CENTIVE
VOL. 4, NO. 1, PP.951-959, DEC 2024
ISBN: 978-602-53004-0-0

Conference on Electrical Engineering, Informatics, Industrial Technology, and Creative Media 2024

Analisis Keamanan dan Pengujian *Access Control* pada Website Pendidikan: Studi Kasus di Universitas Hamzanwadi Lombok

Prayoga Gymnastiar*[1], Nuraini[2], Kusnana[3]

Teknik Informatika, STMIK Komputama Majenang
JL. Majenang – Cimanggu No. 9, Kabupaten Cilacap, Jawa Tengah 53256, Indonesia

[1] prayoga.gymnastiar15@gmail.com
[2] nurainiii6123@gmail.com
[3]nanakusnana@stmikkomputama.ac.id

Dikirim pada 16-11-2024, Direvisi pada 18-11-2024, Diterima pada 29-11-2024

Abstrak

Universitas Hamzanwadi adalah Perguruan Tinggi yang menggunakan *website* untuk informasi pengelolaan akademik dan administrasi. Meningkatnya pengguna website sehingga banyaknya resiko yang akan terjadi jika tidak memiliki keamanan yang baik. Website yang memiliki kerentanan dapat menyebabkan banyak ancaman dari berbagai pihak yang tidak bertanggung jawab untuk mengekploitasi celah kemanan tersebut terutama bagian *access control* yang mengendalikan semua akses penting. Tujuan dari penelitian ini yaitu untuk memperkuat keamanan website terutama *access control* dengan cara analisis *vulnerability* dan pengujian keamanan website hamzanwadi.ac.id yang menggunakan metode penelitian *Automated Security Testing*. Hasil pengujian dari metode tersebut yaitu terdapat kerentanan di bagian *access control* atau halaman admin yang dapat di eksploitasi oleh *attacker* yang tidak bertanggung jawab sehingga dapat merugikan pihak terkait.

Kata Kunci: website, keamanan, *access control*, *attacker*

Penulis Koresponden:
Prayoga Gymnastiar
STMIK Komputama Majenang (*JL. Majenang – Cimanggu No. 9, Kabupaten Cilacap, Jawa Tengah 53256, Indonesia)*
E-Mail : prayoga.gymnastiar15@gmail.com

I. PENDAHULUAN

Berkembang pesatnya Teknologi Informasi, kini menjadi transformasi yang signifikan di berbagai sektor. Peningkatan Teknologi Informasi mengakibatkan banyak sekali penggunanya, salah satunya adalah dalam instansi Pendidikan yang memanfaatkan teknologi tersebut untuk membantu berjalannya operasional dengan baik [1]. Di era digital ini perguruan tinggi harus bisa membangun tidak hanya sekedar memberikan Pendidikan yang berkualitas, tetapi juga membangun citra yang positif, meningkatkan visibilitas dan bisa berkomunikasi secara efektif dengan mahasiswa, calon mahasiswa, dosen, serta Masyarakat umum [2]. Website menjadi konteks utama untuk hal tersebut, karena melalui website instansi Pendidikan dapat memberikan informasi dengan cepat, akurat dan interaktif. Universitas Hamzanwadi adalah salah satu institusi Pendidikan Perguruan Tinggi yang telah menggunakan website sebagai bagian dari sistem informasi untuk mempermudah pengelolaan akademik, administrasi serta menyediakan akses layanan

informasi kepada pengguna. Dengan website tersebut diharapkan mampu menjaga kemanan data dan informasi yang ada di dalamnya.

Namun, dengan mengingat tingginya penggunaan Teknologi Informasi sehingga dapat meningkatkan resiko keamanan siber yang bisa membahayakan kepercayaan pengguna terhadap keamanan sistem tersebut. Seperti, manipulasi data, kebocoran informasi yang sensitif, serta akses tidak sah yang menjadi tantangan dalam sebuah web Pendidikan. Salah satu cara agar keamanan sistem tetap terjaga adalah dengan menerapkan mekanisme *access control* yang memadai. Karena dengan adanya *access control* ini yang menjadi komponen utama dalam keamanan siber untuk menentukan siapa saja yang dapat mengakses, memodifikasi, dan mengelola data pada sistem.

