CHAPTER I
INTRODUCTION

1.1 Background

The development of information technology globally has experienced an extraordinary surge in the form of innovation in artificial intelligence (AI) and the Internet of Things (IoT) which makes human life easier (Aditya Ahmad Fauzi et al., 2023, p.8). The use of the superfast 5G network allows the door to be opened for more sophisticated and revolutionary solutions (Fahreizy & Daulay, 2023). Laudon (as quoted in Hendarsyah, 2019) explained the importance of using website applications to reach a wide range.Web applications have a major rolein facilitating access and use of modern information technology by providing a platform for various services and functions, from e-commerce to social media, as well as integrated business applications (Kurniawan et al., 2023). According to the 2023 Internet Penetration and Behavior Survey, many Indonesians use the internet to access various online services such as social media, news information, online transactions, education and online transportation. Many of these services use website applications as their main platform to maximize the potential of information technology that continues to develop.

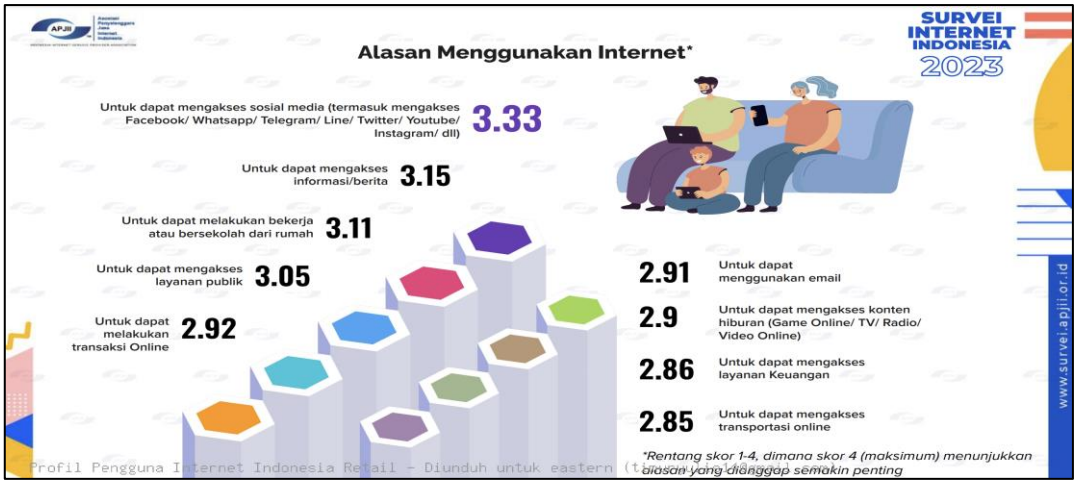

Figure 1.1 2023 Internet User Behavior & Penetration Survey
Source: APJII (2023)

In Indonesia, the use of website applications in the government sector has brought about a significant transformation in the provision of public services and management of state administration (Kesumadewi, 2019).

Various online platforms have been introduced to facilitate citizens' access to various government information and services. According to Kesumadewi (2019), website applications also play an important role in facilitating government transparency and accountability, enabling citizens to monitor and supervise government activities more openly. Through the use of website applications, the Indonesian government sector is experiencing an important digital transformation in an effort to improve the quality of public services and administrative efficiency (Kesumadewi, 2019)

The Indonesian Navy, as an important component of government, actively utilizes information technology in various operational and administrative aspects (Fadli et al 2022). The Indonesian Navy has developed an online platform to facilitate access and management of various information related to maritime activities and sea defense. Through the website application, the Indonesian Navy can provide actual information regarding their operations, personnel training and maritime security in Indonesian waters. Besides that,The use of strong and secure information technology in the Indonesian Navy can significantly improve performance in carrying out national defense at sea and can minimize risks from maritime threats. (INenda, 2019).

Apart from providing many benefits, using website applications also has risks to be aware of, especially those related to information security. The use of website applications carries significant risks to aspects of information security in the form of Confidentiality, Integrity and Availability (Aryandi et al, 2021)explains the risks from the confidentiality aspect, website applications that are not secure enough can threaten data confidentiality. If an attack manages to penetrate the system, sensitive information such as user personal data or financial information can be stolen or exploited. This can result in identity theft, data breach, or even illegal access to confidential information. In the integrity aspect, attacks on data integrity can change or damage information stored in website applications. As a result, the level of trust in the authenticity and accuracy of data will decrease as a result of data manipulation by unauthorized parties. For example, SQL injection attacks can cause data manipulation in an application's database. Threats to the availability aspect of website applications can result in downtime or the inability of users to access

services. DDoS (Distributed Denial of Service) is an example of an attack that aims to flood a server with traffic thereby causing the service to become inaccessible to legitimate users (Sudirman, 2023).

Based on the OWASP Top 10 for 2021, there are a number of main risks that must be identified and overcome in the development and use of website applications. MethodologyevaluationOWASP risk is a simple approach to quantify and assess the risks associated with applications (Setiawan*et al*,2023).

