In Deep Security Management Strategy: Vulnerability Assessment Within Educational Institution

Conference Paper · August 2023

DOI: 10.1145/3592307.3592326

Muharman Lubis
Telkom University
251 PUBLICATIONS **1,474** CITATIONS

In Deep Security Management Strategy: Vulnerability Assessment Within Educational Institution

Syailendra Alzana Putra*
Information System Department,
School of Industrial and System
Engineering,
Telkom University,
Indonesia
syailendraalzana@student.telkomuniversity.ac.id

Muharman Lubis
Information System Department,
School of Industrial and System
Engineering, Telkom Univeristy,
Indonesia
muharmanlubis@telkomuniversity.ac.id

Rd. Rohmat Saedudin
Information System Department,
School of Industrial and System
Engineering, Telkom University,
Indonesia
rdrohmat@telkomuniversity.ac.id

ABSTRACT

Technology is developing rapidly along with the times; one example of technological developments is the development of the use of websites in daily activities. Many institutions and entities have utilized the use of websites to support their business processes. For example, one of the faculties of XYZ University has used a website to help with administrative activities. One of the websites of the faculties at XYZ University is the final assignment proposal dashboard website which contains plots of the final assignment supervisor and the title of the final assignment. However, with the development of a technology, the development of vulnerabilities or attacks against the technology also increases. Therefore, it is necessary to carry out a vulnerability assessment method to be able to find out the vulnerabilities that exist on a website and also solutions that can be implemented to overcome these vulnerabilities. In this study, a vulnerability assessment will be carried out on the XYZ University students' final project proposal dashboard website using Nmap and Acunetix tools. The accuracy level of nmap is 13.25%, while Acunetix has 100% accuracy with the results obtained after the vulnerability assessment process, namely there are 12 vulnerabilities on the XYZ University student final project proposal dashboard website with Nmap detecting 3 medium risk vulnerabilities and 1 low risk vulnerability while Acunetix managed to detect 2 medium risk vulnerabilities and 6 low risk vulnerabilities

CCS CONCEPTS

• **Security and privacy**; • **Network security**; • **Networks**; • **Network architectures**; • **Formal methods and theory of security**;

KEYWORDS

Vulnerability assessment, Cyber security, Digital enterprise, Website, Nmap, Acunetix

ACM Reference Format:
Syailendra Alzana Putra*, Muharman Lubis, and Rd. Rohmat Saedudin. 2023. In Deep Security Management Strategy: Vulnerability Assessment Within Educational Institution. In *2023 The 6th International Conference on Electronics, Communications and Control Engineering (ICECC 2023), March 24–26, 2023, Fukuoka, Japan.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3592307.3592326

1 INTRODUCTION

Both the consumers of information technology and their development are expanding quickly. Technology may be employed in a variety of fields, including education, governance, and health. There is also a system that will monitor the supply of clean water, which demonstrates how far technology has come in recent years. [1] [2]. The case of technological developments in this study is the use of websites to support learning activities. Website is a collection of publicly accessible web pages. Websites can consist of text, images, videos, and other sound media. The development of these technologies also led to the emergence of new studies [3]. However, with the development of a technology, the development of vulnerabilities or attacks against the technology also increases. According to Privacy Rights ClearingHouse, cyber attacks recorded in 2017 have reached more than ten billion [4]. Based on the annual cyber security monitoring report for 2021 by the National Cyber and Crypto Agency of Indonesia, there have been more than 1.6 billion cyber attacks that have occurred in Indonesia.

XYZ University, which is one of the universities in Bandung, has used the website to be able to assist faculty administration activities such as practical work administration, laboratory assistant recruitment, and specialization administration. One of the websites at XYZ University is the final project proposal dashboard website.

With the importance of data security on the final project dashboard website, the final project dashboard website needs to be kept safe from existing vulnerabilities and threats. To deal with this, the management of information security on the final project dashboard website needs to be improved. One way to detect existing vulnerability risks is by conducting a vulnerability assessment. Identifying existing threats is very important for the entire computer network or the web to describe how secure a device and the web are based on the number of identified vulnerabilities.

