

Project Proposal

by Kian Harper-Evans

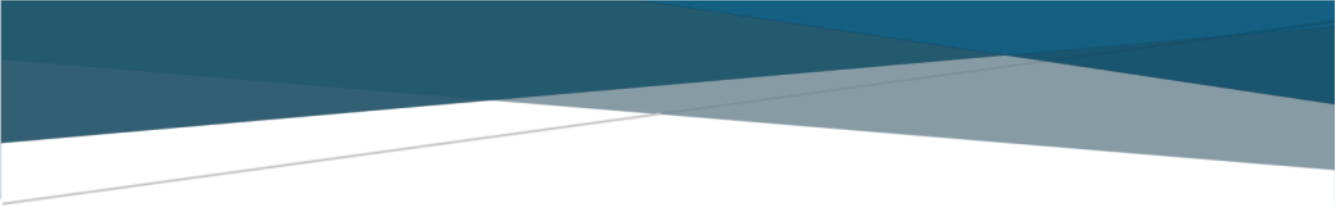
Submission date: 20-Oct-2024 12:07PM (UTC+0100)

Submission ID: 240697711

File name: 41760_Kian_Harper-Evans_Project_Proposal_586419_920304732.docx (184.96K)

Word count: 1953

Character count: 10749



INVESTIGATE AND EVALUATE/TEST THE QUALITY OF DATA SECURITY ON SAMPLE WEB-BASED APPLICATIONS

Computer Networks and Cybersecurity

October 2024

Project Submitted as part of BSc Computing (Computer Networks and Cybersecurity).

Preferred Supervisors: Niteesh Murugan Kaliyamurthy, Munyaradzi Murira.

Word Count:1527 Words

Kian Harper-Evans (2204995)

2204995@student.uwtsd.ac.uk

Table of Contents

Abbreviations	2
1.0 Introduction.....	3
2.0 Background to Proposed Research.....	3
2.1 Definitions of Fields:	3
2.2 Key Developments in Relevant Fields:	4
2.3 Research Problem	4
3.0 Research Problem Statement	5
4.0 Research Aims and Objectives	5
4.1 Research Aim:	5
4.2 Objectives	5
5.0 Methodology.....	6
5.1 Methods.....	6
5.2 Materials	6
6.0 Project Plan.....	8
7.0 References	Error! Bookmark not defined.

Abbreviations

SDL – Security Development Lifecycle.

WBA – Web-Based application

DAST – Dynamic Application Security Testing

RAM – Random Access Memory

NIC – Network Interface Controller

OS - Operating System

1.0 Introduction

In the modern-day world, most people on the planet have regular frequent interactions with websites. People use websites for a range of purposes from personal entertainment to serious uses such as banking, communication and the logging of private personal information. But are users private and sensitive data at risk whenever they are browsing the web? Well, we learn from the source [1, No. 2] that between 2018 and 2019 there were at least 30,000 data breaches in the data set used in said study alone. After taking this into account it justifies the importance of high-quality data security across all websites. This is where the need for my project becomes apparent. The purpose of this project is to test and evaluate an given websites data security quality. This will involve a detailed test of a website's security features, their user data privacy/storage policies, methods users can take to protect their own data and a final evaluation. All of this will be explored in more detail later in this document.

2.0 Background to Proposed Research

2.1 Definitions of Fields:

This project exists within the field of Cybersecurity, the field of Data security and Data analytics. Firstly, a brief description of these fields. What is Cybersecurity? Cybersecurity is a term commonly associated with work that revolves around protecting networks, devices and data from malware and attacks from 'hackers' [2]. What is Data security? Data security can be defined as securing digital data, for example data held in databases from unauthorised actions. Finally data analytics. data analytics can be defined as the process of examining raw data to gain insight into data trends and patterns to help create informed decisions, data analytics requires the use of computation techniques to convert data into something useable. This is according to the definition generated via ChatGPT. [3] ***"Data analytics refers to the process of examining raw data to uncover patterns, trends, correlations, and insights that inform decision-making. It involves the use of statistical, computational, and algorithmic techniques to transform data into actionable knowledge."***

