International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 3, Issue 4, July-August 2014 **ISSN 2278-6856**

A Framework for Analyzing Risk of Web Application Vulnerabilities

[1]Jignesh Doshi, [2]Bhushan Trivedi
[1]LJ Institute of Management Studies, Ahmedabad
[2]GLS Institute of Computer Technology, Ahmedabad

Abstract
Web applications are widely used for business. Many transactions are taking place on web. On other side of coin, number of attacks has grown. Attackers use various means of compromising application security. As a result it has been found that many websites are vulnerable. Web application security has become one of the major threats to an organization. It seems that for organizations to be effective, Risk Management must be a management function. This paper is based on an empirical study of Top 10 Open Web Application Security Projects risks. This paper is representing a risk assessment and mitigation framework using hybrid (multiple) risk measures. Moreover, the findings of our empirical study suggest that effective Risk management is based on collaboration (multiple measures) and the establishment of joint and common risk management processes.

Keywords: Vulnerability analysis, SQL Injection, Risk Management, Risk Exposure, FMEA, Risk Mitigation

1. INTORDUCTION

As per internet usage statics, approx. 30% of total world population is considered as internet users [2]. As per netcraft surveys on April 2014, approximately 3.9 million web sites were added in April 2014. Unfortunately, attacks are growing exponentially along with internet usage [1]. As per CERT, Approx. 59% of cyber security incidents are related to web applications [3]. Security is one of the biggest threat and challenge for organization in current era. Evolution of security risks force organizations to keep changing applications even without writing or modifying application code [15] [21]. Web applications are soft targets of hackers. Organizations are forced to take care for hundreds of security issues even without changing a single line of code. As per OWASP, the top 10 vulnerabilities keep changing over last few years [4]. These vulnerabilities provide easy gateway for attackers to steal data, manipulate data and may cause data loss. Risk exposure and risk mitigation are two measures widely used for risk assessment in various industries [20] [23]. In this paper we have proposed risk analysis framework based on combinational (hybrid) risk measures. The proposed framework is implemented on top 10 web vulnerabilities [1]. Purpose – This paper aims to assess various security risks that could impact a business (web application). We proposed a framework to quantify and mitigate security risks. Design/methodology/approach – Risk measures have been used to quantify information risks. Risk management Plan is employed to understand the interrelationships among the enablers of security risks mitigation.

Focus: Risk management framework for organizational live projects. Our focus of study is on the most serious security risks which currently exist in the web application.
This paper is organized as follows: Section 2 covers literature survey where we define risk, vulnerability and risk management. In section 3, we discuss risk analysis using risk management process for OWASP top 10 security Risks, Conclusion is provided in section 5.

2. LITERATURE SURVEY

a) Vulnerability

Attackers use various techniques to exploit web applications. All these vulnerability are used by hackers to exploit web applications and databases. It has been observed that vulnerabilities keep changing over a period [1]. Top 10 vulnerabilities as per OWASP 2013 are:

i) Injection [4] [5] [6] [7] [8]: In this type of attack, attacker sends untrusted data to an interpreter. Injections are found in SQL, LDAP, Xpath or NoSQL queries, OS commands, XML parsers. Most common attack is SQL Injection (SQLI) in which attacker craft query and execute query. Injection flaws are easy to discover while coding, but difficult to discover during testing. The impact of such attacks is data loss, data access and manipulation. Scanners, fuzzers and research developed solutions are available to mitigate this risk.

ii) Authentication [9][10]: Custom code (authentication form, security question and session management scheme) is most commonly used for user access in web applications. Attacker find flaw in such coding as it is very easy. Impact of such attacks are account access, data loss and manipulation. Advanced single sign of system or strong authentication using API are available to mitigate this risk.

iii) Cross Site Scripting (XSS) [4] [10] [11]: In this attack, an application sent a page which includes user supplied data (scripts) to the browser without properly validating. Three types of attacks are Stored, Reflected, and DOM. Detection of most XSS flaws is fairly easy. Attacker can steal data or misuse cookie information. Risk mitigation of this risk can be done either via disabling scripting languages or enforcing proper encoding / filtering.

iv) Insecure Direct Object Reference (Insecure DOR) [4], [14]: In this attack, attacker is an authorized user, who simply changes some parameter value that directly refers to a system object on which he/she is not authorized. Detection of this flaw is easy and can be mitigated using

code review.