Figure 1.2 OWASP Top 10-2021
Source : OWASP (2021)

Based on the Indonesian Navy's security perimeter data, there were a total of 2,720,027 attacks detected from February 2022 to September 2023 which were divided into 11 types of attacks with the highest number dominated by HTTP Signature violations where the attacks attacked the http protocol used by website applications. (BSSN, 2022)

Based on identification and searching using the Google dorking method with the keyword site: "*tnial.mil.id" "gacor" OR "togelonline" OR "slot" getting 290 search results. This can also mean that there were 290 cases of defacement attacks on the TNI Forces website One of the causes of this incident was the use of a plugin that was no longer updated and malware infection on the Indonesian Navy's computer server. The defacement attack on the Indonesian Navy's website was part of the 2,348 web defacement cases

that occurred on the website. Indonesian site with 290 cases in the defense sector in 2023.

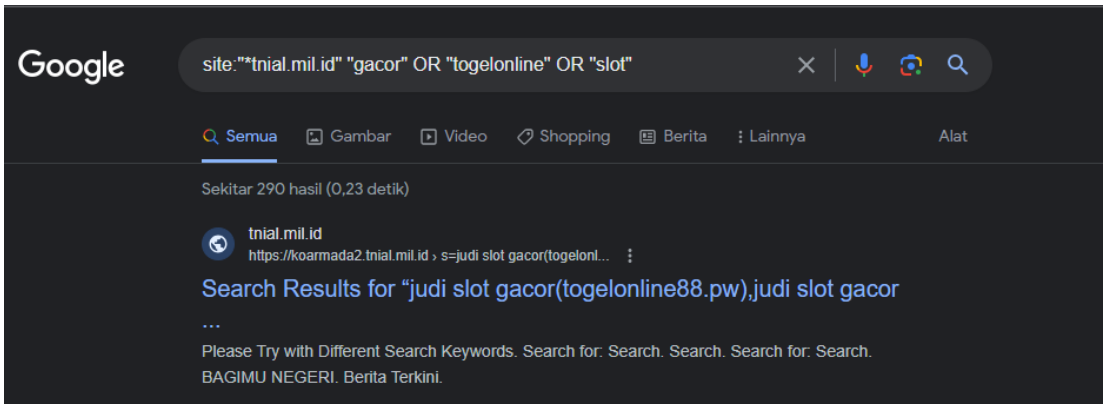

Figure 1.3 Google Dorking Attackweb defacementIndonesian Navy website
Source: processed by researchers (2024)

The site https://www.zone-h.org/ records that 64 cases of defacement have occurred at sites belonging to the Indonesian Navy since 2007 with 45 cases occurring between 2019 and 2023. https://www.zone-h .org/ is a website that contains data on sites that have been affected by defacement attacks.

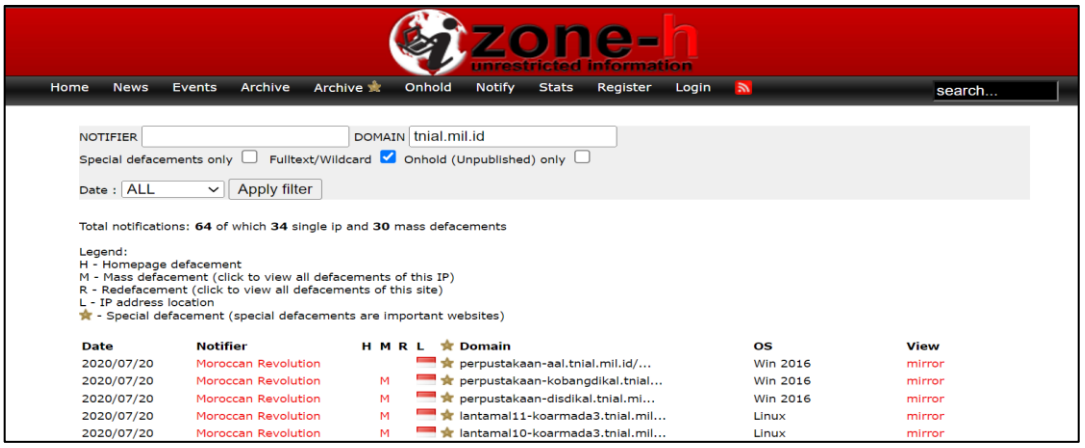

Figure 1.4 Zone-H Attack SitedefacementIndonesian Navy website
Source: processed by researchers (2024)

To overcome the risks and vulnerabilities in the website application is to implement a Web Application Firewall (WAF). Web Application Firewall according to (Sepczuk, 2023)is a system that checks traffic on web applications to filter out potentially dangerous content (Harris, 2021, p.363). Due to its separate location fromweb applications, WAF provides an additional layer of defense that can be tuned independently without having to reconfigure the web application (Harris, 2021, p.363). According to Chapple

(2020, p.77) WAF is a firewall specifically designed to protect website applications from attacks such as SQL Injection and XXS. Chapple (2020, p.495) also explains that WAF can be a defense layer solution if it is not possible to patch website applications.

