



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

University of Wales Trinity Saint David - Faculty of Architecture,
Computing and Engineering

Investigation into Vulnerabilities and the Security Performance of Web Applications

Level 6 Final Major Project Proposal – ACDA 5004 Project
Management and Research Methods

Table of Contents

1.0	Introduction.....	2
1.1	Aim	2
1.2	Objectives	2
2.0	Background Research	3
2.1	Background.....	3
2.2	General Literature review	4
3.0	Research Methodology	10
3.1	Research Philosophy.....	10
3.2	Research Approach	11
3.3	Research Strategies	12
3.3.1	Data collection	12
3.3.2	Suitability.....	13
3.3.3	Time Horizon	14
3.3.4	Data Analysis	14
3.4	Web Application Development Methodology	14
		14
3.5	Expected Outcomes	14
4.0	Resources and Planning.....	16
4.1	Physical resources.....	16
4.2	Stakeholders.....	16
4.3	Planning	16
5.0	Risks.....	18
6.0	Ethical and Legal concerns	20
7.0	Conclusion	21
8.0	References.....	22

1.0 Introduction

"The original idea of the web was that it should be a collaborative space where you can communicate through sharing information." Sir Tim Berners-Lee [1]

The nature of the World Wide Web is to be always available and accessible, making information available to all. Web applications are embedded into everyday life and are used for many different reasons such as shopping, social networking, and online banking. People trust these web applications with their information. These web applications are becoming more sophisticated in their development and architecture, incorporating outside sources such as application programming interfaces (API's) and frameworks to develop them. For these reasons this creates vulnerabilities, leaving opportunity for unethical attackers to steal information and data for their own gain. This makes web application security an important topic within the web development and cyber security domain.

This report proposes a field of study on web application vulnerabilities and security, proposing the aim and objectives, and giving context to justify its need. It will also propose methodologies for the objectives.

1.1 Aim

The aim of this final-year major project is to investigate and assess vulnerabilities specific to websites and web applications.

1.2 Objectives

This aim will be completed through four main objectives:

- **Rigorously Investigate current security vulnerabilities in web applications and produce a systematic assessment of the current measures for preventing security risks.**
- **To establish effective criteria for a secure web application design.**
- **Design and Develop a 'Proof of Concept' web application to evaluate against current security guidelines.**
- **Critically evaluate the security of the implemented web application using recommended guidelines, and penetration testing tools to expose vulnerabilities.**

2.0 Background Research

2.1 Background

Within the ever expanding and evolving ‘World Wide Web’, technology and design trends of applications has changed significantly. This includes frameworks, helping to design progressive web applications (PWA), one-page websites, as well as API driven development and plug-ins as examples.

This opens web applications to vulnerabilities, allowing the all too common continuation of exploitation in the form of injections such as SQL and LDAP, cross site scripting (XSS), XML external entities (XEE) attacks, broken access control or cross site request forgery (CSRF) and many more [2].

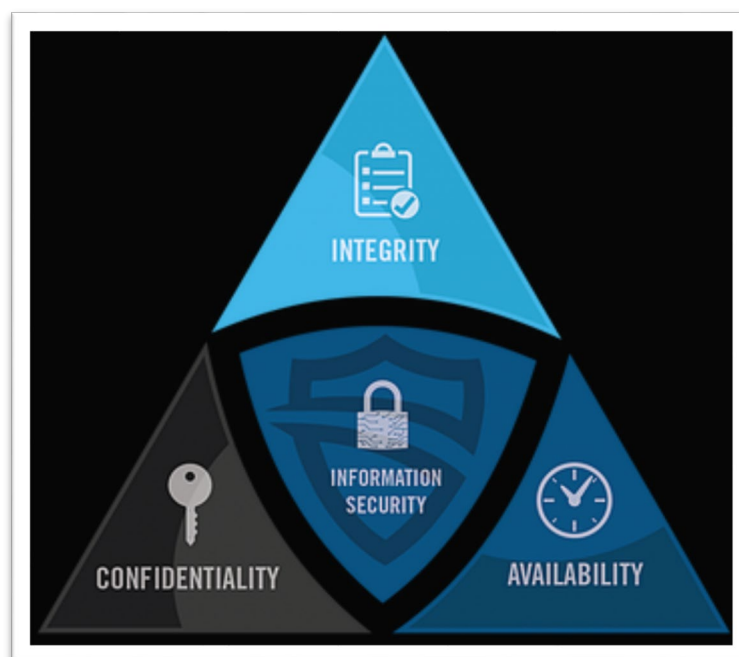


Figure 1- The CIA Triad

The CIA triad gives the principles used to safeguard computer resources and provide a model for computer security. This maintains data confidentiality, integrity, and availability.[3] To adhere to these principles, and in order to hold accountability, there is a need for security to be considered within the development of web applications. This needs to be considered from design stage on in order to protect organisations, brands, and personal data, as this potentially leads to possible breaches of the general data protection regulation (GDPR) [4]. There are a select few organisations offering advice and guidelines, however other than the ISO 27000 family [5] giving a standard, there are no officially set guidelines to web application security for developers. This study aims to use the available guidelines as well as the ISO standards to consider effective best practice criteria for secure web application and website design and development.

2.2 General Literature review

As Appiah et al [5] observe, the business logic and architecture of a website or web application has many moving parts, allowing for a large potential for vulnerabilities to be exploited in the following areas:

- Web server containing the client interface and server-side information.
- The Uniform Resource locator (URL), making a web application known to the client.
- The connection and communication between the client browser and the application's server through the Transmission Communication Protocol and Internet Protocol (TCP/IP).
- The Hyper Text Transfer Protocol (HTTP) allowing the communication and delivery of requests between server and client.
- The formatting of the data within an application using Cascading Style Sheets (CSS) and Hyper Text Mark-up Language (HTML), returning a result to be displayed within the client's browser.