In this study, a vulnerability assessment was carried out on the website dashboard final project managed by XYZ University. In the vulnerability assessment process, the methods used were host-based scanning and web app scanning using Acunetix because it can detect up to 7000 vulnerabilities and can scan all pages. and web apps. Another tool used is nmap because this tool is well documented and updated regularly so that it can detect the latest

ICECC 2023, March 24–26, 2023, Fukuoka, Japan

ACM ISBN 979-8-4007-0000-2/23/03…$15.00
https://doi.org/10.1145/3592307.3592326

vulnerabilities, besides that this tool has many features that can be used to find vulnerabilities on a website and has received many awards, one of which is Information. Security Product of the Year from Linux Journal.

The results of this study can be used as an initial step to overcome the vulnerabilities found on the website dashboard of XYZ University final student project proposal dashboard by identifying vulnerabilities on the website. In further research, penetration testing can be carried out on each vulnerability and fixing each existing vulnerability.

2 METHODOLOGY

The methodology used in this study refers to research systematics whose stages are explained in a systematic and structured manner so that it will make it easier to achieve the research objectives. An evaluation of the problem's vulnerabilities using Nmap and Acunetix is the methodical remedy, The framework used as reference in this study uses the infinity framework that based on target orientation, may keep track of security measures implemented and scan the network for weaknesses., NIST framework that discuss using business goals to focus cybersecurity activities and include cybersecurity risks in risk management processes for the company and also IETF RFC 6632 that discuss management technologies and data models with the Infinity framework as shown in figure 1 [5] [6].

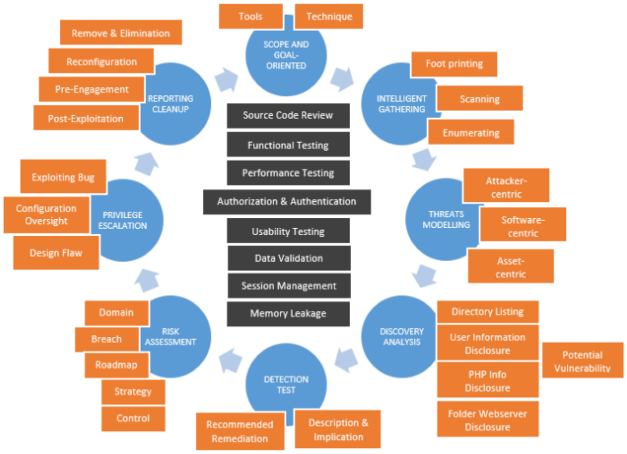


Figure 1: Infinity framework

The reason for choosing acunetix is because acunetix has various features that can be used to scan for vulnerabilities on websites, these features include: Vulnerability Detection, Acusensor, Acumonitor, Target finder, and Subdomain scanner. While nmap was chosen because it has won various awards such as the LinuxQuestions.Org Security App of the Year award and Info World's 1998 Best Information Security Product award, nmap is also capable of being used as a network inventory tool and mapping IP, ports and services as well as detecting vulnerabilities on the network. which implement host-based scanning and web application scanning methods. The two tools also use different methods for their scanning scope but still interconnected. The host-based scan on nmap focuses on scanning for vulnerabilities at the network level. Meanwhile, on the web application scan on acunetix focus to scan websites at the application level [7]. Therefore, it will scan at two different levels but are still interconnected with each other. In the vulnerability assessment, there are five stages, namely the problem identification stage, the problem formulation stage, the data collection stage, the analysis stage, and the evaluation stage. The following is the research systematics used in this study.

2.1 Identification of Problems

The problem identification stage is the first stage carried out which aims to identify problems that exist at the application level. At this stage it begins with identification of problems found at the application level on the XYZ university website. The next activity is to make a hypothesis about how to solve problems that exist at the application level on the website of XYZ University, namely by carrying out the vulnerability scanning method.