2.2 Key Developments in Relevant Fields:

Since online websites have existed security for them has been required. However, in this section I am mainly focused on more recent developments in online website security. When looking for modern developments in cybersecurity used for websites originating from the 2010's and 2020's we get examples such as changes in security architecture and the adoption of machine learning AI for security purposes. Firstly, in the modern day we have seen a widespread adoption of zero trust architecture. What is zero trust architecture? Zero trust architecture means that at constant verification of user must be done and access control restriction must be put in place regardless of a user's location [4] . Secondly AI and machine learning have been adopted widely for use in threat detection. AI is used to analyse vast amounts of data and detect anomalies and patterns in said data. AI can analyse more data than any human can faster than a human can allowing for threat response times to be quicker [4]. Another example of a development in this field is the adoption of cloud security. Why has this been adopted? The reason for the requirement of cloud securities is the widespread adoption of sites that offer cloud services. Cloud security technologies offer automatic security suggestions, which work to keep cloud networks secure [4]. Other examples include the use of automated security testing within continuous integration and deployment pipelines, plus the integration of controls for security into the code that makes up the infrastructure. These tools are more effectively used to find and correct infrastructure vulnerabilities within the beginning early stages of development. This improves overall security quality after development [4].

2.3 Research Problem

Why is this project test necessary? In the modern-day data breaches are becoming increasingly more frequent due to the popularity of transitioning to hosting services through cloud-based platforms. These cloud-based services contain databases which hold sensitive data related to the cloud providers, the site providers and the clients of web services [5]. With data such as this so easily attainable, it leaves thousands or hundreds of thousands of people vulnerable to malicious action such as fraud and identity theft. It also leaves the companies which run these sites data vulnerable to malicious actors as well. Which can lead to company secrets being leaked, corporate espionage and loss of revenue for the company. This is why frequent security tests are important to maintain a high standard of security.

What is the effect of frequent security testing? The positive effects of frequent web application security testing include the ability to find flaws before malevolent actors can take advantage of them. By being proactive, the likelihood of data breaches and other

cyberthreats is decreased [6, Vol. 13]. Another benefit of frequent security testing is a reduce in cost to a hosting organisation by saving them money from data breaches and saving them the high cost of legal fees which proceed data breaches [7]. The final example of the positive effects of regular security testing is that it increases network and system resilience. Consistent testing helps highlight gaps in security so that they can be rectified within a timely manner. This then helps organisations be more prepared for more professional sophisticated attacks [8, p. 202].

3.0 Research Problem Statement

This project aims to address the large number of WBAs that have less than adequate security quality. I aim to test a sample WBA security standard and accurately map out flaws in their security. After this I intend to lay out a detailed plan to bring security up to an acceptable standard and if possible, implement these changes.

4.0 Research Aims and Objectives

4.1 Research Aim:

To investigate, evaluate and test data security quality on a sample WBA.

4.2 Objectives

Methods within the objectives of this project have been developed from the SDL [9], however additional objectives have been added to fit this project's purpose.

1. To acquire consent from a client to run security testing to the back end of their WBA.
2. Begin the requirements evaluation phase.
 - a. Threat Modelling – Identify what the potential threats to the WBA are and any security requirements.
 - b. Compliance- determine what the legal requirements and regulations are for the areas in which the WBA operate within.
3. Initial test of base WBA architecture – test security quality of the WBA architecture before any modification is made.
4. Evaluate quality of Data Security and Give client a review of security quality.
5. Design Phase.

- a. Develop secure architecture design.
 - b. Conduct an accurate threat assessment.
 - c. Ensure that data communication between clients and servers is secure.
6. Implementation Phase (If Possible).
 - a. If allowed by my client, the methods within my review and plan will be implemented into the clients' network.
7. Testing new implementations (If made).
8. Deployment Phase (If required).

5.0 Methodology

5.1 Methods

This Project will contain a mix of quantitative and qualitative research. Qualitative research will be found in research of literature related to web application and data security methods, as well as examples of when said methods have been used.

