

ANALISIS KEAMANAN WEBSITE SMK TAMAN KARYA KEBUMEN MENGGUNAKAN METODE VULNERABILITY ASESEMENT

Nur Cholis¹, Erik Iman Heri Ujianto²
nurcholis2310@gmail.com¹, tugasku.terbaik@gmail.com²
Universitas Teknologi Yogyakarta

Abstrak

SMK Taman Karya Kebumen merupakan sekolah yang menyediakan informasi berbasis Website untuk memudahkan pelayanan administrasi sekolah. Mengingat Website dapat diakses secara luas, maka perlu diperhatikan keamanan pada Website. Salah satunya dengan menggunakan metode Vulnerability Asesment. Metode Vulnerability Asesment salah satu metode untuk melakukan pengujian kerentanan pada Website atau aplikasi yang berpotensi masuknya serangan yang terdiri dari beberapa tahapan seperti Network Discovering, Vulnerability Scanning, Resultt Analisis. Tahapan ini bertujuan untuk mengidentifikasi celah keamanan pada website SMK Taman Karya Kebumen. Pengujian yang telah dilakukan berhasil mengidentifikasi empat tingkat kerentanannya yaitu high, medium, low, dan informational pada Website SMK Taman Karya Kebumen. Adapun tingkat kerentanan high yang didapatkan adalah SQL Injection. Dengan kerentanan SQL Injection memudahkan penyerang mengakses seluruh database. Hasil pengujian yang telah dilakukan menunjukkan bahwa pada Website SMK Taman Karya Kebumen memiliki banyak celah kerentananatau Vulnerability bahwa website SMK Taman Karya Kebumen masih dalam keadaan tidak aman.

Kata Kunci: keamanan,informasi,Open Web Application Security Project (OWASP),Vulnerability Assessment.

ABSTRACT

Analysis of Website Security for SMK Taman Karya Kebumen Using the Vulnerability Assessment Method. SMK Taman Karya Kebumen is a school that provides website-based information to facilitate school administration services. Considering that the Website can be accessed widely, it is necessary to pay attention to the security of the Website. One of them is by using the Vulnerability Assessment method. The Vulnerability Assessment method is a method for testing vulnerabilities on a website or application that has the potential to enter an attack which consists of several stages such as Network Discovering, Vulnerability Scanning, and Result Analysis. This stage aims to identify security holes on the SMK Taman Karya Kebumen website. The tests that have been carried out have identified four levels of vulnerability, namely high, medium, low, and informational on the website of SMK Taman Karya Kebumen. The high vulnerability level obtained is SQL Injection. With the SQL Injection vulnerability makes it easy for attackers to access the entire database. The results of the tests that have been carried out show that the SMK Taman Karya Kebumen website has many vulnerability gaps or Vulnerability that the SMK Taman Karya Kebumen website is still in an unsafe state.

Keywords: security, information; website, e-learning,penetration testing execution standard.

PENDAHULUAN

Perkembangan teknologi saat ini mengalami perubahan yang sangat pesat. Hal ini dapat dilihat dari banyaknya pengguna website yang semakin banyak baik untuk keperluan suatu instansi, pendidikan, organisasi, maupun keperluan pribadi. Keamanan menjadi salah satu aspek penting dalam segala hal.

SMK Taman Karya Kebumen merupakan salah satu Sekolah Kejuruan yang berada Jl. Cincin Kota No.18, Megabiru, Karang Sari, Kec. Kebumen, Kabupaten Kebumen, Jawa Tengah. SMK Taman Karya Kebumen merupakan sekolah yang menyediakan informasi kepada siswa siswi melalui sistem informasi berbasis web untuk memudahkan pelayanan

administrasi sekolah.

SMK Taman Karya Kebumen yang memanfaatkan kemajuan teknologi dalam menyampaikan informasi dengan menggunakan website. Seiring dengan kemajuan teknologi pentingnya keamanan terhadap suatu website menjadi hal utama karena apabila suatu keamanan diabaikan memungkinkan terjadinya pencurian data atau mengubah tampilan dari suatu website.

Dalam pelayanannya SMK Taman Karya Kebumen menyediakan informasi dalam sebuah website <https://tamankaryakbm.com/>. Adapun beberapa tampilan halaman yang ada pada website SMK Taman Karya Kebumen yaitu Visi Misi, Berita, Kepala Sekolah, Kopotensi dan Olahraga atau Prestasi. Beberapa tahun lalu website tersebut pernah diakses oleh orang yang tidak bertanggung jawab dan membuat tampilan dari website tersebut berubah [10].