Penelitian ini bertujuan untuk menganalisis keamanan dan pengujian terhadap keamanan sistem pada website Pendidikan Perguruan Tinggi Universitas Hamzanwadi terutama pada bagian kerentanan Access Control menggunakan metode *Automated Security Testing* dengan pemindaian kerentanan website yang digunakan yaitu *OWASP ZAP*, *NUCLEI*, *WEBKILLER*, dan *DIRSEARCH*. Hasil dari penelitian ini, tidak hanya berguna bagi Universitas Hamzanwadi saja, tetapi juga dapat menjadi panduan bagi institusi Pendidikan lainnya dalam meningkatkan website mereka, sehingga dapat mendukung layanan Pendidikan yang aman dan dapat diandalkan di era digital.

Keamanan Sistem Informasi adalah sebuah proses kita dapat mencegah dari penipuan *(cheating)*, atau bisa mendeteksi adanya penipuan dalam sebuah sistem yang berisi informasi, dimana informasi tersebut tidak memiliki arti fisik [3]. Jadi, keamanan sistem informasi adalah cara kita meningkatkan keamanan pada suatu sistem informasi sehingga bisa meminimalisir terjadinya kebocoran data dan akses yang illegal oleh *attacker*.

Pengujian keamanan atau *security testing* adalah proses untuk mengidentifikasi kerentanan atau kelemahan pada suatu sstem, aplikasi, dan jaringan yang dapat dieksploitasi oleh pihak tidak berwenang atau illegal [4]. *OWASP ZAP* adalah alat pengujian keamanan yang digunakan oleh *attacker* untuk mengidentifikasi kerentanan pada suatu aplikasi web termasuk autentikasi yang dipermasalahkan, terungkapnya data sensitif, kesalahan konfigurasi keamanan, injeksi SQL, skrip lintas situs (XSS), deserialisasi yang tidak aman, dan komponen dengan kerentanan yang diketahui [5]. *Nuclei* adalah alat pemindai kerentanan sumber terbuka yang dikembangkan oleh ProjectDiscovery yang mengotomatiskan deteksi kerentanan dalam sistem Teknologi Informasi [6]. Webkiller adalah salah satu alat pemidai kerentanan yang digunakan untuk memindai dan mengumpulkan informasi dan kerentanan pasa suatu sistem tersebut [7]. *Dirsearch* adalah alat untuk menemukan *directory* atau file tersembunyi yang tidak langsung terlihat pada situs web. *Dirsearch* digunakan sebagai bagian dari *reconnaissance* dalam pengujian keamanan, terutama untuk mencari direktori admin, file konfigurasi, atau file Cadangan yang tidak di indeks atau dilindungi [8]. Kontrol Akses adalah sebuah metode atau cara untuk mengatur siapa saja yang memiliki izin sehingga pengguna dapat mengakses sumber daya atau informasi tertentu setelah mereka mendapatkan akses [9]. *Attacker* adalah orang yang berusaha masuk kedalam sebuah sistem atau orang yang melakukan penyerangan pada sebuah sistem dengan memanfaatkan kerentanan pada web tersebut. *Website* adalah Sebuah elemen yang mencakup teks, gambar, suara, dan animasi sehingga menjadi media informasi yang menarik dan diminati serta dikunjungi oleh banyak orang [10].