2.2 Formulation of the Problem

The problem formulation stage begins with formulating the problem to be discussed in the research conducted by referring to the previous stage, namely the problem identification stage. After that, the limitations of the problem that will be applied to the research will be determined.

2.3 Data Collection

The data collection stage is the stage to identify existing problems and collect the necessary dataThe information utilized in this study is primary data, or information that was gathered by researchers themselves.. The data was taken from the vulnerability scan activity carried out on the XYZ University students' final project proposal dashboard website using Acunetix and Nmap software.

2.4 Analysis Development

In the development stage of this analysis, the steps taken were to carry out an analysis of the results of reports from vulnerability scan activities on the website dashboard of XYZ University student final project proposals which were carried out at the data collection stage. The data is then used to analyze existing vulnerabilities by taking into account the level of vulnerability, describing the vulnerabilities and determining recommendations for solutions that can be implemented to overcome existing vulnerabilities.

2.5 Evaluation

The evaluation stage consists of preparing a final report which is the conclusion of the research carried out and also suggestions that can make further research better than the previous one. In addition, at this stage, documentation was created containing the steps to perform a web vulnerability scan on Acunetix on the XYZ University student final project proposal dashboard web dashboard.

3 LITERATURE REVIEW

3.1 Website and Information Security

Website security is basically protecting websites or web applications from existing threats by detecting, preventing and responding to cyber threats [8]. Whereas in information-based systems, where the information has no physical substance, information security is how we may either identify or prevent fraud (cheating). There are aspects that must be considered in information security, these aspects are Confidentiality, Integrity, and Availability or commonly called the CIA Triad [9], an explanation of each of these aspects is as follows

- Confidentiality which is an element that protects information secrecy and assures only authorized parties may access information.
- Integrity, this is a feature that ensures that information cannot be modified without the authorities' consent.
- Availability, this ensures that data and information may be accessible when consumers need them without being interrupted

3.2 Vulnerabilities

Vulnerability is a vulnerability in a system or its infrastructure that unauthorized parties can exploit to exploit a system. In particular, a vulnerability can be a weakness in a system's hardware or software, in the policies and procedures used within the system, and also in the users of the system itself. [10]

3.3 Threats

Threats are harmful behaviors that aim to steal, corrupt, or otherwise interfere with digital operations. Computer viruses, DoS assaults, and other types of attacks can all constitute threats.

Threat also describes the potential for successful cyberattacks aiming at stealing sensitive data or gaining illegal access to computer networks, information technology assets, or other systems.

3.4 Risk

Risk is the potential for loss or harm as a result of a threat taking advantage of a weakness. Risks might include things like financial loss, loss of privacy, reputational harm, legal repercussions, and even loss of life. These additional definitions of risk

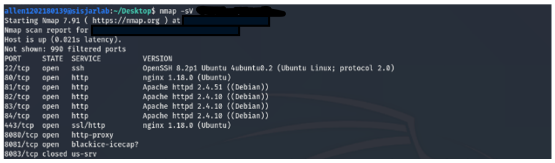
Risk = ThreatxVulnerability

4 RESULTS AND DISCUSSIONS

4.1 Scanning Results Using Nmap

A free and open source utility application called Network Mapper, sometimes known as nmap, is used for network discovery and security audits. Nmap can assist network administrators with a number of tasks, including network administration, service update management, and host and uptime monitoring. [11].

