IoT-Based Recycle Rebate System – Securing Website and Database

Azatulnajihah binti Mohamad Fairuz, Husna Sarirah binti Husin, Delina Beh Mei Yin
azatulnajihah@s.unikl.edu.my, sarirah@unikl.edu.my, delina@unikl.edu.my
Information System
Malaysian Institute of Information Technology
Universiti Kuala Lumpur
Kuala Lumpur, Malaysia

***Abstract*— Web database is a database application that is designed to be managed and accessed through the Internet and has gained the trust of clients and users over the globe. But without having a proper security implementation towards the web database, users and clients may lose trust. To mitigate them, we approach the problem by following the process of security assessment. In this paper, we introduce security assessment method through Vulnerability Assessment and Penetration Testing Process and Risk Matrix results to find the vulnerabilities and threats on the website and database of the Recycle Rebate System. The implementation of mitigation method used are based on the results scanning of the VAPT process and the Risk Matrix Table. All the results of the VAPT scanning were documented into a Risk Assessment Report which calculate the risk level of each existing results found and can be easily viewed and understand in the table form named Risk Matrix.**

Keywords— Security Assessment; Vulnerability Assessment and Penetration Testing Process; Risk Assessment Report.

I. INTRODUCTION

Rebate system is a program that provides a return of portion on a purchase price or can be simply said, it is a platform that gives out discounts by a seller to a buyer on a specified quantity, value or goods within a specified period. The rebate systems consist of vendor rebates, customer rebates, volume pricing, discount, and a way of giving an individual customer the "right price" without altering the original price downwards.

For Malaysian, having a special deal on food or shopping items online would basically hype them up. There are some of rebate system that have been introduced to Malaysian which benefits the customer with some food and beverage deals, entertainment vouchers, shopping discounts, and many more. Example of an existing system that being used by customer in Malaysia is the "Boost E-Wallet". The Boost E-Wallet is an application that gives opportunity to their customer to experience both secure and rewards with the cashless mobile payment. The benefit of using the application for the user is that despite of not using the apps fully, they can still be rewarded with some available coupons and vouchers that can be redeemed.

In Malaysia, there are three types of recyclables such as paper, plastics and bottles that are used for recycling campaigns that were practiced by all populations in Malaysia especially among households [9]. However, there a few obstacles in attracting residents towards recycling especially in the urban areas. This is a global problem for managing household waste fix urban areas in recent years [5]. The condition of narrow roads in residential area especially in Kuala Lumpur pose a huge problem for compactor trucks to pass by [9]. Second problem with the recycle system is that plastic waste is beyond repairs as it was caught floating across the river, beach and ocean which affect the environment. Thus, giving awareness and attitude towards recycling is the primary influencing factors in activating residents towards recycling intention and motivation [13]. By giving motivation towards recycling behavior, it can be driven towards environmental concerns, economic incentives, convenience and the influence of family and friend. The municipals have huge responsibilities to develop news innovative and creative ways to attract residence in their jurisdiction to participate in recycling program.

Thus, comes in with the proposed system called 'Recycle Rebate System' that would motivate and attract user towards participating in recycling program. In this system called 'Recycle Rebate System', residents can get vouchers and deals based on the weight of the trash that they drop off at the designated recycling sites. The system consists of Radio-Frequency Identification (RFID) reader, load cell, websites connection and database. But without having a proper security implementation towards the web database, users and clients may lose trust to use the system. Thus, it is important to know the type of vulnerability and threats occurs within the system and to secure it.

The contributions of this paper include:

(1) security assessment process using Vulnerability Assessment and Penetration Testing Scanning Process and

(2) mitigation approach used based on the scanning results.

The rest of the paper is structured as follows. Section II discusses the related work. Section III presents Scanning Process and Tools used. Mitigation method approach used is discussed in Section IV. The results details are presented and discussed in Section V. Finally, conclusion and ideas for future work are presented in Section VI.

II. RELATED WORK

A. IoT architecture layer

There are two main different opinions given by researchers on the layer of architecture that are used in IoT architecture layer; a 3-Layer architecture of IoT and 4-Layer architecture of IoT. Many researchers have the opinion of using 3-Layer IoT architecture, but there also some researchers think that IoT consists of 4-Layer architecture [3]. The difference in opinion exist due to enhancement in IoT and these requirements cannot be supported in 3-Layer architecture [6].

Three Layer Architecture of IoT

Three-layer architecture is considered as the basic idea of IoT in the early development of IoT. The three-layer architecture consists of Perception Layer, Network Layer and Application Layer.

