Design and Development of Information Sharing and Analysis Center (ISAC) as an Information Sharing Platform

Intan Maratus Sholihah, Hermawan Setiawan and
Olga Geby Nabila

November 22, 2021

Design and Development of Information Sharing and Analysis Center (ISAC) as an Information Sharing Platform

***Abstract*— Cyber attacks are the main focus highlighted in all countries globally, both private and public sectors. It is undeniable that every private and public sector has a significant role in the digital world and cybersecurity. It is a reason for every country to improve and develop everything in cyber technology behind defense or attack. One of the solutions offered is to build a platform that can be used to share information to improve a coordinated and structured cybersecurity defense strategy. Data information, a list of attacks and threats can help stakeholders in each sector identify threats, attacks, and incidents in the cyber world. Therefore, this research will develop a web-based Information Sharing and Analysis Center (ISAC) platform to collect information and view a list of attacks and threats in the cyber world. The list of attacks and threats will be obtained through the Malware Information Sharing Platform (MISP). A two-factor authentication method will be implemented on the login form in the development of the ISAC platform. Two-factor authentication is a method used to secure user data from attackers. The research method used in building this platform is Design Research Methodology (DRM) with a prototyping development method. The results of this study obtained an ISAC portal that can be used to share information and display a list of threats and attacks received from the MISP platform.**

Keywords— cyber attacks, cybersecurity, cyber threats, information-sharing

I. Introduction

The development of technology in the world is directly proportional to the increase in cyber-attacks [1]. These cyber-attacks can attack various sectors, both private and public sectors. For example, in Indonesia, based on data from the National Cybersecurity Operations Center in April 2020, there were 19,490,701 cyber-attacks [2]. When compared with the previous year, the number of these attacks increased by approximately six times. It can be seen that in April 2019, there were 3,483,438 cyber-attacks [2]. Meanwhile, in May 2020, there were 16,503,193 cyber-attacks [2]. Although cyberattacks from April to May 2020 can have decreased, there may be more and more dangerous cyber attacks in the future.

It is one of the reasons why we encourage every country to invest more in cyber technology for defense or attack [1]. Therefore, it is necessary to carry out countermeasures to avoid these threats. The solution to overcome this is to improve a coordinated and structured cybersecurity defense strategy by sharing or sharing information about cybersecurity [1]. The information in question is in cyber threats, attacks, countermeasures, attack analysis, and others [1]. This information-sharing activity can benefit the private and public sectors as the most significant concept for overcoming and overcoming cyber-attacks that affect economic development [1]. Every private and public sector is related to the digital world and cybersecurity [3]. Information sharing is one thing that becomes the basis for use as countermeasures [3] to build security success in the digital and cyber world in the public and private sectors. One way to do information sharing is to create an ISAC system. The Information Sharing and Analysis Center (ISAC) is a non-profit organization that provides services to collect information on cyber threats (especially in critical infrastructure) which can later be used for information sharing between the public and private sectors [4].

In ISAC, three strategies can strengthen cybersecurity, including improving and clarifying functional relationships in government, adequate information sharing processes and implementing integration functions, and analysis in deciding cybersecurity planning in critical infrastructure sectors [5]. In Indonesia, ISAC development is one of the priority activities for strengthening cyber resilience and security in Presidential Decree number 61 of 2019 concerning the government's 2020 work plan. Thus, this is in line with the task of XYZ organizational tasks to carry out the preparation, coordination, implementation, control, evaluation, and reporting of technical policies in the field of information security strategy and governance, classified information protection, counter activities. Sensing, information security audits, and measurement of information security governance of nationally critical information infrastructure sectors of energy and mineral resources, defense and strategic industries, and agriculture [6]. Five crucial points must be considered in ISAC: strategy, technology, resources, human resources, management, and economics [3]. Several things must be regarded, one of which is developing a platform for information sharing [3]. Therefore, this research will develop a web-based ISAC platform to collect information and view a list of attacks and threats in the cyber world. The information data, list of attacks, and threats can be used to assist stakeholders in each sector in identifying, assessing, observing, and determining steps in dealing with cyber threats [7].