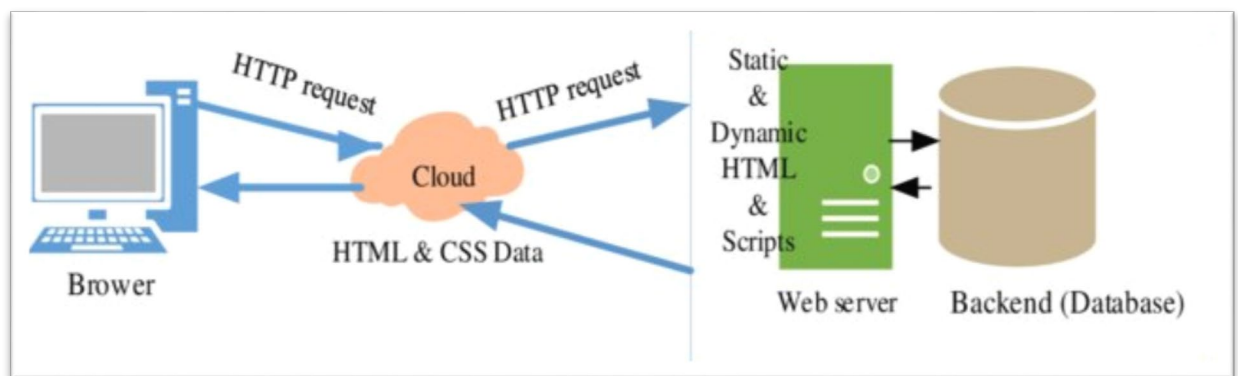


Figure 2 - Architecture of a Website / Web Application [5]

This allows for a weakness of the web environment, allowing attackers to use the following methods. [6]

OWASP 2017 report lists the top ten vulnerabilities as:

- A1 – (Code) Injection
- A2 – Broken Authentication
- A3 – Sensitive Data Exposure
- A4 – XML External Entities (XEE)
- A5 – Broken Access Control
- A6 – Security Misconfiguration

- A7 – Cross Site Scripting (XSS)
- A8 – Insecure Deserialization
- A9 – Using Components with Known Vulnerabilities
- A10 – Insufficient Logging and Monitoring [2]

The Open Web Application Security Project (OWASP) purport that:

“Insecure software is undermining our financial, healthcare, defence, energy, and other critical infrastructure. As our software becomes increasingly complex, and connected, the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.” [2]

This is evidenced within the OWASP top ten, produced every three years [2] and by Kaur and Kaur [7] with an analysis of web attacks between January 2012 and May 2015, taken from the Website Hacking Incident Database (WHID)[8] seen below.

Table 1 - Web Attacks Data Jan2012 - May2015 [6] [7]

Attack	Jan – Dec 2012	Jan – Dec 2013	Jan –Dec 2014	Jan- June 2015
SQLi	352	185	112	71
DDoS	151	178	85	30
XSSs	68	34	6	02
A/c Hijacking	30	106	88	34
Defacement	74	120	135	57
Unauthorized access	10	14	11	1
Directory traversal	0	3	2	1
Phishing	9	2	2	0
PoS/Malware	11	29	74	31
BruteForce	0	4	4	0
Malicious Code injection	0	1	5	0
DNS Hijacking	6	29	15	5
Server Vulnerabilities	1	0	2	0
Others	97	132	129	35
Unknown	265	208	183	68
Total	1074	1045	853	335

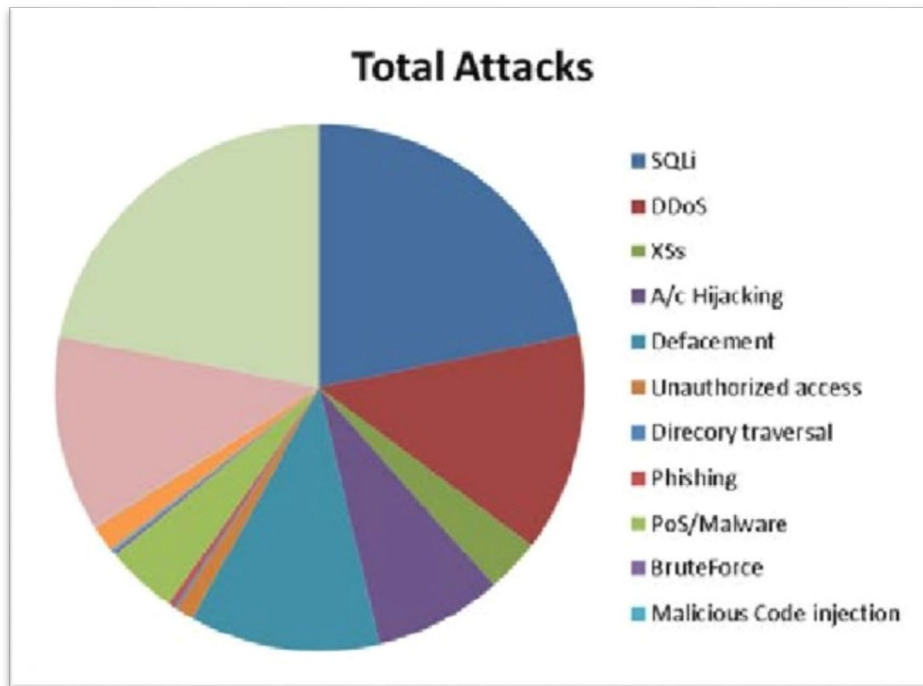


Figure 3 - Total Web Attacks by Category [6] [7]

A more recent study by a leading digital security company, Positive Technologies, backed up by OWASP data reveals that the most common vulnerabilities encountered through web applications in 2019 were security misconfiguration (A6), XSS (A7), broken authentication (A2), broken access control (A5) and code injections (A1). [9]

