COMBINING REUSABLE TEST CASES AND CONTINUOUS SECURITY TESTING FOR REDUCING WEB APPS SECURITY RISKS

Sen-Tarng Lai

Dept. of Information Technology and Management, Shih Chien University,
Taipei, 104, Taiwan

ABSTRACT

In network communication age, information technology is being at the continuous and rapid evolution process. Network access equipment, information system and Web Apps must rapidly and continuously update to meet the user interested requirements. Major challenge of Web Apps frequent changes is the security of user personal data and transactions information. Vulnerability scanning and penetration testing are the routine methods to improve the security of Web App. However, these two ways not only time-consuming, but also require too many resources. For coping the continuous changes, in the limited resources, security testing not only need to be timely completed, but also should concern testing quality. Otherwise, every change maintenance cannot avoid to cause the security risk of new version App. Based on reusable test cases, this paper proposes the continuous security testing procedure (CSTP), using test cases reusability to increase security test efficiency. In Web Apps maintenance process of limited resources, CSTP can timely handle security testing and quickly identify Web Apps vulnerabilities and defects. Assisting Apps maintainer effectively repair security defects and concretely improve the security of user personal data and transaction information.

KEYWORDS

Security test cases, continuous security testing, Web App, security risk, personal data

1. INTRODUCTION

Information Communication Technology (ICT) era, in order to obtain a competitive advantage in the fierce market, enterprises and organizations must fully take advantages of information technology, communications equipment and Web Apps. In addition, with the ICT evolution, Web Apps must ready for multiple user requirements, quick requirements change and adjustment to increase the subscriber numbers and market occupation. Mobile and e-commerce applications (Web Apps) are the important platform of enterprises and organizations for business activities and transaction, also are the critical product of information network business operations. However, frequent changes in Web Apps may cause security defects. Once important personal data or confidential information was leaked or stolen that certainly will impact the user's personal lives and normal operations of the organization and society [1], [2]. Taiwan Industrial Development Bureau Director, Wu pointed out that the "Apps of information security will be divided into low, middle and high three grades." Industrial Development Bureau in accordance with international standards set out an independent security authentication mechanism, involving consumer and other online shopping and financial transaction services through advanced certification. Web Apps are the important tool to enhance business efficiency. However, for the frequent changes Web App, how to enhance the Apps security becomes a critical issue. Enhancement Apps security improve the business operating environment has become worthy of discussion topics.

DOI : 10.5121/ijsea.2016.7606

E-commerce has the advantage of network, customers can quickly complete transaction activities, significantly enhance the efficiency of enterprises conduct business and trading activities [3]. But it also implies the Apps necessary to concern the security risks for the transaction activities. So the development of commerce Web App, in addition to focus on functionality and basic quality, but also pay attention to the efficiency of implementation, network security, and the ability to handle adjustment and moving targets problems [4], [5]. In the beginning of Apps development, introducing into the security requirements and security software development approach can enhance concrete implementation of Web Apps security [6, 7, 8]. Penetration testing and vulnerability scanning are two routine methods to improve the security of Web App. Penetration testing is a formal security vulnerabilities and defects detection operation carried out network operation security from hacker detection angle range beyond viewing Web Apps Security [9]. Penetration testing is generally commissioned and executed by the professionals. Vulnerability Scanning is the internal security weaknesses and defects detection job, you can perform maintenance personnel by the Web App, at least half year should be performed once, the use of vulnerability scanning tools to assist in identifying security vulnerabilities and defects of Web App. Then follow up by the maintenance personnel to repair the security vulnerabilities and defects. However, in changes maintenance jobs, Web Apps security testing belonging to non-routine test. Based on the maintenance request, security test must be continuously taken to effectively control Web Apps security.

In the ongoing evolution of the environment and technology, Web Apps must have a height adjustable and scalable features to enhance companies and organizations business competitive advantage. However, general Web Apps during maintenance, often encounter several challenges: (1) Need to complete the tasks in specified time to ensure that enterprises and organizations to retain competitive advantage. (2) In limited human resources to complete the high-quality features extension and adjustment. (3) Complete functional modules and security testing for the new version App. Frequent changes and limited maintenance resources cause that Web Apps maintenance activities often overlook the test tasks, especially the key security tests. Every time of Web Apps changes, maintenance activities increase the security risk. This paper discusses the frequent changes that cause Web Apps to face the security crisis under limited resources, and investigates the importance and reusable potential of test cases. Based on the reusable test cases, this paper designs the Continuous Security Testing Procedure (CSTP) to reduce the Apps security risk of frequent changes and limited resources. In Section II, discuss the challenges and security risks of Web Apps frequent changes. In Section III, dissect how to overcome the challenges of Web Apps security risks and discuss the importance of the continuous security testing. For reducing the security risk of changes Apps, in Section IV, based on the reusable test cases, the Continuous Security Testing Procedure (CSTP) is designed. In Section V, concretely evaluate the advantages of CSTP for reducing Web Apps security risks. In Section VI, stresses the importance of Web Apps continuous security testing and make a conclusion for this topic.