The perception layer is also called as the recognition layer, which is to collect information or data that are useful from devices or the environment and then transform them into digital form [3]. This layer is made up of physical devices [4] which are responsible to sense and collect information [16] and then the information is transform to digital form [4].

The network layer acts as transmission layer [6] to carry and transmit the information that has been obtained from the physical devise and the converted to internet and communication based network infrastructure such as Z-Wave, Bluetooth Low-Energy(BLE), Wi-Fi, and LTE-A [4].

The last layer is the Application Layer that is to deliver application specific services to users [16]. This layer is acts as the interface for users to access data and interact with their IoT devices [4] which then personalized the services according to the users' specific needs, as well as become the major link gap between the users and application.

Four Layer Architecture of IoT

The four-layer architecture of IoT is improvised to fit into the continuous enhancement of IoT to ensure that is it fool-proof and secure from intruders [6]. The layers that are proposed has the previous function of the three-layer aspects with an added-on layer called Support Layer.

The support layer or also known as the "middleware layer" was created as the security aspects for IoT as it need to be secured to gain trust by user to use the IoT appliances [7]. The purpose of this layer is to ensure that information is sent by authentic users and protection from threats [6]. The second responsibility is sending the information from Application Layer to the Network Layer. This layer is responsible as the decision's maker that has the function to monitor, store, organize and visualize the information, as well as to resolve and create virtual entities [15]. There are many possible attacks could occur during transmission network such as the basic attack like sniffing attack, DDoS attack, Malicious Insider attack and many more.

B. Vulnerability Assessment and Penetration Testing (VAPT)

VAPT is a crucial assessment required for an organization especially those that their business involved with Internet exposure as VAPT can give more detailed view of the threats that are facing the organization's applications; hence can enable the business to protect its systems and data from attacks [2], which may lead to financial and data losses. Throughout the VAPT process must be conduct together with doing the VAPT report to ensures that every process, code, and results were recorded properly. As for the Vulnerabilities Assessment it is used for scanning to find application backdoors, malicious code and other kinds of attacks that may exist in software or applications that are developed internally. On the other hand, vulnerability scanners only scan source codes and do not offer comprehensive assessment because source codes are not typically available in purchased applications [2].

C. Threats and vulnerabilities in websites and database

Web applications are popularly published and used by user to accommodate with their work, retails, personal used, etc. which may deal with sensitive data such as financial and medical data. Therefore, it is vital to protect these applications from hacker attacks [10]. Thus, cyberattacks against the web application vulnerabilities have also increased and had cause tons of damage towards the user, client, customer, etc. [11]. The OWASP Top 10 2013 offers a list of the most critical application vulnerabilities, including such injection, broken authentication and session management, cross-site scripting, and cross-site request forgery [11].

Threats and vulnerabilities usually occur from the coding defects and causes severe damage to the application upon exploitation. Thus, users are exposed to exploitations such as malicious code that are injected into input which is used for interacting with the application [8].

There are many impacts towards clients if they were to ignore the safety measures in using the unsecured web applications. First impact that could occur to them are the client will be restrained to have any potentials visitors from visiting the websites. [1]. Next impact is the websites will be marked as malicious or not be indexed by Google with a warning flag as "not secure" to be shown on the search result and lose traffic. [1]. Lastly, the website will not be provided with a statement that operate with sensitive data like payment transactions. Thus, gave impact towards the business as it will not help to advertise the business and gain trust from user. The longer the websites used without a proper protection, the higher the risk of being attacked.

To reduce the possibility of a web applications from attacks, the programmers should follow the defensive coding practices and guidelines during the development as the basic knowledge before proceeding to develop an application. Upon preventing SQL injection attack, by having a secure programming that

involve proper sanitization and encoding of the user-input, parameterizing queries which refer to user supplied inputs, etc.

The countermeasures that can be used upon vulnerability such as cross-site scripting are focusing on identifying the missing sanitization routines and analyzing effectiveness of the sanitization routines to identifies the possible XSS approach and be able to prevent any malicious scripts approach [8].
Databases are the backbone of any application [12]. Databases gave permit to any authorized user to access, enter and analyze data quickly and without any problem. It's a collection of queries, tables and perspectives. The user interface for databases is called a database management system. Thus, the important and confidential information on the database have a chance to be attack. There are various types of attacks and threats from which a database should be protected. Database is exposed to threats such as excessive database privileges, SQL injections, DB vulnerabilities and misconfigurations and denial of service attack.

