**Vigilant Shield**

*Submitted in partial fulfillment of the requirements for the degree of*

**Bachelor of Technology**

in

**Computer Science with specialization in Bioinformatics**

*by*

# RIA ARORA

**15BCB0066**

**Under the guidance of**

**Prof. Srivani A.**

**SCOPE**

### VIT, Vellore.



April, 2019

**DECLARATION**

I hereby declare that the thesis entitled “Vigilant Shield" submitted by me, for the award of the degree of *Bachelor of Technology in Computer Science with specialization in Bioinformatics* to VIT is a record of bonafide work carried out by me under the supervision of Srivani A.

I further declare that the work reported in this thesis has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place : Vellore Date :

### Signature of the Candidate

**CERTIFICATE**

This is to certify that the thesis entitled “Vigilant Shield” submitted by **Ria Arora (15BCB0066)**, **SCOPE**, VIT University, for the award of the degree of *Bachelor of Technology in Computer Science with specialization in Bioinformatics*, is a record of bonafide work carried out by him under my supervision during the period, 07.01. 2019 to 3.05.2019, as per the VIT code of academic and research ethics.

The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university. The thesis fulfills the requirements and regulations of the University and in my opinion meets the necessary standards for submission.

Place : Vellore

Date : **Signature of the Guide**

### Internal Examiner External Examiner

Lakshmanan K

Department of Analytics

# ACKNOWLEDGEMENT

The internship opportunity I had with Deloitte & Touche Assurance & Enterprise Risk Services India Private Limited, was a great chance for learning and professional development. Therefore, I consider myself as a very lucky individual as I was provided with an opportunity to be a part of it. I am also grateful for having a chance to meet so many wonderful people and professionals who led me through this internship period.

I feel immense pleasure and privileged in expressing my deepest and most sincere gratitude to Mr Arun Kalikota and Mr Pulkit Sahani for their support and suggestions during the course of project work in "Vigilant Shield".

**I will strive to use gained skills and knowledge in the best possible way, and I will continue to work on their improvement, in order to attain desired career objectives.**

**Ria Arora**

**Executive Summary**

This report is a log of my four-month internship carried in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science with Specialization in Bioinformatics. The internship was carried out within the esteemed organization, Deloitte & Touche AERS India Pvt. Ltd. Undergoing this training is the best way of acquiring knowledge, Experience and a deeper understanding about programming and software.

The name of the project I was working on during my internship is “Vigilant Shield”. This project includes web application security testing. Web application security testing is a proactive method to detect application vulnerabilities and safeguarding websites against various attacks.

The project has four main threads:

1. **DAST (Dynamic Application Security Testing)**

Dynamic Application Security Testing (DAST) is a [black-box security testing](https://www.acunetix.com/blog/articles/black-box-security-testing/) methodology in which an application is tested from the outside. A tester using DAST examines an application when it is running and tries to hack it just like an attacker would.

1. **SAST (Static Application Security Testing)**

Static Application Security Testing (SAST) is a white-box testing methodology. A tester using SAST examines the application from the inside, searching its source code for conditions that indicate that a security vulnerability might be present.

1. **Internal Infrastructure**

The internal infrastructure consists of all the resources that are used by all the analysts working on the project.

1. **Reporting and Documentation**

In each and every project, all the activities including testing and their findings are to be reported in the form of a document. Reporting and Documentation is an essential part of the project.

|  |  |  |
| --- | --- | --- |
|  | **CONTENTS** | **Page**  **No.** |
| **Acknowledgement** | i |
| **Executive Summary** | ii |
| **Table of Contents** | Iii |
| **List of Figures** | ix |
| **List of Tables** | xiv |
| **Abbreviations** | xvi |
| **Symbols and Notations** | xix |
| 1 | **INTRODUCTION** | 1 |
|  | 1.1 Objective | 1 |
|  | 1.2 Motivation | 2 |
|  | 1.3 Background | 3 |
| 2 | **PROJECT DESCRIPTION AND GOALS** | 3 |
| 3 | **TECHNICAL SPECIFICATION** | 3 |
| 4 | **DESIGN APPROACH AND DETAILS (as applicable)** | . |
|  | * 1. Design Approach / Materials & Methods   2. Codes and Standards | .  . |
|  | 4.3 Constraints, Alternatives and Tradeoffs | . |
| 5 | **SCHEDULE, TASKS AND MILESTONES** | . |
| 6 | **PROJECT DEMONSTRATION** | . |
| 7 | **COST ANALYSIS / RESULT & DISCUSSION (as applicable)** | . |

