Software Application Security Test Strategy with Lean Canvas Design

Padmaraj Nidagundi
Riga Technical University
Faculty of Computer science and Information technology
Riga, Latvia.
padmaraj.nidagundi@gmail.com

Marina Uhanova
Riga Technical University
Faculty of Computer science and Information technology
Riga, Latvia.
marina.uhanova@rtu.lv

***Abstract*— Software security play key role to keep software application user's personal information safe from the hackers who breach defenses of the software and exploit weaknesses in it. In software development, most of the time companies give less priority for security while developing the software because of lack of skilled professional or less budget and time constraints. The software security testing main goal is to identify the all possible loopholes and weakness in the system before it starts using by the end customers. It is important to consider the security testing in each phase of the systems development life cycle (SDLC) and it needs to cover the confidentiality, integrity, authentication, availability, authorization and non-repudiation of the system. The making software error free with security issues, software test engineer need to have an effective strategy to mitigate security risks. This paper emphasizes on the possibilities of lean canvas design for the security test strategy building in the software testing process.**

Keywords*— *security testing, security test strategy, lean canvas for security testing, software testing, test strategy

I. INTRODUCTION

The growth of technology increases the Internet of things (IoT), cloud, web software products complexity and increased the possible threats to attackers from different endpoints with the system. Every year small to reputed companies also faces many type software security issues and these incidents directly impacted on the business, brand reputation and customer trust on the software products. In recent years' companies are started spending more time, resources and money to make security testing as the number one Information technology (IT) priority [1]. In the software security testing, different types of security test need to be done before application reach to the intended end user, such as vulnerability scanning, security scanning, penetration testing, risk assessment, security auditing, ethical hacking, posture assessment.

Software security testing considered as a non-functional testing, in this process software tester test the application and make sure it is secured or not with different possible attacks [5]. In this process, tester determines the data protection, leakage of sensitive data with developed software for intended hardware. Every year Open web application security project (OWASP) doing possible research in the wide range and releasing the possible risks with the software products. In last few years' lean canvas design is used for the building the strategy for the number of different companies, this research article focus on the developing the prototype and its possible utilization for the software security testing [2].

II. THE PROBLEM STATEMENT

In software security testing quality assurance [10], [13] team faces many challenges.

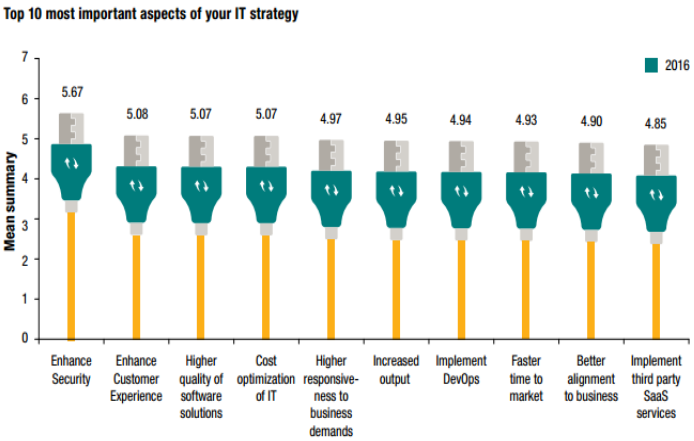

Fig. 1. Security testing is a key of IT strategy [13].

- Lack in developing security testing strategy in each phase of SDLC.
- Not start security testing at the early stage of software development.
- Not having the well-trained security tester in a team.
- Not having appropriate security test tools for custom developed software.
- Lack in building the security test planning and test data.

III. ANALYSIS OF SOFTWARE SECURITY TESTING IN SDLC AND LEAN CANVAS DESIGN

In recent research by Harvard business school's, 75% of all start-ups fail survey done by the Shikhar Ghosh and noticeable most of the start-ups are focused on the software as their

product. But rest 25% start-up companies are successful because of the adaptation of the lean principles [9]. In recent years, lean canvas design is adopted by the companies to build the strategy with the product, services, describe, design, challenge, and pivot the business model. It is a one-page lightweight document with blocks and appropriate title.

Lean canvas is a tool to validate the ideas with more creativity, experimentation [6]. Considering the lean canvas as a base model our research for software security testing will help us to address the many security test strategy and planning.

