Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 6, No. 1, June 2020, pp. 36~41
ISSN: 2338-3070, DOI: 10.26555/jiteki.v6i1.17019

Web-Based Dashboard for Monitoring Penetration Testing Activities Based on OWASP Standards

Yansyah Saputra Wijaya[1], Imaniar Ramadhani[2]
[1]Department of Informatic, STMIK Amik Riau, Pekanbaru, Indonesia
[2]Bank Rakyat Indonesia, Jakarta, Indonesia

ARTICLE INFO

Article history:

Received 20 June 2020,
Revised 09 July 2020,
Accepted 25 July 2020.

Keywords:

OWASP,
Cybersecurity,
Penetration Testing,
Dashboard,
Application Security.

ABSTRACT

Financial Services Authority Regulation concerning Application of Risk Management in the Use of Information Technology by Commercial Banks which requires Banks to ensure information security to maintain which must be done periodically at least once a year. The most popular way to have security is through pentest, to determine an application whether it is safe and successfully passed the pentest, we need a measurement standard, specifically for web applications, the standard commonly used is OWASP. However, OWASP has a very large list of vulnerabilities, so to simplify the process of monitoring the pentest process in an organization we need a tool that can visualize existing vulnerabilities from various applications to be more easily measured, calculated, and monitored during the pentest process. The tool commonly used to present information to managers is a Dashboard. The dashboard produced in this research is the monitoring dashboard of pentest monitoring activities, it is made using the PHP programming language so that it is web-based and uses the OWASP standard until 2017. The system is also capable of displaying application vulnerabilities based on their frequency of appearance.

Corresponding Author:

Yansyah Saputra Wijaya,
Department of Informatic, STMIK Amik Riau, Pekanbaru, Indonesia
Email: yansyahwijaya@stmik-amik-riau.ac.id

1. INTRODUCTION

The development of Information Technology (IT) has become an inseparable part of human life. Badan Siber dan Sandi Negara (BSSN) BSSN states that IT contains strategic information assets and has an impact on the lives of many people so that its role is very important and vital [1]. Besides, IT has triggered the development of Industry 4.0 which is characterized by automation and digitalization to obtain the ease of achieving competitive advantage. This is marked by the development of the Internet of Things (IoT), Artificial Intelligence (AI), robotics, automated physical systems, smart cities, and blockchain [2]. Industry 4.0 provides the integration of large data, interactive systems between humans and machines, and increased communication between digital and physical environments [3]. Moreover, the integration of IT has also brought new issues and challenges, especially in the field of cybersecurity.

Cybersecurity is an activity to protect systems, networks, and programs from digital attacks [4]. Digital attacks or cyber-attacks usually aim at accessing, changing, or even destroying sensitive information, extortion of money, or business process interruption. Cybersecurity consists of technology, processes, and actions designed to protect individuals and organizations from cybercrime. At present implementing effective cybersecurity measures is a very important and challenging activity. There are three pillars in implementing effective cybersecurity, namely people (people), processes (processes), and technology (technology) [5]. If all three are not met, then it will create vulnerabilities that can interfere with cybersecurity. Cybersecurity applies in various contexts, one of which is application security.

According to Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) records 88,414,296 cyber-attacks have occurred from January 1 to April 12, 2020. Out of 88,414,296 cyberattacks, around 884 such attacks are web application based attacks [6], although classified as only a small amount that about 1% of the total attacks, but of course it cannot be underestimated, especially for organizations engaged in finance such as banking. The application security breach for banks is very fatal because it will reduce the level of public trust in the bank so that it affects the value of the company. According to Stefinko, the most popular way to investigate security is through a penetration test (pentest) conducted by an ethical hacker/pentester team [7].

Pentest is a security test conducted by a pentester by mimicking the actual attack to damage the security features of an application, system, or network so that known vulnerabilities [8] [9]. Pentest also becomes an obligation that must be done because it can help companies prevent financial failures and compliance with regulations by regulatory regulations, Peraturan Otoritas Jasa Keuangan (POJK) No. 38/POJK.3/2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks which requires Banks to ensure information security to maintain confidentiality, integrity, and availability effectively and efficiently, one of which is using pentest. Pentest testing must be conducted regularly at least once a year [10].