The list of attacks and threats will be obtained through the Malware Information Sharing Platform (MISP) [7]. This study aims the develop a secure ISAC platform by implementing two-factor authentication. A two-factor authentication method will be implemented on the login form. Two-factor authentication is a method used to secure user data from attackers [8]. This method is applied to the login form to protect the user's username and password before entering the system [9]. This research uses the Design Research Methodology (DRM) research method with a prototyping development method. Based on research conducted by A. Pala and J. Zhuang explained the benefits of ISAC, one of which is to provide knowledge about threats and attacks in the cyber world. This study discusses the implementation of threat and attack data integration taken from the MISP platform [10].

II. Related Works

Solange Ghernaouti, Léonore Cellier, and Bastien Wanner were analyzing the needs and constraints on information sharing to produce cyber security and resilience [3]. Their study recommends the development of a platform for Information Sharing and Analysis. The things needed in the development of the ISAC platform are defining the type of information to be shared, defining the IT infrastructure requirements needed on the ISAC platform, and defining how the information is collected, stored, processed, served, returned, and secured [3].

McCarthy et al. [5] discussed what must be in ISAC, including [5]:

- Provide an effective forum for sharing information in specific sectors with other organizations or governments.
- Provide analysis of relevant threats, vulnerabilities, and incidents.
- Provides features to share threat alerts, threat assessments, and threat notifications with ISAC members.
- Provide a quick response in an emergency effectively by communicating and coordinating among ISAC members.

Based on the four points above, ISAC can function as a platform to communicate cybersecurity in each sector and support information sharing activities between ISAC members and the government and the National Critical Infrastructure (IKN) sector [5]. This study also discusses the scope used for establishing and operating ISAC, namely key services, vulnerability, and threat analysis, incident response, risk assessment, cyber security training, and cyber security working groups. Key services contain the types of vulnerabilities and incidents that can be used for information sharing, the use of information-sharing protocols, the level of threat and vulnerability, and the level of warning indicators [5]. There are five general elements to form an ISAC: the director, the funding model, the collection and distribution of information, the Security Operations Center and the platform used, and the mechanisms used to ensure that the information is received by the rightful and interested people [5].

III. Methodology

In this research, we used Design Research Methodology (DRM). DRM is one of the research methods used to make research designs more effective and efficient [11]. This research uses application development with an SDLC prototyping approach. The application development stages will be included in the DRM process [12].

A. Research Clarification

At this stage, several requirements and indications are collected that support the formulation of the problem and research objectives—in addition, looking for factors related to the factors that affect the classification of tasks and research success. There are key factors and success criteria determined to create an initial reference model. Key factors are factors that are useful for explaining the problems that will be the subject of research. The success criteria is a criterion for achieving the success of the program or research conducted. Preliminary key factor. Preliminary success criteria that were successfully determined were platform information sharing, preliminary measurable criteria were a threat and attack data displayed, and preliminary success criteria were building an effective ISAC platform.

B. Descriptive Study I (DS-I*)*

At this stage, the researcher strengthens the key factors and success criteria that have been determined in the previous step by reading some other literature and conducting interviews with interested parties. After maintaining the key factors and success criteria, the next step is to update the initial impact model by adding factors that affect the key factors or success criteria. Figure 1 shows the success criteria for developing an effective ISAC platform, the measurable criteria is the threat and attack data displayed, and the key factor is the information-sharing platform.

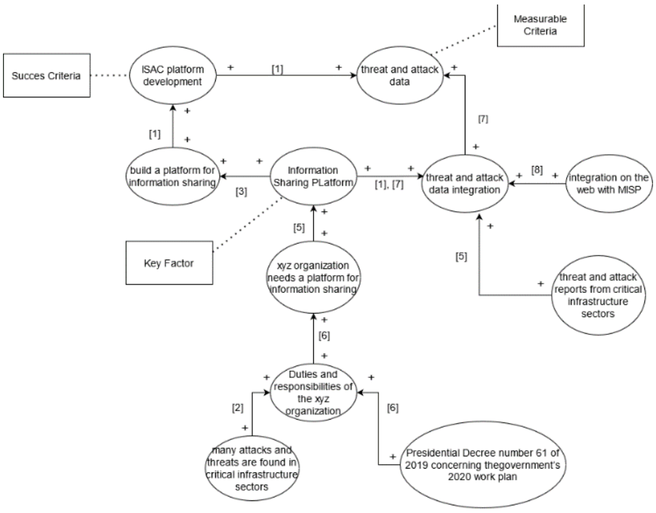

Measurable Criteria
Succes Criteria
ISAC platform development
threat and attack data
build a platform for information sharing
Information Sharing PLatform
threat and attack data integration
integration on the web with MISP
Key Factor
xyz organization needs a platform for information sharing
threat and attack reports from critical infrastructure sectors
Duties and responsibilities of the xyz organization
many attacks and threats are found in critical infrastructure sectors
Presidential Decree number 61 of 2019 concerning thegovernment's 2020 work plan
[1]
[3]
[1], [7]
[7]
[8]
[5]
[5]
[6]
[2]
[6]
+

