Jurnal Sistem Informasi (TEKNOFILE) Vol. 2, No. 6 Juni 2024, Hal. 409 - 420
E-ISSN : 3026-4936

ANALISIS KERENTANAN KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN OWASP-ZAP DI UNIVERSITAS ISLAM INDRAGIRI

[1]Sabrina Asiah Febriani, [2] Abdul Muni, [3]Bayu Rianto, [4] Muhammad Jalil, [5]Chrismondari
[1234]Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Islam Indragiri,
[5]Sekolah Tinggi Teknologi Pekanbaru
Email: sabrinaaf010203@gmail.com[1], abdulmuni@live.com[2], rianto.bayu91@gmail.com[3], m.jalil10000@gmail.com[4], Chrismondari123@gmail.com[5]

ABSTRAK

Universitas Islam Indragiri, salah satu institusi pendidikan di Indragiri Hilir, menggunakan sistem informasi akademik yang disebut SIAKAD CLOUD dalam melakukan kegiatan akademik. Namun, penggunaan teknologi meningkatkan risiko pelanggaran data, sehingga analisis keamanan data menjadi penting untuk menjaga integritas dan keamanan data. OWASP ZAP adalah aplikasi yang dapat digunakan untuk mengidentifikasi kerentanan pada aplikasi web, seperti injeksi SQL, cross-site scripting (XSS), dan konfigurasi yang lemah. Vulnerability Assessment merupakan sebuah keretanan, kekurangan atau celah pada sistem, yang dapat dimanfaatkan oleh satu atau lebih penyerang untuk melakukan serangan yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan suatu system. Penelitian ini menggunakan website sebagai alat untuk menyelidiki kerentanan website terhadap penelitian yang dilakukan menggunakan OWASP ZAP. Penelitian menggunakan metode Studi Literatur dengan mengumpulkan data dan informasi dari internet dan artikel jurnal. Peneliti kemudian menganalisis dan menyelidiki kerentanan website menggunakan OWASP ZAP dan mencari solusinya. Studi tersebut menemukan bahwa situs web memiliki 14 kerentanan, mulai dari sedang hingga rendah, dan 4 kerentanan pada tingkat informasi. Total 18 kerentanan ditentukan oleh jenis, level, dan rekomendasi penelitian. Jika situs web dianggap rentan, perbaikan harus dilakukan untuk melindunginya dari potensi ancaman. Namun, kerentanan pada web SIAKAD CLOUD ini masih tergolong rendah, dan administrator mungkin perlu meningkatkan keamanan situs web untuk mencegah serangan lebih lanjut.

Kata Kunci: Keamanan, Sistem Informasi, *SIAKAD CLOUD, OWASP ZAP, Vulnerability Assessment*

ABSTRACT

Indragiri Islamic University, one of the educational institutions in Indragiri Hilir, uses an academic information system called SIAKAD CLOUD in conducting academic activities. However, the use of technology increases the risk of data breaches, so data security analysis is important to maintain data integrity and security. OWASP ZAP is an application that can be used to identify vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and weak configuration. Vulnerability Assessment is a vulnerability, flaw or gap in the system, which can be exploited by one or more attackers to carry out attacks that can compromise the confidentiality, integrity, or availability of a system. This research uses the website as a tool to investigate website vulnerabilities to research conducted using OWASP ZAP. The research uses the Literature Study method by collecting data and information from the internet and journal articles. The researcher then analyzed and investigated website vulnerabilities using OWASP ZAP and looked for solutions. The study found that the website has 14 vulnerabilities, ranging from moderate to low, and 4 vulnerabilities at the information level. A total of 18 vulnerabilities are determined by the type, level, and recommendations of the study. If a website is deemed vulnerable, improvements should be made to protect it from potential threats. However, these vulnerabilities on the SIAKAD CLOUD website are still relatively low, and administrators may need to improve website security to prevent further attacks.