II.METODE PENELITIAN

Kami menggunakan metode penelitian *Automated Security Testing* untuk melakukan analisis keamanan dan pengujian *Access Controll* pada website Pendidikan Universitas Hamzanwadi. Dalam metode tersebut terdiri dari 4 tahap, yaitu *Planning*, *Information Gathering*, *Penetration Testing*, dan *Reporting.*

Gambar 1. Alur Penelitian

Adapun rancangan dari alur penelitian *Automated Security Testing* terdiri dari Perencanaan *(Planning) p*ada tahap ini yaitu penyusunan metode analisis, menentukan tujuan penelitian, dan menentukan alat untuk pengujian atau *tools scanning* [11]. Jadi, dalam tahapan planning ini yaitu mempersiapkan alat dan bahan yang dibutuhkan untuk melakukan pengujian sebuah system. Pengumpulan Informasi *(Information*

*Gathering) p*ada tahap ini yaitu proses pengumpulan informasi pada website mengenai *Directory* yang terbuka sehingga *attacker* (orang yang melakukan penyerangan) dapat mengakses sistem tersebut [12]. Uji penetrasi *(Penetration Testing) p*ada tahap ini yaitu melakuan eksperimen serangan setelah menemukan kerentanan dalam sebuah system [13]. Pelaporan *(Reporting) p*ada tahap akhir ini, yaitu membuat laporan yang mencakup langkah-langkah pengujian, hasil dari kerentanan keamanan yang terdeteksi dengan menggunakan parameter keamanan *automated scanning* [14].

III. HASIL DAN PEMBAHASAN

Dalam penelitian ini, Langkah-langkah yang dilakukan untuk menemukan celah keamanan pada sebuah website yaitu *planning, information gathering, penetration testing, dan reporting.* Pada *information gathering* terkumpulnya direktori yang terbuka dengan menggunakan *tools automated scanning vulnerability* yaitu *Dirsearch, Webkiller, OWASP ZAP*, dan *Nuclei* pada website hamzanwadi.ac.id. Selanjutnya, dilakukan penetration testing berdasarkan kerentanan yang telah ditemukan pada proses information gathering menggunakan *tools automated scanning Dirsearch* dan *Webkiller*. Hasil dari penelitian ini yaitu berupa *Reporting* atau pelaporan hasil pengujian *access control* pada tahap *penetration testing*.

1. Planning

Planning atau perencanaan adalah tahapan awal untuk melakukan pengujian sebuah system. Tahapan ini, meminta persetujuan kepada pihak kampus untuk melakukan analisis dan pengujian sistem *Access Control* terkait website agar analisis dan pengujian ini bersifat legal atau resmi, menentukan tujuan pengujian, metode dalam pengujian, serta menentukan alat yang diperlukan untuk pengujian sistem, salah satunya adalah menggunakan *virtual machine* Kali Linux yang di dalamnya terdapat banyak *tools scanning* untuk membantu jalannya pengujian. Objek yang akan di uji yaitu website Universitas Hamzanwadi dengan alamat website **hamzanwadi.ac.id.**

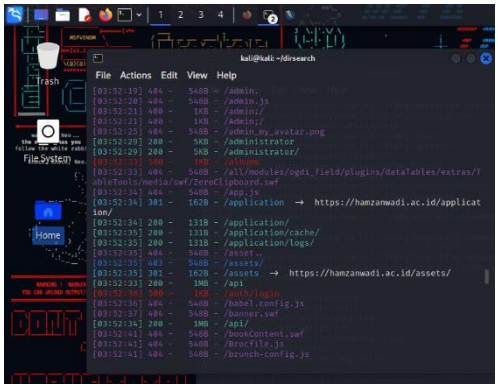
Gambar 2. Tampilan Website Hamzanwadi.ac.id

2. Information Gathering

Setelah menentukan planning, tahapan selanjutnya yaitu information gathering. Maksud dari information gathering itu sendiri adalah mengumpulkan informasi pada website yang akan di uji terkait directory yang terbuka, sehingga *attacker* atau orang yang melakukan penyerangan bisa mendapatkan akses. Dalam tahapan ini juga di bantu dengan tools scanning, yang dalam penelitian menggunakan *automated scanning vulnerability atau* alat pemindaian celah otomatis. Alat yang digunakan yaitu *Dirsearch, Webkiller*, OWASP ZAP, dan *Nuclei.*