Maka dari permasalahan tersebut penulis menawarkan solusi yaitu dengan menganalisa keamanan website menggunakan tool Open Web Application Security Project (OWASP). Dalam analisa tersebut akan diperoleh berbagai macam kerentanan yang memungkinkan penyerang masuk dalam website SMK Taman Karya Kebumen. Kemudian peneliti akan memberikan rekomendasi dari hasil analisa keamanan website tersebut [11].

Dengan adanya analisa keamanan website SMK Taman Karya Kebumen, diharapkan mampu menjadi solusi bagi SMK Taman Karya Kebumen agar dapat meningkatkan keamanan Website.

METODE PENELITIAN

Dalam melakukan penelitian di SMK Taman Karya Kebumen dengan judul Analisis Keamanan Website SMK Taman Karya Kebumen Menggunakan Metode Vulnerability Asesment.

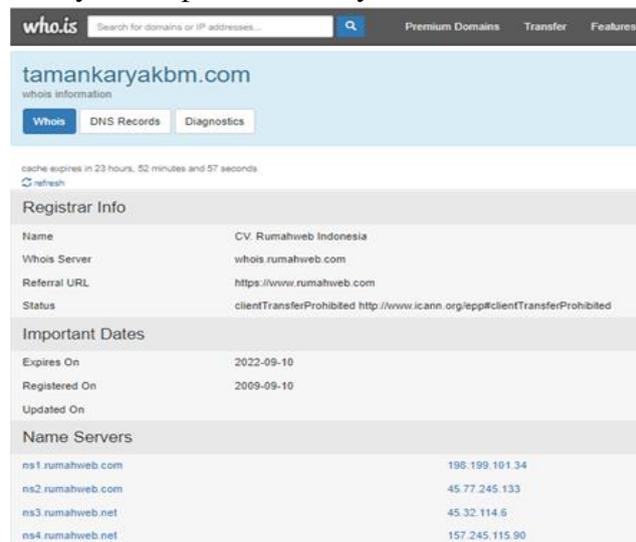
HASIL DAN PEMBAHASAN

Hasil dan Diskusi

Pengecekan halaman Website

a. Who.is

Untuk mengambil informasi sebuah alamat domain dari website SMK Taman Karya Kebumen, maka penulis menggunakan website Who.is. Adapun hasil informasi domain yang didapatkan yaitu <https://tamankaryakbm.com>.



The screenshot shows the Who.is website interface for the domain tamankaryakbm.com. It includes a search bar at the top, navigation tabs for Whois, DNS Records, and Diagnostics, and a refresh button. The main content is divided into three sections: Registrar Info, Important Dates, and Name Servers.

Registrar Info	
Name	CV. Rumahweb Indonesia
Whois Server	whois.rumahweb.com
Referral URL	https://www.rumahweb.com
Status	clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Important Dates	
Expires On	2022-09-10
Registered On	2009-09-10
Updated On	

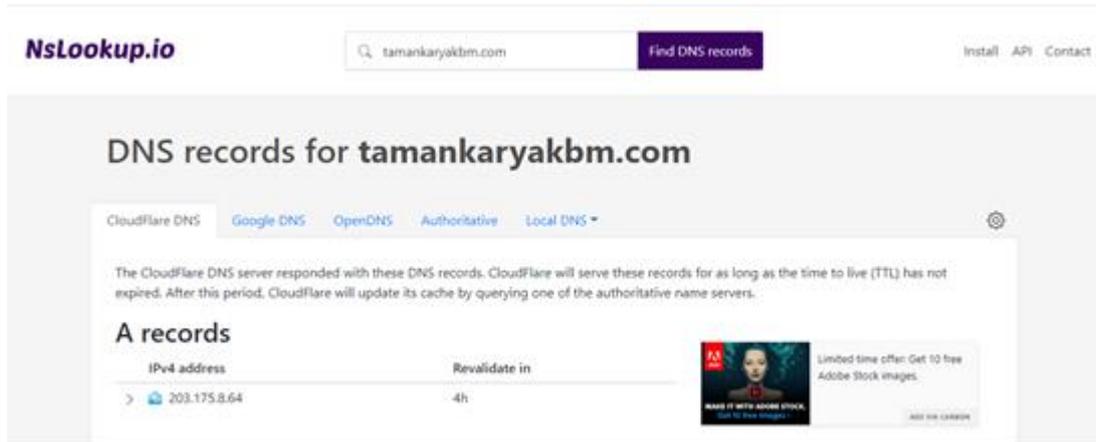
Name Servers	
ns1.rumahweb.com	198.199.101.34
ns2.rumahweb.com	45.77.245.133
ns3.rumahweb.net	45.32.114.6
ns4.rumahweb.net	157.245.115.90