- Identify and design the more appropriate lean canvas design prototype for security testing.
- Simplify the software security test strategy with SDLC.
- Undertaking the lean principles for the design of the software security testing compatible lean canvas.
- Identify and design software security testing metrics and blocks on the lean board.

A. *Waterfall VS Agile approach*

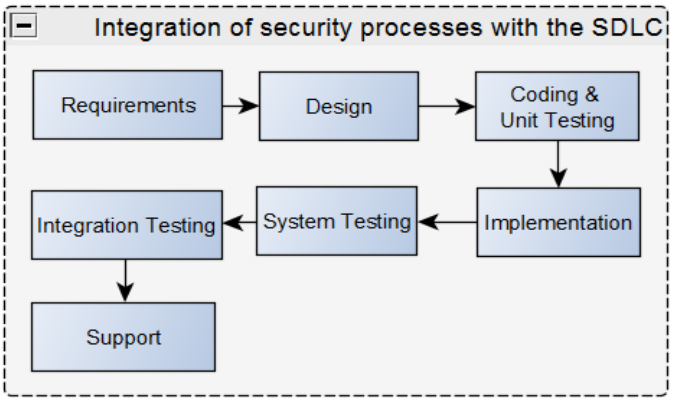

Fig. 2. Waterfall development security testing in SDLC.

Table. 1. Waterfall security tests in SDLC.

Waterfall Phases	Security Tests
Requirements	Detailed security analysis of the abuse and misuse test cases.
Design	Design risk analysis with the system.
Coding and Unit Testing	Identity, Authentication & Access Control, Encryption, Input Validation & Encoding, User and Session Management, Error and Exception Handling and Auditing and Logging.
Integration Testing	Black box system testing.
System Testing	SQL injection vulnerabilities - White box system testing
Implementation	Vulnerability Scan & Penetration Test
Support	Software patches & updates, its impact analysis

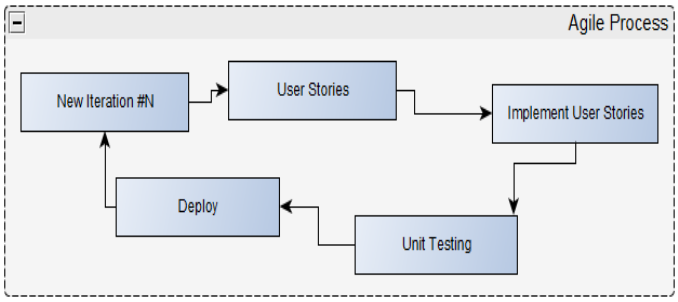

Fig. 3. Agile process flow overview.

Table. 2. Agile security testing.

Agile Phases	Security Tests
New Iteration #N	Gather security requirements
User Stories	Security architecture review
Implement User Stories	Security code review
Unit Testing	Application vulnerability testing
Deploy	External application security testing

B. *Related research*

The first time Alex Osterwalder and his co-author introduced business model canvas in the year 2000. Onward it started used by the number of startups to big companies to manage the strategy. The business model canvas shows the possible predefined blocks; those help to define the problem and possible solution using the different channel blocks showed on the one-page document. It helps make a clearer strategy for the business problem. Lean canvas life cycle starts with the ideas, build, product, measure, data, learn and each of the gives valuable feedback continuously to next stage.

IV. LEAN CANVAS DESIGN ADAPTION INVESTIGATION IN THE SECURITY TEST

In recent years, agile based software development is growing with a number of projects it created new opportunity and challenges for the software based product and it impacted on the software security testing as well. Agile development focus on the adaptive planning, early delivery, and constant improvement [12]. In again development. Agile development needs to start with risk analysis and it brings the new requirements.

- It focuses on the more request product release.
- A number of dynamic features changes.
- Increasing business level risk when product backlogs changes.
- Technical risk with each new sprint.
- Validations risk with every code check in and product release.

In such situation, effective security test strategy will help to tackle the situation and there is no slandered strategy approach has been investigated that fit in agile to overcome security testing issues.

C. *Approaching lean canvas design for security testing strategy.*

Description: Software security testing is essential in each stage of software development, in such situation test strategy play key role to improve the software security in each stage [5], [7]. According to OWASP 2017 there are a number of possible threats injection, broken authentication and session management, Cross-site Scripting (XSS), broken access control, security misconfiguration, sensitive data exposure, insufficient attack protection, cross-site request forgery (CSRF), using components with known vulnerabilities and under protected application programming interface (API).