2. WEB APPS MAINTENANCE OPERATIONS AND SECURITY ISSUES

Internet and information age has changed the way of business activity and transaction behaviour. Web Apps brings many competitive advantages for enterprises and organizations, but also implies the security issues.

2.1. Challenges of Web Apps Maintenance Operations

Web Apps are the efficient instrument to enhance market competitiveness of enterprises and organizations. Therefore, in order to attract the more customers and extend the market business operations, Web Apps must able to meet the pluralism requirements of users, and has rapidly change and extension characteristics for overcoming the ICT continuous evolution. Web Apps

should value software maintainability to handle continuous change requests. Software systems pass through acceptance testing, transfer, and install to users operation environment, then software enter delivery maintenance phase. According to the maintenance request, the job properties of software maintenance can be divided into four types [10, 11, 12]:

(1) Corrective maintenance: In Apps using process, the users found that some features or user manual specification does not match the user requirements. Base on the content of requirement specifications, users can request maintenance units for corrective maintenance.

(2) Perfective maintenance: Environmental evolution or change requirements make software users require the more new features or adjust and extend existing functionality. According to the provisions of the contract, the users can request maintenance units for perfective maintenance.

(3) Adaptive maintenance: Software system used for a period of time or be affected by the external environment. Software systems need changes the software operating platform or hardware devices to meet the actual needs of the market. According to the provisions of the contract, the users can request maintenance units for adaptive maintenance.

(4) Preventive maintenance: Software system needs for regular maintenance and repairs the facilities, and timely elimination or update old equipment hardware and software to enhance the reliability of the software system operating environment. Combining the units partners to develop preventive maintenance contracts, in order to enhance reliability of enterprises or organizations and user trust.

For the released software system, in the early phase, corrective maintenance request has high proportions. When the system enter stabilized status, software maintenance work will be transferred to perfective maintenance. Web Apps with frequent changes and extensions should belong to the perfective maintenance type, the maintenance change process must often endure several challenges (as shown in Figure 1):

- Timeliness of change completion: Web Apps challenge is that each revision version must be promptly completed within the stipulated time. New version Apps timely assist the enterprises or organizations to promote new business or service activities for taking the advantage of market competition.

- Change affected functional quality: Web Apps revision process not only care completion timeliness, but also pay attention to the key product quality, especially functional correctness, completeness, consistency and friendly user interface after system integration. Perfect functional quality can attract more users using willingness and successfully promote the new business services and transaction manner.

- Change affected security quality: Each maintenance process and quality requirements need to invest many resources. Complicate maintenance jobs often have not enough human resources to cope with the requirements for security quality. Therefore, security testing is often ignored by the maintenance process, making frequent changes of Web Apps existing the high security risk.

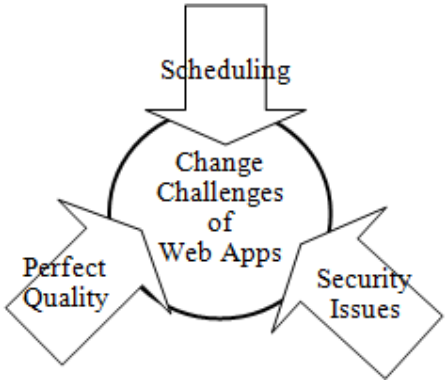

Figure 1. Three change affected factors of Web App

2.2. Web Apps Security Risks

Web Apps is a very critical tool in E-commerce. Continuous evolution of E-commerce operation environment forcing Web Apps should have high flexibility to accept the challenges of change requirements and additional services. In order to overcome the challenges, Web Apps need to be continuously adjusted and extended. However, frequent changes bring many risks, the most noteworthy of which is security risk. E-commerce system must meet the privacy, integrity, non-repudiation, and confirmatory etc. four items of indivisible security requirements [13]. These security requirements must be implanted into Web Apps in development process timely. However, each time Apps change may threat the four security requirements to become a security risk of business activities. Web Apps with high security characteristics is the enterprise must pay attention to and strengthen the key project. It is because of Web Apps security vulnerabilities may cause the great loss and impact of enterprises. Therefore, Web Apps must maintain four important security requirements (as shown in Figure 2). Based on Web Apps security risks, the following discusses how to manage and control four security items:

- Data confidentiality: user personal data and transaction information have a high degree of trade secret that must limit authority of Web Apps for access or reference. Confidential information must be strictly protected, does not allow any security holes to cause the hacker through the intrusion or steal the way to get the stakeholders confidential information. Web Apps of business or organization must enhance the security of confidential information.