Keywords: Security, Information System, SIAKAD CLOUD, OWASP ZAP, Vulnerability Assessment

1 PENDAHULUAN

Universitas Islam Indragiri merupakan sebuah perguruan tinggi yang didirikan di wilayah Indragiri Hilir, Riau. UNISI berkomitmen untuk memberikan pendidikan berkualitas yang menggabungkan nilai-nilai Islam dengan perkembangan ilmu pengetahuan dan teknologi. Sebagai bagian dari visi dan misinya dalam meningkatkan kualitas pendidikan dan pengelolaan institusi, UNISI telah mengimplementasikan berbagai sistem informasi yang memadukan kebutuhan administrasi dengan teknologi.

Sebagai institusi yang berkomitmen pada penerapan teknologi untuk mendukung proses akademik dan administratif, UNISI terus berupaya memperbarui dan meningkatkan keamanan sistem informasi mereka yang senantiasa mengutamakan prinsip-prinsip keamanan data dan privasi, sesuai dengan standar dan regulasi yang berlaku. Hal ini penting untuk memastikan bahwa informasi yang dikelola oleh sistem informasi UNISI tidak hanya dapat diakses dengan mudah, tetapi juga terlindungi dari potensi risiko keamanan yang mungkin timbul.

SIAKAD CLOUD merupakan produk unggulan SEVIMA sebagai solusi manajemen akademik terintegrasi yang terlengkap, aman, dan terbukti powerfull dalam memudahkan tata kelola perguruan tinggi dan pelaporan PDDIKTI. Siakad Cloud merupakan sistem informasi akademik berbasis cloud yang digunakan oleh perguruan tinggi untuk mengelola data mahasiswa, jadwal perkuliahan, nilai, dan informasi akademik lainnya secara terpusat dan mudah diakses

Sistem informasi akademik memiliki peran yang sangat penting dalam menunjang berbagai aktivitas di institute Pendidikan tinggi, seperti pendaftaran, pengelolaan data mahasiswa, jadwal kuliah, dan penilaian. Dengan meningkatnya digitalisasi, keamanan sistem informasi akademik menjadi isu yang semakin kritis. Kerentanan dalam sistem ini dapat membuka peluang bagi pelaku jahat untuk mengakses atau merusak data, yang pada gilirannya dapat berdampak buruk pada institusi, staf, dan mahasiswa.

Universitas Islam Indragiri, sebagai salah satu institusi pendidikan tinggi di Kabupaten Indragiri Hilir juga mengadopsi sistem informasi akademik untuk mengelola aktivitas akademiknya dengan menggunakan website yang Bernama SIAKAD CLOUD. Namun, seiring dengan penggunaan teknologi, risiko terkait keamanan informasi juga meningkat. Oleh karena itu, analisis kerentanan pada sistem ini menjadi langkah yang sangat penting untuk memastikan integritas dan kerahasiaan data.

OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) adalah salah satu alat yang dapat digunakan untuk mengidentifikasi kerentanan pada aplikasi web. Alat ini menawarkan berbagai fitur untuk mendeteksi kerentanan umum yang sering terjadi pada sistem informasi akademik, seperti injeksi SQL, cross-site scripting (XSS), dan keamanan konfigurasi yang lemah.[1]

Dalam penelitian ini, akan dilakukan analisis kerentanan keamanan sistem informasi akademik Universitas Islam Indragiri menggunakan OWASP ZAP. Tujuan dari penelitian ini adalah untuk mengidentifikasi potensi risiko keamanan yang ada, serta memberikan rekomendasi untuk meningkatkan keamanan sistem informasi akademik tersebut. Dengan hasil analisis ini, diharapkan Universitas Islam Indragiri dapat meningkatkan keamanan sistem informasinya dan melindungi data dari ancaman keamanan yang semakin kompleks.

Dalam upaya menyempurnakan penelitian ini maka dilakukan kajian literatur pembanding yang searah mengenai penelitian, diantaranya yaitu :

Pada penelitian sebelumnya [2] menganalisis tentang Keamanan Sistem Informasi Pada Universitas Duta Bangsa Surakarta Menggunakan Sudomy dan OWASP ZAP. Hasil uji menunjukkan Sudomy memberikan laporan yang infomatif sebagai pendukung keputusan pihak manajemen. Laporan OWASP ZAP harus diolah kembali supaya mempermudah manajemen dalam mengambil keputusan terkait celah keamanan yang ditemukan. Baik Sudomy dan OWASP ZAP memiliki lisensi yang selaras dengan Free Open Source Software sehingga mudah didapatkan dan rendah biaya.