|  |  |  |
| --- | --- | --- |
| 8 | **SUMMARY** | . |
| 9 | **REFERENCES** | . |
|  | **APPENDIX A** | . |

**List of Figures**

|  |  |  |  |
| --- | --- | --- | --- |
| **Figure No.** |  | **Title** | **Page No.** |
| 2.1 | Figure caption |  | 13 |
| 2.2 | Figure caption |  | 15 |

(In the chapters, figure caption should come below the figure and table caption should come above the table. Figure and table captions should be of font size 10.)

## List of Tables

**Table No. Title Page No.**

2.1 Table caption 28

# List of Abbreviations

3GPP Third Generation Partnership Project

2G Second Generation

3G Third Generation

4G Fourth Generation

AWGN Additive White Gaussian Noise

# Symbols and Notations

f CFO

 NCFO

## INTRODUCTION

* 1. ABOUT DELOITTE

Deloitte is a multinational professional services network. Deloitte is one of the "Big Four" accounting organizations and the largest professional services network in the world by revenue and number of professionals.

Deloitte provides audit, tax, consulting, enterprise risk and financial advisory services with more than 286,200 professionals globally. In FY 2018, the network earned a record $43.2 billion USD in aggregate revenues. As of 2017, Deloitte is the 4th largest privately-owned company in the United States. Deloitte has been ranked number one by market share in consulting by Gartner, and for the fourth consecutive year, Kennedy Consulting Research and Advisory ranks Deloitte number one in both global consulting and management consulting based on aggregate revenue.

Deloitte member firms offer services in the following functions:

* **Audit**

Audit provides the organization's traditional accounting and audit services, as well as internal auditing and IT control assurance. In 2018, audit grew by 7.7%.

* **Consulting**

Consulting assists clients by providing services in the areas of enterprise applications, technology integration, strategy & operations, human capital, and short-term outsourcing. In 2018, consulting grew by 15.7%.

* **Financial advisory**

Financial advisory provides corporate finance services to clients, including dispute, personal and commercial bankruptcy, forensics, e-discovery, document review, advisory, mergers & acquisitions, capital projects consulting and valuation services. In 2018, financial advisory grew by 8%.

* **Risk advisory**

Risk advisory provides offerings in enterprise risk management, information security and privacy, data quality and integrity, project risk and cyber risk, and business continuity management and sustainability. In 2018, risk advisory grew by 12%.

* **Tax and legal**

Tax & legal helps clients increase their net asset value, undertake the transfer pricing and international tax activities of multinational companies, minimize their tax liabilities, implement tax computer systems, and provides advisory of tax implications of various business decisions. In 2018, tax & legal grew by 8.7%.

* **GovLab**

GovLab is the internal think tank of Deloitte Consulting LLP's Federal Government consulting practice, focused on innovation and government reform. Created in 2010, GovLab is based in the Washington, D.C. metro area and typically undertakes 8 or 9 research topics per year, focusing on how future trends, technologies, and business models will affect government.

* 1. OBJECTIVE

A security test is a method of evaluating the security of a computer system or network by methodically validating and verifying the effectiveness of application security controls. A web application security test focuses only on evaluating the security of a web application. The process involves an active analysis of the application for any weaknesses, technical flaws, or vulnerabilities. Any security issues that are found will be presented to the system owner, together with an assessment of the impact, a proposal for mitigation or a technical solution. [Security Testing](https://www.softwaretestinghelp.com/how-to-test-application-security-web-and-desktop-application-security-testing-techniques/) is the process which checks whether the confidential data stays confidential or not i.e. it is not exposed to individuals/ entities for which it is not meant for and the users can perform only those tasks that they are authorized to perform.