- Data accuracy and timeliness: Business activities provided by Web Apps often involve many important data and transaction information. The data accuracy and timeliness is a necessary condition to ensure the normal operation of commercial activities. Therefore, Web Apps must have security features of data accuracy and timeliness.

- System operation stability and efficiency: Web Apps connection with various business activities must have a high stability and efficiency operating environment. Excluding the impact caused by the hardware facilities, Web Apps need to strengthen the security measures to enhance the high stability and efficiency of the business operation environment.

- Transactions non-repudiation: Web Apps must have a clear, complete and accurate record for any transaction of application activities. The record writes down the behavior of both parties

to confirm the transaction has completed, either party must recognize the validity of this trading activity, reach normal trading behavior of non-repudiation.

In order to enhance Web Apps security, the requirement workflow of Web Apps need to submit a set of security requirements to protect the privacy security of user personal data and transactions activities. In Web Apps development and maintain process, each level security testing must follow the security specifications to identify the security vulnerabilities and flaws. For the working Web Apps, periodic vulnerability scanning and penetration testing are two important approaches that detect the security vulnerabilities and flaws and avoid security risks continuous extension.

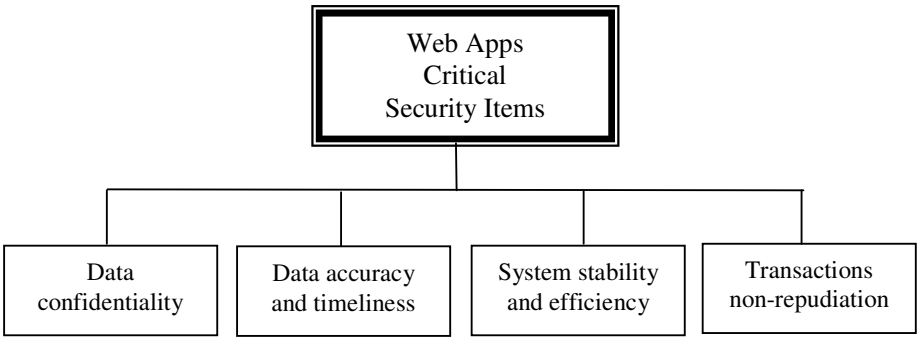

Figure 2. Critical security items of Web App

3. SECURITY TEST OF WEB APP

Web Apps involving many users' personal data and transaction information, the major challenge of Web Apps is how to effectively ensure information security.

3.1. Importance of continuous security testing

In the maintenance phase, software system must accept the various maintenance requests (MR) and accomplish corrections, modifications, expansion and adaption tasks to meet the user new requirements and the environment evolution [10]. The complete and effective testing is critical jobs for each MR to determine quality of maintenance work items have been reached. However, maintain jobs often changes the content which should not be changed, resulting in the phenomenon of regression faults. In order to avoid the regression faults caused the negative impact of maintain jobs, maintenance tasks must through repeat regression testing to ensure regression faults can be excluded [11, 14, 15].

General MR always focus on the functional change requirements. Therefore, most of maintenance jobs only focus on the functional testing and ignore the importance of security testing. The more MR are submitted the more security regression test are ignored again when complete each MR. Finally, software systems security risks continue to rise with the MR. Lacking security testing, software system had high functional integrity but embedded high security risk with security flaws. Security testing belongs to the security precautions of software development and maintenance, any correction, modifications, expansion and adaption jobs cannot ignore the security testing. After maintenance operations should timely complete security testing to ensure doesn't security defects of the maintenance job to effectively prevent or reduce the significant losses of security vulnerabilities or defects. Four type MR may impact the Web Apps security as follows description:

- Maintenance items relates to the data confidentiality: after completion of the relevant modification jobs, the security testing for data confidentiality need to be conducted. Based on the affected items, some STCs of data confidentiality must be added or modified to conduct the security testing and ensure security quality of data confidentiality. In addition, for removing the regression faults of the maintenance jobs, regression testing should use the existing STCs to automatically test the security requirement of data confidentiality.