To determine whether an application is safe and successfully passes the pentest, we need a measurement standard so that all applications get a balanced or equal value. Especially for web applications, the standard commonly used is OWASP (Open Web Application Security Project). When this research was made OWASP with the latest edition which is 2017 which focuses on injection, broken authentication, sensitive data exposure, xxe, broken access control, security misconfiguration, xss, insecure deserialization, using a component with known vulnerabilities, and insufficient logging & monitoring [11]. OWASP has a very large list of vulnerabilities and each vulnerability in OWASP is given a certain code, therefore to simplify the process of monitoring the pentest process in an organization a tool that can visualize existing vulnerabilities of various applications to be more easily measured, calculated, and monitored during the pentest process.

The tool commonly used to present information to managers is a Dashboard [12], the concept of the dashboard has been widely adopted by companies or businesses for various purposes such as administrative dashboards [13], monitoring dashboard [14] [15], evaluation dashboard [16], and even for just visualization [17]. Each dashboard created has its characteristics and objectives according to the needs of the organization, but the basic purpose of all dashboards is only to assist decision-makers in making decisions.

The dashboard created in this research is the monitoring dashboard of pentest activities so that it does not need to be manually recapitulated using data management applications such as spreadsheets (Ms. Excel). The dashboard is made using the PHP programming language so it is web-based and uses the OWASP standard until 2017. It is expected that with this dashboard, it can find out the application vulnerabilities that often arise during the pentest so the results of data visualization can be taken into consideration and evaluation to determine the priority of improvements in application development.

2. RESEARCH METHOD

There are 4 steps undertaken in this research to create a monitoring dashboard, namely data collection, designing system, testing, and implementation, as shown in Figure 1 [18].

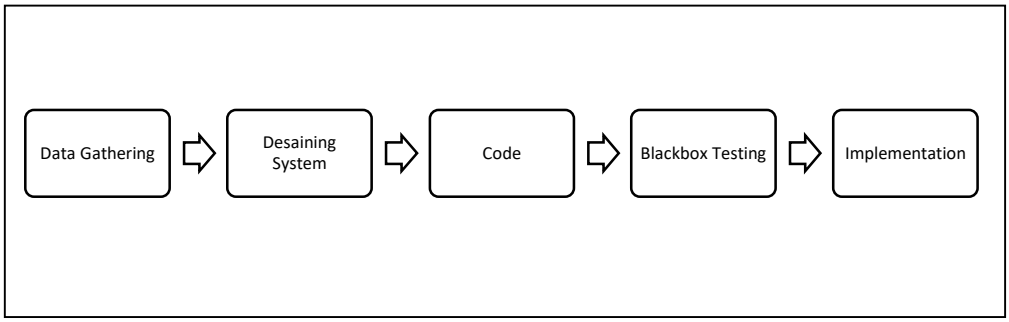

Fig. 1. Research Step.

Stages of research carried out as shown above are divided into several processes, i.e.:

1. Data collection: There are 2 data used in the study, namely the dummy pentest report data that will be used during the implementation process, the second is a list of vulnerability collected from the page owasp.org.
2. System design: Done by designing a dashboard system that will be built later.

3. Code: Making the application will use the PHP programming language and MySQL database.
4. Black box Testing: Dashboard testing will be done using black-box testing to prove that the program runs properly.
5. Implementation: Dummy data that has been prepared previously during the data collection process will be applied to the system.

3. RESULTS AND DISCUSSION

Data collected from Owasp.org is data in 2017 especially OWASP top 10, while for dummy data it consists of 16 applications with a total of 200 vulnerability findings. The next step is to make a design of the system, the system consists of 2 parts, namely the front-end which is useful for the pentester in reporting the results of the pentest into the system, while the back-end part is useful for the stakeholder in doing management, more details can be seen in Figure 2.

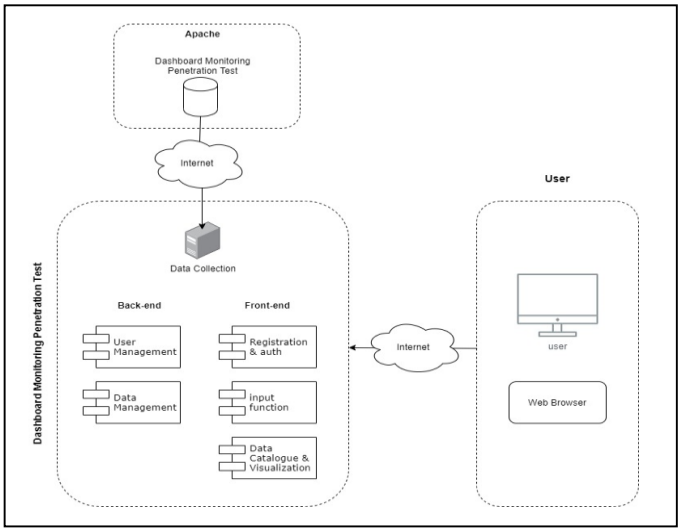

Fig. 2. System Architecture.