Fig. 1. Reference Model

C. Prescriptive Study

At this stage, the desired situation description identification is carried out based on the researcher's understanding. This description contains how to solve one or more problems to get the desired result and is developed. After that, the researcher clarified the task and conceptual design, later producing a software concept to support the research problem. The researcher defined the task based on the factors determined at the DS-I stage and from the well-developed description. After that, the researcher implemented the results of the formulation of the problem. Table I shows the stages of system design and development.

TABLE I. Functional Requirements

Stages	Input	Process	*Output*
1. Planning	-	1. Study the system overview. 2. Make a work plan.	1. Work plan. 2. Schematic of the system built.

Stages	Input	Process	*Output*
2. Analysis	1. Work plan. 2. Schematic of the system built.	1. Observing similar systems. 2. Conducting interviews.	1. Functional Needs. 2. Non-functional requirements.
3. Design	1. Functional Needs 2. Non-functional requirements	Create application designs using use case diagrams, activity diagrams, and sequence diagrams using Enterprise Architect.	1. Use case diagrams 2. Activity diagrams. 3. Sequence diagrams.
1. Implementation I	1. Use case diagrams 2. Activity diagrams. 3. Sequence diagrams.	1. Build the system using the Django framework and Visual Studio. 2. Perform application testing.	1. Prototype design. 2. Test analysis results.
2. Implementation II	1. Prototype design. 2. Test analysis results.	1. Build the final system. 2. Perform application testing.	Final application

D. Descriptive Study II (DS-II)

This stage is carried out to determine whether the implemented system has been efficient and effective following the criteria previously defined in the DS-I step. At this stage, the final testing and evaluation of the system that has been developed will be carried out. The final testing process at this stage will be carried out using the black box testing method. In this study, the TOTP function is used, which is a feature of the Django framework. The algorithm used in the TOTP function in Django is the HMAC-based One-Time Password (HOTP) algorithm. The HOTP algorithm stores two pieces of information, including the secret key and the counter. The secret key stores the token and server used to validate the sent OTP code [13]. At the same time, the counter is used as an OTP counter to be validated. HOTP uses the SHA-1 hash function, which produces a 160-bit value which is then reduced to 6 or 8 decimal digits [13]. The token will display the result of the decimal digit. In the TOTP function in Django, the counter used in the HOTP algorithm is time or commonly called timestep. Timesteps are usually 30 to 60 seconds long [13]. Based on this information, each OTP sent can be valid if it is by the timestep [13]. Django itself also has an SSL/HTTPS feature that can be used to build a more secure system. This feature can be enabled by setting SECURE_SSL_REDIRECT to True, so the HTTP feature changes to HTTPS [14].

IV. Design and implementation

A. Planning and Analysis

The planning stage is carried out by conducting literature studies. The Information Sharing and Analysis Center (ISAC) system is a web-based system developed to make it easier to access it from various electronic devices. In general, this ISAC system was created to make it easier for users to share and obtain information related to threats, attacks, and news within the scope of cybersecurity. Informing this ISAC system prototype, the design method includes an overview of the system created, analysis of functional and non-functional requirements, system design, and implementation of the ISAC system prototype.

Functional requirements are requirements related to a process in the system that must be met. Functional requirements are obtained from benchmarking results on ENISA's ISAC products, which then obtains the minimum features in the ISAC product. The data displayed is retrieved from the MISP platform. Malware Information Sharing Platform (MISP) is a platform that contains a list of open-source threats and attacks that can be used by any organization to identify, assess, control, and respond to cyber threats [7]. MISP is an open-source platform that can be used by an organization to store, manage, visualize, and as a means of sharing knowledge about cyber security threats [15]. The primary purpose of the MISP platform is to provide a database of knowledge about cyber threats and cyber operations [15]. MISP is used to display technical information (such as TTP and observations) and non-technical information (such as attribution, victimology, etc.) [15]. MISP data retrieval can be done by integrating with the Application Programming Interface (API). The information data can be modified automatically by the user to produce an attractive data visualization according to the user's needs [15]. The API integration process on MISP can be done with the PyMISP library in the Django framework [15]. After that, a literature study was conducted on the existing aspects. A list of functional requirements was obtained, which is shown in Table II. and non-functional requirements in Table III.