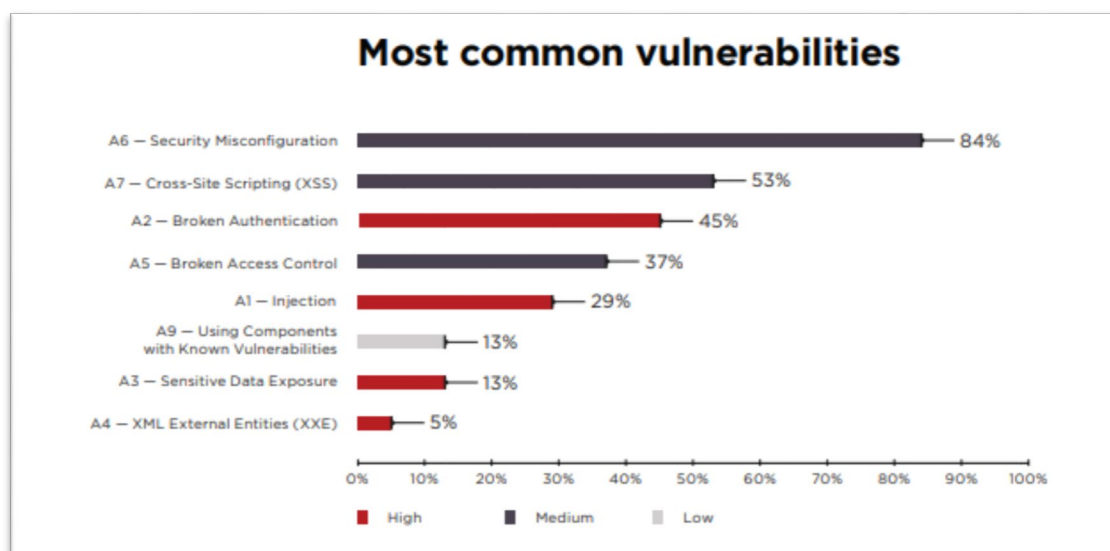


Figure 4 - Most common OWASP Top 10 vulnerabilities by percentage of web applications [8]

From conference proceedings in 2010, Serrao suggests a correlation between the growth of available information on the internet and a growth in the number of attacks to web systems, with web applications becoming the new target to attackers. The observation made is that this is due to the popularisation of Web 2.0 and 3.0 as well as access to API's, specifically social network API's, Software As A Service (SaaS) and cloud computing models. [10] Positive Technologies establish that the percentage of web applications containing high-risk vulnerabilities in 2019 fell by seventeen percentage points. However one out of five vulnerabilities has high severity and 82% of vulnerabilities were located in application code, allowing attacks in nine out of ten web applications, with breaches of data being a threat in 68%. [9]

Similar results were found in an independent study conducted for the International Journal of Computer Engineering & Technology (IJCET) that shows 85% of websites are vulnerable to hacking and concludes that:

“Getting a grip on web security is the next important thing for Web Services” and that “security is inherently empirical to its nature in that certain vulnerabilities will not be discovered until a particular technology is widely used in real world situations and subject to massive attacks”.[11][12]

One would argue, however, that once a technology is used widely, it is too late. There is a need for knowledge of vulnerabilities within the industry to mitigate exploitation prior to implementation.

Saxena et al [12] argue that, whilst a lot of the vulnerabilities noted are server-side, as highlighted by most research papers, there is another classification of client-side vulnerabilities and flaws. This has been classified as Client-Side Validation (CSV). It is claimed these are likely due to the growing complexity of Javascript and AJAX applications. Although these are a part of a wider input validation vulnerabilities class, they are different from the traditional vulnerabilities. As an example, this could involve data entering the application through the browser's “cross-window communications abstraction” and processed completely by Javascript code, or a web application sanitising the data entered sufficiently for the initial HTML response, but not sufficiently sanitised for the use in the Javascript component. [13] This reflects the importance for the study to take a holistic approach to incorporate full stack testing of applications.

Curphey and Arawo [13] observe that there needs to be careful thought and planning to security testing web applications due to the immaturity of both tools and industry. There is a need to analyse the development environment, the process and the web application's complexity to be able to find the most suitable tools. [14]

Razzaq et al [14] suggest that traditional solutions to and protecting web applications by mitigating application level attacks are ineffective as more than 80% of attacks are at application layer. It is also purported that 90% of applications are vulnerable to these attacks.[15]

Scambray et al [15] describe the key aspects to a web application security program as being three-fold.

- Threat modelling
- Code review
- Security testing

It is also asserted that, based on the experiences of major software companies

“threat modelling is one of the most critical steps you can take to improve the security of your web applications”. [16]

This is reflected in other books such as Writing Secure Code, 2nd Edition [17] and The Security Development Lifecycle [18]