- Maintenance operations involving data accuracy and timeliness: after completion of the relevant modification jobs, the security testing for data accuracy and timeliness need to be conducted. Based on the affected items, some STCs of data accuracy and timeliness must be added or modified to conduct the security testing and ensure security quality of data accuracy and timeliness. In addition, for removing the regression faults of the maintenance jobs, regression testing should use the existing STCs to automatically test the security requirement of data accuracy and timeliness.

- Maintenance items relate to the system stability and efficiency: after completion of the relevant modification jobs, the security testing for system stability and efficiency need to be conducted. Based on the affected items, some STCs of system stability and efficiency must be added or modified to conduct the security testing and ensure security quality of system stability and efficiency. In addition, for removing the regression faults of the maintenance jobs, regression testing should use the existing STCs to automatically test the security requirement of system stability and efficiency.

- Maintenance items involve non-repudiation of transactions: after completion of the relevant modification jobs, the security testing for non-repudiation of transactions need to be conducted. Based on the affected items, some STCs of non-repudiation of transactions must be added or modified to conduct the security testing and ensure security quality of maintenance jobs. In addition, for removing the regression faults of the maintenance jobs, regression testing should use the existing STCs to automatically test the security requirement of non-repudiation of transactions.

3.2. Major tasks of continuous security testing

Web Apps frequent changes is an unavoidable problem. In additional, each MR of Web Apps has its timeliness. Maintenance tasks must be completed within the limited time, resources and norms to meet the specific requirements of the users and to keep enterprises or organizations market competitive advantages. Therefore, continuous security testing should have a high efficiency testing procedure and environment for timely completing the important security testing with limited resources [10]. In order to enhance the efficiency and quality of security testing, this paper divides Web Apps security testing jobs into five work items (as shown in Figure 3):

- STCs (Security Test Cases) management: STCs are the core items of Web Apps continuous security testing. Appropriate management each level test STCs can significantly enhance the efficiency of continuous security testing in maintenance activities.

- Maintenance job analysis: Based on the MR of Web Apps, the maintainers need to concretely analyse and plan maintenance tasks for smoothly completing the maintenance mission. Clearly identifying the affected items of Web Apps, the maintainers proceed to parse the effected security items of Web Apps. Then the modified source codes are tested according to new added and adjusted STCs, and proceed the complete regression security testing to reduce the security risks of maintenance activities.

Increase STCs: When the maintenance requirements are add new functions or extension operations, existing STCs may not achieve complete testing. Adjustment or maintenance jobs should add new STCs or adjust existing STCs for continuous security testing, and proceed the complete regression security testing to ensure the security of maintenance activities.

- Automated security testing: Before maintenance, most of the test cases have been completed security testing and delivered to CM (configuration Management) management. These test cases can be combined with testing tools, to achieve automated security testing can improve the plight of insufficient resource.
- Security testing evaluation and improvement: Before the new version release, maintenance jobs need to evaluate the affected security items of Web App. Collecting the security testing results of maintenance activities to assess test completeness, correctness and defects for subsequent adjustment and improvement reference.

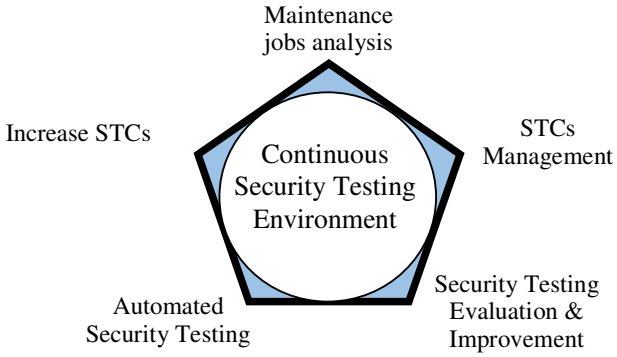

Figure 3. Major tasks of continuous security testing

3.3 Important items of STCs

In order to increase test cases reusability, STCs should have management, retrieval, adjustment, modification capabilities, and suitable for automated regression testing. Important items of test cases should include identifier, designer, create date, test objective, test level, for security items, test script, test data, and expected results [16]. Test data, expected results and test script are three critical items for automated regression testing. For this, Test script should be collected and completely recorded at first time manual testing. Combining the complete test data, expected results with test script can make the automatic regression testing. Major items of STCs describe as follows:

(1) Test case id: test case with unitary and clear identifier can increase test cases manageability.
(2) Test case designer: designer of test case can assist to maintain the test cases.
(3) Created date: creation date of test case can trace back the lift cycle of test cases.
(4) Test objective: based on the design specification, test case designer clearly describes the purpose of this test cases for detecting the errors or defects.
(5) Security item: This item is the very important for the regression testing. Designer need clearly specify the security requirement or one of four security items which to be tested.
(6) Testing level (unit, integration, system or acceptance testing): Define the testing level of this test cases.
(7) Test data: Based on the design specification, test data and test script for each level testing should be indeed generated. Test data is critical item for detecting undiscovered errors and

defects. Combining the complete test data, expected results with test script can make the automatic regression testing.

(8) Test script: In software testing, the test script is a set of instructions that will be performed on the system under test to test that the system functions as expected [16].

(9) Expected results: Based on the design specification, the expected results and test script for each level testing should be indeed generated. Expected result is critical item for detecting undiscovered errors and defects.

4. OPERATION ENVIRONMENT OF CONTINUOUS SECURITY TESTING

For reducing the security risk of changes Apps, in Section IV, based on the reusable STCs, the CSTP is designed.

4.1. Continuous security testing operation environment

Lacking of maintenance resources, frequent changes of Web Apps often ignore the security testing of maintenance activities. Insufficient security testing makes Web Apps security risks continue to rise and impacts the user personal data and transaction information privacy security. In order to enhance Web Apps attention on security testing, the security testing environment should be specific improve continuous security testing efficiency [15]. For this, continuous security testing environment must be combined with the security testing assistant tools and reusable STCs to reduce human involvement and improve the efficiency of maintenance jobs. In this paper, the security testing operations environment (as shown in Figure 4) is divided into four parts, and are described as follows:

- STCs control and management tools: Security testing is a key to ensure the security quality of Web App. Web Apps passed the complete security testing, then Web Apps can be releases and deployed for using. In Apps development process, the STCs through careful plan and design are important reusable assets. It is necessary use the proper version control and management tools to manage and maintain the STCs to assist Web Apps automated security regression testing.
- Analysis tools of affected security items: developing a judgment rule, help analysing tools to analyse the processing job of each maintenance request. Based on maintenance request, the analysing tools can identify the affected security items of Web Apps maintenance. For completely testing the affected security items, before entering security testing, STCs should be planned, designed or adjusted. And, security testing cases need to submit to management tools for managing and controlling to help efficiently execute Apps security testing in maintenance operations.
- Automated security regression testing tools: the preserved and managed STCs is divided into test data and Expected Results two parts. For the automated testing tools, test data can automatic input and the expected test results can be automatic compare to judge the security testing jobs. In continuous security testing activities, automated security testing tools significantly reduce the intervention of human resources, particularly to enhance the efficiency and quality of security testing operations
- Security testing assessment tools: Combining the data generated from the automated security testing tools, this tool collects and integrates the relevant information of security testing activities, automatically generates testing reports for each security testing and assess the security testing completeness and imperfect defects [17].

4.2. Continuous security testing procedure

Continuous security testing not only need a complete testing operations environment, but also need a perfect operating procedure for assisting the maintenance personnel to proceed security testing.

Based on STCs, the paper integrates the software development tools to design a continuous security testing procedure (CSTP). CSTP divided into four stage (as shown in Figure 4) describes as follows:

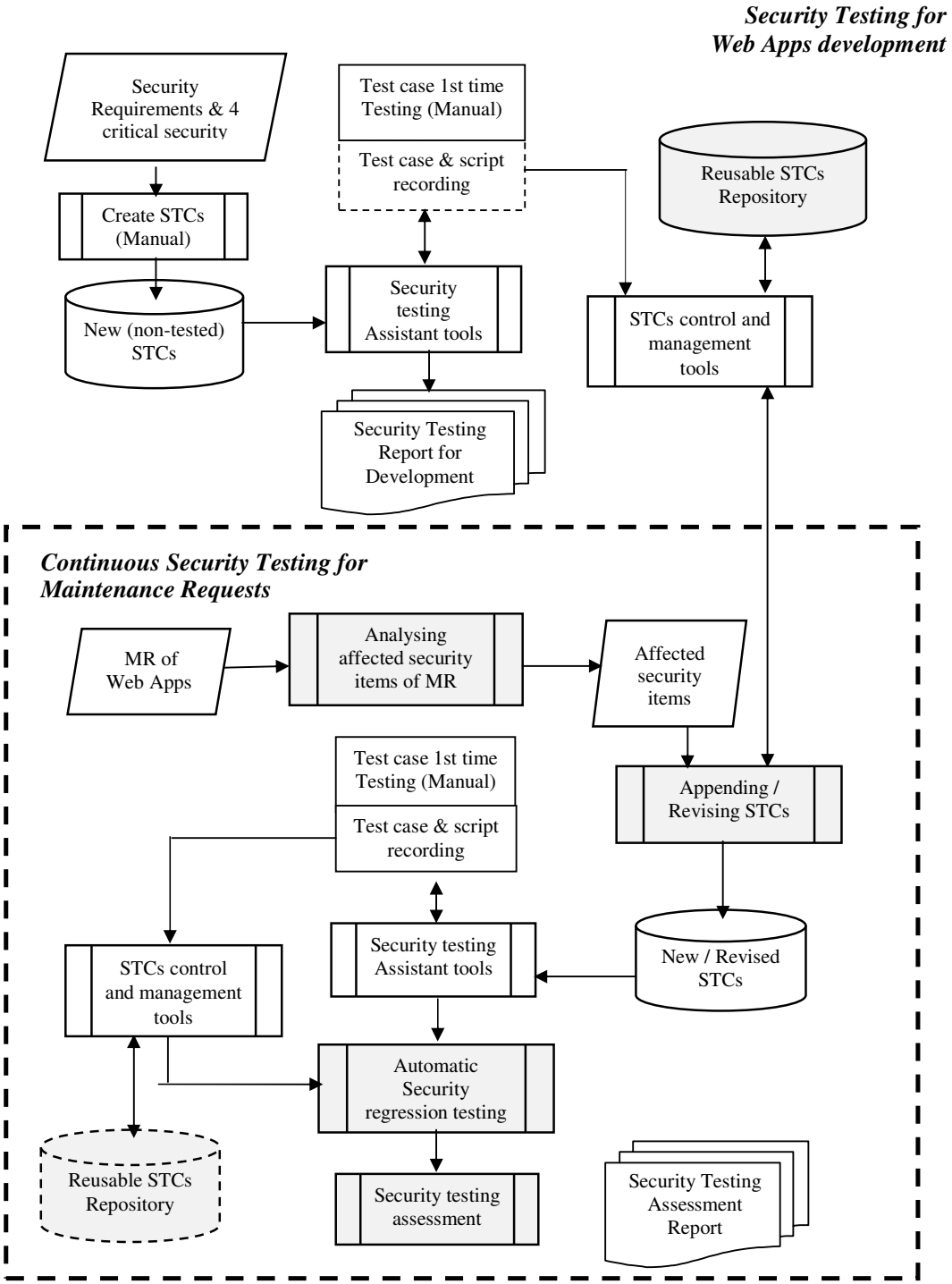

Figure 4. Continuous security testing operation environment

- Affected Security Items Identification (ASII) phase: according to the MR, maintainer should careful analysis the maintenance items do or do not relate to the security requirements. For ensuring the security of Web Apps, the affected security requirements must proceed complete security testing after maintenance activities.
- STCs Design (STCD) phase: If the security items of Web Apps are not affected by MR, reusable STCs with test script can make automatic regression testing, and does not need to design new STCs. If the security items of Web Apps are affected by MR, the MR need to carefully analyse to identify the affected security items. According to affected security items, testers should design new STCs or revise existed STCs. Based on new added or revised STCs, test script can collect at the first security testing. STCs with test script can be a reusable STCs and to storage and manage by the test case management tool.
- Automatic Security Testing (AST) phase: This phase need to complete two parts of security testing. For the affected security items, some STCs are new appended or adjusted in maintenance testing. Therefore, the assistant testing tools can only help to make partial security testing. For the unaffected security items, the reusable STCs with test script can complete automatic regression testing for identifying the regression faults.
- Security Testing Evaluation (STE) phase: Frequent changes Web Apps need to invest more resources for maintenance activities. Continuous security testing lacks human resources to cause the critical security testing often to be neglected. The maintenance activities of Web Apps always takes more security risks. For controlling and managing the security risks, security test coverage degree, accomplish ratio, correctness and compliance should completely collected. After security testing, the assessment tools generate the security testing evaluation report to concretely improve the completeness and critical quality of security testing [16].