TABLE II. Functional Requirements

ID	Functional Requirements
1	The ISAC platform will provide a page that lists threats that occur within the scope of cybersecurity.
2	The ISAC platform will provide a page of attacks that occur within the scope of cybersecurity.
3	The ISAC platform will provide two-factor authentication on the login form.

Table III shows the non-functional requirements of the ISAC platform. One of them is using two-factor authentication to avoid brute-force attacks, and security tests are carried out using OWASP ZAP [16].

TABLE III. NON-FUNCTIONAL REQUIREMENTS

ID	Non-Fungsional Requirements
1	The application can run well on Mozilla Firefox and Google Chrome.
2	The applications use of Two-Factor Authentication to prevent brute-force attacks.

B. Design

The design stage is carried out based on the functional needs analysis that has been carried out. The steps taken are the same as in the prescriptive study. There are three diagrams, namely use case diagrams, activity diagrams, and sequence diagrams. The following is a use case diagram shown in Figure 2.

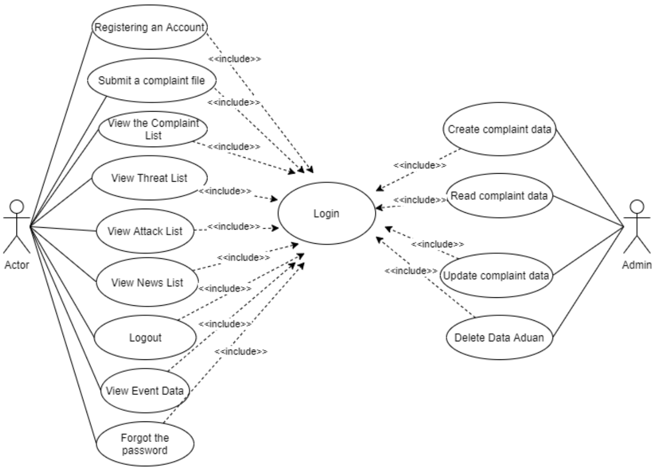


Fig. 2. Use Case Diagram

Based on Figure 3, the user can see the list of threats, and the system will fetch data from the MISP server using API. Next, the system displays a list of threats, and users can view information from the threat data.

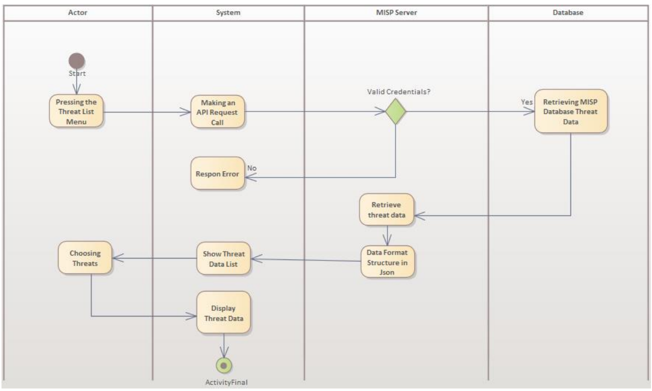


Fig. 3. Activity Diagram of Threat List

Figure 4 describes the relationship between the user and the boundaries of the home page, the threat list page, the MISP server, and the process of storing the MISP database entity.