A system has an iterative cycle or path, this cycle facilitates interaction between system users. This data cycle and system architecture guide the more detailed system design process.

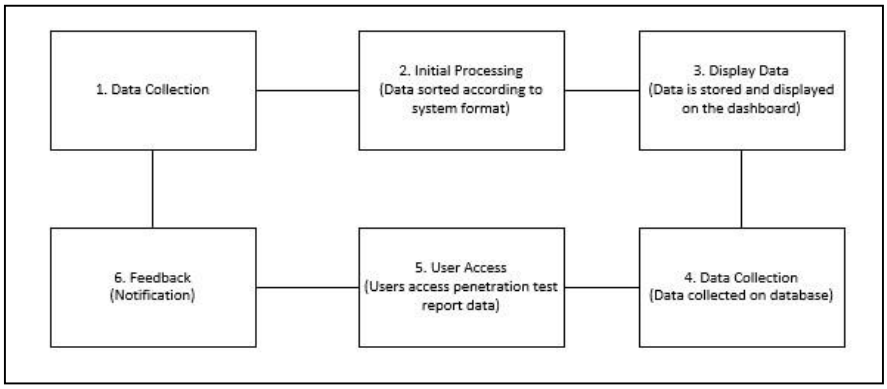

Fig. 3. Data cycle on the pentest report dashboard.

After defining the system architecture and the data cycle, the next step taken is functional mapping to define the system in more detail and depth. Functional requirements are represented by the use case diagram as shown in Figure 4. The features of the system prototype were developed based on the results of functional analysis. Furthermore, the system prototype was developed as a means to test the design and concept of the system that was created. After the prototype is developed, several testing stages will be carried out, such as functional testing. Testing is done using the blackbox system method to ensure that the system can run in an operational environment, meet user needs, and achieve system design goals. To ensure this, several stages of

system testing are carried out following the design of the test, the results of the black box testing are as shown in Table 1. Overall based on the results obtained from the test case system it is found that the expected results are under the objectives of the system functionality.

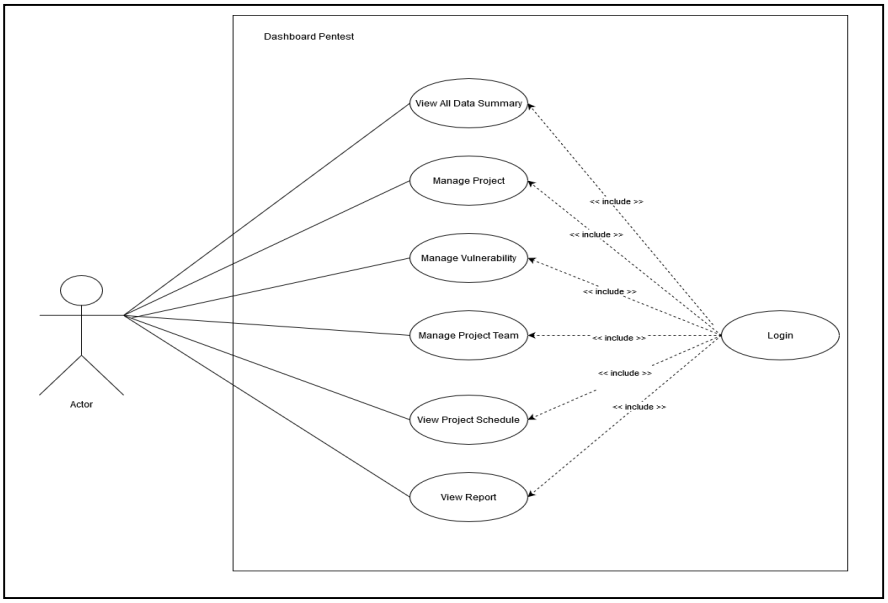

Fig. 4. Functional System.