Penelitian Ariyadi [3] menganalisis dan menguji kerentanan sistem informasi akademik Universitas Bina Darma menggunakan OWASP. Hasil uji menunjukkan kerentanan keamanan website didominasi pada tahap medium (sedang) namun tidak menutup kemungkinan untuk administrator

meningkatkan keamanan website tersebut agar tidak mudah di eksploitasi oleh pihak internal maupun eksternal.

Adapun penelitian Perdana [4] menganalisis tentang Audit Keamanan Sistem Informasi Akademik Menggunakan Framework NIST SP 800-26 pada Universitas Sangga Buana YPKP Bandung. Dengan hasil uji menunjukkan bahwa prosedur dan pengendalian yang ditetapkan oleh pihak institusi sudah dijalankan. Hal tersebut didapat berdasarkan hasil penilaian audit keamanan secara keseluruhan yang berada pada angka 3,7005 dari 5.

Penelitian selanjutnya [5] menganalisis tentang Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 pada Sistem Informasi Akademik Universitas XYZ. Dengan hasil uji menunjukkan penilaian risiko berbasis keamanan informasi, universitas xyz memiliki 1 tingkat risiko tinggi, 5 tingkat risiko sedang dan 52 tingkat risiko rendah.

Dan Penelitian berikutnya Mu'min [6] menganalisis sistem informasi akademik dengan menggunakan open web aplication security project framework pada SIA STIKES Guna Bangsa Yogyakarta. Dengan hasil pengujian website masih memiliki tingkat kerentanan yang tergolong cukup aman dari serangan hacker.

Sistem Akademik atau Sistem Informasi Akademik adalah suatu system yang dirancang untuk keperluan pengelolaan data data akademik dengan penerapan teknologi computer baik hardware maupun software sehingga seluruh proses kegiatan akademik dapat terkelola menjadi informasi yang bermanfaat dalam pengelolaan manajemen perguruan tinggi dan pengambilan Keputusan-keputusan.[7] Sistem Informasi akademik yang dibangun untuk memberikan kemudahan kepada pengguna dalam kegiatan administrasi akademik kampus secara online, seperti proses Penerimaan Mahasiswa Baru (PMB), pembuatan jadwal kuliah, pengisian Kartu Rencana Studi (KRS), pengisian nilai, perwalian, pengelolaan data dosen dan mahasiswa.

Keamanan system informasi merupakan segala Tindakan yang dilakukan untuk memastikan bahwa data dalam suatu system terlindungi dari ancaman. Ancaman bisa berupa serangan dari luar seperti hacking, virus, atau walware, maupun dari dalam seperti kebocoran data oleh oknum karyawan.[8] Vulnerability Assessment merupakan sebuah keretanan, kekurangan atau celah pada sistem, yang dapat dimanfaatkan oleh satu atau lebih penyerang untuk melakukan serangan yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan suatu system.[9]

Open Web Application Security Project (OWASP) adalah sebuah framework yang bersifat open source yang berfokus dalam memperbaiki keamanan software aplikasi.[10] OWASP merupakan organisasi yang dibangun untuk menemukan celah keamanan dari sebuah aplikasi website.[11]