Gambar 1. Hasil Pengecekan Website SMK Taman Karya Kebumen

Berdasarkan gambar diatas Hasil dari pengambilan informasi domain dari website SMK Taman Karya Kebumen menggunakan who.is terhadap target domain yang telah ditentukan didapatkan berbagai informasi terkait pendaftaran nama domain masa berlakunya serta Domain Name System (DNS) server yang digunakan.

b. Nslookup

Untuk mengetahui IP dari sebuah domain pada website SMK Taman Karya Kebumen.

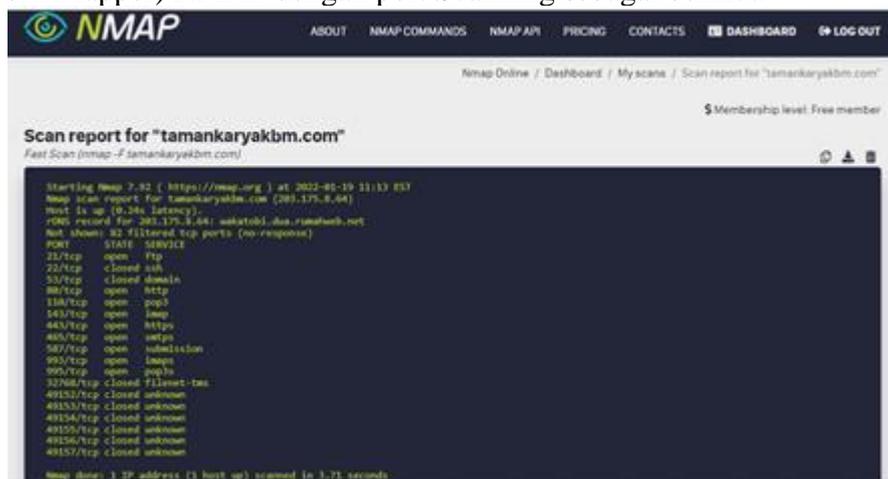


Gambar 2. Hasil Scanning dengan tool Nslookup

Berdasarkan pengujian port scanning diatas, dapat terlihat alamat website dan IP adress pada website SMK Taman Karya Kebumen. Adapun hasil Scanning oleh tool Nslookup pada website SMK Taman Karya Kebumen menampilkan informasi IP yaitu “203.175.8.64”

c. Scanning Port

Untuk melihat server atau port terbuka pada SMK Taman Karya Kebumen penulis menggunakan tool Network Mapper (NMAP). Adapun hasil dari pengujian menggunakan tool (Network Mapper) NMAP dengan port Scanning sebagai berikut.



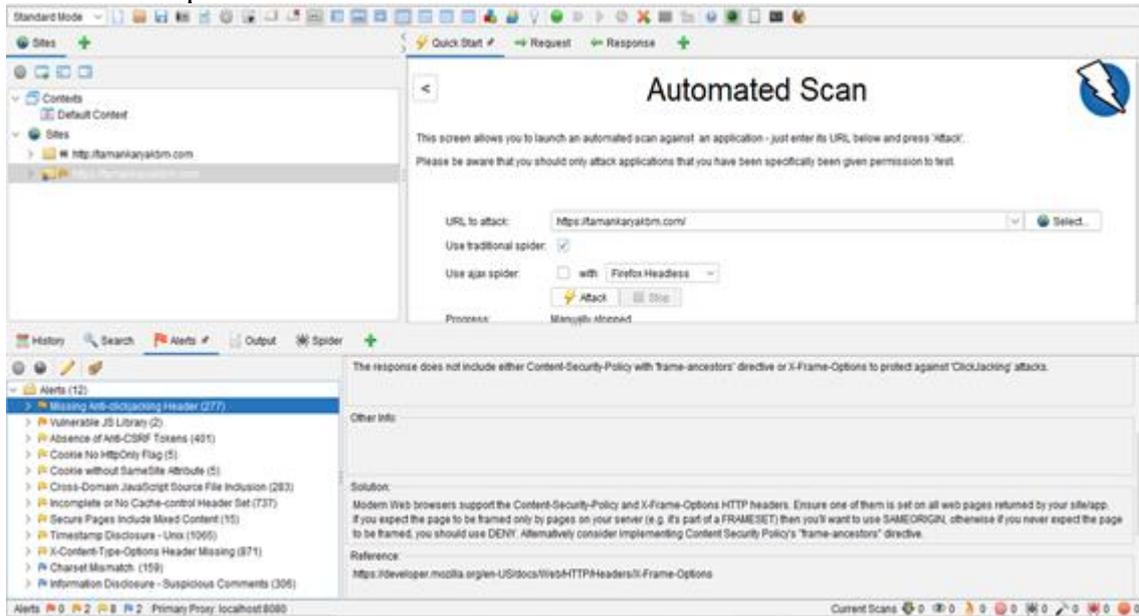
Gambar 3. Hasil Port Scanning dengan Tool Nmap