V) Security Misconfiguration [4] [14]: Here, attackers can be insider or outsider. Attacker accesses default accounts, unused pages, un-patched flaws, unprotected files and directories, etc. to gain unauthorized access. These flaws can happen at any level like platform level, database level, or network level. This risk can be mitigated via disabling default accounts.

vi) Sensitive Data Exposure (SDF) [4] [14]: In this attack, attackers steal data typically by not breaking crypto directly but via different means like steal keys, man-in-the middle attack etc. It is hard to exploit. This attack compromises all sensitive data like credit card number, social security number, personal data etc.

vii) Missing Function Level Access Control [4] [14]: In this attack, attacker who is having access will change URL or parameter used for function. It is very easy to detect such attacks as they are caused due to inefficient function level protection.

viii) Cross Site Request Forgery (CSRF) [4] [14]: In this attack, attacker tricks user via forged HTTP, image tag or XSS and get data submitted. This risk can be mitigated using penetration testing or code review.

ix) Using components with known vulnerabilities (Components) [4] [14]: In this attack, attacker identifies weak components (e.g. Framework libraries) either by scanning or via manual analysis and exploitation of web application. Maximum impact of this attack is complete host takeover or data manipulation.

x) Un-validated Redirects and Forwards [4], [14]: In this attack, Attacker tricks victims via attaching links to invalidated redirect. It is very easy to detect invalidated redirects. Impact of these attacks is loss of user password or account access.

b) Related work

Risk Management is successfully implemented by various industries like software, construction, manufacturing, supply chain, Information Technology etc. [15] [20] [21] [23]. Risk exposure as a risk measure is widely used in IT industry for risk analysis [21][22]. While Failure Mode and Effects Analysis [FMEA] risk measure is widely used in manufacturing industries for risk evaluation [18][20][21][22]. It is found that for organizations to be effective, Risk Management must be a management function [20][21][22][23][24][25]. The key objective of risk management is to increase the probability and impact of positive events, and decrease the probability and impact of negative impacts on project [19][24]. Risk management mainly focuses on proactively preventing things which can go wrong and helping things to go right [23][24].

Key benefits of effective Risk Management are [16] [17[18][19][20] [22] [23][24]:

- Can reduce project risk by up to 90%.
- lead to better project decision making
- May help in achieving a higher degree of project success.

3. Problem Statement

In order to mitigate such risks, we have three types of solutions available are Penetrate & Patch, Operational environment and Secure software engineering [15] [21]. Risk management is a requirement at CMM Level 3. Risk management activities are carried out during development of web application, starting from requirement analysis to testing phase [19] [22].

Research Question:

a) How to manage risks for live or rolled in projects?
b) Which and how many risks to be mitigated?

Also, the risk impact varies from application to application so we need some mechanism to identify most critical risk and mitigate.

4. Risk Assessment and Mitigation Framework

General framework consists of 3 major activities: Risk management planning, assessment and tracking[19][22]. Risk management activities flow is sequential and iterative. Figure 1 show most proposed risk analysis framework[19][22].

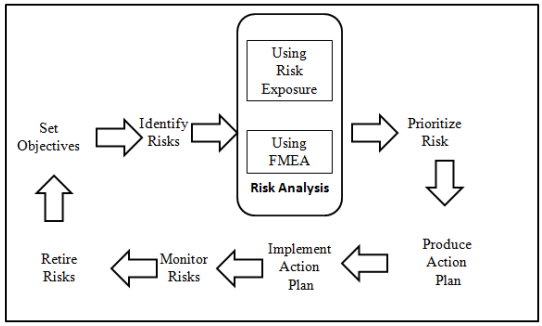

Figure 1. Proposed Risk Analysis Framework

a) Risk Identification

Generally, here exhaustive list of flaws for system are identified and list is prepared. Various methods like checklist, surveys and interviews are used to identify risks. For our study, we will use top 10 security risks identified by OWASP (2013) [4].

b) Risk Analysis and Prioritization

There may be many risks for an application. Risks road maps are either trivial or difficult to find and exploit. Similarly, the impact of risks may be negligible or severe. It may put you out of business. Under risk analysis, risk is analyzed for its cause, impact and delectability. All identified risk may not occur or impact projects. Different risk may have different impact. It is practically not feasible to mitigate or handle all risks so risk prioritization is done for identified risks. Prioritization requires proper risk analysis (impact and effect). For risk analysis various quantitative risk measures are used like risk exposure, FMEA etc. Here, we are performing risk analysis using two risk measures as a combined approach.

I) Risk Assessment using Risk exposure

Risk exposure represents expected loss for a risk. Risk exposure is a product of the probability of the risk's occurrence and consequences of risk it occurs.

It is calculated using following formula:

Risk Exposure = Probability * Loss

Here, Probabilities are measured on scale of 0 to 1, consequences and delectability are measured on scale of 1 to 10 (refer Appendix Table 1) We have calculated risk exposure for OWASP top 10 risks (refer to table 1).