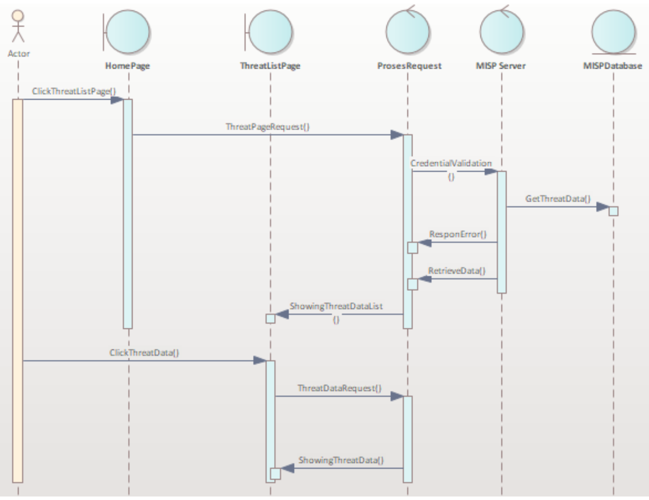


Fig. 4. Sequence Diagram of Threat List

Figure 5 shows a system overview of the ISAC portal. Based on Figure 5, the ISAC system is run using the Django webserver, SQLite database, and data integration using the API from the MISP server. Users can access the ISAC system using a web browser.

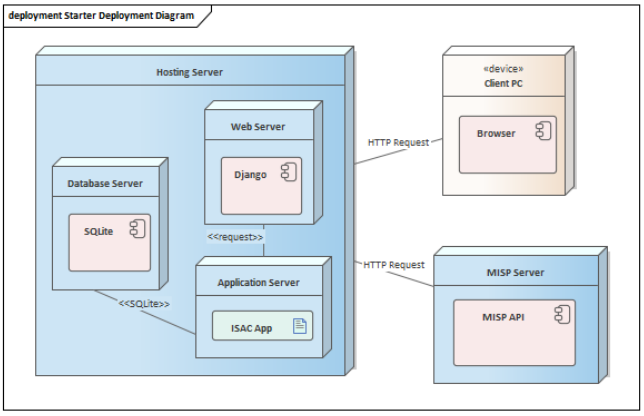


Fig. 5. Deployment Diagram

C. Implementation (Application I)

Figure 6 is a display of the threat list page. On this page, a list of threats will be provided, which will display a description of the threat when clicked by the user. The threat in question is a threat that has the possibility of occurring in cybersecurity. The threat list can only be accessed by the user when they have logged in to the system.

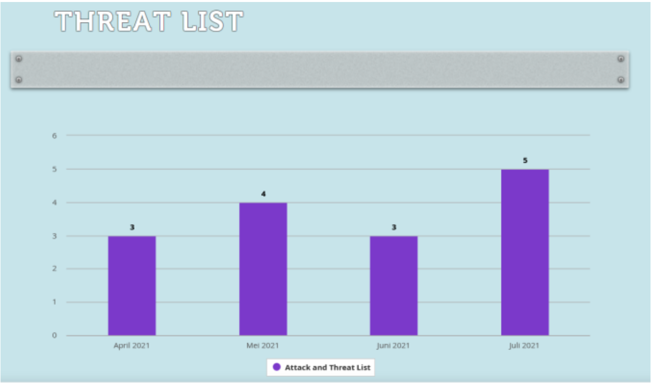
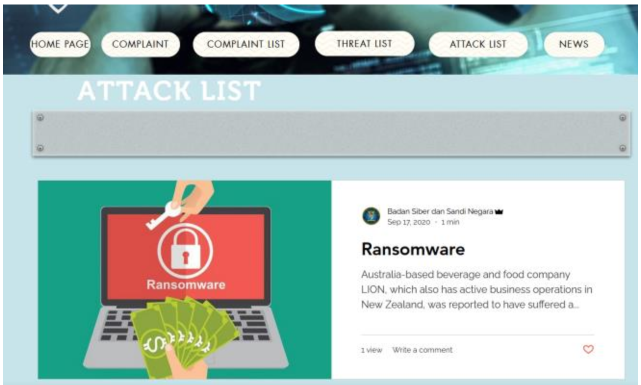


Fig. 6. Threat List Page

Figure 7 is a page view of the attack list from the ISAC system. This page contains a list of attacks that the user can access. When clicked, it will display a description page of the attacks that were accessed. The data displayed is the same as in the threat list, using the API on the MISP platform.



Badan Siber dan Sandi Negara
Sep 17, 2020 · 1 min

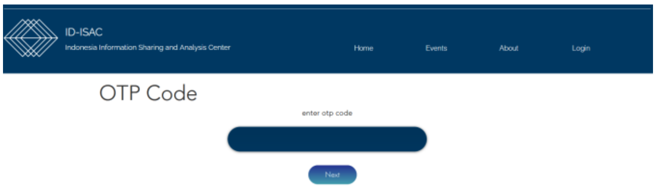
Ransomware

Australia-based beverage and food company LION, which also has active business operations in New Zealand, was reported to have suffered a...

