p-ISSN: 2252-3006
e-ISSN: 2685-2411

OWASP Framework and OCTAVE Method for Penetration Testing Web Apps of College X

I Putu Gede Angga Mas Darmayuda[a1], Gusti Made Arya Sasmita[a2], Gusti Agung Ayu Putri[a3]
[a]Departement of Information Technology, Faculty of Engineering, Udayana University
E-mail : [1]yudadarma88@gmail.com, [2]aryasasmita@unud.ac.id, [3]agung.ayuputri@unud.ac.id

Abstrak

Keamanan sistem informasi menjadi fokus utama bagi banyak organisasi karena serangan siber yang semakin canggih mengancam kerahasiaan, integritas, dan ketersediaan layanan online. Penelitian ini bertujuan untuk mengidentifikasi dan menilai kerentanan pada aplikasi web di Perguruan Tinggi X dengan menggunakan kerangka kerja OWASP dan metode OCTAVE. OWASP digunakan untuk mengidentifikasi kerentanan web yang umum dan kritis, sementara OCTAVE memberikan pemahaman holistik tentang risiko keamanan organisasi. Pengujian dilakukan dengan alat dan teknik yang direkomendasikan oleh kedua kerangka kerja tersebut. Hasil penelitian menemukan sejumlah kerentanan, termasuk dua dengan tingkat rendah dan satu dengan tingkat tinggi. Temuan ini menggarisbawahi pentingnya pengujian penetrasi sistematis dan penilaian risiko untuk menjaga keamanan aplikasi web di lingkungan pendidikan.

Kata Kunci: *Metode OCTAVE, Manajemen Resiko, OWASP, Penetration Testing*

Abstract

Information system security is a major focus for many organizations as increasingly sophisticated cyberattacks threaten the confidentiality, integrity and availability of online services. This research aims to identify and assess vulnerabilities in web applications at College X by using the OWASP framework and OCTAVE method. OWASP is used to identify common and critical web vulnerabilities, while OCTAVE provides a holistic understanding of an organization's security risks. Testing was conducted with the tools and techniques recommended by both frameworks. The results found a number of vulnerabilities, including two low-level and one high-level. The findings underscore the importance of systematic penetration testing and risk assessment to keep web applications secure in educational environments.

Keywords: *OCTAVE Method, Risk Management, OWASP, Penetration Testing*

1. Introduction

This technological advancement has made the internet an essential requirement in every activity carried out by society as a whole, The increasingly advanced digital era allows systems and applications connected to the internet to become potential targets for cyber attacks. Attackers use a variety of methods and techniques to exploit security weaknesses in these systems, which can result in significant losses, such as theft of sensitive data, infrastructure damage, or reputational damage so to protect systems and applications from such attacks, organizations must proactively identify and address existing security weaknesses. [1]. In recent years, many people have become aware of how their information can be used by others and more and more organizations are paying attention to information security risks that can negatively impact and cause financial losses to business processes, organizational reputation, customer trust, and affect relationships with their customers or business partners [2].

Penetration Testing is the process of simulating attacks that are conducted to test the security of a system or application. Penetration Testing is conducted so that organizations can detect potential security weaknesses and take the necessary remedial action before attackers take advantage of them [3].

The Open Web Application Security Project (OWASP) is a global organization focused on web application security. OWASP provides guidance, tools, and other resources that help security professionals identify, prevent, and address security weaknesses in web applications. In

addition, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method can be used to holistically analyze and manage security risks in a national education environment [4]. The OCTAVE method helps educational institutions to identify critical assets, recognize existing threats, and analyze possible vulnerabilities. The OCTAVE method is applied so that organizations can take effective actions to reduce security risks and protect sensitive data, systems, and infrastructure used [5].

This research conducted penetration testing on College X Web Apps. Penetration testing using OWASP and OCTAVE methods at College X aims to help College X identify and address security weaknesses in the systems and applications used and by combining these approaches, College X can improve security and protect sensitive data and maintain the smooth running of educational and administrative processes effectively.

2. Research Methodology

Research on Penetration Testing using the OWASP framework and OCTAVE Method on the College X web application is carried out through eight steps, which are described in a flow chart that can be seen in Figure 1 below.