Berdasarkan pengujian port scanning diatas dapat terlihat port Service seperti ftp, http, pop3, imap, https, smtps, submission, imaps, dan pop3s yang statusnya terbuka.

Pengujian Kerentanan

Vulnerability Scanning mencari celah kerentanan keamanan pada Website SMK Taman Karya Kebumen penulis menggunakan tool Open Web Application Security

Project (OWASP). Berikut tampilan pengujian kerentanan keamanan Website yang telah dilakukan oleh penulis.



Gambar 4. Hasil Analisis Kerentanan Tool OWASP

Berdasarkan hasil pengujian yang dilakukan pada tool Open Web Application Security Project (OWASP), didapatkan beberapa celah keamanan yang ada di Website SMK Taman Karya Kebumen diantaranya berupa : X-Frame Options Header Not Set, Absence of Anti-CSRF Tokens, Cookie No flag, Cookie Without Same Site Attribute, Cross-Domain Java Script Source File Inclusio, Server Leaks Information via”X-By “HTTP Response Header Field (s), Timestamp Disclosure-Uni, Dll.

Penilaian Kerentanan

Berikut hasil dari pengujian kerentanan keamanan Website SMK Taman Karya Kebumen dapat dilihat pada tabel berikut :

TITLE	SCAN TYPE	TARGET	THREAT LEVEL	STATUS	LAST DETECTED ▼
Vulnerable JS Library	OWASP_...	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
X-Frame-Options Header Not Set	OWASP_...	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Application Error Disclosure	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
Absence of Anti-CSRF Tokens	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
Cookie No HttpOnly Flag	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
Incomplete or No Cache-control Header Set	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
Cookie without SameSite Attribute	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
Cross-Domain JavaScript Source File Inclusion	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
Information Disclosure - Debug Error Messages	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
Secure Pages Include Mixed Content	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
X-Content-Type-Options Header Missing	OWASP_...	https://tamankaryakbm.com/	LOW	CLOSED	2 days ago
Open TCP Port: 80	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 21	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 110	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 143	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 993	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 443	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 995	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 2080	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 2082	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 2083	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 2087	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 2091	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago
Open TCP Port: 2095	NMAP	https://tamankaryakbm.com/	MEDIUM	CLOSED	2 days ago

Gambar 5. Gambar Tabel Pengujian Kerentanan

Hasil dan Rekomendasi

Berikut sebuah saran yang direkomendasikan oleh tool Open Web Application Security Project (OWASP).

Tabel 2. Hasil Tool Open Web Application Security Project (OWASP)

No	Sistem Vulnerability	Jumlah Vulnerability	Rekomendasi Perbaikan
1	Missing Anti-clickjacking Header	277	Browser Web modern mendukung header HTTP Content-Security-Policy dan X-Frame-Options. Pastikan salah satunya disetel di semua halaman web yang ditampilkan oleh situs/aplikasi Anda.