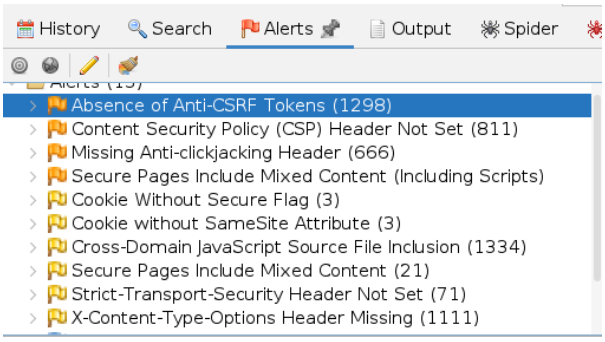
Gambar 3. Hasil information gathering dengan webkiller

Hasil scan dari *tools webkiller* ditemukan bahwa terdapat *admin finder* yang terbuka.



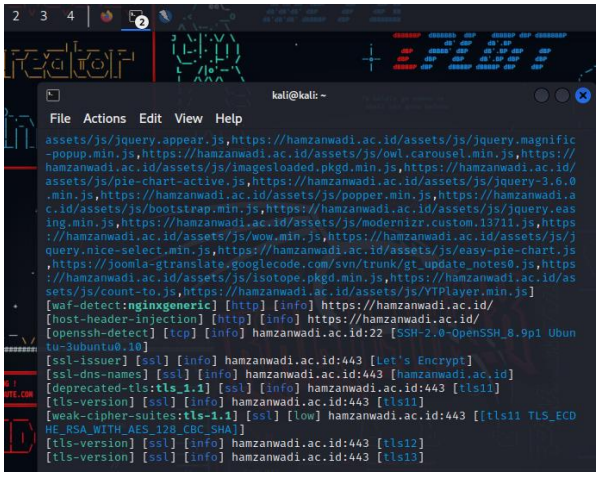
Gambar 4. Hasil information gathering dengan Dirsearch

Hasil scan dari *tools Dirsearch* terdapat directory yang terbuka dengan nilai keterangan 200.



Gambar 5. Hasil information gathering dengan OWASP ZAP

Hasil scan *tools OWASP ZAP* terdapat informasi *vulnerability* yang berjumlah 9 kerentanan.



Gambar 6. Hasil Information Gathering dengan Nuclei

Hasil dari scan *tools Nuclei* menunjukan adanya kelemahan di SSL dengan keterangan ***Risk Rating Low***. Hasil analisis dari proses scanning yang telah dilakukan dirangkum dalam tabel berikut. Tabel ini memuat informasi terkait jenis kerentanan, lokasi temuan, serta bukti yang mendukung. Temuan ini diharapkan dapat memberikan gambaran mengenai potensi risiko keamanan yang perlu diperhatikan untuk meningkatkan perlindungan website Universitas Hamzanwadi.

