WEB APPLICATION FOR RISK ASSESSMENT WITH SECURITY FEATURES

Abhijeet Vijay Shirsat
Student, MTech(Information-Security),
K.J. Somaiya College Of Engineering,Vidyavihar, Mumbai
abhijeet.shirsat@somaiya.edu

Manuscript History
Number: **IJIRIS/RS/Vol.05/Issue04/APIS10080**
DOI: 10.26562/IJIRAE.2018.APIS10080
Received: 10, April 2018
Final Correction: 18, April 2018
Final Accepted: 22, April 2018
Published: **April 2018**
Citation: Shirsat (2018). WEB APPLICATION FOR RISK ASSESSMENT WITH SECURITY FEATURES. IJIRIS:: International Journal of Innovative Research in Information Security, Volume V, 21-24.
doi://10.26562/IJIRIS.2018.APIS10080
Editor: Dr.A.Arul L.S, Chief Editor, IJIRIS, AM Publications, India

Abstract—Auditing is characterized by way of reliance on a number of concepts such as risk assessment, incident management and so on. Those concepts should help to make the audit a powerful and dependable tool in support of management guidelines and controls, by way of supplying facts on which a corporation can act a good way to enhance its performance. Adherence to those ideas is a prerequisite for imparting audit conclusions which might be applicable enough for allowing auditors, operating independently from each other, to attain similar conclusions in similar situations. The risk assessment tool is required to find out the risk in the processes. Moreover the appropriate user interface is required in the tool. To avoid the confusion in the entries to be filled in the text fields, the placeholders are considered obligatory to help the risk owner to get the idea for what is the proper entry to be filled into the text field. The processes in the company and all the information related to them are highly confidential and they need to be secure enough that no hacker can access any of the data included. The confidentiality, integrity and availability of the information had to be attained. Thus this risk assessment tool which is a web application has attained the necessary security features required to stay protected from the hackers. SQL injection and cross site scripting which are highly rated security vulnerabilities are also taken care. Creation of database was also needed to do the proper create, update and delete operations. Risk Assessment tool is useful for ISO 27001 lead auditor and help him find out all the possible risk related to the processes in the company. Thus he then treats, tolerate, transfer and mitigate the risks in the processes
Keywords— ISO; ISMS; SQL; XSS;

I. INTRODUCTION

Data is an important aid for all organizations in view that statistics helps business community and commerce and facilitates managers and workforce to make suitable and powerful choices. Securing organizational statistics and its crucial elements, which include the systems and hardware that use, save, and transmit that records have turned out to be increasingly important [1]. If the business enterprise cannot ease its records, excessive impact on business continuity and commercial enterprise credibility can occur. If the company's information properties are lost, pass into the wrong fingers or in any clever hands are misused, it is able to be catastrophic to the organization, and similarly catastrophic to different events doing business, immediately or indirectly, with this organization.

An organization needs to focus on safeguarding its information. In order to achieve this, organizational and technological challenges of IT security management must be determined followed by the implementation of a strategy that can manage and minimize the effect of these security challenges [2]. Finally, a defect document must be prepared such that it proves its relevancy to the information security objectives of the organization.

An organization is largely dependent on various Information Assets and personnel of an organization share the responsibility of keeping all these assets secure. To offer speedy and suitable reaction to security incidents and to make certain interoperability between organizations, there is a need for a systematic and pre-described approach for it. Information Security Management System is an overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. ISO/IEC 27001 provide guidelines to develop a framework to initiate, implement, maintain and manage information security within the organization. This framework has been defined as Information Security Management System (ISMS) that helps the organization to determine the current status of their information security programs and, where necessary, establish a target for improvement. ISMS is a broader concept used to build a secure organization which incorporates Security policy, Information Security Manual, Information Asset Inventory, Risk Assessment Methodology, Risk Assessment Reports, and do training programs to employees intended for Information security [3]. Risk assessment is the process of finding the risk in the processes in the company. The risk assessment is done by the Lead Auditor based on the standards of the ISO 27001:2013. The risk assessment is done basically on how the processes are confidential.