Nmap employs raw IP packets to identify the hosts that are present on a network, the program utilized by each host, its name and version, the operating system, and the firewall [12]. Linux, Windows, and Mac OS X are just a few of the operating systems that Nmap can run on.



```
allen1202180139@sisjarlab:~/Desktop$ nmap -sV [redacted]
Starting Nmap 7.91 ( https://nmap.org ) at [redacted]
Nmap scan report for [redacted]
Host is up (0.021s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE          VERSION
22/tcp   open   ssh              OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http             nginx 1.18.0 (Ubuntu)
81/tcp   open   http             Apache httpd 2.4.51 ((Debian))
82/tcp   open   http             Apache httpd 2.4.10 ((Debian))
83/tcp   open   http             Apache httpd 2.4.10 ((Debian))
84/tcp   open   http             Apache httpd 2.4.10 ((Debian))
443/tcp  open   ssl/http         nginx 1.18.0 (Ubuntu)
8080/tcp open   http-proxy
8081/tcp open   blackice-icecap?
8083/tcp closed us-srv
```

Figure 2: Nmap scanning result.

Based on the results of the vulnerability scanning using nmap that has been carried out, there are 9 ports open at the network level on the XYZ University student final project proposal dashboard website, namely ports 22, 80, 81, 82, 83, 84, 443, 8080, and 8081 as shown in figure 2.

4.1.1 *Port 22.*

Port 22 is the port used for ssh or secure shell which functions to log in remotely or remotely safely to the Virtual Private Server used [13]. The way the ssh protocol works is by using the client-server concept. It is normal for this port to be open because it functions to access the VPS remotely. The OpenSSH version used on this port is version 8.2p1. There are 4 vulnerabilities that exist on port 22 which will be explained in table 1 which are grouped based on the Nmap tools used as follows.

4.1.2 *Port 80.*

Port 80 is the commonly used HTTP server / web server port. This port serves to access the internet. This port is used to connect the web server with the client [14]. On the XYZ University students' final project proposal dashboard website, the web server used is nginx with version 1.18.0 and nmap has not detected any vulnerabilities on this port.

4.1.3 *Port 81-84.*

Ports 81-84 are the ports used for alternative web server ports. At the default setting of the network level on the XYZ University Virtual Private Server, ports 81-84 are used for the Apache HTTP Server service, but Apache is not installed on the XYZ University Virtual Private Server. The nmap tool used in this study assumes that ports 81-84 really use the Apache HTTP Server on that port so that it detects vulnerabilities based on the version, namely version 2.4.51 for port 81 and 2.4.10 for port 82-84. The total number of unverified vulnerabilities is 49 vulnerabilities

4.1.4 *Port 443.*

Port 443 is a A Secure Sockets Layer (SSL) certificate protects the port 443 of the HTTPS protocol, which is used to handle encrypted client and web server connections[15] . When port 443 is open, there is software from the server running which means that the web server is waiting for a connection from the web browser. The tools nmap have not detected any vulnerabilities on this port.

4.1.5 *Port 8080.*

Port 8080 is the port used for the web proxy server port used by the web server to establish a TCP connection if port 80 is busy [16]. The tools nmap have not detected any vulnerabilities on this port.

4.1.6 *Port 8081.*

Port 8081 is a port that functions as an alternative Hyper Text Transfer Protocol (HTTP) port used for website network traffic [17]. The tools nmap have not detected any vulnerabilities on this port.

Table 1: Vulnerability on port 22

No	Vulnerability models	Vulnerability value	Description
22.1	CVE-2020-15778	6.8	By including the command as part of the name of the file being copied on the server, an attacker with the ability to scp files to a remote server can run commands on the remote server.
22. 2	CVE-2021-28041	4.6	An attacker with access to the socket agent might leverage the double free memory corruption vulnerability in the ssh-agent in OpenSSH versions lower than 8.5 to direct the agent to a host under the attacker's control or an account shared with an unauthorized user.
22. 3	CVE-2020-14145	4.3	Observable Discrepancy happens on the client side of OpenSSH versions 5.7 to 8.4 and results in algorithm negotiation information leaking. With the use of a man-in-the-middle attack, an attacker was able to target an initial connection attempt when the client had not yet cached the server's host key.
22. 4	CVE-2021-36368	2.6	In versions of OpenSSH below 8.9, if the client uses public key authentication with agent forwarding but does not use -oLogLevel=verbose, and the attacker has secretly modified the server to support the no-authentication option, the user will not be able to determine whether FIDO authentication will confirm that user's ability to connect to that server or whether the user wants to permit that server to connect to another server on that user's behalf.