Tabel 1. Hasil Analisis

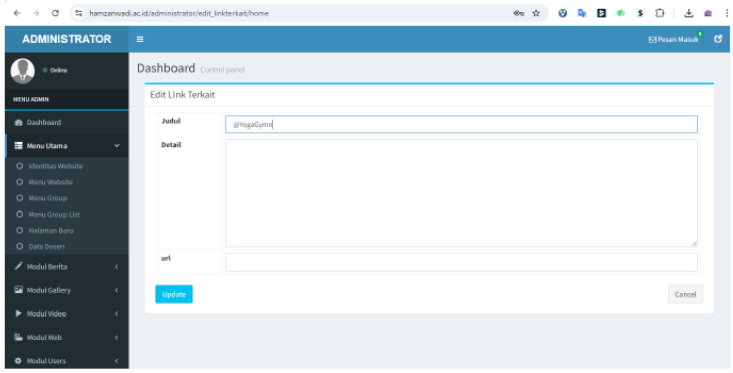
No	Tools	Temuan	Detail URL/ Evidence
1	Webkiller	Direktori Terbuka	https://hamzanwadi.ac.id//administrator/found
2	Dirsearch	Direktori Terbuka	/administrator, /application/, /api/, /composer.json, /contributing.md, /download, /index.php, /maintenance.html, /system
3	Nuclei	Weak Cipher Suites	hamzanwadi.ac.id:443 [[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]]
4	OWASP ZAP	Absence of Anti-CSRF Token	URL: http://hamzanwadi.ac.id/ Evidence: <form method="POST" action="http://hamzanwadi.ac.id/berita">
5	OWASP ZAP	Content Security Policy (CSP) Header Not Set	URL: http://hamzanwadi.ac.id/robots.txt
6	OWASP ZAP	Missing Anti-clickjacking Header	URL: http://hamzanwadi.ac.id/agenda/detail/building-human-resource-awarness-in-the-implementation-of-inclusive-education-
7	OWASP ZAP	Secure Pages Include Mixed Content (Including Scripts)	URL: https://hamzanwadi.ac.id/download Evidence: http://s7.addthis.com/js/250/addthis_widget.js#pubid=ra-4f8aab4674f1896a
8	OWASP ZAP	Cookie Without Secure Flag	URL: https://hamzanwadi.ac.id/berita/kategori/kerja-sama?text=ZAP Evidence: Set-Cookie: ci_session
9	OWASP ZAP	Cookie Without SameSite Attribute	URL: https://hamzanwadi.ac.id/berita/kategori/kerja-sama?text=ZAP Evidence: Set-Cookie: ci_session

No	Tools	Temuan	Detail URL/ Evidence
10	OWASP ZAP	Cross-Domain JavaScript Source File Inclusion	URL: http://hamzanwadi.ac.id/agenda/detail/building-human-resource-awarness-in-the-implementation-of-inclusive-education-Evidence: <script type="text/javascript" src="https://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit2"></script>
11	OWASP ZAP	Strict-Transport-Security Header Not Set	URL: https://hamzanwadi.ac.id/%3C%20?php%20echo%20base_url();%20?%3Eassets/img/download.jpg
12	OWASP ZAP	X-Content-Type-Options Header Missing	URL: http://hamzanwadi.ac.id/agenda/detail/building-human-resource-awarness-in-the-implementation-of-inclusive-education-

3. *Penetration Testing*

Setelah mengetahui informasi terkait *directory* yang terbuka sehingga *attacker* dapat masuk ke dalam website hamzanwadi.ac.id. Berdasarkan hasil scan *webkiller* dan *Dirsearch* yaitu: https://hamzanwadi.ac.id/administrator/. Berdasarkan hasil halaman *Access Control*, *Attacker* dapat mengakses dan mengontrol halaman admin tetrsebut dengan berbagai cara antara lain: *unprotected admin request parameter*, *brute force*, dan *bypass SQL*.

Halaman tersebut terdapat *security code*, sehingga untuk melakukan simulasi serangan melalui brute force dan bypass SQL tidak dapat dilakukan sebab serangan *brute force* melakukan Upaya terus menerus untuk menebak informasi login melalui payload yang telah di kumpulkan. Sedangkan *bypass SQL* melakukan input login dengan memanfaatkan kerentanan dalam *Query SQL* yang tidak memvalidasi input dengan benar. Sehingga *brute force* dan *Bypass SQL* tidak dapat masuk karena terdapat *security code* yang berfungsi sebagai penghalang tambahan sehingga menyulitkan serangan otomatis dan memperlambat Upaya akses yang berulang atau tidak sah. Dikarenakan *brute force* dan *bypass SQL* tidak bisa masuk ke halaman log in, *attacker* hanya bisa melakukan serangan *unprotected admin.*