Auditors should exercise carefulness in the use of information taken in the course of their duties [4]. There should be a legal way of checking whether the data is handled properly or not. This concept includes the proper handling of sensitive or confidential information. Moreover the processes which contain confidential information should be preserved with property of confidentiality [5]. Integrity is the property of information to not get changed by an unauthorized person. Thus integrity is one of the important aspects of information security.

Availability within the context of a computer machine refers back to the capability of a user to get right entry to records or sources in a designated location and in the best format. The probability of the threats and severity of the vulnerability also helps in finding out the risk in the processes. Thus confidentiality, integrity, availability and more parameters are necessary to find risk in the processes. The risk has to be treated, tolerated, terminated or transferred if there is a risk which is to be treated, tolerated, transferred or terminated, respectively.

II. RISK ASSESSMENT TOOL

The risk assessment tool is a web application which is helpful in finding the risk but in an automated way. It is used by the information security administrator not by the risk owner. It takes all the values from the lead auditor and gives the decision of treating, tolerating, terminating or transferring the risk. This web application helps in guiding for the lead auditor to fill out the fields using the proper examples which are given in the tools. It also guides the risk owner to avoid the confusion by getting the example of what would be the field answer. Sometimes it would be confusing to fill out the fields but there are the directions for entries to be filled in the placeholder. The beauty of the tool lies in the placeholders and also the security features included in the tool.

The tool handles all the important information handled by the risk owner and thus the information is very precious. This information can be misused if the tool is not secured. There can be many flaws in the security and thus it has been sent through a vulnerability scanner.

The tool developed has six sheets which are used to give an overall idea to the risk owner of how the risk should be handled instead of typing all the matter in the excel sheet. The placeholders give the idea of how the data has to be entered.

The criticality of the processes is found out on the basis of the confidentiality, integrity and availability. The impact on the business is found out using the loss to the internal parties, external parties, financial loss, and legal implications. The threats and vulnerabilities are found out in the business which gives the business impact on the basis of the probability of the threat and severity in the vulnerability. Risk register is where the residual risk is counted and decided whether the risk has to be treated, tolerated or terminated.

III. SECURITY FEATURES IN RISK ASSESSMENT TOOL

Nowadays, every person use websites for their comfort and entertainment. How much are the websites secured is a huge question which everyone ignores and still surf through those unsecured websites. Thus each vulnerability coming into the tool should be focused and required countermeasures to avoid the vulnerabilities shall be taken. Thus some of the most dangerous vulnerabilities are discussed as below and implemented in the tool.

A. SQL Injection and Countermeasures to avoid the vulnerability

Many web pages are to be given parameters from user, and generate SQL queries to the database. SQL Injection is a trick to inject script/command and enter through the web front end [6]. Consider an example of SQL injection. Application may be vulnerable to SQL injection attacks while you enter invalid user input into the database queries in particular inclined is a code that builds dynamic SQL injection. SqlDataAdapter gCom= new

SqlDataAdapter ("SELECT * FROM Users WHERE UserName='"+id.Text+"'", conn);
Hackers can inject SQL query by ending the SQL query with the single quote followed by a semicolon to start a new command thereby taking control over the system and executing the query which could be of their choice.

Consider the following "id" field.
' OR 1==1- -
Following query can be sent to the database:
SELECT * FROM table1 WHERE uName='' OR 1=1 –
Because 1=1 is always true, the attacker retrieves every row of data from table1 table. The two hyphens are used to end the statement.
Countermeasure is an action taken to counteract a danger or threat. Countermeasures for SQL injection includes that input validation should be done and validation of the input string should be done before sending a request to the database. For

e.g. the input validation has been done in the following code where number field is supposed to take only numbers strictly [6]. Whenever a user tries to input other values except numbers, it doesn't get entered. Use SQL parameterized queries when building SQL commands.
After entering an apostrophe (') after the URL of the webpage, there is an error which will be showing that the webpage is vulnerable to the SQL injection. If the website is vulnerable to the SQL injection, it would show error after putting an apostrophe, but the success page is displayed which shows that there is no error and thus protecting from SQL injection [6].