4.2 Scanning Results Using Acunetix

Acunetix Web Vulnerability Scanner is a security testing tool from the Invicti Security company which is a web application that will audit web applications by examining vulnerabilities such as SQL injection that allows any organization to intentionally attempt to access unauthorized network data without authorization or permission, cross-site scripting (XSS), and other vulnerabilities that can be exploited [18] [19]. Acunetix is a web security scanner that has been continuously improved since 2005. For a variety of operating systems, including Windows, macOS, and Linux, Acunetix is accessible.. In addition, Acunetix can also be used as a cloud product so that it can save memory used [20].

Based on the results of the vulnerability scanning using Acunetix that has been carried out, there are 8 vulnerabilities on the XYZ University student final project proposal website which will be described in table 2 below.

4.3 Comparison of Tools

After scanning using each tool, the next step is to describe the results and characteristics of the Nmap and Acunetix tools. Nmap is an application that focuses on scanning vulnerabilities at the network layer using the host-based scan method, while Acunetix is an application that focuses on scanning vulnerabilities at the application layer using the web application scan method. The comparison between the two tools is described in table 3 below.

4.4 Solutions for Every Vulnerability

The vulnerabilities obtained through scanning using Nmap and Acunetix can be grouped based on their level of severity. This division includes moderate and low risk vulnerabilities for which the solution will be recommended in the following sections.

4.4.1 Upgraded OpenSSH to version 9.0. OpenSSH versions that are not updated may have bugs that have been patched in newer versions [21]. On the XYZ University Virtual Private Server using OpenSSH version 8.2p1. In this OpenSSH version, there are vulnerabilities that have been fixed in the new version, for that The OpenSSH version should be updated to at least version 9.0.

4.4.2 Create a script that is used in order to filter the metacharacter of the input results entered by the user. There are two ways that can be used to filter the input results entered by the user, namely by using black-list and white-list input validation [22]. In black-list input validation it works by making a list of values that are not allowed in the user input results, if there are values that are not allowed then the request will be blocked. Whereas white-list input validation works by creating a list of values that the user may input, if there is a value that is not in the list, the request will be blocked.

4.4.3 Upgraded the jQuery library to version 3.6.0. JQuery is a cross-platform JavaScript library that can do event handling and other things. With the help of methods that may be invoked with only one line of code, jQuery aims to make it simpler to utilize JavaScript on websites.

Using an outdated jQuery library can cause various vulnerabilities [23]. The version of the jQuery library used for the XYZ University students' final project proposal dashboard website is version 3.3.1 which is a version that has cross-site Scripting (XSS) and prototype pollution vulnerabilities so it is recommended to upgrade the jQuery library to version 3.6.0

4.4.4 Configure the web server to include the X-Frame-Options header and CSP header using the frame-ancestors directive. X-Frame-Options and the frame-ancestor directive allow you to specify which