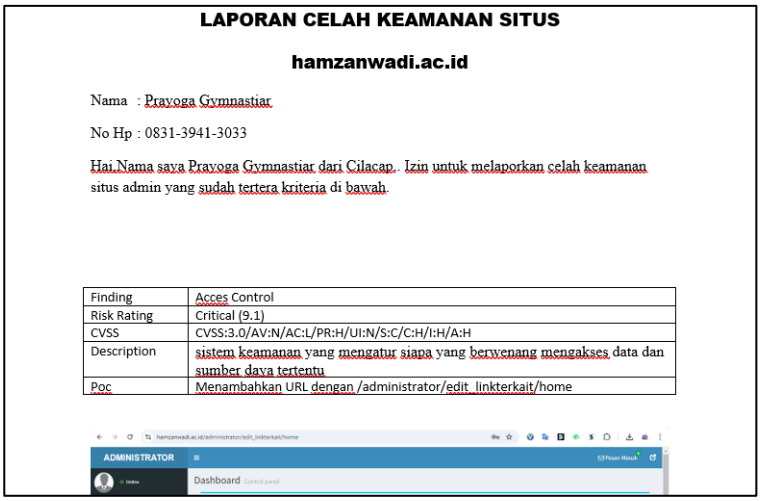
Gambar 7. Hasil Login Access Control

Untuk masuk ke halaman admin yaitu memanfaatkan kerentanan menggunakan cara *unprotected access control* dengan memanfaatkan bagian-bagian sistem atau data yang seharusnya dibatasi, tanpa harus melewati autentikasi atau otorisasi yang diperlukan. Cara masuk *acces control* atau halaman admin tersebut adalah dengan memanfaatkkan celah *unprotected admin* dengan cara memodifikasi URL website tersebut dengan menambahkan /administrator/edit_linkterkait/home.

4. *Reporting*

Pada tahap ini yaitu melaporkan hasil dari *scanning vulnerability access control* pada website hazanwadi.ac.id kepada civitas kampus beserta Solusi untuk memperbaikinya.

Berdasarkan *penetration testing* pada tahapan sebelumnya ditemukan bahwa pada website hamzanwadi.ac.id terdapat kerentanan di *access control* atau halaman admin.



LAPORAN CELAH KEAMANAN SITUS

hamzanwadi.ac.id

Nama : Prayoga Gymnastiar

No Hp : 0831-3941-3033

Hai,Nama saya Prayoga Gymnastiar dari Cilacap.. Izin untuk melaporkan celah keamanan situs admin yang sudah tertera kriteria di bawah.

Finding	Acces Control
Risk Rating	Critical (9.1)
CVSS	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
Description	sistem keamanan yang mengatur siapa yang berwenang mengakses data dan sumber daya tertentu
Poc	Menambahkan URL dengan /administrator/edit_linkterkait/home

Gambar 8. Laporan Hasil Kerentanan dan Report

Tabel 2. Hasil Penetration Testing

No	Kerentanan	Temuan (Tools)	Kategori (OWASP)	Standar Keamanan	Rekomendasi Perbaikan
1	Direktori Terbuka	Dirsearch dan Webkiller	Sensitive Data Exposure	Jangan mengekspose direktori.	Gunakan file `.htaccess` untuk membatasi akses direktori sensitif.
2	Weak Cipher Suites	Nuclei	Security Misconfiguration	Nonaktifkan cipher lemah.	Perbarui TLS ke versi terbaru dan gunakan cipher suite yang lebih aman.
3	Absence of Anti-CSRF Token	OWASP ZAP	Cross-Site Request Forgery (CSRF)	Harus ada token CSRF.	Terapkan token CSRF unik untuk setiap sesi pengguna.
4	Content Security Policy (CSP) Header Not Set	OWASP ZAP	Security Misconfiguration	Header CSP wajib ada.	Tambahkan header CSP yang mengontrol sumber konten yang diizinkan.
5	Missing Anti-clickjacking Header	OWASP ZAP	Clickjacking	Header X-Frame-Options penting.	Tambahkan header `X-Frame-Options` dengan nilai `DENY` atau `SAMEORIGIN`.
6	Cookie Without Secure Flag	OWASP ZAP	Security Misconfiguration	Cookie harus aman.	Tambahkan atribut `Secure` dan `HttpOnly` pada cookie.
7	Cross-Domain JavaScript Source File Inclusion	OWASP ZAP	Cross-Domain Inclusion	Hindari JavaScript eksternal.	Hindari penggunaan file eksternal dari domain yang tidak terpercaya.