III. RISK ASSESSMENT

The purpose of this risk assessment is to evaluate the adequacy of the Recycle Rebate System Website and Database security. This risk assessment provides a structured qualitative assessment of the operational environment. It addresses sensitivity, threats, vulnerabilities, risks, and safeguards. The assessment recommends cost-effective measures to safeguards and to mitigate threats and associated exploitable vulnerabilities.

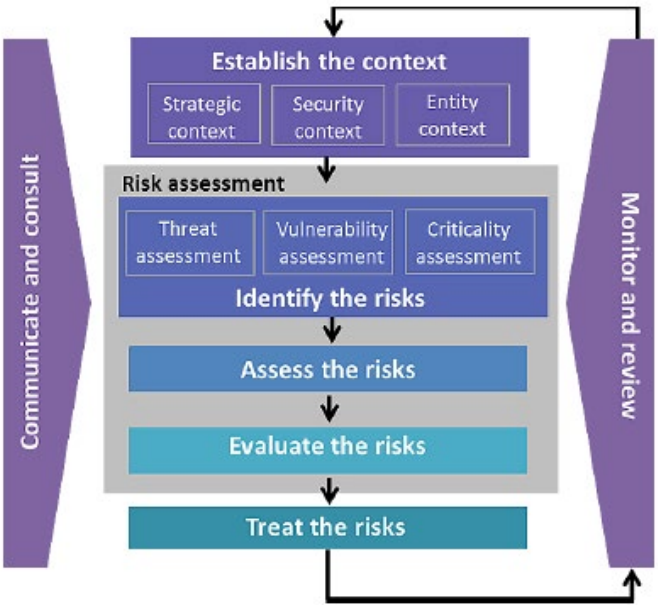

Fig. 1 Security Risk Management Process [14]

This risk assessment methodology and approach was conducted using the guidelines set by the Australian Government Protective Security Policy Framework, Security Risk Management Process [14] as shown in Fig. 1. The process is divided into identify the risks, assess the risks, and evaluate the risks phases.

A. *Phase I – Identify the risks*

In this phase, determining the target details and identifying the tools used to perform and conducting the VAPT process. First is by determining the target details by knowing the IP address of the target web system and the machine used as shown

The tools used to conduct the VAPT process for this project is by using the Metasploit Framework, OpenVAS, Nikto, Arachni, OWASP Zap, and Wapiti.

B. *Phase II – Assess the risks*

To start assessing the risks, by using the tools that had mentioned in Phase I this phase will elaborate the details on how to conduct or open each tool to scan and exploit the targeted system.

- Nikto: As for Nikto, the tools are already available in the Kali Linux machine. The scanning process will start after entering the code 'nikto -h "http://recyclerebatesystem/Website".
- OWASP Zap: As for this tool, it is also already installed in the Kali Machine. Once click on the apps, it will redirect to the Zap and to start the scanning, we just need to enter the targeted URL for a quick scan.
- Metasploit Framework: As for Metasploit, it is also a tools that readily available in the Kali Machine, we can either start the tools by clicking on the apps or we can enter manually through the terminal by using the code command "msfconsole" to start the tools.
- Arachni: To start the scanning for this tool just use the command in the terminal by typing "arachni http://recyclerebatesystem/Website --report-save-path=Desktop/Arachni-Report.afr" to start the exploitation. The command code "—report-save-path" that were used below are to save generate the report scan.
- OpenVAS: As for this tool, to start using the tool we will have to start it through terminal by typing the command code as shown in the Figure 12 below. Once it complete to start the service, we can enter the link given on the browser with the password that given during the starting process in the terminal, the username is admin.
- Wapiti: This tool performs "black-box" scans of the web application by crawling the webpages of the deployed webapp, looking for scripts and forms where it can inject data. To start the scanning, just entering the Terminal the command "wapiti -u http://recyclerebatesystem/Website" to start the exploitation.

C. Phase III – Evaluate the Risk

In this phase, the process scanning results will be determined and evaluate the risk and vulnerabilities found.

Nikto Scan

From the result of the Nikto scan, we can see that the targeted system is vulnerable to cross-site scripting attack and possible to clickjacking attack as cookie are not well set.

OWASP Zap Scan

OWASP Zap provides with summary report of alerts with two number of alerts as High and four as Medium/Moderate level of risk. The scanning report shows that the targeted system is vulnerable to SQL Injection, Cross-Site Scripting (XSS) as a high risk while Application Error Disclosure, X-Frame-Options Header not set, Directory Browsing and Parameter Tampering as Moderate risk level alert.

Metasploit Framework Scan

The tools detected that there is a possibility to HTTP Host Header Injection Detection on the targeted system.

Arachni Scan

From the scanning, the results show that there are total of 42 types of Cross Site Scripting and Blind SQL Injection done on the target machine. This is a sign of possible vulnerabilities.