Whereas quantitative research will be used to gather results from experiments run on the client's current security architecture and if carried out our newly implemented one.

The research strategy for this project will be an experiment, testing the data security quality of the given client's web application. This experiment will be supported by secondary research from trusted article and research papers.

Throughout this project analysis of data collected from security tests will be required. First attempts will be made to circumvent the security of the current architecture, data related to how security was breached, what was breached and how many times a breach was successful will be recorded and then these values will be used to gain the average percentage of successful breaches and the percentage of times that security devices were successful in both old and new architecture.

5.2 Materials

Secondary Research:

- Research databases: Google Scholar, UWTSD Library, IEEE Explore – Used to find articles and research papers.

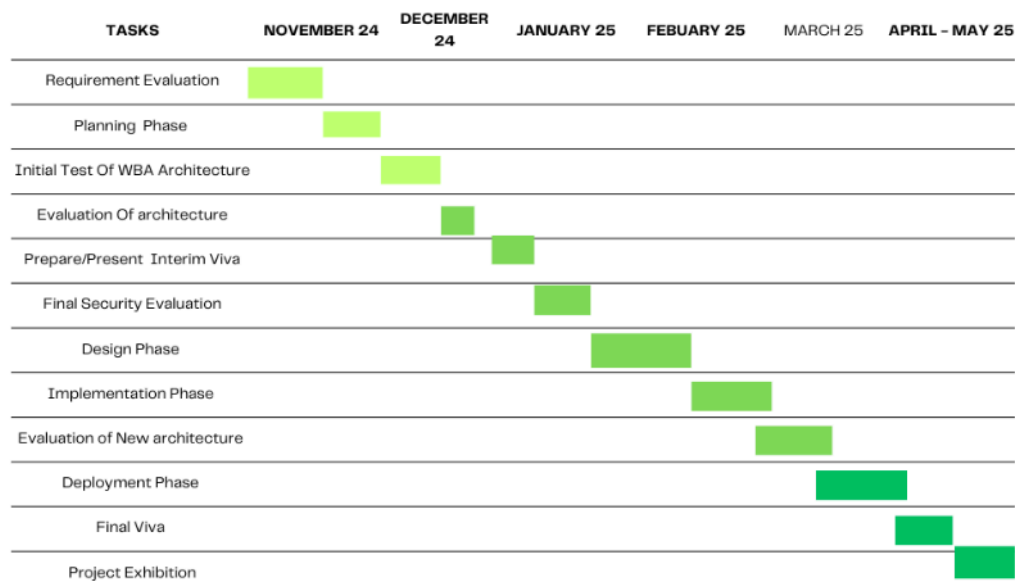
- Referencing tool: RefWorks – Used for referencing and citing research sources.
- These methods for collecting secondary research are appropriate because the databases only offer peer reviewed professional studies, articles and conference papers. RefWorks is a trusted tool that shortens the time it takes to gather and site research sources.
- ChatGPT used only for the generation of definitions

Primary Research/Tests

- Methods For Testing data security:
 - Penetration Testing [10].
 - Dynamic Application Security Testing (DAST) [11].
 - Fuzz Testing [12].
- Ethical Considerations – All data collected during this project will be stored only during the deration of the project then will be removed shortly after. No data will be disclosed with third parties outside those involved in the project.
- Hardware Requirements:
 - Multi-Core Processor
 - 8-16 GB RAM
 - SSD Storage
 - NIC's
- Software Requirements:
 - Windows OS
 - Burp Suite tool (used for Web vulnerabilities like SQL Injection)
 - OWASP ZAP (open-source tool for finding vulnerabilities within a WBA)
 - Network scanning tools (Wireshark or Nmap)
 - DAST tools (Nessus)
 - Fuzz Test Tool (Peach Fuzzer)
 - Web Browser (Chrome)