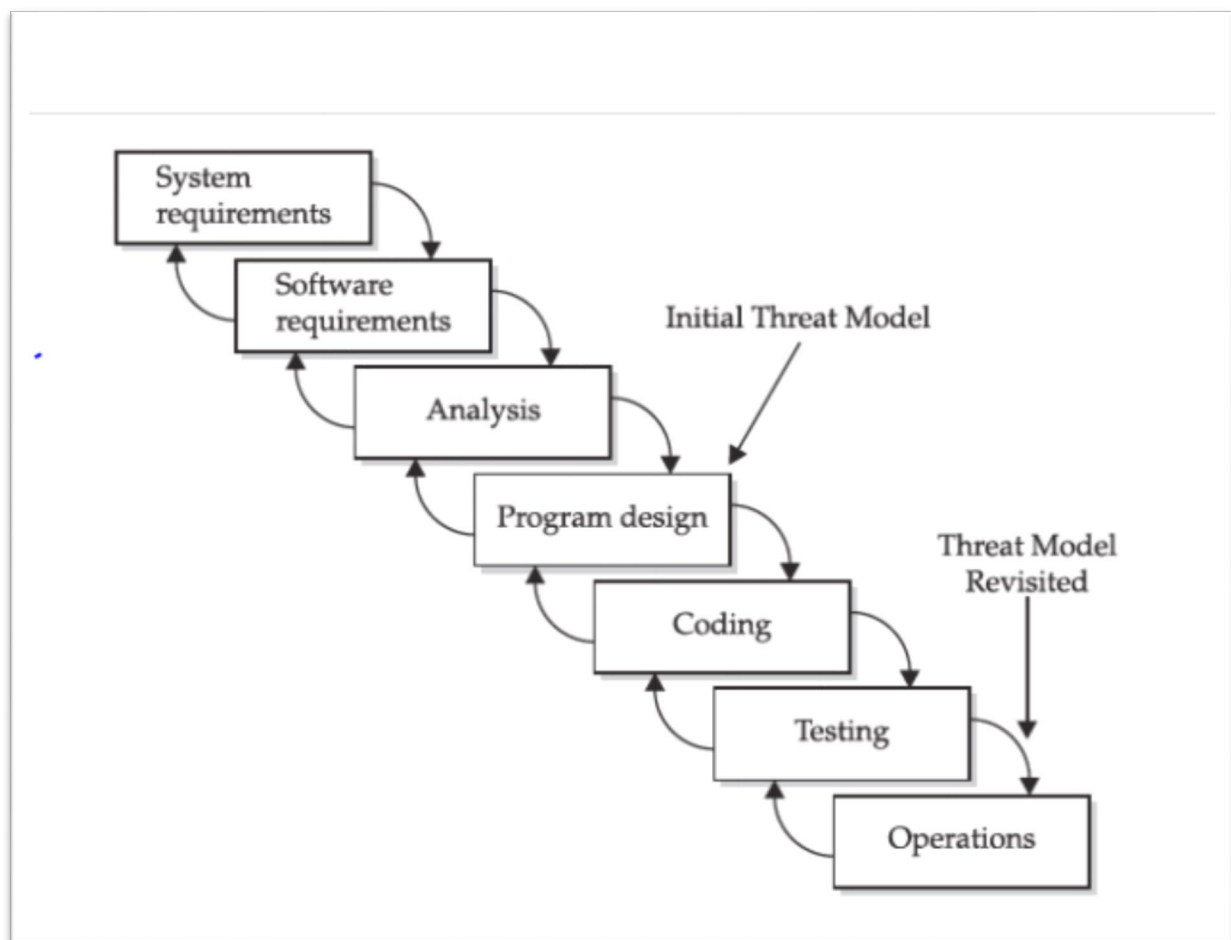


Figure 5 - Threat Modelling within the development process [15]

This will make for a good model to consider in the development of the proof of concept application with consideration also given to the OWASP Application Security Verification Standard (ASVS). This is described by OWASP to be a list of application security requirements or tests that can be used in defining, building, testing and verifying secure applications. [19]

	Applicability	Building			Building, Configuration, Deployment Assurance and Verification			Assurance and Verification	
Level 1	All apps		Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Penetration Testing	DAST
Level 2	All apps	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Level 3	High Assurance	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
	Legend	Acceptable	Suitable						

Figure 6 - - OWASP Application Security Verification Standard 4.0 Levels

OWASP do provide an objective view and model as they are vendor-neutral and a not-for-profit organisation, and so become a good base point for this research. Using their ‘Top 10 Vulnerabilities’ [1] as well as ASVS [16] and the OWASP Testing Guide 4.0. [20] The testing guide supports the view that testing should take place in each of the phases of the software development life cycle (SDLC).

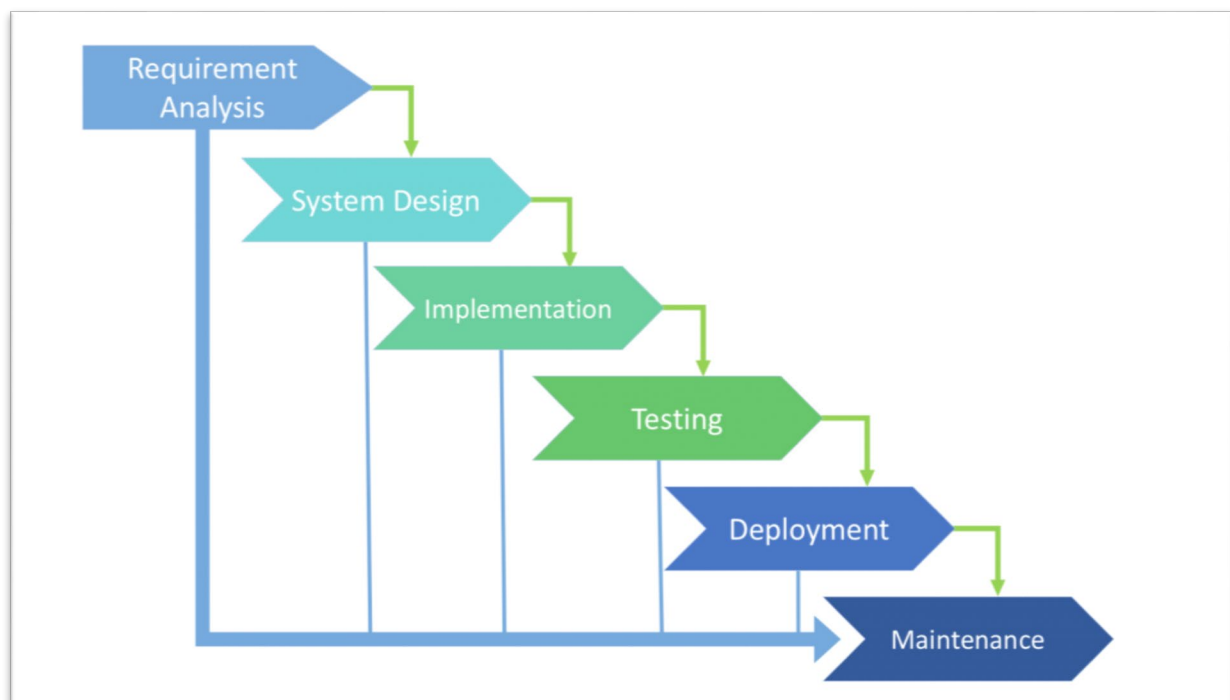


Figure 7 - Generic SDLC waterfall model

3.0 Research Methodology

As stated in section 1.1, the aim of this study is to investigate and assess vulnerabilities specific to websites and web applications. For this it is important to follow a structured process to determine a methodology for the research of this study.