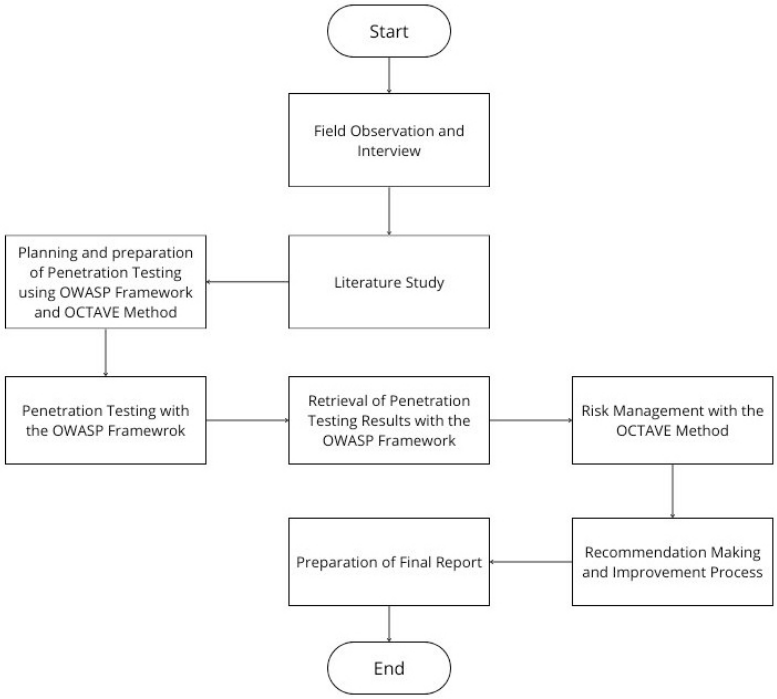

Figure 1. Flow of Research

Figure 1 is a flowchart of an overview of Penetration Testing research on College X Web Apps using the OWASP Framework and OCTAVE Method. The implementation of the stages of making research consists of eight stages, namely field observations and interviews, literature studies, planning and preparation for penetration testing using the OWASP framework and OCTAVE method, penetration testing with the OWASP framework, retrieving penetration testing results with the OWASP framework, risk management with the OCTAVE method, making recommendations and the improvement process and preparing the final report.

3. Literature Study

The ideas and concepts in this research were obtained from a literature review, including scientific journals, research reports, and various books relevant to this topic. These theories support the implementation of this research as well as previous studies related to this topic.

p-ISSN: 2252-3006
e-ISSN: 2685-2411

3.1 Information Technology Security

Information security aims to ensure the confidentiality, availability and integrity of all corporate information resources. Information security management includes day-to-day protection called information security management and post-disaster operational preparation known as business continuity management [6]. Information Security occurs because the system that is built is more oriented to the maker so that the result is that the system used is difficult to use or less user friendly for the user, the system is less interactive and less comfortable for the user, the system is difficult to understand the interface of the menu system and the layout does not pay attention to the user's behavior habits, the system is felt to force the user to follow the procedures built so that the system feels rigid and less dynamic, the security of the information system built is not guaranteed [7]. Information security contains several important aspects, such as Confidentiality, Integrity, and Integrity [8].

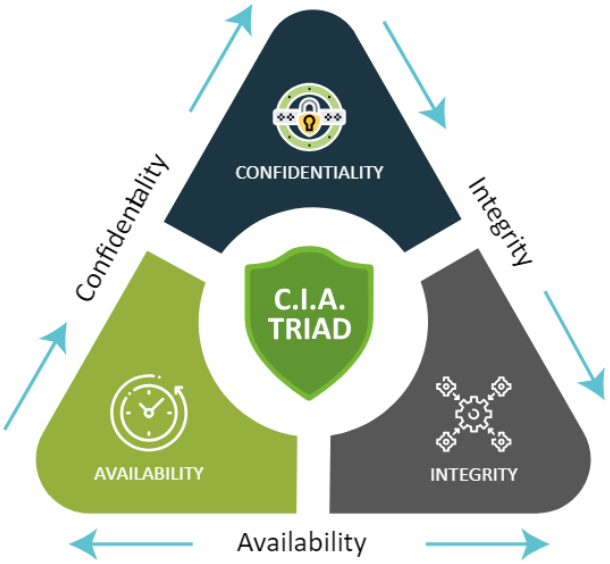

Figure 2. C.I.A Triad

Figure 2 is the concept of C.I.A Triad from the aspect of information technology security. Seen in the picture consists of three aspects in it, namely confidentiality, integrity, and availability. The explanation of each aspect is as follows.