Table 2: Acunetix scan result

No	Vulnerability	Level	Description
1	Cross-site scripting (content-sniffing)	Medium	Cross-site scripting (XSS) attacks may be possible for some programs. A vulnerability called cross-site scripting enables an attacker to deliver malicious code to other users, typically in the form of JavaScript. As a result, the browser will run the script in the context of the user, giving the attacker access to any cookies or session tokens the browser has saved. This can happen because the browser cannot determine whether the script should be trusted or not.
2	Vulnerable use of JavaScript libraries	Medium	The XYZ University students' final project proposal website uses jQuery version 3.3.1 which is a vulnerable JavaScript library.
3	Clickjacking : X-Frame-Options header missing	Low	The X-Frame-Options header is not returned by the server, which puts this website at danger of clickjacking attacks. To specify whether the browser should be permitted to render the page inside an iframe or a frame, use the X-Frame-Options response header. This can help websites prevent clickjacking attacks by preventing the unapproved embedding of their content on other websites.
4	Cookies lacking the Samesite attribute.	Low	There are cookies that do not have the SameSite attribute. This can lead to unexpected behavior by apps which can later lead to secondary security issues.
5	Cookies without the HttpOnly flag	Low	Some cookies are HttpOnly flagged while others are not. A key security measure for session cookies is the HttpOnly setting, which tells the browser that the cookie can only be viewed by the server and not by client-side scripts.
6	Cookies without the Secure flag.	Low	Cookies that lack the Secure indication include some. When the secure flag is set on a cookie, the browser is informed that the cookie can only be viewed over secure SSL/TLS channels. This is a crucial session cookie security measure.
7	Does not implement HTTP Strict Transport Security (HSTS)	Low	Browsers are informed by HTTP Strict Transport Security (HSTS) that HTTPS is the sole method for accessing this website. Due to the absence of the Strict Transport Security header in the response, the TA1 web application does not implement HTTP Strict Transport Security (HSTS).
8	Sensitive pages are at risk of being cached	Low	There are some pages that may be cached even on secure SSL routes that include sensitive information, such as password parameters. SSL terminators, intermediate proxies, and intermediary proxies can all store this sensitive information.

Table 3: Comparison of Tools

Indicator	nmap	Acunetix
Method	Host-based scan	Web application scan
Application type	Command line based application	Web based application
The number of vulnerabilities detected	53	8
Appropriate vulnerabilities	4 (13.25%)	8 (100%)
Terdapat informasi detail tiap kerentanan	No	Yes
Application scheme	Free	Paid application

parent URL can frame the current resource. By using the frame-ancestor CSP directive, we can block or allow pages to be placed in frames or iframes so as to prevent clickjacking [24].

4.4.5 Sets the value of the Samesite attribute on an existing cookie. On the XYZ University student final project proposal dashboard website, cookies do not have the SameSite attribute. The SameSite attribute on cookies is an attribute that allows you to declare whether your cookies can be accepted when a new request comes from a third-party [25]. The samesite attribute can contain three values namely Strict, Lax, and None.

Cookies will only be transmitted if the site for the cookie matches the site that is presently visible in the URL bar of the browser if the SameSite attribute value is set to Strict [26]. The browser will, however, let the majority of cross-domain cookie-sharing as long as it originates from a top-level GET request if the SameSite attribute's value is set to Lax.

4.4.6 Sets the HttpOnly flag on existing cookies. HttpOnly is an attribute on cookies that can help reduce the risk of scripts on the client side to access protected cookies by creating a gate that prevents protected cookies from being accessed by anyone other than the server which makes it more secure [27].

4.4.7 *Sets the Secure flag for existing cookies.*

When providing a new cookie to the user in an HTTP response, the application server has the option of setting the secure cookie property. Because cookies are sent in cleartext, this attribute's goal is to prevent them from being watched or seen by unauthorized persons [28]. By configuring the secure property, browsers that permit its usage will only deliver cookies with the secure attribute when an HTTPS website is requested. In other words, the browser won't deliver secure cookies across HTTP requests that aren't encrypted.

4.4.8 *Implementing HTTP Strict Transport Security (HSTS)..*

If a website accepts a connection via HTTP and then redirects to HTTPS, the web visitor can still communicate with the unencrypted website just before being redirected. These redirects can be exploited to redirect website visitors to malicious sites. [29]

An HSTS implementation is announced by publishing a HSTS policy, which is manifested along with the "Strict-TransportSecurity" HTTP Response Header [30]. Any requests to reach websites that were previously accessible through HTTP are automatically converted to HTTPS when the HTTP Strict Transport Security header is present in the request [31].