* 1. MOTIVATION

Security testing has a distinct relationship with software quality. Just because software meets quality requirements related to functionality and performance, it does not necessary mean that the software is secure. A security measure which protects against the disclosure of information to parties other than the intended recipient that is by no means the only way of ensuring the security. The most effective way to achieve secure software is for its development life cycle processes to rigorously conform to secure development, deployment, and sustainment principles and practices. Security testing is a process to determine that an information system protects data and maintains functionality as intended. Software security testing services helps in identify implementation errors that were not discovered during code reviews, unit tests, or security white box tests, discover security issues resulting from boundary conditions not identified during the design and implementation phases, uncover software security issues resulting from incorrect product builds, or the interaction with the underlying environment and verify that software security components and security-specific sub-systems are operating properly. Security is always relative to the information and services being protected, the skills and resources of adversaries, and the costs of potential assurance remedies; security is an exercise in risk management. Risk analysis, especially at the design level, can help us identify potential security problems and their impact. Once ranked and identified, software risks can then help guide software security testing. Security testing must necessarily involve two diverse approaches: Security testing involves determining who should do it and what activities they should undertake. Testing security mechanisms to ensure that their functionality is properly implemented and performing risk-based security testing motivated by understanding and simulating the attacker’s approach.

* 1. BACKGROUND

The new technologies of today’s dynamic digital world, such as cloud computing, IOT, and the interconnected supply chain, bring a new level of uncertainty, but also new possibilities. Securing proprietary information and other critical business assets becomes exponentially more difficult and meeting regulatory requirements more complex. Deloitte’s Secure services help organizations drive productivity, business growth, and cost-optimization while establishing effective controls around sensitive assets. In an era where cyber is everywhere, it’s possible to invest in cybersecurity controls and preventive measures to ensure you can take your business anywhere. The services offered by Deloitte are:

* **Infrastructure protection** – We address potential infrastructure vulnerabilities by improving network strategy and implementation, cloud security, and instituting anti-DDoS Attack protection.
* **Vulnerability management** – We identify and manage potential security risks through rigorous testing and the use of cutting-edge vulnerability management tools.
* **Application protection** – We keep key applications protected and up-to-date through routine testing and management, including enterprise application security, source code review, and source by design: secure SDLC protocols.
* **Identity and access management (IAM)** – We establish protocols that only allow authorized users and customers to access an organization’s infrastructure and data. I solutions help enhance the security of online transactions while minimizing friction in the user experience.
* **Information privacy and protection** – We help clients keep valuable personal, user, and customer data private by adopting industry-leading holistic and integrated data solutions. We also help prevent unauthorized access to confidential corporate, user, and customer data to avoid expensive legal, financial, reputation, and regulatory issues.

1. **PROJECT DESCRIPTION AND GOALS**

The project Vigilant Shield works on the security testing of the Deloitte’s internal applications. The web application security testing includes front-end testing and back-end testing. For front-end testing we use Dynamic Application Security Testing(DAST) and for back-end we use Static Application Security Testing(SAST).

Static Application Security Testing, shortened as SAST and referred to as White-Box Testing, is a type of security testing which analyzes an applications source code to determine if security vulnerabilities exist. SAST solutions looks at the application ‘from the inside-out’, without needing to compile the code. Gartner states that “SAST should be a mandatory requirement for all organizations developing applications,” and with 80% of attacks aimed at the application layer, according to Gartner, SAST is one of the top ways to ensure your application security is sound. The back-end code is scanned using the tool. The tool then finds the possible vulnerabilities and then categorize them into for main groups, critical, high, medium and low. The critical category consists of vulnerabilities like XXS (Cross-Site Scripting), Open redirect, JSON Injection, etc., the high category consists of vulnerabilities like Access Control, Null Dereference, SSRF (Server-Site Request Forgery), Header Manipulation, etc., the medium category consists of vulnerabilities like Misused File Upload, MIME Sniffing, etc. and the low category consists of vulnerabilities like Code Correctness, Cookie Security, DOS (Denial of Services), Dead Code, Poor Logging etc.. The analyst has to review the marked line of code and verify whether there is a vulnerability or not. The analyst can view the vulnerabilities grouped by category, file name, kingdom, source, analysis type etc.. After verifying the line of code, the analyst has to do the analysis and mark it as not an issue, suspicious, bad practice, exploitable etc. and then the analyst has to post a comment which will be reviewed by the developer. These tags can be modified according to the application code and the requirement of the project. Once the analysis of all the suspected vulnerabilities is done a report is generated.