OpenVAS Scan

Results on the vulnerability found with OpenVAS scanner of the targeted system with three high risk and thirty-five Medium risk found. The result shows that the targeted system is vulnerable towards weak password, prone to SQL Injection attack, using HTTP Method: TRACE, etc.

Wapiti Scan

The targeted system is vulnerable to blind SQL injection as it will not show error message on the web system yet still be able to do injection towards the web system.

Risk Assessment Table

In this step, from the result received from all the scanning tools will be combined into one table to know the priority of risk that need to be assess and the risk that with the less priority so we can initiate a mitigation method to be used. The results show that the systems are vulnerable towards attack such as SQL injection, Cross-Site Scripting, Cleartext Password over HTTP and Clickjacking attack.

IV. MITIGATION METHODS

Based on the results found, there are vulnerabilities towards Blind SQL Injection, Cross-Site Scripting, Cleartext Password over HTTP, Clickjacking attack and Headers are not properly set on the website. As for the results that had found, there are five mitigations method approach that were used to counterattack the vulnerabilities that were found. The five mitigations method approach that were used are listed as below:

a) Enabling the SSL certificate of the Recycle Rebate System Website.

b) Disabling the HTTP Trace Method.

c) Securing the website from Clickjacking Attack.

d) Securing the website from the X-FRAME-Options.

e) Validating the parameter query to secure from the Blind SQL injection.

a) Enable the SSL Certificate

Enabling the SSL Certificate is to help in converting the website into a more secure URL by HTTPs the website. To enable the SSL using the Kali Machine, we will use the Terminal to run the command below:

The command “openssl genrsa req -x509 -days 365 -newkey rsa:2048 -keyout /etc/httpd/httpscertificate/rrb.key” is used to generate the RSA Key for the SSL Certificate. While the command entered after “sudo nano /etc/apache2/sites-available/https.conf” is used to configure Apache to use the SSL Certificate. The command “sudo a2enmod ssl” is used to enable the SSL Module and the command code of “sudo a2ensite https.conf” is used to enable the sites that had been declared in the Apache. Next is the command code of “openssl s_client -connect 127.0.20.5:443” is used to verify the HTTPs Service of the website. And the last command used is the “sudo nano /etc/apache2/apache2.conf $Include /etc/phpmyadmin/apache.conf” is for connecting the database with the website by configuring the Apache.

b) Secure from Clickjacking Attack

The command “sudo a2enmod headers” are used to enable the headers in Apache. Then entered the command “Header set Set-Cookie;HttpOnly,Secure” to enable the header set. While the command “sudo apachectl -t” is used to check for any syntax error on the command newly inserted.

c) Disable the HTTP Trace Method

To use this method, it is just by entering new command line name “TraceEnable Off” in the Apache Configuration File.

d) Secure from X-FRAME-Options

For this method, inserting the command line of “$Header always append X-FRAME-OPTIONS ALLOW FROM $ Header always append X-FRAME-OPTIONS DENY” in the Apache Configure file. The restart the apache by using the command “service apache2 restart”.

e) Secure from X-FRAME-Options

Last mitigation method is by validate the parameter query in the database command of the website.

Once all the mitigation method approach implemented on the website, restart the apache to ensure that all changes were made on the website and database.

V. RESULTS AND RISK ASSESSMENT REPORT

Upon completing all the mitigation method on the website and database, process of rescanning using the VAPT Process must be conducted once again to proof that the mitigation approach has successfully reduce or remove the vulnerabilities found. To perform the rescanning process, we will be using the tools of Nikto, OWASP Zap, OpenVAS, and Wapiti. Part A discussed and elaborate on the results received from the Vulnerability Assessment and Penetration Testing Rescanning Process.

A. Results of the VAPT Rescan

a) Nikto Results

Result shows that the SSL and X-Frame-Options has been set on the site. Thus, prove that the site is now using a HTTPs and now protected from the Clickjacking attack.

b) OWASP Zap Results

Compared to the results before mitigation method applied on the website it has been lessen. By not having any High Risk Possible found on the site rather than having 3 High Risk on the site before the security implementation. With the result above, it shows that the website is now secured from the SQL Injection attack and Cross-Site Scripting attack.

c) OpenVAS Results

From the results, shows that the OpenVAS scanning results were a lot lesser that the previous scanning with only one High Risk were found on the site which related to the missing bug fixes. With this result of the rescanning process, it shows that the sites are now secured from SQL Injection, Cross-Site Scripting attack, Cleartext-password over HTTP and Clickjacking attack.

d) Wapiti Results

Based on the results, shows that the Recycle Rebate System is now are no longer vulnerable towards Blind SQL Injection.