			Jika Anda mengharapkan halaman dibingkai hanya oleh halaman di server Anda (mis. itu bagian dari FRAMESET) maka Anda akan ingin menggunakan SAMAORIGIN, jika tidak, jika Anda tidak pernah mengharapkan halaman dibingkai, Anda harus menggunakan DENY. Atau pertimbangkan untuk menerapkan arahan "frame-ancestors" Kebijakan Keamanan Konten.
2	Vulnerable JS Library	2	Harap tingkatkan ke versi jquery terbaru.
3	Absence Of Anti CSRF Tokens	401	Fase: Arsitektur dan Desain, Gunakan perpustakaan atau kerangka kerja yang diperiksa yang tidak memungkinkan kelemahan ini terjadi atau menyediakan konstruksi yang membuat kelemahan ini lebih mudah untuk dihindari. Misalnya, gunakan paket anti CSRF seperti OWASP CSRFGuard.
4	Cookie No Http Only Flag	5	Pastikan bahwa flag HttpOnly disetel untuk semua cookie.
5	Cookie Without Same Site Attribute	5	Pastikan atribut SameSite diatur ke 'lax' atau idealnya 'strict' untuk semua cookie.
6	Cross- Domain JavaScript Source File Inclusion	283	Pastikan file sumber JavaScript dimuat hanya dari sumber tepercaya, dan sumber tidak dapat dikontrol oleh pengguna akhir aplikasi.
7	Incomplete or No Cache-control Header Set	737	Jika memungkinkan, pastikan header HTTP kontrol-cache disetel dengan no-cache, no-store, must-revalidate.
8	Secure Pages Include Mixed Conten	15	Halaman yang tersedia melalui SSL/TLS harus sepenuhnya terdiri dari konten yang dikirimkan melalui SSL/TLS. Halaman tidak boleh berisi konten apa pun yang dikirimkan melalui HTTP yang tidak terenkripsi. Ini termasuk konten dari situs pihak ketiga.
9	Timestamp Disclosure	1065	Konfirmasikan secara manual bahwa data stempel waktu tidak sensitif, dan bahwa data tidak dapat digabungkan untuk <u>mengungkapkan pola yang dapat dieksploitasi</u> .
10	X-Content-Type-Option Header Missing	871	Pastikan aplikasi/server web menyetel header Content-Type dengan tepat, dan menyetel header X-Content-Type-Options ke 'nosniff' untuk semua halaman web. Jika memungkinkan, pastikan bahwa pengguna akhir menggunakan browser web yang sesuai standar dan modern yang tidak melakukan sniffing MIME sama sekali, atau yang dapat diarahkan oleh aplikasi web/server web untuk tidak melakukan sniffing MIME.
11	Charset Mismatch	159	Paksa UTF-8 untuk semua konten teks di header HTTP dan tag meta dalam HTML atau deklarasi penyandian dalam XML.
12	Information Disclosure-Suspicious Comment	306	Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang dan perbaiki masalah mendasar yang mereka rujuk.

KESIMPULAN

Berdasarkan pengujian dan analisis keamanan website SMK Taman Karya Kebumen dapat disimpulkan bahwa website SMK Taman Karya Kebumen memiliki banyak celah kerentanan yang dibuktikan dengan pengujian kerentanan menggunakan Open Web Application Security Project (OWASP) dari hasil pengujian yang dilakukan ditemukan beberapa kerentanan salah satunya SQL Injection dimana kerentanan tersebut memudahkan penyerang mengakses seluruh database. Adapun rekomendasi penanganan SQL Injection yaitu mengimplementasikan algoritma kriptografi untuk melindungi username

dan password pengguna.

DAFTAR PUSTAKA

- Bekti, bintu humairah. (2015). Mahir Membuat Website Dengan Adobe Dreamweaver CS6. CSS dan JQuery. Yogyakarta: Andi.
- Digdo, G. P. (2017). Panduan Audit keamanan Komputer Bagi Pemula. PT. Elex Media Komputindo. Jakarta.
- Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning). *JUPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, 5(1), Hal. 45. Tersedia : <https://doi.org/10.29100/jipi.v5i1.1565>
- Ika yusnita sari, Muttaqin Muttaqin, J. J. (2020). keamanan data dan informasi. Yayasan Kita Menulis.
- Orisa Mira, & Ardita, M. (2021). Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web. *Jurnal Mnemonic*, 4(1), Hal. 16–19. Tersedia : <https://doi.org/10.36040/mnemonic.v4i1.3213>
- Riadi, I., Yudhana, A., & W, Y. (2020). Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 7(4), Hal. 853. Tersedia : <https://doi.org/10.25126/jtiik.2020701928>
- Satori, A. komariah dan D. (2014). Metodologi Penelitian Kualitatif. Bandung: Alfabetha.
- Sugiyono. (2015). Metode Penelitian Kombinasi (Mix Methods). Bandung: alfabetha.
- Suharsaputra, U. (2012). Metode Penelitian Kuantitatif, Kualitatif, dan Tindakan. Bandung, Refika Aditama.
- Utoro, S., Nugroho, B. A., Meinawati, M., & Widiyanto, S. R. (2020). Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard. *Multinetics*, 6(2), Hal.169–178, Tersedia : <https://doi.org/10.32722/multinetics.v6i2.3432>
- Yayasan OWAPS. (2010). Versi Indonesia.
- Mulyanto Yudi, Haryati Eka (2021) Analisa Website SMAN 1 Sumbawa Menggunakan Metode Vulnerability Asesment, Hal. 394-400, Tersedia : <http://www.jurnal.uts.ac.id/index.php/JINTEKS/article/view/1260>.