4.4.9 *Added "Cache Control: No-store" and "Pragma: no-cache" in HTTP header responses.*

Cache-control is an HTTP header that controls how browser cache rules are handled in client requests and server responses. The no-store directive prevents the browser from caching the response; instead, it forces the browser to retrieve it from the server each time a request is made. Sensitive data often uses this option.

The request-response chain is impacted by the pragma HTTP/1.0 general header, which is an implementation-specific header [32]. Pragma: no-cache forces the cache to contact the origin server for verification before releasing the cached copy.

5 CONCLUSION

Considering the results of the investigation, it can be said that the Nmap tools that focus on scanning at the network layer can detect 53 vulnerabilities with an accuracy of 13.25% while the Acunetix tools that focus on scanning at the application layer can detect 8 vulnerabilities with 100% accuracy so that there are 12 vulnerabilities that detected on the website dashboard of XYZ University student final project proposal dashboards with 5 medium risk vulnerabilities, and 7 low risk vulnerabilities. The recommended solution to overcome the vulnerabilities that exist on the XYZ University student final project proposal dashboard website is by upgrading the ssh and jQuery versions and configuring cookies with complete attributes. The results of this study can be used as an initial step to overcome the vulnerabilities found on the website dashboard of XYZ University final student project proposal dashboard by identifying vulnerabilities on the website. In further research, penetration testing can be carried out on each vulnerability and fixing each existing vulnerability.

REFERENCES

[1] Almaarif and M. Lubis, "Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government's Website," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 10, no. 5, pp. 1874–1880, 2020.

[2] M. I. Alhari, H. Nuraliza, and A. A. N. Fajrillah, "Implementasi Aplikasi Smart City Pada Management Informasi Mitigasi Bencana Kekeringan," J. Ilm. Teknol. Inf. Asia, vol. 16, no. 1, pp. 9–18, 2022.

[3] Hatice Işık Özata, Önder Demir, and Buket Doğan, "Analysis of Patents in Cyber Security with Text Mining," International Journal of Computer Theory and Engineering vol. 13, no. 1, pp. 24-28, 2021.

[4] Rania Hodhod, Shuangbao Wang, and Shamim Khan, "Cybersecurity Curriculum Development Using AI and Decision Support Expert System," International Journal of Computer Theory and Engineering vol. 10, no. 4, pp. 111-115, 2018.

[5] M. Lubis and M. Kartiwi, "Privacy and trust in the Islamic perspective: Implication of the digital age," 2013 5th Int. Conf. Inf. Commun. Technol. Muslim World, ICT4M 2013, no. August 2018, 2013.

[6] F. Lubis and M. Lubis, "Network Fault Effectiveness and Implementation at Service Industry in Indonesia," *J. Phys. Conf. Ser.*, vol. 1566, no. 1, 2020,

[7] EE Angel, "Web Vulnerability Scanners: A Case Study Angel Rajan, Emre Erturk Eastern Institute of Technology, Hawke's Bay," no. 2016, 2017.

[8] A. Zirwan, "Testing and Analysis of Website Security Using the Acunetix Vulnerability Scanner," Journal

[9] J. Andress, The Basics of Information Security, 2nd ed., vol. 1. Elsevier, 2019.

[10] M. Abomhara and GM Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," J. Cyber Security. Car., vol. 4, pp. 65–88, 2015,

[11] I. Malinich, V. Mesyura and I. Arseniuk, "Analysis of Traffic Usage by Scanning Computer Networks with Different Versions of Nmap", Visnyk of Vinnytsia Politechnical Institute, vol. 155, no. 2, pp. 92-97, 2021.

[12] S. Jetty, Network Scanning Cookbook, 1st ed. Packt Publishing Ltd., 2018.

[13] A. Slameto and L. Lukman, "Implementation of Openssh and Bash Script for Simultaneos Remote Access Client in STMIK Amikom Yogyakarta Laboratory", Respati, vol. 9, no. 27, pp. 23-32, 2017.