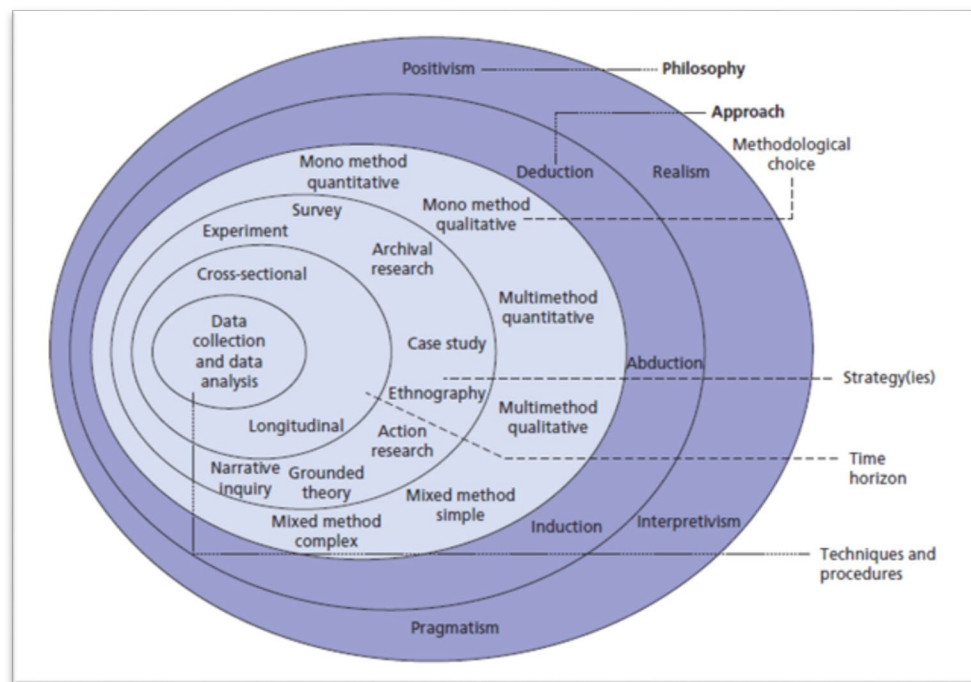


Figure 8- Research Philosophy using the Research Onion [21]

3.1 Research Philosophy

When considering a paradigm, it is prudent to consider the nature of the study such as:

- Is the subject and outcome to be objective or subjective?
- Is the observer independent or part of what is observed?
- Will the researcher focus on facts or meanings?
- Is the research a search for causality and fundamental laws or an attempt to understand what is happening?
- Is the researcher looking to formulate hypotheses and then test them or develop ideas through induction of data? [22]

The nature of the discussed study is investigative, developmental, and evaluative. By its nature it is fundamentally:

- Objective – it is an external view of the data to investigate current security vulnerabilities in web applications
- The researcher is independent to the assessment of the data to establish the current measures for preventing security risks.
- The study will mostly be focussing on the facts to establish effective criteria for a secure web application design. Although, there is room for interpretation of meaning within this area.
- Through critically evaluating the security of the implemented web application, this shows a search for causality and fundamental laws.
- Through designing and developing a ‘Proof of Concept’ web application to evaluate against current security guidelines, the researcher is looking to test against a hypothesis.

For the reasons listed above, this study is a developmental project following the positivist paradigm, bordering to the phenomenology paradigm in as much as there will be case studies involved. This lends itself well to the researcher’s pragmatist nature.

3.2 Research Approach

The research and study will rely strongly on previous theory, heavily dependent on document and literature review. This will then allow the formulation of a hypothesis, or a set of hypotheses tested through the development of a proof of concept application. The empirical data obtained will be used to check if these hypotheses are true or not. This is the deductive approach.

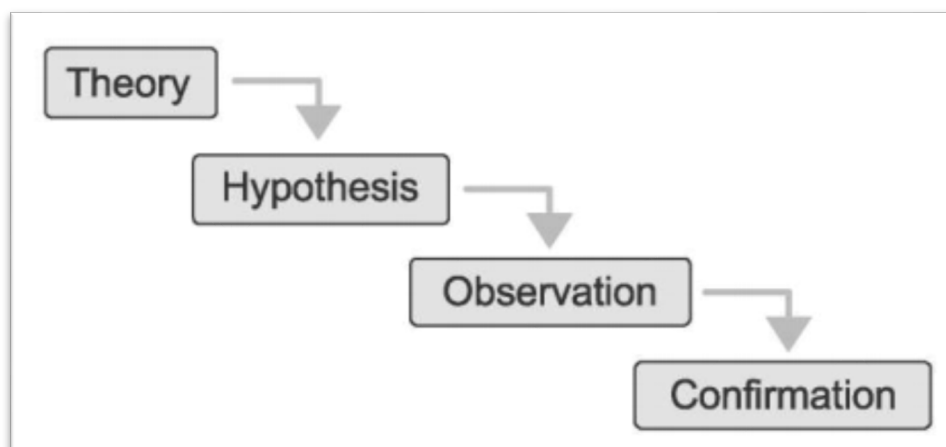


Figure 9 - Schematic representation of Deductive Reasoning [23]

In opposition to this there is the inductive approach. This may involve analysing or observing some phenomena and building the theory using empirical data and pattern through a tentative hypothesis. [23]

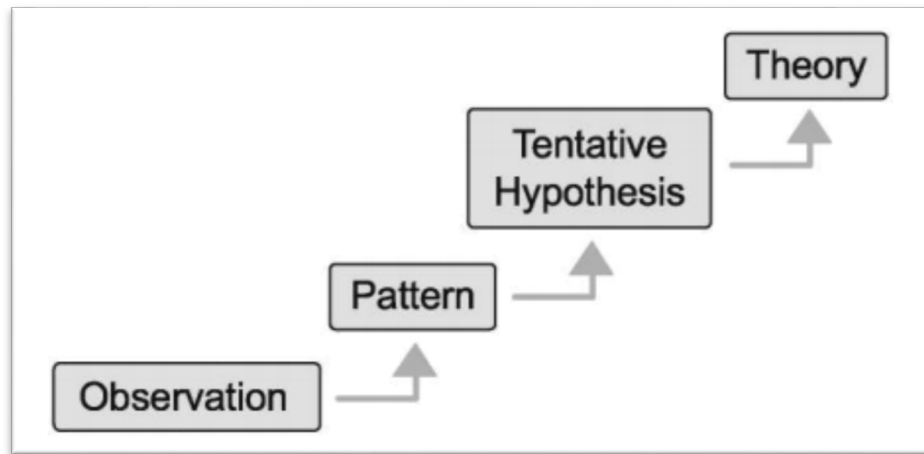


Figure 10 - Schematic representation of Inductive Reasoning [23]