1. Confidentiality, is an aspect that guarantees the confidentiality of data and information stored, sent, and received and ensures that the information can only be accessed by parties who have the rights and authority.
2. Integrity, is an aspect of integrity that guarantees the accuracy and integrity of information and ensures that no data changes occur, unless there is a request from parties who have the rights and authority to the data.
3. Availability, is an aspect of availability that ensures authorized users can use information when needed and guarantees that data will be available at all times.

3.2 Penetration Testing

Penetration Testing is a method for maintaining data and information security. It involves a series of steps taken to test the security of a system. Penetration Testing includes several stages that involve analyzing the system to find potential security holes, such as system configuration errors, bugs in software or hardware development, and weaknesses in process logic [9]. Penetration Testing is a method of evaluating the security of a computer system or network by simulating attacks from malicious sources and is part of a security audit. Simulated attacks are made like cases that can be made by black hat hackers, crackers, and so on. The goal is to determine and know the kinds of attacks that may be carried out on the system along with the consequences that can occur due to system weaknesses. Penetration Testing also requires intensive analysis for each vulnerability caused by system weaknesses and after all analysis is

completed, it will be documented and provided to the owner along with solutions and impacts that can result from existing security gaps [10].

3.3 Framework OWASP

OWASP (Open Web Application Security Project) is an open community focused on building an organization that aims to develop, purchase, and maintain reliable applications. OWASP supports the view that application security is an issue involving individuals, processes, and technology, because the most effective approach to application security requires improvements in all aspects. Analysis of web application vulnerabilities with the OWASP version 4 method can evaluate the security level of an application [11]. Analysis of web-based application vulnerabilities with OWASP version 4 techniques can determine the security of an application. Based on the results of vulnerability testing on the website using several stages of the category, namely the Authentication Testing Authorization stage, Session Management Testing, Input Validation Testing, and Error Handling in the OWASP version 4 method can be used as a standard for assessing the security of web-based applications [12].

3.4 OCTAVE Method

The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method is an approach developed by the Software Engineering Institute (SEI) in 2001. This method serves as a tool, technique, and procedure for evaluating and planning information system security strategies by identifying risks related to the security of information systems [13]. The OCTAVE method focuses on an organization's essential IT (Information Technology or Information Systems) assets to identify, prioritize, and manage information security risks. OCTAVE comprehensively, systematically, and contextually defines the essential components of information security risk evaluation. Through the use of this method, organizations can make risk-based decisions to protect their information OCTAVE defines key components in a comprehensive, systematic and context-based manner for information security risk evaluation. By using the OCTAVE method, organizations can create protection for information by making risk decisions The OCTAVE criteria require an evaluation to be conducted by an interdisciplinary team consisting of the organization's information technology and business personnel [14].

4. Result and Discussion

Results and discussion of Penetration Testing research activities on College X Web Apps using the OWASP Testing Guide Version 4 Framework and recommendations for improvements needed to close security gaps found in the system.

4.1 Implementation using OWASP Testing Guide V4

Implementation, namely Penetration Testing based on the OWASP Testing Guide Version 4 framework. The test results on College X Web Apps using the OWASP Framework are as follows.