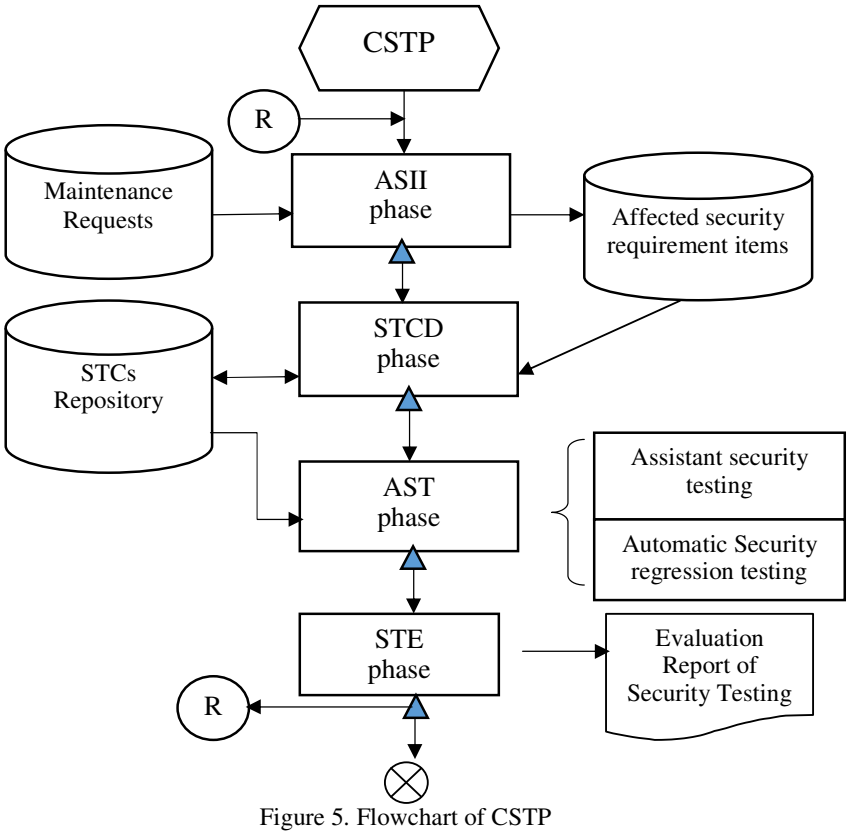

Figure 5. Flowchart of CSTP

5. EVALUATION OF CSTP

Web Apps need to continuously extend new services and adjust business activities to maintain enterprises or organizations competitive advantage. In Section II, depicts the challenges of Web Apps faced the frequent changes, which often cause Web Apps security vulnerabilities or defects and impact the transaction security of enterprise and organization. In this paper, combing the reusable STCs with the continuous security testing operations [15] to design the CSTP. CSTP can assist to overcome insufficient maintenance resources and detect Apps security vulnerabilities and defects as early as possible. Based on four evaluation items, the advantages of CSTP described as follows:

(1) Collect and record complete test scripts: In Apps development process, the STCs of completed design have high reusable potential. Adding the complete test scripts can enhance the reusability of STCs for follows testing. CSTP adequately reuse the existing STCs to efficiently reduce the human resource investment in continuous security testing.

(2) CVS-based reusable STCs management: Appropriate maintain and management reusable STCs can improve the efficiency and quality of security testing. Continuous security testing insufficient resources can be obtained significant improvement.

(3) Automated security regression testing: Using the reusable STCs to complete security regression testing, without intervention of personnel, can automatically detect security vulnerabilities and defects of maintenance jobs. Making Web Apps security testing quickly reach continuous security testing task.

(4) Assessment and improvement: General Web Apps lack automated regression testing tools, and does not provide a perfect test cases control and management tools. Base on reusable STCs, CSTP apply VCS and testing tools cope with the continuous security testing to reduce Web Apps security risk. Each extension or change version can collect the data of security vulnerabilities and defects to assess the disadvantages of CSTP and develop improvement manner.

In continuous security testing of Web Apps maintenance jobs, regression testing can make reusable STCs with 90% to 100% reuse ratio. But the increase of affected security items, the others reusable STCs are relative reduction. However, the reusable STCs still can overtake the challenges of Web Apps security risk. Using percentages of the reusable STCs are shown in Table 1.