6.0 Project Plan

PROJECT TIMELINE



- Requirement Evaluation: 5th – 15th November
- Planning phase: 16th -29th November
- Initial Test phase: 30th November – 12th December
- Evaluation: 15th – 21st December
- Interim Viva: 23rd – 31st December
- Final evaluation: 1st – 8th January
- Design Phase: 10th January – Febuary 10th
- Implementation Phase: 12 Febuary – March 1st
- Evaluation of Architerture: March 2nd - March 13th
- Deployment Phase: 15th March – March 31st
- Final Viva: 1st – 12th April
- Project Exhibition: 15th April – May 1st

7.0 References

[1]

X. Liu *et al.*, "Cyber security threats: A never-ending challenge for e-commerce," vol. 13, Oct. 2022, doi: 10.3389/fpsyg.2022.927398.

[2]

OpenAI, "Definition of Data Analytics Generated by Generative AI (ChatGPT)."

[3]

S. Lipner, "The_trustworthy_computing_security_development_lifecycle." .

[4]

S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," vol. 421, pp. 43–69, 2017, doi: 10.1016/j.ins.2017.08.063.

[5]

D. Chen, M. M. Chowdhury, and S. Latif, "Data Breaches in Corporate Setting," Oct. 2021, doi: 10.1109/iceccme52200.2021.9590974.

[6]

S. Islam and L. Xiangdong, "Guardians of the Web: The Evolution and Future of Website Information Security." MDPI AG, Jul. 01, 2024, doi: 10.20944/preprints202407.0108.v1.

[7]

G. A. Pimenta Rodrigues *et al.*, "Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review," vol. 9, no. 2, Jan. 2024, doi: 10.3390/data9020027.

[8]

S. Charles, H. Hajimiri, and P. Mishra, "Proactive Thermal Management using Memory-based Computing in Multicore Architectures."

[9]

M. Bay, "WHAT IS CYBERSECURITY? In search of an encompassing definition for the post-Snowden era." .

[10]

K. Scarfone, M. Souppaya, A. Cody, A. Orebaugh, C. M. Gutierrez, and P. D. Gallagher, "Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology." Sep. 01, 2008.

[11]

IBM, "Cost of a Data Breach Report 2024." 2024.

[12]

J. Hulkkonen and M. Moisio, "System Performance Evaluation of GERAN Flexible Layer One Concept."

[13]

X. Dong, L. Zhao, X. Zhou, K. Li, D. Guo, and T. Qiu, "An Online Cost-Efficient Transmission Scheme for Information-Agnostic Traffic in Inter-Datacenter Networks," vol. 10, no. 1, p. 202, Jan. 2022, doi: 10.1109/tcc.2019.2941688.

Project Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

75/100

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project Good clear title shows the full intent. A brief introduction gives context and a little insight into the project idea. Good succinct and achievable aim. Objectives feed into the aim well, it would have been desirable to see less objectives being made more to the point in a SMART way. Clearly and logically thought out process that shows a deliverable.	20	15
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8	20	14

journal papers and book chapters rather than just websites; Selection of relevant models & concepts Less reliance on ChatGPT would have been desirable, however only used for the definitions and has been referenced. A reasonable background researched for this project has led to a reasonably thought out project subject and process. A good range and amount of literature has been used to back up the points made in the text (layout of the bibliography could have been made better although follows IEEE). More detail could have been discussed as far as web app vulnerabilities and testing.		
Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed Good clear problem statement showing intended outcome to the project. Shows it has been thought through well.	30	23

Good clear methodology based on SDLC. Does need some tweaking. Good understanding of the philosophy for the research and the use of quantitative and qualitative data, and what mostly needs to be done.		
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices Good detail to how the project will take place and move forward. Good consideration to the ethics and data storage as well as hardware and software to be used. Good amount of detail shown in the Gantt chart and resources shows good consideration to the roadmap of the project.	15	13
Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit	15	10

Well laid out report with clear sections that logically flow.		
The report would have benefited from a conclusion that summarises the whole of the narrative.		
Third person terminology would have been more desirable than using 'I'.		
Overall a good clear direction.		
TOTAL	100	75

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6
PAGE 7
PAGE 8
PAGE 9
PAGE 10