Harris (2021, p.105) explains four categories of software licenses which include freeware, shareware, commercial and open source. Freeware is software that is publicly available for free and can be used, copied, studied, modified and redistributed without restriction. Shareware is software used by vendors to market their software where users get a free trial version of the software and after the user tries the program, the user is asked to purchase a copy. Commercial software is software that is sold or presented for a commercial purpose. Open source applications are software provided for academic purposes at low cost. Like other software, WAF has a commercial version that requires users to purchase a license and is open source. According to the ISO 27001 Standard, every organization is required to manage planned changes and map the consequences of undesirable changes and implement the necessary actions to mitigate the worst possible impacts. The Indonesian Navy itself has implemented WAF Imperva which is included in the commercial WAF category to protect its websites. The obligation to purchase a license for a commercial WAF places a fairly high financial burden on the organization, in this case the Indonesian Navy. In addition to burdens related to implementation costs, the Navy must also consider the costs of license renewals and regular security updates, which can be important factors in long-term IT management. Based on the problems above, one alternative to overcome this problem is to use WAF-based*open source*.One example of a ModSecurity WAF is ModSecurity. The use of WAF with its open source nature means that the features of ModSecurity can be adapted to the needs of the relevant agency to strengthen the security of web applications by minimizing the cost of extending the license. In this research, the author developed WAF ModSecurity which was integrated with YARA Rules to increase the ability to automate detection and appropriate mitigation for malware that could harm the Indonesian Navy Website. It is hoped that this research can provide an alternative solution for managers of the Navy's

vital information infrastructure in providing security perimeter backup using WAF ModSecurity technology but still paying attention to security aspects on the Indonesian Navy Website.

1.2 Identification of problems

Based on background behindproblem above, a problem was identified, namely that there was a research gap related to the condition of Information Security in the Indonesian Navy with the following details:

a. Cyber attacks on the Indonesian Navy website are quite high
b. One of the web server security in the Indonesian Navy with a website security system using WAF Imperva is hampered by large maintenance costs.
c. There is no additional solution that can act as a backup when the security services provided by WAF are cut off due to non-renewal of the license.
d. ModSecurity has limitations in handling rules only for the OWASP top 10, it requires detecting malware attacks and mitigating these malware attacks.
e. ModSecurity has limitations in detecting shell uploads or malware so it is necessary to add functions related to integrity checking using YARA Rules.

1.3 Restricting the problem

The boundaries of the problem are made in such a way as to not deviate from the problems that have been considered and can draw correct conclusions, therefore the authorlimit the problem as follows:

a. The research object is limited only to the use of WAF for technical control.
b. The research object does not interfere with the production server.
c. The information system that will be attacked is a website prepared by researchers with source code and a database that is identical to the Indonesian Navy website.
d. Development was carried out by researchers and testing was carried out by the Indonesian Navy's Satsiber.
e. The test is a simulation of an attack with the target, namely the Indonesian Navy's website being tested.
f. Developed WAF using ModSecurity.
g. The WAF that will be compared is the Imperva WAF which is currently

used by the Indonesian Navy.

h. *Dashboards*The SIEM used is Wazuh SIEM.

i. Use of malware detection based on YARA rules.

1.4 Formulation of the problem

Based on the attack data in Table 1.1, there was a cyber attack on the Indonesian Navy website. Based on the problem formulation, the research questions are as follows:

a. How to develop WAF with*ModSecurity* as one solution to mitigate attacks againstwebsiteIndonesian Navy?

b. How to develop WAF ModSecurity by comparing the performance of WAF Imperva and WAF ModSecurity systems against SQL Injection, XSS and Malware attacks?

c. Howdevelop*customize*WAF ModSecurity to improve the detection and mitigation capabilities of handling Malware attacks?

1.5 Research purposes

The objectives of this research are as follows:

a. Can mitigate attacks on Indonesian Navy websites with the development of WAF ModSecurity.

b. Can analyze the comparison regarding the performance of the WAF Imperva system with WAF ModSecurity in detecting and mitigating SQL Injection, XSS and Malware attacks on the Indonesian Navy website.

c. Increased malware detection capabilities on the Indonesian Navy Website.

1.6 Benefits of research

1.6.1 Benefits of Scientific Development

With research regarding the development of WAF ModSecurity by adding integrity checking functions and signature-based malware detection. It is hoped that this will make it easier for the Security Operation Center (SOC) team to understand the types of malware attacks and the mitigation required. This malware detection system is signature-based which allows adding ModSecurity WAF performance to detect malware that enters the Indonesian Navy's web server based on signature-based YARA rules.

1.6.2 Benefits of Research for Organizations

a. For the Indonesian Navy. Can be used as a security system detection and protection tool against Indonesian Navy cyber attacks.
b. For the Indonesian Navy. Provide information and references in policies related to system maintenance cost savings.
c. For the Indonesian Navy. Contribute to supporting system backup for existing system security

1.6.3 Benefits of Research for Writers

Providing contributions and references for researchers in completing the literature regarding the application of WAF Imperva and WAF*ModSecurity* on system security management in the field of information security in the Indonesian Navy or in other organizations.