Table 1. Risk assessment using Risk Exposure

Risk	Probability	consequences	Risk Exposure
Injection	0.6	10	6
Authentication	0.8	10	8
XSS	0.9	6	5.4
Insecure DOR	0.6	6	3.6
Misconfig	0.6	6	3.6
Sens. Data Expo.	0.4	10	4
Function Acc.	0.4	6	2.4
CSRF	0.4	6	2.4
Components	0.9	6	5.4
Redirects	0.2	6	1.2

II) Risk Assessment using FMEA

Failure Modes and Effects Analysis (FMEA) is a systematic, proactive method[26][27]. It is used for evaluating a process to identify where and how it might fail and to assess the relative impact of different failures, in order to identify the parts of the process that are most in need of change[26][27]. We have calculated FMEA for OWASP top 10 risks (refer to table 1).

The Failure Mode and Effects Analysis are calculated as:

RPN = Probability * Delectability * Severity

Table 2. Risk Assessment using FMEA

Risk	Prob.	Det.	Consequences	RPN
	(P)	(D)	(C)	(P*D*C)
Injection	0.6	6	10	36
Authentication	0.8	6	10	48
XSS	0.9	1	6	5.4
Insecure DOR	0.6	1	6	3.6
Misconfig	0.6	1	6	3.6
Sens. Data Expo.	0.4	6	10	24
Function Acc.	0.4	6	6	14.4
CSRF	0.4	1	6	2.4
Components	0.9	8	6	43.2
Redirects	0.2	1	6	1.2

As per industry best practice top few risk are prioritized and mitigation plan is prepared [15] [16] [17] [18] [19]. The basic idea of combining different risk measures analysis is to obtain improved list of top risks and make risk management more efficient. Table: Combined Top 3 Risks

	Risk Rank		
Risk Rank	Risk Exposure	FMEA	Combined
Authentication	**1**	1	1
Injections	2	3	2.5
Components	3	2	2.5
XSS	3	6	4.5

c) Risk Management Planning

High level Risk management plan is prepared for top 3 risks.

Risk	Mitigation Plan
Authentication	1 Single sign on authentication mechanism 2 Use of API for authentication
Components	1 identify all components and monitor security of it 2 Monitor versions of components 3 disable default accounts, unused functionalities of components
Injection	1. Defensive Coding for new coding 2. Implement Scanners / Fuzzers 3. Develop training plan

d) Risk monitoring

We need to monitor risks periodically. If required new risks can be added or can retire irrelevant risks. The set of risk management activities (refer figure 1) are repeated [15] [19] [22].

5. CONCLUSION

Findings –We discuss risk analysis mechanism which can be used to monitor web application vulnerabilities continuously. Research presents a risk index to quantify security risks using multiple risk measures. As per OWASP, the Component risk was identified as number 9. However, during our risk assessment it was identified as number 2 (using FMEA) and 3 (using Risk Exposure). Practical implications – The proposed combined risk measured-based framework would help to develop suitable strategies to manage most appropriate security risks. Originality/value – The major contribution of this paper lies in the application risk management framework to quantify top 10 security risks using hybrid risk measures. Risk analysis coverage comparison: Proposed framework with two risk measures is summarized as below

Focus	Risk Measure		
	Risk Exposure	FMEA	Proposed Combined
Probability	X	-	X
Loss	X		X
Failure Mode	-	X	X
Effect Analysis	-	X	X
Process		X	X
Product		X	X
Design		X	X

In conclusion, Our Risk framework provide following benefits:

1) Eliminate the dependency of security surveys
2) Provide flexibility to focus on most severe risk based on probability, process and effect
3) Dynamic to use
4) The results of this study show that risk management framework provide more dynamic and comprehensive risk assessment.

Appendix 1

a) Risk Probability [19] [23]

Probabilities	Range
Very Low	0.0 – 0.2
Low	0.3 – 0.4
Medium	0.5 - 0.6
High	0.7 – 0.7

b) Risk Impact and delectability categories [19] [23]

Categories	Range
Low / Easy	00-04
Moderate / Average	05-7
Severe/ Difficult	08-10

6. REFERENCES

[1] April 2014 Web Server Survey http://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html,[visited on 11th May 2014]

[2] Internet usage statistics The Internet Big Picture World Internet Users and Population Stats www.internetworldstats.com/ stats.htm ,[visited on 11th May 2014]

[3] National Vulnerability Database : http://web.nvd.nist.gov/ view/vuln/statistics, visited on 10th Jun 2014

[4] OWASP Top 10–2013 Projects: https://www.owasp.org/ index.php/ Top10# OWASP_Top_10_for_2013

[5] SQL Injection: http://www.us-cert.gov/security-publications/sql-injection: ,[visited on 11th April 2014]

[6] Su and G. Wassermann, "The Essence of Command Injection Attacks in web Applications", The 33rd Annual Symposium on Principles of Programming Languages (POPL 2006), 2006.