Table 1. OWASP Testing Guide V4

Submodul	Objective	Tools	Results
Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001)	This submodule aims to find accidental or unintentionally leaked information on the internet.	Self-test in chrome	No vulnerabilities found
Fingerprint Web Server (OTG-INFO-002)	This submodule aims to find potential security flaws that can be exploited by an attacker.	Netcraft	No vulnerabilities found
Review Webserver Metafiles for Information Leakage (OTG-INFO-003)	This submodule aims to find and fix potential information leaks that can be exploited by attackers.	Self-test in chrome	No vulnerabilities found

p-ISSN: 2252-3006
e-ISSN: 2685-2411

Submodul	Objective	Tools	Results
Enumerate Applications on Webserver (OTG-INFO-004)	This submodule aims to count the number of web applications running on the target web server and find out the ports that are open on the website.	NMAP	Vulnerabilities found
Testingl for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)	This submodule aims to count the number of web applications running on the target web server and find out the ports open on the website.	Self-test in chrome, Burp Suite	No vulnerabilities found
Testing for default credentials (OTG-AUTHN-002)	This submodule aims to check if the application is still using default credentials that may be known to the attacker.	Burp Suite	No vulnerabilities found
Testing for Weak lock out mechanism (OTG-AUTHN-003)	This submodule aims to evaluate the strength of the account locking mechanism in the web application.	Self-test in chrome, Burp Suite	Vulnerabilities found
Testing for Insecure Direct Object References (OTG-AUTHZ-004)	This submodule aims to identify vulnerabilities where applications provide direct access to objects based on inputs provided by the user.	Burp Suite	Vulnerabilities found
Testing for Reflected Cross Sites Scripting (OTG-INPVAL-001)	This submodule aims to identify vulnerabilities where a web application receives data in an HTTP request and includes that data in the same HTTP response in an insecure manner.	Burp Suite	No vulnerabilities found
Testing for Stored Cross Site Scripting (OTG-INPVAL-002)	This submodule aims to identify vulnerabilities where a web application receives input from a user that may be malicious, stores that input in data storage for later use, and then displays that input in an HTTP response without performing proper filtering.	Self-test in chrome	No vulnerabilities found
Testing for HTTP Verb Tampering (OTG-INPVAL-003)	This submodule aims to test how the web application responds to various HTTP methods that access system objects.	Burp Suite	No vulnerabilities found
Testing for HTTP Parameter pollution (OTG-INPVAL-004)	This submodule aims to evaluate how the web application responds when it receives multiple HTTP parameters with the same name.	Burp Suite	No vulnerabilities found

Submodul	Objective	Tools	Results
Testing for SQL Injection (OTG-INPVAL-005)	This submodule aims to evaluate and ensure the security of the database from SQL Injection attacks.	Sqlmap, Burp Suite	No vulnerabilities found

Table 1 is a detail of the test results on College X Web Apps using OWASP Testing Guide V4. Seen in the table, there are 3 test submodules that successfully found vulnerabilities and 10 test submodules that did not find vulnerabilities in the College X Web Apps.

4.2 Implementation using OCTAVE Method

The OCTAVE method in the context of penetration testing can be interpreted as a framework used to identify and manage information security risks that may affect the system or application being tested. The OCTAVE method has principles and stages that are used in improving the penetration testing process in the following way.

4.2.1 Identification of Assets and Threats

Asset and Threat Identification is the process of identifying potential sources of threats that could jeopardize web application assets. Threats can come from nature or humans, and can be intentional or unintentional. The following is a table of Asset and Threat Identification.

Table 2. Identification of Assets and Threats

Assets	Threat Category	Threat Type
Email dan Password	Authentication	Brute Force Sniffing Cookie Replay Dictionary Attack Session Attack
Student Personal Data (Personal Biodata)	Validation	SSI Injection SQL Injection
Student Personal Documents	Validation	Improper validation of file names Incorrect file content and size validation Missing proper validation of Malicious and Unexpected Files Insecure Direct Object Reference

Table 2 is a detail of asset identification and possible threats that can occur in College X Web Apps. Judging from the table, there are eleven threats that might be carried out by attackers including Brute Force, Sniffing, Cookie Replay, Dictionary Attack, Session Attack, SSI Injection, SQL Injection, Missing Proper Validation of file name, Missing Proper validation of file content and size, Missing proper validation of Malicious and Unexpected Files and Insecure Direct Object Reference.

4.2.2 Threat and Vulnerability Evaluation

Threat and Vulnerability Evaluation is a process to identify, analyze, and measure risks associated with security in the cyber field. The following is a table of threat and vulnerability evaluations obtained when testing using the OWASP module on College X Web Apps.