Table 1. Black-Box testing results

Test Case	Results		
	Expected results	**Results obtained**	**Information**
Login	The system verifies the user	Users who are not registered, cannot enter the system	Succeed
User Registration	The system will save a new user account	The system successfully saved a new user account	Succeed
Displays an overall summary of the data	The system will display the dashboard display	The system displays the dashboard display	Succeed
Showing graph	The system will display a dashboard graphic display	The system displays a dashboard graphic display	Succeed
Manage Projects (add, delete, edit)	The system can execute add, edit and delete commands at a time to manage the project	The system successfully carried out Add/Delete/Edit Project	Succeed
Processing Data Vulnerability (add, delete, edit)	The system can execute add, edit and delete commands at a time to manage the project	The system successfully added/delete/edit vulnerability	Succeed
Manage Users (verify, delete)	The system can make add, edit, and delete commands at one time to manage Users	The system successfully verified/deleted the user	Succeed
Displays project schedule	The system will display the project schedule	The system displays the project schedule	Succeed
Make a report based on data	The system will print the report according to the menu chosen by the user	The system prints the report according to the user	Succeed
Manage project team members	The system will limit the menu available to each member depending on their access rights	The system limits the menu available to each member depending on their access rights	Succeed

Test Case	Results		
	Expected results	Results obtained	Information
Manage Nodin (add, delete)	The system can do incorrect add and delete commands at a time to manage Nodin	The system successfully added/removed Nodin	Succeed

After the system functionality runs as it should, the next step is to implement the dummy data that has been prepared previously into the monitoring dashboard, the following is a dashboard program display using dummy data, as shown in Figures 5 and Figure 6.

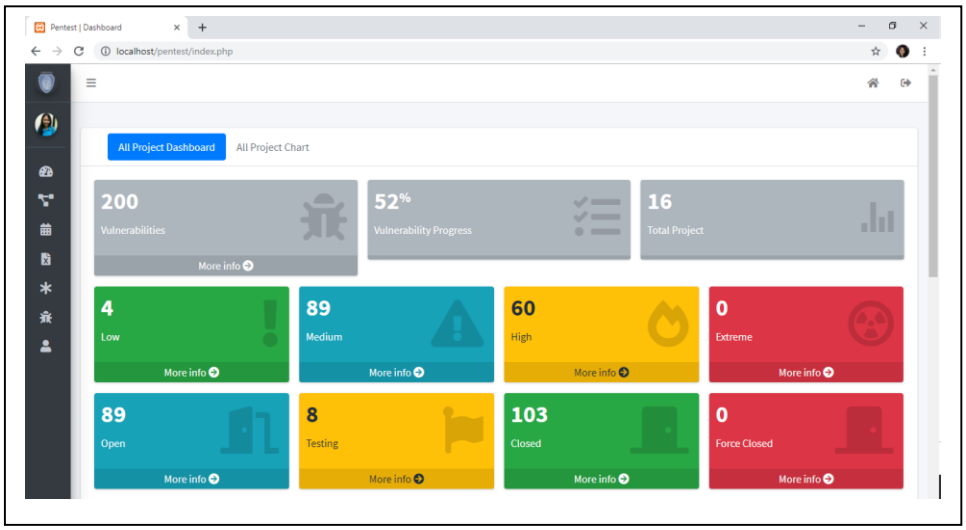

Fig. 5. The home page of the pentest report dashboard system

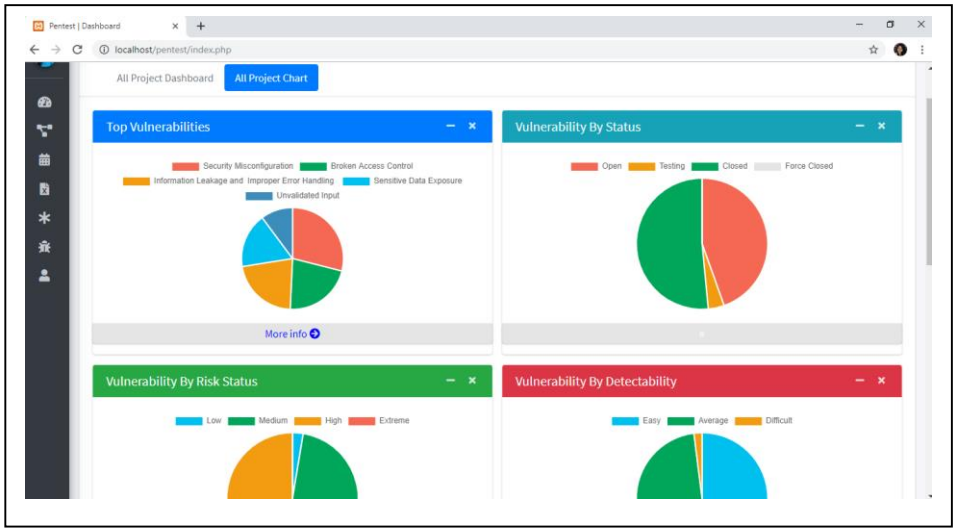

Fig. 6. Detailed display of overall data in graphical form.