Table 1. Using percentages of the reusable STCs

Testing jobs	Affected security items	Reusable STCs (percentage)
Regression testing	Not affected security items	90%~100%
Retesting partial STCs	Partial affected security items	50% ~ 70%
Retesting majority STCs	Majority affected security items	20% ~ 50%
Testing of new STCs	New append security items	10% ~ 20%

6. CONCLUSIONS

In the Internet age, a variety of the pursuit of high efficiency of business activities and transactions must be closely integrated with the network technology. Web Apps must enhance the flexibility and high efficiency of trading activities to accept the user of pluralism various requirements, and quickly achieve functions extension and services change requests. Frequently change and extension of Web Apps often causes Apps security vulnerabilities and defects. At limited time and resources, for preventing personal data and transaction information has been stolen or tampered, security testing should put to good use the existing STCs. For this, based on reusable STCs, the paper design the continuous security testing procedure (CSTP) for enhancing efficiency of the Web Apps continuous security testing. CSTP divides into four phases which are security items impact analysis, test case preparation and management, automated security testing and security testing and assessment to effectively control and reduce security risks of Web Apps. Combining the reusable STCs, CSTP assist Web Apps continuous security testing and get the following four specific results:

- Combining automated testing tools to simplify testing steps and reduce continuous security testing effort.
- Putting to good use the existing STCs to improve the continuous security testing quality and efficiency.
- Timely identifying Apps security vulnerabilities and defects to develop a revision manner in time.
- At limited time and resources, effectively reduce the Web Apps security risks of frequently change and extension.

Frequently change and extension of Web Apps need to take more resource to handle Apps security risk. Based on reusable STCs, CSTP simplify security testing steps and improve continuous security test efficiency, so that Web Apps security risks can be controlled effectively.

ACKNOWLEDGMENTS

The research was supported by Ministry of Science and Technology research project funds (Project No.: MOST 105-2221-E-158-002)

REFERENCES

[1] CIS Critical Security Controls - Version 6.0 (http://www.cisecurity.org/critical-controls/) (2016/6)
[2] OWASP Top 10 for 2013 (https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013)
[3] Niranjanamurthy M, Kavyashree N, Mr S.Jagannath, Dharmendra Chahar (2013), "Analysis of E-Commerce and M-Commerce: Advantages, Limitations and Security issues," International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013, pp.2360-2370.
[4] Al-Fedaghi, Sabah (2011), "Developing Web Applications," International Journal of Software Engineering and Its Applications, Vol. 5 No. 2, April, 2011, pp.57-68.
[5] Brandon, Daniel M., Software Engineering for Modern Web Applications: Methodologies and Technologies, IGI Global, 2008.
[6] McGraw, G., (2004), "Software Security," IEEE Security and Privacy, vol. 2, no.2, pp. 80–83.
[7] Potter, Bruce and McGraw, G., (2004), "Software Security Testing," IEEE Security and Privacy, vol. 2, no.5, pp. 32–36.
[8] McGraw, G., (2006), Software Security – Building Security In, Addison-Wesley.
[9] Engebretson, Patrick, (2011), The Basics of Hacking and Penetration Testing: Ethical Hacking, Elsevier Inc.
[10] April, Alain and Abran, Alain, (2008), Software Maintenance Management. New York: Wiley.

[11] Schach, S.R., (2011), Object-Oriented and Classical Software Engineering, Eighth Edition, McGraw-Hill, New York.
[12] Pressman, R.S., (2010), Software Engineering: A Practitioner's Approach, McGraw-Hill, New York.
[13] Holcombe, C., (2007), Advanced Guide to eCommerce, LitLangs Publishing, 2007.
[14] Saff, D. and Erns, M. D., (2003), "Reducing Wasted Development Time via Continuous Testing," Proceeding of IEEE International Symposium on Software Reliability Engineering (ISSRE), 2003, pp.281-292.
[15] Glenford J. Myers, Corey Sandler, Tom Badgett, (2011) "The Art of Software Testing," 3rd Edition, 2011, Wiley Publishing.
[16] Randall Rice, "How to Develop Test Cases and Test Scripts for Web Testing," Rice Consulting, http://riceconsulting.com/home/index.php/Web-Testing/how-to-develop-test-cases-and-test-scripts-for-web-testing.html (accessed November 9, 2016)
[17] Curphey M., Arawo R., and Foundstone M.V., (2006) "Web application security assessment tools," IEEE Security & Privacy, 4(4):32–41, 2006.

Authors

Sen-Tarng Lai was born in Taiwan in 1959. He received his BS from Soochow University, Taiwan in 1982, master from National Chiao Tung University, Taiwan in 1984 and PhD from National Taiwan University of Science and Technology, Taiwan in 1997. His research interests include software security, software project management, and software quality. He is currently an assistant professor in the Department of Information Technology and Management at Shin Chien University, Taipei, Taiwan.