B. Cross site scripting (xss) and Countermeasures to avoid the vulnerability

Cross Site scripting attack is an attack approach that forces a web website to echo attacker supplied executable code that loads in a user's browser [6]. While an attacker gets a user's browser to execute his code, the browser will run the code and the attacker receives the capability to examine, regulate, and transmit and execute malicious code in the browser. CSS vulnerability is resulting from the failure of a site to validate user entered input and then returning into the client's web browser. Cross site scripting assaults essentially compromise the trust relationship between an user and the web page.
Consider an example of a web site link. www.mywebapplication.com/logon.aspx?username=bob
The following is a malicious link www.mywebapplication.com/logon.aspx?username=<script>alert('hacker code')</script>

If the web page sends the query string to server and fails to correctly validate it, thereby returns it to the browser, the script code executes within the browser. With the precise script, the attacker can extract the user's authentication cookie, put it up to his site, and ultimately make a request to the target website and attack the system.

Cross site scripting can be causing theft to the cookies, server interference and also the data theft. Thus countermeasures such as using regular expression to validate entered data received through query string, HTML form fields, and cookies. Validate all input for known valid values and then reject all other input. Specify the character encoding for the HTML document [6].

IV. CONCLUSION

The risk assessment tools which were used before in the market lacked a proper user interface with proper placeholders. The tool developed in JSP and Servlet is now used to do the risk assessment. A web application which is useful for proper risk assessment is helping the risk owner with the proper placeholders which help in giving the examples for filling out the sheets. This gave the solution for every text field and mitigating the confusion for the entries which were wrongly put before. The creation of the database was another issue as the database was not created initially and it leads to overhead for saving the data to a place and save it securely. Proper creation of database is now done and the data is now safeguarded at one place.

Nowadays, SQL injection and cross site scripting are the huge vulnerabilities for the web application which are really needed to be taken care of. These are taken care of in this tool and the important data which is vulnerable to these two vulnerabilities are going to be secured which will save a huge amount of money loss. Risk assessment has been a sharp tool for the lead auditor of the company to know which kind of action should be taken and react accordingly. The tool will be helping in automating the decision of the lead auditor. The vulnerability assessment tool is used to find out the vulnerabilities in the web site. The vulnerability assessment tool is important to ensure the security in the web application.

ACKNOWLEDGMENT

I express my deep sense of gratitude to my teachers for their valuable help and guidance, I am thankful to them for encouragement they have given in completing the project. I am thankful to my family and friends for providing the moral support and encouragement.

REFERENCES

1. Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems", Recommendations of the National Institute of Standards and Technology, Special Publication 800-30, pp.1-5, July 2002
2. Richard Kissel, Kevin Stine, Matthew Scholl, Hart Rossman, Jim Fahlsing, Jessica Gulick, "Security Considerations in the System Development Life Cycle ",October 2008, pp. 2-3
3. Ugur Aksu, Hadi Dilek, ˙Islam Tatlı, Kemal Bicakci,˙Ibrahim Dirik,Umut Demirezen, Tayfun Aykır,"A Quantitative CVSS- Based Cyber Security Risk Assessment Methodology For IT Systems", 23-26 Oct. 2017,IEEE
4. Daniel Tse, Zehan Xie, Zhaolin Song,"Awareness of information security and its implications to legal and ethical issues in our daily life",10-13 Dec. 2017,IEEE
5. Ayesha M. Talha, Ibrahim Kamel, Zaher Al Aghbari, "Enhancing Confidentiality and Privacy of Outsourced Spatial Data", 2015 IEE9E 2nd International Conference on Cyber Security and Cloud Computing, 2015
6. 074747474.5ark Stamp's, "Information Security Principle and Practice",Vol-4, Wiley Interscience, pp. 386, 405, 2006