No	Kerentanan	Temuan (Tools)	Kategori (OWASP)	Standar Keamanan	Rekomendasi Perbaikan
8	Strict-Transport-Security Header Not Set	OWASP ZAP	Security Misconfiguration	Header HSTS wajib ada.	Tambahkan header `Strict-Transport-Security` untuk memaksa HTTPS.
9	X-Content-Type-Options Header Missing	OWASP ZAP	Security Misconfiguration	Header X-Content-Type wajib ada.	Tambahkan header `X-Content-Type-Options` dengan nilai `nosniff`.

VI. KESIMPULAN

Hasil penelitian ini menunjukkan bahwa sistem access control pada website Universitas Hamzanwadi masih memiliki beberapa kerentanan yang dapat dieksploitasi oleh pihak tidak berwenang. Salah satu temuan utama adalah direktori sensitif seperti /administrator yang dapat diakses tanpa autentikasi, serta absennya header keamanan seperti Strict-Transport-Security (HSTS). Kondisi ini meningkatkan risiko serangan akses tidak sah terhadap sistem, yang berpotensi membuka peluang manipulasi data atau kontrol terhadap fungsi-fungsi kritis website. Berdasarkan temuan ini, penelitian menyimpulkan bahwa perlindungan terhadap akses ke direktori sensitif harus menjadi prioritas utama. Implementasi kontrol akses berbasis peran (Role-Based Access Control/RBAC), penggunaan token autentikasi yang aman, serta validasi input URL sangat penting untuk memastikan keamanan sistem.

1. Penemuan Kerentanan pada Access Control
   Berdasarkan hasil pengujian keamanan, ditemukan beberapa kerentanan pada sistem access control website Universitas Hamzanwadi, seperti direktori admin yang terbuka dan mekanisme autentikasi yang tidak optimal. Hal ini berpotensi memungkinkan penyerang mendapatkan akses tidak sah ke sistem, yang dapat berdampak signifikan pada integritas data dan keamanan pengguna.
2. Analisis Tingkat Risiko
   Kerentanan seperti direktori terbuka dan absennya header keamanan seperti Strict-Transport-Security memiliki tingkat risiko tinggi terhadap serangan akses tidak sah. Implementasi mekanisme autentikasi dan otorisasi yang kuat sangat diperlukan untuk mengatasi masalah ini.
3. Rekomendasi Utama
   Terapkan kontrol akses berbasis peran (Role-Based Access Control/RBAC) untuk membatasi akses ke direktori sensitif hanya kepada pengguna yang memiliki izin.
   Implementasikan autentikasi berbasis token yang aman untuk melindungi endpoint sensitif.
   Validasi input URL dan batasi akses terhadap direktori admin menggunakan autentikasi tambahan serta mekanisme enkripsi komunikasi melalui HTTPS.
4. Implikasi untuk Sistem Pendidikan Digital
   Penelitian ini memberikan wawasan penting bagi institusi pendidikan dalam memperkuat access control sebagai bagian integral dari keamanan siber. Implementasi sistem keamanan yang lebih baik tidak hanya melindungi data pengguna, tetapi juga meningkatkan kepercayaan terhadap layanan digital Universitas.

UCAPAN TERIMAKASIH

Peneliti mengucapkan terima kasih kepada semua pihak yang telah membantu peneliti dalam menyelesaikan penelitian ini Terkhusus kepada segenap pihak Universitas Hamzanwadi yang telah memberikan persetujuan kepada peneliti untuk melakukan analisis dan pengujian system Access Control pada website hamzanwadi.ac.id. Kepada bapak Kusnana, M.Kom selaku dosen pembimbing dari STMIK Komputama Majenang yang telah membantu peneliti, pada penelitian yang kami lakukan ini dengan judul *"Analisis Keamanan dan Pengujian Access Control pada Website Pendidikan: Studi Kasus Universitas Hamzanwadi Lombok."*

DAFTAR PUSTAKA

[1] Prihandoyo Teguh, M. (2018). Unified Modeling Language (Uml) Model Untuk Pengembangan Sistem Informasi Akademik Berbasis Web. Jurnal Informatika: Jurnal Pengembangan It (Jpit), Vol.03, No.01.