B. Risk Assessment Report

The purpose of writing the risk assessment report is to minimize and control the risks in an appropriate way and to protect the targeted site from having damage during countermeasure process. The content of the Risk Assessment Report is the scope of the RA (Risk Assessment), the RA approach used, the System Characterization and the RA results.

By using the table Risk Matrix, shows that the results of implementing the security towards the system are successful with the method used to mitigate the risk.

VI. CONCLUSION AND RECOMMENDATION

In this paper, we presented the securing and mitigation method used on the Recycle Rebate System Website and Database by going through the steps in Security Risk Management Process. From the mitigation and result of process scanning, the successfulness of mitigation method implemented on the Recycle Rebate System Website can be summarize as in Table 1 below.

Table I Results of Securing the Recycle Rebate System

First VAPT Scan Result	Mitigation Approach Result
SQL Injection	Successful by implementing the Parameter Query and HTTPS the website.
Cross-Site Scripting	Successful by preventing from the clickjacking attack and set the Parameter Query.

For future project, security implementation method used on this Recycle Rebate System can be more up to date such as using a two-factor authentication and secure the data transferring between physical device and the website can be implemented to it. It is essential to ensure that the website and database are a lot more secure and convincing towards the users to keep using the system. This is a big challenge to apply the two-factor authentication and securing the data transferring as it would involve network connection of the physical device and the system. More study and research on that matter must be done to make it successful.

REFERENCES

[1] Marsh, A. (2019, May 16). What Your Website is Going to Lose if it is Not Secured. Retrieved from WebSitePulse Blog: https://www.websitepulse.com/blog/what-your-website-is-going-to-lose-if-it-is-not-secured

[2] Paine, L. (2019). VULNERABILITY ASSESSMENT AND PENETRATION TESTING. Retrieved from Veracode Security: https://www.veracode.com/security/vulnerability-assessment-and-penetration-testing

[3] Bilal, M. (2017). A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers. 1–21. http://arxiv.org/abs/1708.04560

[4] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002

[5] Bom, U., Belbase, S., & Bibriven Lila, R. (2017). Public Perceptions and Practices of Solid Waste Recycling in the City of Laramie in Wyoming, U.S.A. Recycling, 2(3), 11. https://doi.org/10.3390/recycling2030011

[6] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. Sensors (Switzerland), 18(9), 1–42. https://doi.org/10.3390/s18092796

[7] Cvitić, I., Vujić, M., & Husnjak, S. (2015). Classification of security risks in the iot environment. Annals of DAAAM and Proceedings of the International DAAAM Symposium, 2015-Janua(2016), 731–740. https://doi.org/10.2507/26th.daaam.proceedings.102

[8] Deepa, G., & Thilagam, P. S. (2016). Securing web applications from injection and logic vulnerabilities: Approaches and challenges. Information and Software Technology, 74, 160–180. https://doi.org/10.1016/j.infsof.2016.02.005

[9] Jordan, J. J., & Rand, D. G. (2019). Electronic copy available at : https://ssrn.com/abstract=1618202 Electronic copy available at. 1(1), 1–14.

[10] Lam, M. S., Martin, M., Livshits, B., & Whaley, J. (2008). Securing web applications with static and dynamic information flow tracking. Proceedings of the ACM SIGPLAN Symposium on Partial Evaluation and Semantics-Based Program Manipulation, 3–12. https://doi.org/10.1145/1328408.1328410

[11] Makino, Y., & Klyuev, V. (2015). Evaluation of web vulnerability scanners. Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2015, 1(September), 399–402. https://doi.org/10.1109/IDAACS.2015.7340766

[12] Malik, M., & Patel, T. (2016). Database Security - Attacks and Control Methods. International Journal of Information Sciences and Techniques, 6(1/2), 175–183. https://doi.org/10.5121/ijist.2016.6218

[13] Nguyen, H. T. T., Hung, R. J., Lee, C. H., & Nguyen, H. T. T. (2018). Determinants of residents' E-waste recycling behavioral intention: A case study from Vietnam. Sustainability (Switzerland), 11(1), 1–24. https://doi.org/10.3390/su11010164

[14] Purpose, A., & Core, B. (n.d.). 3 Security planning and risk management.

[15] Rashmi. (2018). IoT (Internet of Things) Concept and Improved Layered Architecture. International Journal of Engineering Development and Research, 6(2), 481–484. www.ijedr.org

[16] Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017. https://doi.org/10.1155/2017/9324035