1 view Write a comment

Fig. 7. Attack List Page

Figure 8 shows a two-factor authentication page. The two-factor authentication page is used when the user performs verification when logging in to the system. The OTP code obtained by the user via email can be entered in the OTP code column. After the user presses the submit button, the system will verify whether the code entered is correct. If appropriate, the system will display the home page.



OTP Code

enter otp code

Fig. 8. Two-Factor Authentication Page

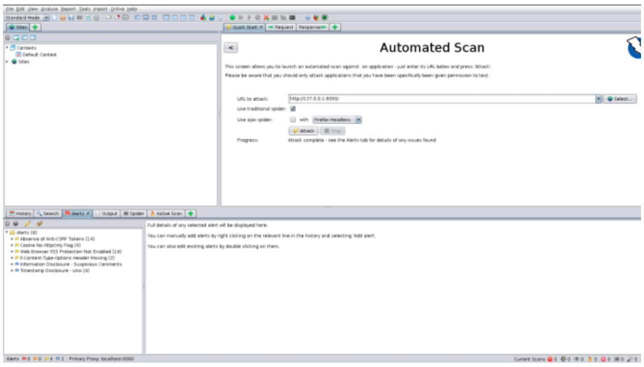
V. Testing

Testing is carried out using the black-box testing method, which focuses on functional requirements by the software use case and security testing. Table IV shows an example of the test results of three successful features.

TABLE IV. Aspects of black-box testing

No	Field	Testing Scenario	Expected results	Test result	Information
1	Field email (login & registration form)	Doing input with the valid email format	Display the home page or main page	as expected	succeed
		Doing input with an invalid email format	Showing a pop-up “Invalid email.”	as expected	succeed
2	Field password (login)	Doing input with the valid password	Display the home page or main page	as expected	Succeed
		Doing input with the invalid password	Showing a pop-up “invalid password.”	as expected	Succeed
3	Complaint field	Perform input in the form of a combination of letters, numbers, and symbols.	Showing a pop-up “error complaint.”	as expected	Succeed
		Input documents in .pdf, .doc and .docx formats.	Showing a pop-up “complaint sent”	as expected	Succeed

Security testing is carried out using OWASP ZAP tools by checking the entire system. Based on the manual issued by the OWASP Foundation, it is explained that multi-factor authentication can be used to avoid brute-force attacks [16]. The following are the results of scanning using the OWASP ZAP tools shown in Figure 9. There are a total of four vulnerabilities with details of two low vulnerabilities and two informational vulnerabilities. Two low vulnerabilities include Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS). In this test, we found Cross-Site Request Forgery (CSRF) twice on the news and home pages. This can be prevented by ensuring that the library or framework used does not have the vulnerabilities that cause these vulnerabilities to appear [17]. Cross-Site Scripting (XSS) occurs on news pages; to overcome this vulnerability countermeasures can be made by setting the response header from X-XSS-Protection HTTP to ‘1’ [17]. Two informational exposures consist of Information Disclosure – Suspicious Comments and Timestamp Disclosure. Information Disclosure Vulnerability – Suspicious Comments can be avoided by removing all comments that might help attackers access the system [17]. Timestamp disclosure vulnerabilities can be avoided by manually confirming that the data is not sensitive so that the data cannot be used to display exploitable patterns [17]. Based on the test results, several vulnerabilities still appear, but no exposures can trigger brute-force attacks.



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://127.0.0.1:8000/
Use traditional spider: ☑
Use ajax spider: □ with Firefox Headless
Progress: Attack complete - see the Alerts tab for details of any issues found

Alerts (6)
- Absence of Anti-CSRF Tokens (14)
- Cookie No HttpOnly Flag (4)
- Web Browser XSS Protection Not Enabled (16)
- X-Content-Type-Options Header Missing (2)
- Information Disclosure - Suspicious Comments
- Timestamp Disclosure - Unix (4)

Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

Alerts 0 0 4 2 Primary Proxy: localhost:8080

Fig. 9. OWASP ZAP Scan Results

VI. CONCLUSION

The MISP platform integration has been successfully carried out, and data from the platform can be displayed by integrating the website with the MISP API. Server running on the Ubuntu 20.04 LTS Virtual Machine. The implementation of two-factor authentication using OTP sent via email and the TOTP function, a two-factor authentication feature of the Django framework, was successfully carried out. The results of the security testing test have four vulnerabilities that have information, two of which are low, and the other two are informational. Based on the security testing, the implementation of two-factor authentication can be said to be successful. In future research, integration with the OpenCTI platform can be carried out so that it can display threat and attack data in real-time. The information-sharing feature still uses a simple data-sharing scheme for further research. It can be developed using the STIX/TAXII format. Add user grouping according to public sector and private sector.