[2] Harahap Parlindungan & Ilka Zufria. (2024). Analisis Keamanan Pada Website Upm Saintek Uinsu Medan Menggunakan Metode Vulnerability Assesment. Cosmic Jurnal Teknik, Vol. 2 No. 1.

[3] Indri Widya Wulandari & Hwihanus (2023). Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan. Jkpim: Jurnal Kajian Dan Penalaran Ilmu Manajemen Vol.1, No.1 Januari 2023.

[4] Mochammad Dzaki Al Vriano (2023). Pengujian Keamanan Web Juice Shop Dengan Metode Pentesting Berbasis Owasp Top 10. Kohesi: Jurnal Multidisiplin Saintek, Volume 01, No. 06 2023, Pp. 81-90.

[5] M. Fery Afrizal Ramadhan, Asri Samsiar Ilmananda (2024). Analisis Ancaman Keamanan Pada Sistem Informasi Akademik Kampus Menggunakan Metode Owasp Zap. Jati *(Jurnal Mahasiswa Teknik Informatika)* Vol. 8 No. 4, Agustus 2024.

[6] Vaadata.Com. (2024). "Introduction To Nuclei, An Open Source Vulnerability Scanner". Https://Www.Vaadata.Com/Blog/Introduction-To-Nuclei-An-Open-Source-Vulnerability-Scanner/. Diakses Pada, Kamis, 31 Oktober 2024.

[7] Geeksforgeeks.Org. (2021). "Webkiller V2.0 – Alat Pengumpul Informasi Alat Di Kali Linux." Https://Www.Geeksforgeeks.Org/Webkiller-V2-0-Tool-Information-Gathering-Tool-In-Kali-Linux/ . Diakses Pada, Kamis, 31 Oktober 2024.

[8] Nugroho Agung Prasetiyo, Dkk (2024). Audit Dan Analisis Website Pemerintah Menggunakan Pengujian Penetrasi Sql Injection. Jurnal Teknologi Informasi, Komputer Dan Aplikasinya (Jtika) Vol. 6, No. 2, September 2024, (Terakreditasi Sinta-4, Sk No:164/E/Kpt/2021).

[9] Esra Abdullatif Altulaihan, Dkk (2023). A Survey On Web Application Penetration Testing. Electronics 2023, 12, 1229.

[10] Mia Zattu Maharani, Dkk (2017). Analisis Keamanan Website Menggunakan Metode Scanning Dan Perhitungan Security Metriks. E-Proceeding Of Applied Science : Vol.3, No.3 Desember 2017 | Page 1775.

[11] Fazrin Tri Wahyuni, Dkk (2024). Analisis Vulnerability Dan Risk Assesment Terhadap Website Pt. Dapur Cokelat Indonesia Menggunakan Metode Penetration Testing. Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (Senafti), 7 September 2024 – Jakarta, Indonesia.

[12] Buthayna Alsharaa, Dkk (2023). Selected Advanced Themes In Ethical Hacking And Penetration Testing. Computer Science And Information Technologies Vol. 4, No. 1, March 2023, Pp. 69~75.

[13] Laila Fadila Burhani & Diah Priyawati (2024). Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (Ptes). Jipi (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika) Vol. 9, No. 1, Maret 2024, Pp. 307-319.

[14] Ferby Septian1, Dkk. (2024). Pengujian Keamanan Website Dengan Metode Penetration Testing (Studi Kasus: Universitas Esa Unggul). Innovative: Journal Of Social Science Research Volume 4 Nomor 5 Tahun 2024 Page 3629-3647.