[14] J. Wang and Z. Kissel, Introduction to Network Security Theory and Practice, 1st ed. Wiley, 2015.

[15] M. Arman, "Design and Build FTP Server Security Using Secure Sockets Layer", INTEGRATION JOURNAL, vol. 9, no. 1, pp. 16-23, 2017.

[16] A. Lavrenovs and G. Visky, "Exploring features of HTTP responses for the classification of devices on the Internet," 27th Telecommun. Forum, TELFOR 2019, pp. 21–24, 2019

[17] O. Dini, F. Sari, D. Kurniawati, and F. Muriyanto, "Server Optimization Using Docker Microservice Load Balancing on Telegram Bots," J. Innov. Res. Knowl., vol. 1, no. 7, 2021.

[18] A. Mahrouqi, P. Tobin, S. Abdalla, and T. Kechadi, "Simulating SQL-Injection Cyber-Attacks Using GNS3," International Journal of Computer Theory and Engineering vol. 8, no. 3, pp. 213-217, 2016.

[19] R. Mayasari, A. Ali Ridha, D. Juardi, and K. Ahmad Baihaqi, "Vulnerability Analysis on the Singaperbangsa Karawang University Website using Acunetix Vulnerability," Systematics, vol. 2, no. 1, p. 33, 2020.

[20] M. Habibi, MA Fazli, and A. Movaghar, "Efficient distribution of requests in federated cloud computing environments utilizing statistical multiplexing," Futur. gene. Comput. syst., vol. 90, pp. 451–460, 2019

[21] J. Kälkäinen, "Collection and analysis of malicious SSH traffic in Oulu University network," 2018,

[22] A. Sadiq *et al.*, "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0," Hum. Behav. Emerg. Technol., vol. 3, no. 5, pp. 854–864, 2021.

[23] T. Lauinger, A. Chaabane, S. Arshad, W. Robertson, C. Wilson, and E. Kirda, "Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web," no. September, 2017, doi: 10.14722/ndss.2017.23414.

[24] WJ Buchanan, S. Helme, and A. Woodward, "Analysis of the adoption of security headers in HTTP," IET Inf. Secur. , vol. 12, no. 2, pp. 118–126, 2018 .

[25] G. Franken, T. Van Goethem, and W. Joosen, "Who left open the cookie jar? A comprehensive evaluation of third-party cookie policies," Proc. 27th USENIX Security. Symp., pp. 151–168, 2018.

[26] S. Khodayari and G. Pellegrino, "The State of the SameSite: Studying the Usage, Effectiveness, and Adequacy of SameSite Cookies," Proc. - IEEE Symp. Secur. private, vol. 2022-May, pp. 1590–1607, 2022.

[27] Y. Takata, D. Ito, H. Kumagai, and M. Kamizono, "Risk analysis of cookie sharing by link decoration and cname cloaking," J. Inf. Process. , vol. 29, no. July 2020, pp. 649–656, 2021

[28] D. Fett, R. Kusters, and G. Schmitz, "The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines," Proc. - IEEE Comput. Secur. Found. Symp. , pp. 189–202, 2017

[29] L. Uden, I. -H. Ting, and K. Wang, Knowledge Management in Organizations. 2021.

[30] I. Dolnak and J. Litvik, "Introduction to HTTP security headers and implementation of HTTP strict transport security (HSTS) header for HTTPS enforcing," ICETA 2017 - 15th IEEE Int. Conf. Emerg. eLearning Technol. appl. Proc., pp. 1–4, 2017,

[31] N. Park, K. Sun, S. Foresti, K. Butler, and N. Saxena, Security and Privacy in Communication Networks Part 1. 2020.

[32] G. Gou, Q. Bai, G. Xiong, and Z. Li, "Discovering abnormal behaviors via HTTP header fields measurement", Concurrency and Computation: Practice and Experience, vol. 29, no. 20, p. e3926, 2016.