Although the study has been defined as deductive, it is prudent in this case to adopt a methodological pluralist approach, meaning the developmental project will employ the inductive approach of case study initially to investigate vulnerabilities and generate the hypotheses and use the deductive approach to verify them by comparing additional cases. As discussed in section 3.1, this then crosses the boundary between the deductive approach using positivist philosophy, and the inductive approach using phenomenology. [22] [23]

3.3 Research Strategies

The strategies for this research, mainly following the deductive approach, will incorporate three steps:

- **Case study** – to investigate current security vulnerabilities in web applications and assess current measures for preventing security risks.
There will be an investigation into previous cases, especially using organisations such as OWASP, National Institute of Standards and Technology (NIST), WHID, The Web Application Security Consortium (WASC), and Cloud Security Alliance (CSA).
- **Document review and analysis** – to produce a systematic assessment of the current measures for preventing security risks and to establish effective criteria for a secure web application design.
- **Software development** - for a ‘Proof of Concept’ web application to evaluate against current security guidelines in iterative testing, using a variety of tools.

3.3.1 Data collection

This study will use an assortment of both primary and secondary data. Initially in the investigative and assessment process, there will be a curation of secondary data within case studies, document reviews,

and literature reviews, and the possibility of meta-analysis, to establish theories and hypotheses on security vulnerabilities and assessing current measures for preventing security risks and establishing criteria for secure web applications. This will help to build the theory and specifications for the development of the proof of concept application.

Once the application is developed, primary data will be produced by testing it. The results will be evaluated and explored to prove and construct the concept of a secure application. [24]

3.3.2 Suitability

Prior checks will be made to make sure that the research objectives can be fulfilled and that the right questions can be answered using both categories of data. Consideration is given to ensure:

- **Credibility**

It will be imperative to authenticate the data researched, more specifically the secondary data, by ensuring that the source of the information is credible. This means analysing the organisations publishing the data, critically think through the nature of the information, the type of organisation, the motive and the purpose of the data supplied. Further analysis will be given to the authors' line of reasoning and point of view with a mind to possible hidden agendas. Checks will be made to logical progression within the information as well as premises and reasoning within the narrative. More importantly, the supporting evidence will be evaluated and cross referenced with further research papers, ensuring correct assumptions are being made and trends are produced. [23]

For primary data captured, two main principles will be followed, homogeneity – measuring one construct, convergence – similarity in measuring concepts. The criteria for this will be:

- **Reliability**

The data produced will be reliable. The raw data will be observed and evaluated with no manipulation so as not to taint the results. Moreover, there will be consistency through all testing, at every iteration so that the data can be replicable.

- **Generalisability**

The test data, although being tested on a small sample scale, will be produced in such a way that theories and results are able to be applied across the board, and scaled through the industry. For this it will be important to consider guidelines and criteria for testing outlined by the aforementioned organisations.

- **Validity**

It will be ensured that the concept will be accurately measured against the correct and intended theory and criteria at every iteration.

3.3.3 Time Horizon

The time horizon for testing will be short term as opposed longitudinal. The reason for this is that the test and evaluation of the proof of concept application will be a snapshot evaluation.

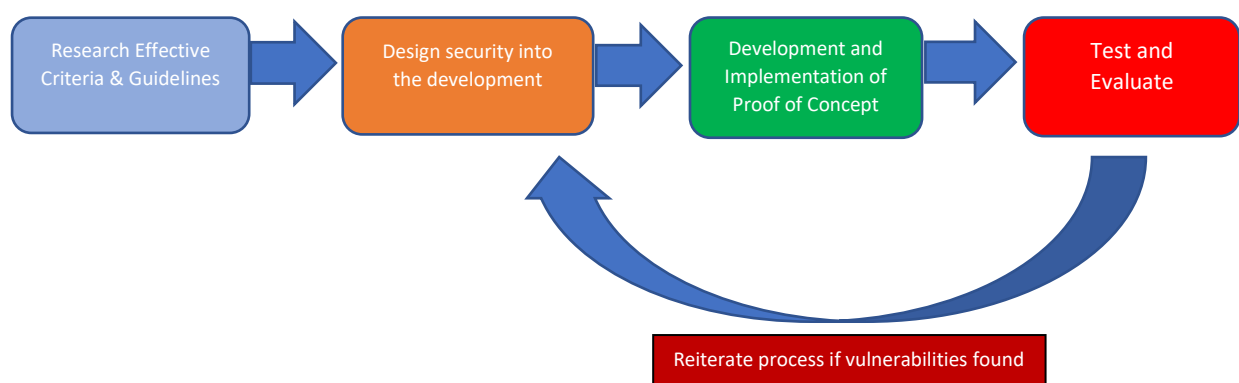
3.3.4 Data Analysis

The options for the data analysis are generally qualitative, associated with phenomenology, or quantitative, associated with positivism.

The data collected will be in the main quantitatively evaluated, following the positivist paradigm and the deductive approach of the study. The reasons for this are that the study is looking to discover generalisation in the field and refine hypotheses and the researcher will be neutrally observing from an objective point of view.

3.4 Web Application Development Methodology

The development of the web application will be designed around the traditional Agile software development lifecycle (SDLC). The requirements and design section will be the case study and research to establish suitable criteria for a secure web application. The development and implementation will be followed by testing and evaluation. The latter two parts will be iterative to build in more security each time with the end aim being total security with no vulnerabilities.



3.5 Expected Outcomes

From the research and development of a secure web application the expected outcomes will be:

- A full understanding of potential web application vulnerability and forms of attacks established.

- Effective criteria established for a secure web application.
- A fully secure web application developed with full mitigation of known vulnerabilities.
- A set of recommendations produced for recognising and mitigating vulnerabilities in web applications at design and development stage based on the research and development, and the evaluation of the web application.

4.0 Resources and Planning

4.1 Physical resources

For this study, the requirements will be:

- Access to available computers and normal laboratory software.
Needed to research and case study, develop the proof of concept web application, and test and evaluate it.
- Access to the library for research papers and books.
Needed to research and review academic literature.
- Internet connectivity.
- Access to vulnerability testing and penetration testing tools.
Needed to be able to test and evaluate the developed application.

