CHAPTER V

CONCLUSION, IMPLICATIONS AND RECOMMENDATIONS

Based on the test results, there are several findings related to research on preventing cyber threats with WAF modsecurity on the Indonesian Navy's information system. Some of these findings include:

a. In the attack detection process, WAF Imperva has a tendency to be stricter in categorizing SQL injection and XSS attacks when compared to WAF ModSecurity.

b. When looking at security control, WAF ModSecurity has a better percentage when compared to WAF Imperva. However, if analyzed and reviewed further based on permitted attacks, WAF Imperva is able to recognize changes in the behavior of the penetration tester when launching an attack, which cannot be done by WAF ModSecurity which only relies on identification based on SQL injection or XSS signatures.

c. False positive diagnosis results were found on WAF Imperva and WAF ModSecurity. On Imperva WAF, false positives do not have a significant impact and are only informational because they occur when response code 404 appears. Response code 404 appears as an indication of information gathering by the penetration tester targeting the website directory. In ModSecurity WAF, a false positive occurs when an XSS attack payload is identified as a SQL Injection attack and is not blocked.

d. In the malware detection process, WAF Imperva has a better percentage when compared to WAF ModSecurity which is integrated with YARA rules.

e. In the malware blocking process, WAF Imperva has a higher number of malware blocks when compared to WAF ModSecurity. However, WAF Imperva cannot respond when malware manages to escape the block and enter the system. This is different from WAF ModSecurity which is integrated with YARA rules, where even if the malware manages to escape the block, the YARA rules will be active to identify the malware signature which then carries out malware quarantine.

5.1. Conclusion

Based on several analyzes and findings above, conclusions can be drawn, including:

a. Based on the relationship between the test results and the opinions of previous researchers and the results of research development related to WAF ModSecurity which was integrated with Yara Rules, it succeeded in mitigating attacks on the Indonesian Navy Website.

b. Based on test results, the ModSecurity WAF development was successful in mitigating attacks launched on websites belonging to the Indonesian Navy as proven by blocking 90.84% of SQL injection attacks and 99.94% of XSS attacks, this shows that the use of Modsec increases detection results by a percentage of 0.16 % SQL Injection and 2.40 % XSS attacks from Imperva WAF currently. Apart from that, the results of comparing performance with WAF Imperva show that WAF ModSecurity succeeded in carrying out the main function of WAF in identifying signatures for SQL injection and against malware attacks.

c. Based on test results, the development of WAF ModSecurity which is integrated with YARA rules can detect and mitigate malware that manages to escape the block and enter the server by implementing malware quarantine. It is hoped that this research can be an alternative in mitigating malware attacks on the Indonesian Navy Website.

5.2. Implications

Based on the research results, several problems were found, the implications that arise if WAF ModSecurity is not developed are:

a. Regarding the high cost of procurement and maintenance of WAF Imperva, the development of WAF ModSecurity to mitigate attacks on Indonesian Navy websites, if not implemented, will result in the loss of attack mitigation capabilities on websites which could endanger the confidentiality, integrity and availability of information if the WAF Imperva license is not renewed.

b. Not developing WAF ModSecurity also has implications for the absence of an additional layer of protection behind the Indonesian Navy's firewall

which specifically provides protection for websites.

c. The failure to develop WAF ModSecurity also has implications for the Indonesian Navy's website being affected by malware injection, which has become increasingly common lately.

5.3. Recommendations

5.3.1 Theoretical Recommendations

The development of ModSecurity WAF with YARA rules integration still has shortcomings that need to be corrected for development in further research. The following are suggestions for this development:

a. A mechanism needs to be added to detect changes in penetration tester behavior in carrying out attacks.

b. Development of ModSecurity WAF with YARA rules integration in Windows Server environment.

c. Integrate ModSecurity WAF with YARA rules integration in the Security Orchestration, Automation, and Response (SOAR) system to respond to security threats more efficiently.

d. Further research needs to be done to measure WAF performance and its impact on server resources.

5.3.2 Implementation Recommendations

In order to optimize the implementation of WAF ModSecurity with YARA rules integration, the following are suggestions for implementation:

a. If it will be implemented on a high risk system, it is recommended to add a security perimeter in the form of a Next Gen Firewall to optimize the performance of the ModSecurity WAF with the integration of YARA rules.

b. The active role of security analysts is to routinely check security events from WAF ModSecurity to identify the emergence of false positive alarms.

c. So that security engineers actively make additions or changes to YARA rules to optimize the malware detection process.