4. CONCLUSION

Based on the stages of the research that has been done before, it can be concluded that this study produced a dashboard report dashboard design system. The system can record, manage, and display application vulnerabilities based on the frequency of occurrence. Some suggestions can be given for further research that is displaying other analytical data related to statistics of vulnerability data per week/month/year time period and logs of user activity have not been recorded as a whole, such as who changed the status of a vulnerability from open to close.

REFERENCES

[1] BSSN, "BSSN Selenggarakan National Internet Security Days 2018," *BSSN*, 2018. Online
[2] M. Lezzi, M. Lazoi and A. Corallo, " Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, December 2018, pp. 97-110 doi: 10.1016/j.compind.2018.09.004
[3] A. Ustundag and E. Cevikcan, "Industry 4.0: Managing The Digital Transformation," *Springer Ser. Adv. Manuf.*, no. January, pp. 1–283, 2018, doi: 10.1007/978-3-319-57870-5.
[4] Cisco, "What Is Cybersecurity?," 2019. Online
[5] J. Dutton, "Three pillars of cybersecurity," 2017. Online
[6] BSSN, "Rekap Serangan Siber (Januari – April 2020)," 2020. Online
[7] Y. Stefinko, A. Piskozub, and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," *Mod. Probl. Radio Eng. Telecommun. Comput. Sci. Proc. 13th Int. Conf. TCSET 2016*, vol. 1, pp. 488–491, 2016, doi: 10.1109/TCSET.2016.7452095.
[8] R. E. L. De Jimenez, "Pentesting on web applications using ethical - Hacking," *2016 IEEE 36th Cent. Am. Panama Conv. CONCAPAN 2016*, no. 503, 2017, doi: 10.1109/CONCAPAN.2016.7942364.
[9] NIST 800-115, "Technical Guide to Information Security Testing and Assessment," *Nist Spec. Publ.*, vol. 800, pp. 1–80, 2008. Online
[10] OJK, "Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum." Online
[11] V. Dehalwar, A. Kalam, M. L. Kolhe, and A. Zayegh, "Review of web-based information security threats in smart grid," *2017 7th Int. Conf. Power Syst. ICPS 2017*, pp. 849–853, 2018, doi: 10.1109/ICPES.2017.8387407.
[12] D. Christian, D. Trisnawarman and Z. Rusdi, "Dashboard inventori pt. petra sejahtera abadi," *Jiksi: Jurnal Ilmi Komputer dan Sistem Informasi*, vol. 7, no. 2, pp. 240–244, 2004. Online
[13] S. Sofiana, "Rancang Bangun Dashboard Administrasi Akademik di SMK Fadilah Tangerang Selatan," *J. Inform. Univ. Pamulang*, vol. 2, no. 1, p. 1, 2017, doi: 10.32493/informatika.v2i1.1498.
[14] F. Y. Hartanti, "Rancang Bangun Dashboard Admin Pemantauan Berbasis Web di PT . Astra Graphia Information Technology," 2018, doi: 10.5281/zenodo.1218677.
[15] M. Ropianto, O. Veza, and M. Donald, "Sistem Informasi Dashboard Monitoring Untuk Pengorderan Barang Dan Jasa Pada Pt Energi Listrik Batam," *J. Tek. Ibnu Sina*, vol. 3, no. 1, pp. 1–13, 2018, doi: 10.36352/jt-ibsi.v3i1.107.
[16] F. C. Saputro, W. Anggraeni, and A. Mukhlason, "Pembuatan Dashboard Berbasis Web Sebagai Sarana Evaluasi Diri Berkala Untuk Persiapan Penilaian Akreditasi Berdasarkan Standar Badan Akreditasi Nasional Perguruan Tinggi," *J. Tek. ITS*, vol. 1, no. 1, pp. A397–A402, 2012. doi: 10.12962/j23373539.v1i1.1141
[17] A. Khatulistiwa, H. B. Setyawan, and A. Sukmaaji, "Dashboard Untuk Visualisasi Penjualan Voucher Pulsa Elektrik Di Rajawali Reload Mojokerto," vol. 5, no. 8, pp. 1–7, 2016. Online
[18] Junadhi and Mardainis, "LINE Chatbot Informasi Cuaca Wilayah Indonesia," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 10, no. 1, pp. 101–109, 2019, doi: 10.31849/digitalzone.v10i1.2467.