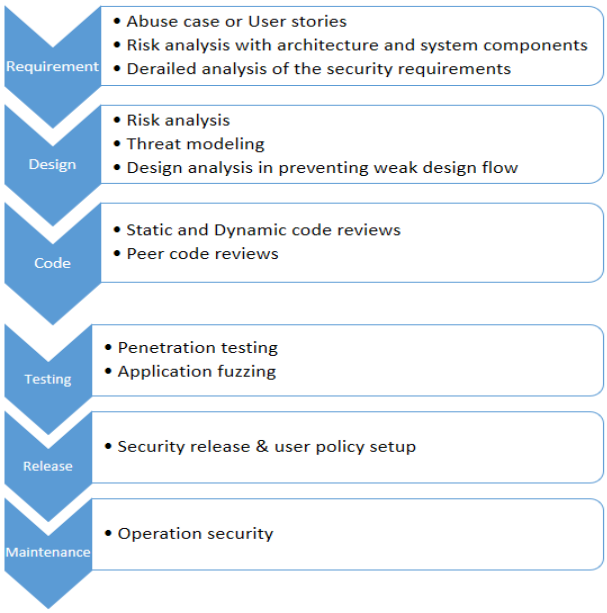

Fig. 4. Overview on security testing architecture.

Prerequisites: What type of security test need to be done with application and knowledge about security test tools to be used with the application [3]. According to the pentest-standard need to consider in the test execution pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post exploitation and reporting.
Complexity: Each application is unique and each code or user story can bring new challenges to test engineer with technology and technical point of view.
Pro: Lean canvas will help to set a proper strategy with each user story or developed code.
Con: It will bring the limitation with in-depth analysis report visualizing on the single page, to overcome we need to use external hyperlinks from the board.
Recommendation: With changing the scope of the software application lean canvas design need to redesigned with a new title for the existing blocks with descriptions.

Example: Consider a web application testing with the reconnaissance, configuration management, authentication testing, session management, authorization testing, data input validation, denial-of-service (optional) and web / API services testing need to be done [8]. In such situation, we can visualize the all possible test strategy one single page.

D. *Discover of the security test metrics for lean canvas board*

Considering the lean principles, we will identify the more proper roadmap for the design of the lean canvas.

- Transport – Security test needs to wait until full code or software module is ready.
- Inventory – Not fully developed code or module according to business re-equipment not able consider for the testing.
- Motion – Once part of code or module is already tested then we can consider it re-testing only with the full system.
- Waiting – Some time security test is interrelated to each other in such situation it need to pre-planned for the scope.
- Overproduction – It does not bring any value some time testing component or code that not fulfill the business requirement.
- Over processing – Poor system architecture or selection of wrong security test tools will consume more time.
- Defects – Identified security weakness of the system or code, need to be fixed and such issues need to be retested.

Considering the lean principle for the lean canvas design we extract several blocks & test metrics and these we can use to visualize the board. It is continuing process of finding the correct metrics with the scope of the project.

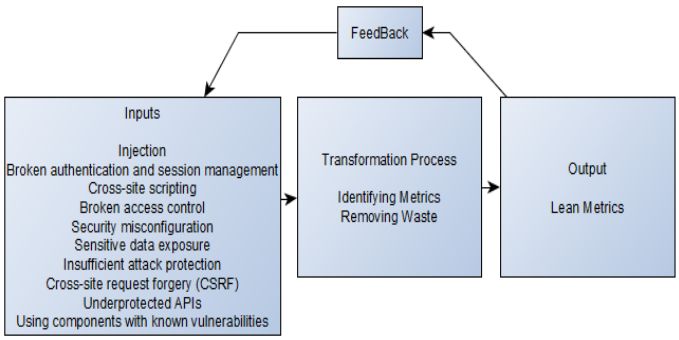

Fig. 5. Overview on security testing lean metrics finding.

E. *Approaching lean canvas prototype design for software security testing*

Considering section 2 and 3 various input and possibilities we draw a prototype lean canvas board with several sections and related text fields on the single page [11].