Table 3. Threat and Vulnerability Evaluation

Modul	Risk Name/Risk Code	Vulnerability
Testing for Information Gathering	Enumerate Applications on Webserver/OTG-INFO-004	The attacker can know the number and which websites are hosted on the same server as the target website. This may be misused by the attacker to reach the target website through other websites that have low security on the same server.

Modul	Risk Name/Risk Code	Vulnerability
Authentication Testing	Testing for Weak lock out mechanism/OTG-AUTHN-003	Attackers can find out the weaknesses of security protection on the website such as the absence of a block function when entering the wrong password for more than a few tries. This can be utilized by attackers to conduct password experiments or use the help of scripts / tools.
Authorization Testing	Testing for Insecure Direct Object References/OTG-AUTHZ-004	Attackers can take advantage of the Insecure Direct Object References weakness by modifying the parameters or name of the image file on the website and taking a picture of the image file, so that the attacker can access the file directly.

Table 3 is an evaluation of threats and vulnerabilities that have been identified on the College X website based on testing using the OWASP Testing Guide framework version 4. Seen in the table, 3 vulnerabilities were found that could endanger the system if not handled further.

4.2.3 Risk Mitigation Strategy and Plan Development

The development of risk mitigation strategies and plans in this research is a process that involves identifying, assessing, and managing security risks that may affect the success of a system, network, or application. This process aims to reduce the likelihood of risks and negative impacts that may arise from security vulnerabilities. The following is a table of Risk Mitigation Strategy and Plan Development.

Table 4. Risk Mitigation Strategy and Plan Development

Risk Level	Risk/Threat Name	Risk Description	Risk Mitigation Strategy/Plan Development
Low	Enumerate Applications on Webserver (OTG-INFO-004)	Identify the number of applications running on the same domain (Reverse IP Lookup) and open ports.	Close open ports that have the potential danger of being attacked by attackers.
Low	Testing for Weak locked out mechanism (OTG-AUTHN-003)	Identify account locking mechanism vulnerabilities caused by brute force attacks or password guessing attacks.	Implement an account lock scheme for users who try to log in with the wrong username/password repeatedly more than a few times to avoid brute force attack methods on the website.
High	Testing for Insecure Direct Objects a References (OTG-AUTHZ-004)	Identify website vulnerabilities that provide direct access to objects, such as database records or files, based on unverified or uncontrolled user input.	Implement the use of a content management system CMS (Content Management System) or security rules (custom claims) where only authenticated users can access the storage). If CMS (Content Management System) is too heavy as a solution, consider using indirection to label unpredictable files or file names.

Table 4 is a table of Strategy Development and Risk Mitigation Plan based on vulnerabilities found in College X Web Apps. Seen in the table there are 2 vulnerabilities at low level and 1 vulnerability at high level. Risk level assessment in this study uses the OWASP Risk Rating Methodology method.

4.2.4 Testing Results After Improvement

The results of testing again after applying the improvement recommendations to the system aim to re-identify the vulnerabilities found in the previous penetration test. After applying

the improvement recommendations, the results of the penetration test this time are expected to have an impact on changes from the findings of vulnerability gaps in the previous penetration test. The test results after improvement on the College X Web Apps can be seen in the following table.

Table 5. Results After Improvement

Risk Name	Before	After	Description
Enumerate Applications on Webserver (OTG-INFO-004)	Low	Note	**APPLIED** The Web Apps Manager has closed ports that have the potential to be dangerous
Testing for Weak locked out mechanism (OTG-AUTHN-003)	Medium	Note	**APPLIED** The Web Apps Manager has implemented restrictions on excessive login attempts or login spam, so that attackers cannot perform Brute Force attacks on the website.
Testing for Insecure Direct Objects a References (OTG-AUTHZ-004)	High	Note	**APPLIED** The Web Apps Manager has updated the security rules (custom claims) where only authenticated users can access the storage) so that taking pictures on the website cannot be done.

Table 5 is the result of testing again after the implementation of improvement recommendations on the system. After implementing the improvement recommendations, there are several vulnerabilities that are no longer detected.

