 2024].
- [7] Aristi, “Penetration Testing,” [Online]. Available: <https://www.aristi.co.uk/services/penetration-testing>. [Accessed 11 09 2024].
- [8] Prism Infosec, “Cyber Security Assessments and Penetration Testing,” [Online]. Available: <https://prisminfosec.com/service/cyber-security-assessments-and-penetration-testing/>. [Accessed 11 09 2024].
- [9] Tenable, “Tenable Vulnerability Management,” 2024. [Online]. Available: <https://www.tenable.com/products/vulnerability-management>. [Accessed 11 09 2024].



# References

- [10] Qualys, “Web Application Scanning & API Security,” [Online]. Available: <https://www.qualys.com/apps/web-app-scanning/>. [Accessed 11 09 2024].
- [11] OWASP, “OWASP Top Ten,” 2021. [Online]. Available: <https://owasp.org/www-project-top-ten/>. [Accessed 11 09 2024].
- [12] OWASP, “OWASP Top 10 API Security Risks – 2023,” 2023. [Online]. Available: <https://owasp.org/API-Security/editions/2023/en/0x11-t10/>. [Accessed 11 09 2024].
- [13] NIST, “The NIST Cybersecurity Framework (CSF) 2.0,” pp. 8-10, 2024.
- [14] International Standards Organisation , “ISO/IEC 27001:2022,” 2022.
- [15] Y. S. P. Park, L. M. P. Konge and A. R. J. P. Artino, “The Positivism Paradigm of Research,” *Academic Medicine*, vol. 95, no. 5, pp. 690-694, 2020.
- [16] J. Dudovskiy, *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance*, 2024.
- [17] C. Kivunja and A. B. Kuyini, “Understanding and Applying Research Paradigms in Educational Contexts,” *International Journal of Higher Education*, vol. 6, no. 5, pp. 26-41, 2017.
- [18] University of Warwick, “inductive or deductive approaches,” 2012. [Online]. Available: <https://warwick.ac.uk/fac/soc/ces/research/current/socialtheory/maps/when/>. [Accessed 11 09 2024].



# Recording link

[https://1drv.ms/v/s!AhSJVwJwYlfHgsQphH6WD29NoBD\\_4A?e=Neuk6O](https://1drv.ms/v/s!AhSJVwJwYlfHgsQphH6WD29NoBD_4A?e=Neuk6O)