A Dynamic Application Security Testing (DAST) tool is a program which communicates with a web application through the web front-end to identify potential security vulnerabilities in the web application and architectural weaknesses. It performs a [black-box](https://en.wikipedia.org/wiki/Black-box) test. Unlike [Static Application Security Testing](https://en.wikipedia.org/w/index.php?title=Static_Application_Security_Testing&action=edit&redlink=1) tools, DAST tools do not have access to the source code and therefore detect [vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computing)) by actually performing attacks. DAST tools allow sophisticated scans, detecting vulnerabilities with minimal user interactions once configured with host name, crawling parameters and authentication credentials. These tools will attempt to detect vulnerabilities in query strings, headers, fragments, verbs (GET/POST/PUT) and DOM injection. DAST tools facilitate the automated review of a web application with the expressed purpose of discovering security vulnerabilities and are required to comply with various regulatory requirements. Web application scanners can look for a wide variety of vulnerabilities, such as input/output validation: (e.g. [cross-site scripting](https://en.wikipedia.org/wiki/Cross-site_scripting) and [SQL injection](https://en.wikipedia.org/wiki/SQL_injection)), specific application problems and server configuration mistakes.

The goal of the application is to remove probable vulnerabilities and to secure the internal web applications from potential cyber-attacks. Web application security is a branch of [information security](https://en.wikipedia.org/wiki/Information_security) that deals specifically with security of [websites](https://en.wikipedia.org/wiki/Website), [web applications](https://en.wikipedia.org/wiki/Web_application) and [web services](https://en.wikipedia.org/wiki/Web_service). At a high level, web application security draws on the principles of [application security](https://en.wikipedia.org/wiki/Application_security) but applies them specifically to [internet](https://en.wikipedia.org/wiki/Internet) and [web](https://en.wikipedia.org/wiki/World_Wide_Web) systems. We need to secure web applications because attackers are exploiting web application security vulnerabilities to gain access to private data, organizations must go to even greater lengths to protect websites and apps than they do to protect their computers and other network-connected devices.

1. **TECHNICAL SPECIFICATIONS**

The tools used for DAST and SAST

1. **SCHEDULE, TASKS AND MILESTONES**

# References

1. Sergiy Fefilatyev, “Algorithms for Visual Maritime Surveillance with Rapidly Moving Camera”, Doctoral dissertation, University of South Florida, 2012.
2. Domenico Bloisi, Luca Iocchi, Michele Fiorini, Giovanni Graziano, “Automatic Maritime Surveillance with Visual Target Detection”, International Defense and Homeland Security Simulation Workshop (DHSS), September 2011.
3. Domenico Bloisi, Luca Iocchi, Michele Fiorini, Giovanni Graziano, “Camera Based Target Recognition for Maritime Awareness”, Information Fusion (FUSION), 15th International Conference, July 2012.

[4]. Rodrigo Da Silva Moreira, Nelson Francisco Favilla Ebecken, Alexandre Soares Alves, Frédéric Livernet4, Aline Campillo-Navetti, “A Survey on Video Detection and Tracking of Maritime Vessels”, IJRRAS 20, July 2014.

1. Digi-key Corporation. <http://www.digikey.com/>
2. Alldatasheet. <http://www.alldatasheet.com/>