The last resource to mention, as it is often overlooked, is time. It is important to allocate time to the study and this is covered in section 4.3.

4.2 Stakeholders

Stakeholders considered within the process will be:

- The researcher
- The researcher's supervisor.
- Other lecturers and university staff including librarians who will provide an input.
- The researcher's family and circle of friends.

4.3 Planning

The project will run throughout the academic year 2020 – 2021. In preparation to this, leading up to the start of the academic year, the background research and literature review will take place. Throughout the academic year, twelve hours a week will be allocated within university time to study and develop. Outside of that time research, study and development will continue. The Gantt chart below gives a timeline for the proposed project and is to be used as a working document, subject to review and adjustment.

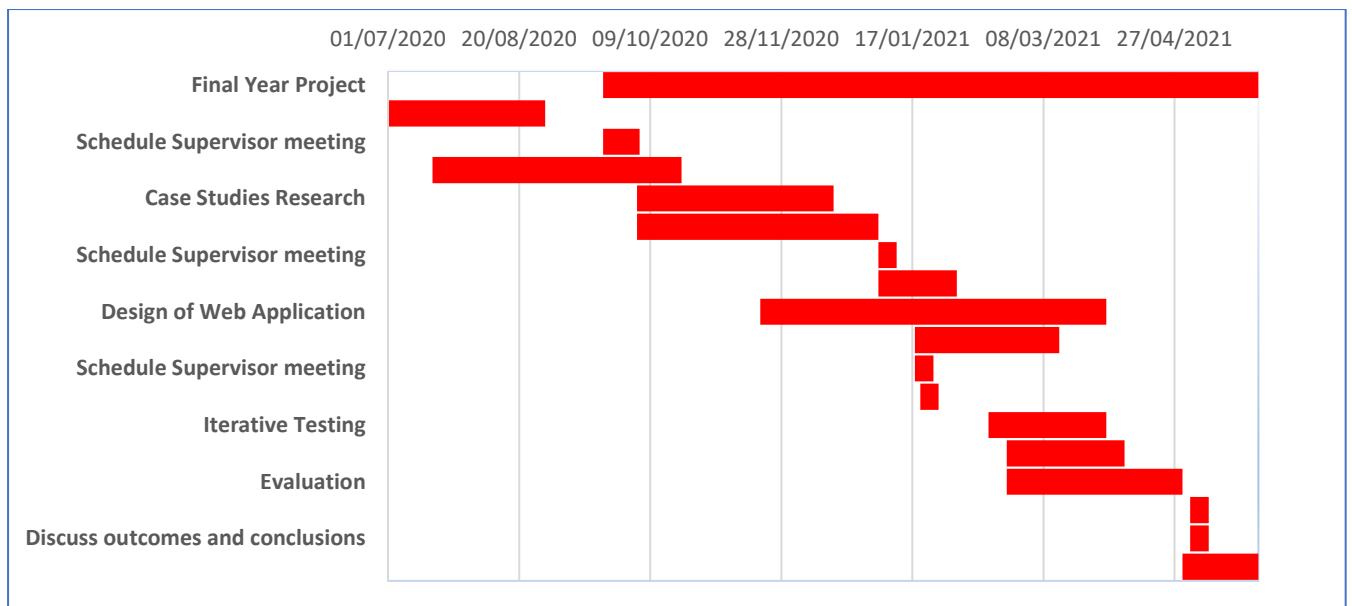


Figure 11 - Gantt chart timeline as a first iteration of a working document

It is important also to consider some contingency time, so the final report and the length of the project should show on the Gantt chart to finish a little prior to submission to allow the extra time if needed. Also, possible contingency time should be considered at the development stage as that is the time for the largest potential to risk.

5.0 Risks

Risk, in the context of this project, is the potential for negative outcomes within the project. The top five risks are highlighted, and the priority of that risk listed within a risk matrix. These risks are:

- **R1 - Prioritising wrongly** – The potential for this is that the enjoyable or most exciting tasks, the ones that the researcher finds most interesting, will be prioritised and there will not be as much time needed for other tasks.
- **R2 - Scope creep** – The potential here is that the scope of the project is extended beyond its initial limits. It is expected that the scope will shift during the process as research is conducted, however it will be to the detriment of the project to go beyond the limitations.
- **R3 - Allocating resources wrongly** – It is important to allocate resources correctly, with the biggest being time. The potential here is that resources can be wrongly allocated or attributed, meaning that the right allocation is not prioritised. This can be detrimental to the project as resource could run out before completion of the prioritised tasks.
- **R4 - Lack of knowledge**- The potential lack of knowledge could have a negative effect on the project, as a whole. More specifically, it could be in certain areas such as software, application development, partial understanding of the subject and more.
- **R5 - Loss of technology** – This is probably the largest risk. There is great potential for the computer to fail, data corruption, loss of internet, software crash, hardware theft or even damage. As a result, this could hinder or push work back, and in the worst-case scenario, lose everything, imposing the need to restart.

These risks are rated in order of priority in the risk matrix.

Impact	Significant		R5		
	High			R3	R1
	Moderate		R4	R2	
	Low				
		Very Unlikely	Unlikely	Likely	Very Likely
		Probability			

The priority is to mitigate the risks in the red, above the tolerance line. This is done through action planning. The actions for the mitigation of R1, R3 and R5 are as follows:

- **R1** – Mitigation will be achieved by planning and allocation. A plan will be made for the order of priority and a reviewed timeline worked to. Lists will help to keep a focus on what is needed.
- **R5** – Mitigation will be achieved by a redundancy and backup strategy. All work will be backed up in at least four separate places daily, providing a recovery method should any get destroyed. One of these places will be the cloud. Also allow for redundancy by ensuring a secondary computer, storage, and software as well as internet connection is available.
- **R3** – Mitigation will be achieved by planning. A full plan will be created and followed showing where resources should be allocated and when in order of importance and priority. This will be constantly reviewed as a working document.

It is prudent to note that with the current situation regarding Covid-19, there may be limited access to the university and library. This may result in a risk that could potentially hinder the research in the short term.

6.0 Ethical and Legal concerns

It is important to state that the researcher aims to behave professionally and ethically in all activities and conduct.