5. Conclusion

Based on the research that has been carried out, the conclusions that can be drawn regarding the implementation of Penetration Testing using the OWASP Framework and the OCTAVE Method on College X Web Apps are the results of penetration testing using the OWASP Testing Guide version 4 Framework successfully identified a total of 3 vulnerabilities in College X Web Apps and Risk management based on the OCTAVE Method framework in analyzing security risks on College X Web Apps getting analysis results based on OWASP Risk Rating Methodology found 2 vulnerabilities at low level and 1 vulnerability at high level. Based on the results of exposure and discussion with related parties managing Web Apps, there are 3 recommendations for improvements that are suggested to be applied to the College X Web Apps and the recommendations for improvement have been successfully implemented by the college X Web Apps manager.

References

[1] R. Butarbutar, “Kejahatan Siber Terhadap Individu: Jenis, Analisis, DanPerkembangannya,” *Technol. Econ. Law J.*, vol. 2, no. 2, pp. 299–317, 2023, [Online].
[2] H. L. Alexander Dharmawan, Yani Prihati, “PENETRATION TESTING MENGGUNAKAN OWASP TOP 10 PADA DOMAIN XYZ. AC. ID,” vol. 8 No 1, 2022.
[3] M. Tekege, “Analisis Kerentanan Aplikasi Web Dan Upaya Penetrasi,” *J. FATEKSA J. Teknol. dan Rekayasa*, vol. 8, no. 2, pp. 29–39, 2023.

[4] S. Alhidamkara and I. Lucia Kharisma, “Analisis Keamanan Website Sekolah Menengah Atas Negeri 1 Surade Dengan Pendekatan Comprehensive Website Security Assessment Website Security Analysis for State Senior High School 1 Surade with a Comprehensive Website Security Assessment Approach,” pp. 57–65, 2023.
[5] A. H. Putri, “Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi Menggunakan Metode Octave Dan FMEA,” *Tecno.com*, vol. 16, no. 4, pp. 367–377, 2017.
[6] S. Nurul, S. Anggrainy, and S. Aprelyani, “Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim),” *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022.
[7] Y. M. Putra, “KEAMANAN INFORMASI,” no. November, 2019.
[8] H. Ikhsan and N. Jarti, “Analisis Risiko Keamanan Teknologi Informasi,” *J. Responsive*, vol. 2, no. 1, pp. 31–41, 2018.
[9] A. Fajaryanto Cobantoro, “PENERAPAN OWASP VERSI 4 UNTUK UJI KERENTANAN WEB SERVER (STUDI KASUS EJURNAL SERVER KAMPUS X MADIUN),” 2016, [Online]. Available: www.contoh.com/adduserp.php
[10] R. Pangalila, A. Noertjahyana, and J. Andjarwirawan, “Penetration Testing Server Sistem Informasi Manajemen,” *Penetration Test. Serv. Sist. Inf. Manaj. dan Website Univ. Kristen Petra*, pp. 1–6, 2015.
[11] A. I. Rafeli, H. B. Seta, and W. Widi, “Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ,” 2022.
[12] M. Yunus, “Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4,” *J. Ilm. Inform. Komput.*, vol. 24, no. 1, pp. 37–48, 2019, doi: 10.35760/ik.2019.v24i1.1988.
[13] N. Budarsa, “Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro dan Analytical Hirarchy Process pada Data Center Pemerintah Kabupaten Buleleng,” *J. Ilmu Komput. Indones.*, vol. 7, no. 1, pp. 13–15, 2022.
[14] R. Fitria Hamzah, I. Dwi Jaya, and U. Mizani Putri, “Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode Octave Pada Perguruan Tinggi Negeri X,” 2020.
[15] B. Supradono, “MANAJEMEN RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION).” [Online]. Available: http://jurnal.unimus.ac.id
[16] N. L. Kuntari, Y. H. Chrisnanto, and A. I. Hadiana, “MANAJEMEN RISIKO SISTEM INFORMASI DI UNIVERSITAS JENDERAL ACHMAD YANI MENGGUNAKAN METODA OCTAVE ALLEGRO,” 2018.