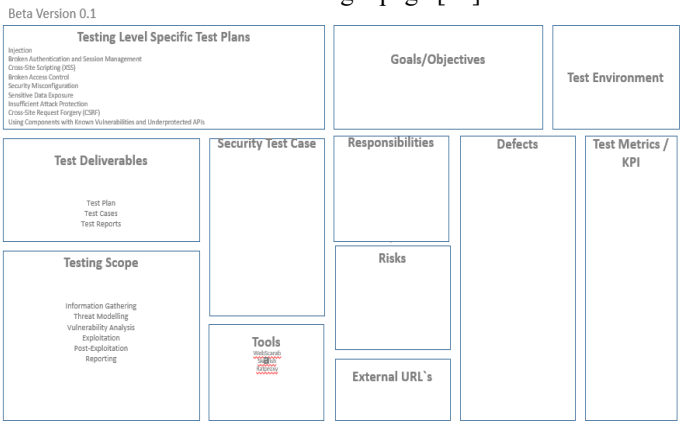

Fig. 6. Prototype design for building the security testing strategy.

V. LEAN CANVAS DESIGN ADAPTION INVESTIGATION IN THE SECURITY TEST

The study explains the new possibilities for usage of the visualized lean canvas in the software security testing purpose this single page template can impact on the security testing plan and security test strategy and simplify the software test process. Also, help to build the secured software product to the end customers.

To extend the prototype lean canvas design for the software security testing, it is necessary to carry out the following research activities to gather more information.

- Need to carry out a detailed experiment in the software security testing process for identifying the lean metrics.
- Need to carry out a detailed experiment to how lean canvas design best fit for security testing.
- Identified & collected list existing security standards and evaluate for the lean canvas design.
- Investigate possibilities more appropriate design for the security testing using lean canvas visualization.
- Need to develop algorithms to developing and optimize the lean metrics.
- Need to develop an intelligent software that gathers information from input and design a more appropriate lean canvas design.
- Investigation needed about machine learning possibilities to lean canvas design generation.

The author wish is to increase the adoption on lean canvas design in test process to improve the software security testing strategy to simplify the complex process and long documentation. Improving software testing strategy process is continues ongoing research. The author wishes this paper will generate more ideas, new aspect on prototypes design and experiment on creating software test strategy using lean canvas design.

REFERENCES

[1] T. Nakajima H. Ishikawa E. Tokunaga F. Stajano, “Technology challenges for building Internet-scale ubiquitous computing”.

[2] Yang S, Liao C, “A study of critical success factors on software quality assurance of cloud networking devices”, 3rd International Conference on Systems and Informatics (ICSAI), 2016.

[3] Omotunde H, Ibrahim R, “A Hybrid Threat Model for Software Security Requirement Specification”, International Conference on Information Science and Security (ICISS), 2016 pp 1-4.

[4] Wotawa F, “On the Automation of Security Testing”, International Conference on Information Science and Security (ICISS), 2016 pp 11-16.

[5] Jain M, Gopalani D, “Testing application security with aspects”, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) 2016, pp 3161-3165.

[6] Jiménez R, “Pentesting on web applications using ethical – hacking”, IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI), 2016, pp 1-6.

[7] Vibhandik R, Bose A, “Vulnerability assessment of web applications - a testing approach”, Forth International Conference on e-Technologies and Networks for Development (ICeND) 2015, pp 1-6.

[8] Steven J, “Threat Modeling - Perhaps It's Time”, IEEE Security & Privacy, 2010, Volume 8, Issue 3, pp 83-86.

[9]] X. Wang, “The Combination of Agile and Lean in Software Development: An Experience Report Analysis”, Agile Conference (AGILE), 2011, pp. 1–9.

[10] D. G. Rex Black, Erik Van Veenendaal, Foundations of software testing: ISTQB certification, 3rd Edition. *Cengage Learning EMEA*, 2012.

[11] Nidagundi P, Novickis L, “New method for mobile application testing using lean canvas to improving the test strategy”, Computer Sciences and Information Technologies (CSIT) 2017, pp 171-174.

[12] M. Ide, Y. Amagai, M. Aoyama, Y. Kikushima, “A Lean Design Methodology for Business Models and Its Application to IoT Business Model Development,” in Agile Conference, AGILE, 2015, pp. 107–111.

[13] World Quality Report 2016—2017, Capgemini, Sogeti, and HP, 2017.