REFERENCES

[1] A. Pala and J. Zhuang, "Information sharing in cybersecurity: A review," Decis. Anal., vol. 16, no. 3, pp. 172–196, 2019, doi: 10.1287/deca.2018.0387.

[2] "Jumlah Serangan Siber Meningkat." .

[3] S. Ghernaouti, L. Cellier, and B. Wanner, "Information sharing in cybersecurity : Enhancing security, trust and privacy by capacity building," 2019 3rd Cyber Secur. Netw. Conf. CSNet 2019, pp. 58–62, 2019, doi: 10.1109/CSNet47905.2019.9108944.

[4] ENISA, Information Sharing and Analysis Centres (ISACs) Cooperative models. 2017.

[5] C. McCarthy, K. Harnett, A. Carter, and C. Hatipoglu, "Assessment of the Information Sharing and Analysis Center Model," Nhtsa, no. October, 2014.

[6] B. S. dan S. N. R. Indonesia, "Peraturan Badan Siber Dan Sandi Negara," Bssn, vol. 1, no. 9, p. 20, 2019.

[7] K. Rantos, A. Spyros, A. Papanikolaou, A. Kritsas, C. Ilioudis, and V. Katos, "Interoperability challenges in the cybersecurity information sharing ecosystem," Computers, vol. 9, no. 1, pp. 1–17, 2020, doi: 10.3390/computers9010018.

[8] K. Reese et al., "A Usability Study of Five Two-Factor Authentication Methods This paper is included in the Proceedings of the," pp. 357–370, 2019.

[9] R. U. S. A. Data, "(12) Patent Application Publication (10) Pub . No .: US 2015 / 0258769 A1 lifted-off layer Patent Application Publication," file///Users/paulinamohring/Desktop/UNI/MSc IMM CPH/Semester 3/SMM/Predicting ROI Sport Spons. - Formula 1.pdf file///Users/paulinamohring/Desktop/UNI/MSc IMM CPH/Semester 3/SMM/Sport Spons. Relatsh. Between Team Loyal. Spons., vol. 1, no. 19, pp. 0–4, 2015.

[10] A. Pala and J. Zhuang, "Information sharing in cybersecurity: A review," *Decis. Anal.*, vol. 16, no. 3, pp. 172–196, 2019, doi: 10.1287/deca.2018.0387.

[11] P. Taylor, D. C. Chou, and A. Y. Chou, "a Manager ' S Guide To," vol. 1, no. March, pp. 37–41, 2006.M. J. Kwon, G. Kwak, S. Jun, H. J. Kim, and H. Y. Lee, "Enriching Security Education Hands-on Labs with Practical Exercises," *Proc. - 2017 Int. Conf. Softw. Secur. Assur. ICSSA 2017*, pp. 100–103, 2018, doi: 10.1109/ICSSA.2017.8.

[12] A. C. Lucienne T.M. Blessing, *DRM, a Design Research Methodology*, vol. 7, no. 2. London: Springer, 2009.

[13] "Implementing 2FA in Python Django using Time-Based one-time password (TOTP) - https://pythoncircle.com." https://pythoncircle.com/post/731/implementing-2fa-in-python-django-using-time-based-one-time-password-totp/ (accessed Aug. 23, 2021).

[14] "MISP features and functionalities." https://www.misp-project.org/features.html (accessed Aug. 24, 2021).

[15] "Security in Django | Django documentation | Django." https://docs.djangoproject.com/en/3.2/topics/security/ (accessed Aug. 31, 2021).

[16] O. F. This, C. C. Attribution-sharealike, O. Testing, and O. Foundation, "Owasp testing guide 2008," 2008.

[17] "OWASP ZAP." https://www.zaproxy.org/docs/alerts/10096/ (accessed Aug. 23, 2021).