The nature of this study may lead an assumption that there will be ethical issues, however, this is reduced drastically in as much as the application being tested for penetration through vulnerabilities will be a self-developed, benign application specifically for that purpose. This removes ethical issues within the field of study, and there will be no sensitive data collected of any form.

The ethical issues, therefore, lie within the academic activities. It is important to state that the relevant guidelines and codes of practice will be followed. For this there are two main guidelines that will be observed and adhered to:

- The British Computer Society (BCS) Code of conduct for BCS members (5th version reviewed on 5th June 2019) including the BCS Code of Ethics. [25]
- The University of Wales Trinity Saint David (UWTSD) Research Ethics and Integrity Code Of Practice. [26]

7.0 Conclusion

Security in general is a very important area of study, furthermore online security, specifically web application security is an essential topic of consideration within development, from planning stage all the way through the process, and should be considered to be an ongoing review and development process throughout the life of a web application.

The proposed project looks to investigate current security vulnerabilities in web applications through document reviews and produce a systematic assessment of the current measures for preventing security risks through case studies. It will aim to establish effective criteria for a secure web application design and develop a 'Proof of Concept' web application to evaluate it against current security guidelines. The application will be tested using testing tools available through open source and evaluate the results to expose vulnerabilities. The process will be reiterated, as necessary. The study will follow a positivism philosophy with a deductive approach. The web application will be developed following a traditional Agile software development lifecycle model, with iterative testing on implementation.

8.0 References

- [1] "BBC NEWS | Technology | Web's inventor gets a knighthood."
<http://news.bbc.co.uk/1/hi/technology/3357073.stm> (accessed Apr. 30, 2020).
- [2] T. Ten, M. Critical, W. Application, and S. Risks, "Owasp Top 10(En)," 2017.
- [3] S. Mohanty, M. Ganguly, and P. K. Pattnaik, "CIA Triad for Achieving Accountability in Cloud Computing Environment," *Int. J. Comput. Sci. Mob. Appl.*, vol. 6, no. 3, pp. 38–43, 2018, Accessed: Apr. 27, 2020. [Online]. Available: www.ijcsma.com.
- [4] "Guide to the General Data Protection Regulation - GOV.UK."
<https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation> (accessed Apr. 26, 2020).
- [5] "ISO - ISO/IEC 27001 — Information security management." <https://www.iso.org/isoiec-27001-information-security.html> (accessed Apr. 26, 2020).
- [6] V. Appiah, M. Asante, I. K. Nti, and O. Nyarko-Boateng, "Survey of websites and web application security threats using vulnerability assessment," *J. Comput. Sci.*, vol. 15, no. 10, pp. 1341–1354, 2019, doi: 10.3844/jcssp.2019.1341.1354.
- [7] D. Kaur and P. Kaur, "Empirical Analysis of Web Attacks," in *Physics Procedia*, 2016, vol. 78, pp. 298–306, doi: 10.1016/j.procs.2016.02.057.
- [8] "(No Title)." http://projects.webappsec.org/f/WHIDWhitePaper_WASC.pdf (accessed Apr. 26, 2020).
- [9] "Web Applications vulnerabilities and threats: statistics for 2019."
<https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/> (accessed Apr. 26, 2020).
- [10] "(PDF) Automating Web Applications Security Assessments through Scanners | Carlos Serrao - Academia.edu."
https://www.academia.edu/2670212/Automating_Web_Applications_Security_Assessments_through_Scanners (accessed Apr. 25, 2020).
- [11] Rajendra Maurya, "(PDF) Research Challenges and Issues in Web Security.pdf | Rajendra Maurya - Academia.edu."
https://www.academia.edu/34606795/Research_Challenges_and_Issues_in_Web_Security.pdf?email_work_card=view-paper (accessed Apr. 23, 2020).
- [12] "(PDF) RESEARCH CHALLENGES AND ISSUES IN WEB SECURITY | IAEME IAEME - Academia.edu."
https://www.academia.edu/13064585/RESEARCH_CHALLENGES_AND_ISSUES_IN_WEB_SECURITY?email_work_card=view-paper (accessed Apr. 23, 2020).
- [13] D. S. Prateek Saxena, Steve Hanna, Pongsing Poosankam, "FLAX: Systematic Discovery of Client-side Validation Vulnerabilities in Rich Web Applications," 1395.
- [14] M. Curphey and R. Araujo, "Web application security assessment tools," *IEEE Security and Privacy*, vol. 4, no. 4, pp. 32–41, Jul. 2006, doi: 10.1109/MSP.2006.108.
- [15] A. Razzaq, A. Hur, N. Haider, and F. Ahmad, "Multi-layered defense against web application attacks," in *ITNG 2009 - 6th International Conference on Information Technology: New Generations*, 2009, pp. 492–497, doi: 10.1109/ITNG.2009.77.
- [16] C. S. Joel Scambray, Vincent Liu, *Hacking Exposed Web Applications: Web Application Security*

- [17] M. Howard and D. LeBlanc, *Writing Secure Code*. 2015.
- [18] G. Larry, *the Security Development Lifecycle: Microsoft*. 2007.
- [19] OWASP, "Application Security Verification Standard (2014)," no. October, p. 47, 2014.
- [20] M. Meucci and A. Muller, "4.0 Testing Guide." Accessed: Apr. 27, 2020. [Online]. Available: <http://www.owasp.org>.
- [21] "Research Philosophy - Research Methodology." <https://research-methodology.net/research-philosophy/> (accessed Apr. 28, 2020).
- [22] P. Zaborek, "Piotr Zaborek Qualitative and Quantitative Research Methods in Management Science," no. September, pp. 41–50, 2009, doi: 10.13140/2.1.1413.4725.
- [23] W. M. Trochim, *The Research Methods Knowledge Base*. 2018.
- [24] N. Walliman, *Research Methods, The Basics*, vol. 2, no. 8. 1971.
- [25] BCS, "Code of CONduct for BCS Members," 2019.
- [26] UWSTD, "Research Ethics and Integrity Code of Practice," p. 19, 2017, [Online]. Available: <https://www.uwtsd.ac.uk/media/uwtsd-website/content-assets/documents/research/research-ethics-integrity-code-practice.pdf>.