[7] Diallo Abdoulaye and Al-Sakib Khan Pathan, " A Survey on SQL Injection: Vulnerabilities, attacks AND Prevention Techniques", IEEE 15th International Symposiam on Consumer Electronics, 2011

[8] Nina Godbole and Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensic and Legal Perspective", Wiley India Pvt. Ltd, First Edition 2011 page 164

[9] Preshika Tiwari, Ashish Kumar Srivastava, A Survey on Authentication Mechanism against SQL Injection in XML, International Journal of Computer Applications, 10.5120/13501-1249, November 2013

[10] Guide to Authentication, https://www.owasp.org /index.php/Guide_to_Authentication, visited on 11th April 2014

[11] Rahul Johri and Pankaj Sharma " A Survey on Web Application Vulnerabilities (SQLIA and XSS) Exploitation and Security Engine for SQL Injection", IEEE 2012

[12] Jeremiah Grossman, Xss Attacks: Cross Site Scripting Exploits and Defense, Syngress Media, Elsevier Limited, Oxford, 2007, ISBN- 978-1597491549

[13] You Yu, Yuanyuan Yang, Jian Gu, and Liang Shen, "Analysis and Suggestions for the Security of Web Applications", International Conference on Computer Science and Network Technology 978-1-4577-1587-7/111

[14] Fakhreldeen abbas saeed, 2eltyeb e. Abed elgabar, assessment of open source web application security scanners ,Journal of Theoretical and Applied Information Technology, 20th March 2014. Vol. 61 No.2

[15] Navdeep Kaur, Parminder Kaur, SQL – Injection – Anatomy and Risk mitigation, CSI Communication June 2014, Volume 38 Issue 3

[16] Project Management Institute, A Guide to the Project Management Body of Knowledge, (PMBOK Guide), Fourth Edition, ANSI/PMI 99-001-2008, pp. 273-312.

[17] The MITRE Institute, September 1, 2007, MITRE Systems Engineering (SE) Competency Model, Version 1, pp. 10, 40-41.

[18] Garvey, P.R., 2008, Analytical Methods for Risk Management: A Systems Engineering Perspective, Chapman-Hall/CRC-Press, Taylor & Francis Group (UK), Boca Raton, London, New York, ISBN: 1584886374.

[19] Roger Pressman, "Software Engineering A Practioner's approach", 7th Edition, Chapter 28

[20] D. R. Prajapati :Application of FMEA in Automobile Industries: A Case Study, The IUP Journal of Mechanical Engineering, Vol. IV, No. 4, pp. 7-21, November 2011

[21] M. Lisa Yeo, Erik Rolland, Jackie Rees Ulmer, Raymond A. Patterson: Risk Mitigation Decisions for IT Security, ACM, Volume 5 Issue 1, April 2014 Article No. 5

[22] A practical approach for managing risk: http://www.sei.cmu.edu/risk/ Visited 11th Jul 2014

[23] Pankaj Jalote, CMM in Practice; Processes for executing software Projects at Infosys, Pearson, Chap.8

[24] National Institute of Standards and Technology. An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12,1995

[25] Olivier Lavastre, Angappa Gunasekaran, Alain Spalanzani: Supply chain risk management in French

companies, Decision Support Systems, Volume 52 Issue 4,March 2012, Elsevier Science Publishers B. V.

[26] FMEA in Six Sigma Methodology: http:// www.sixsigmaonline.org/six-sigma-training-certification-information/articles/fmea-in-six-sigma-methodology.html, Visited 11th Aug 2014

[27] http://www.whatissixsigma.net/failure-mode-and-effects-analysis-fmea/http://www.whatissixsigma.net /failure-mode-and-effects-analysis-fmea/, Visited 11th Aug 2014

AUTHOR

Jignesh Doshi received the B.Sc (Maths) and M.C.A. degrees in 1989 and 1992, respectively. He has nearly 22 years of experience. During 1992-2008, he worked in various IT firms like Patni Computer Systems, Vodafone (Fascel), Gujarat Lease Financing Ltd., Erhardt + Leimer (I) Ltd. Since 2008, he is working as associate professor at L J Institute of Management studies, He received Oracle Certified Professional (10g) in 2012.

Bhushan Trivedi received Ph.D. in 2008, Currently guiding 8 students in their Ph D process. He has nearly 25 years of teaching experience. Areas of interest are Intrusion Detection with mobile agents, Sensor Networks, Using artificial intelligence techniques to solve real world Problems. Conducted nearly 20 workshops on Effective Teaching, 15 workshops on "how to debug a network with TCPDUMP and WireShark" and quite a few other workshops across India. Have written two books, both published by Oxford University Press. The first book is on ANSI C++ and another on Computer Networks. The first book is adopted at three different places and the second is adopted at one place. The ANSIC++ book enjoys best selling position in Oxford Higher Education currently.