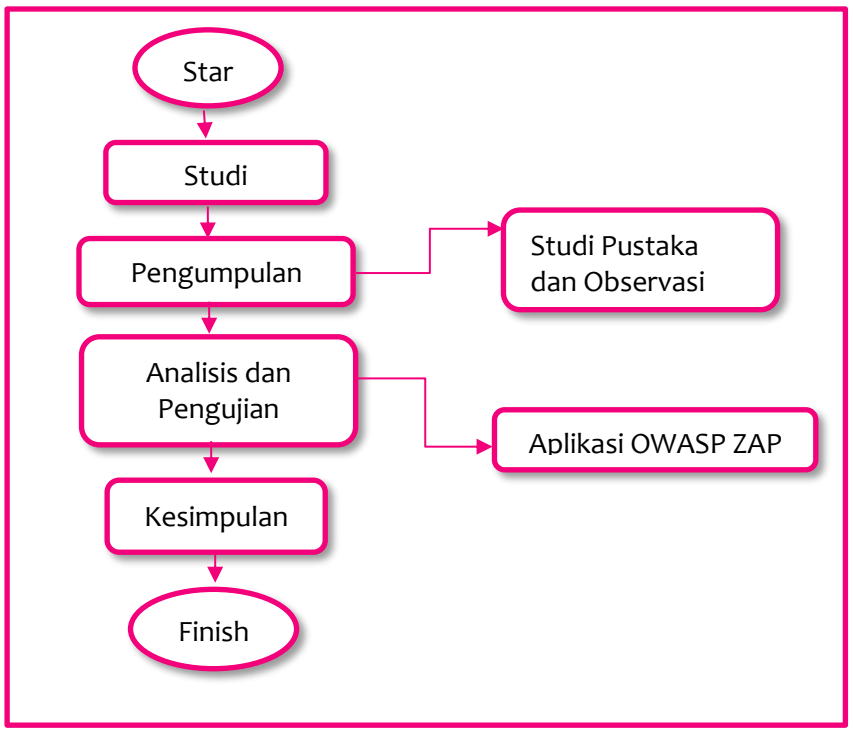
Zed Attack Proxy (ZAP) merupakan tools alat pengujian penetrasi open-source gratis yang dikelola dibawah payung Open Web Aplication Security Project (OWASP). ZAP dirancang khusus untuk menguji aplikasi web dan fleksibel serta dapat diperluas. ZAP yang dikenal dengan "proxy man-in-the-middle"ini berdiri diantara browser penguji dan aplikasi web sehingga dapat mencegat dan memeriksa pesan yang dikirim antar browser dan aplikasi web.[12]

OWASP ZAP merupakan sebuah aplikasi yang digunakan untuk Penetration Testing dalam menemukan vulnerabilities/celah keamanan pada suatu aplikasi website.[13]

2 METODE PENELITIAN

2.1 Kerangka Kerja Penelitian

Berikut ini merupakan kerangka kerja penelitian yang dilakukan dalam melakukan analisis kerentanan suatu website menggunakan aplikasi OWASP ZAP. Dalam penelitian ini, peneliti menggunakan website sebagai bahan untuk menguji bagaimana kerentanan website tersebut tehadap serangan-serangan yang dilakukan melalui aplikasi OWASP ZAP. Dalam hal ini, adapun tahapan yang akan dilakukan yaitu peneliti menggunakan metode studi literatur, sebagai teknik untuk Mengumpulkan data dan informasi yang berkaitan dengan penelitian melalui internet dan rata-rata berupa Artikel atau Jurnal Penelitian.[14] Selanjutnya peneliti melakukan analisis dan melakukan Pengujian kerentanan website menggunakan aplikasi OWASP ZAP dan mencari solusinya, lalu langkah terakhir peneliti menarik kesimpulan dari hasil penelitian yang telah dilakukan.[15] Hal ini berdasarkan dengan gambar 1 di bawah ini:



Gambar 1 Kerangka Kerja Penilitian

2.2 Pengumpulan Data

Dalam penelitian ini, Peneliti menggunakan 2 cara, yaitu:

a. Studi Pustaka

Dalam hal ini peneliti mempelajari, meneliti dan menelaah berbagai literatur dari berbagai sumber seperti jurnal ilmiah, situs internet dan bacaan lainnya yang berkaitan dengan penelitian yang dilakukan.

b. Observasi dan Wawancara

Dalam hal ini peneliti melakukan observasi dan wawancara untuk memperoleh data dan informasi yang akurat tentang penelitian yang dilakukan dengan cara melakuan penelitian pada objek dan percobaan secara langsung pada website yang akan digunakan yaitu *https://siakadcloud.unisi.ac.id/gate/login*

Berikut merupakan dokumentasi pada saat peneliti melakukan observasi di Universitas Islam Indragiri.

Gambar 2 Observasi di Universitas Islam Indragiri

Gambar 3 Wawancara

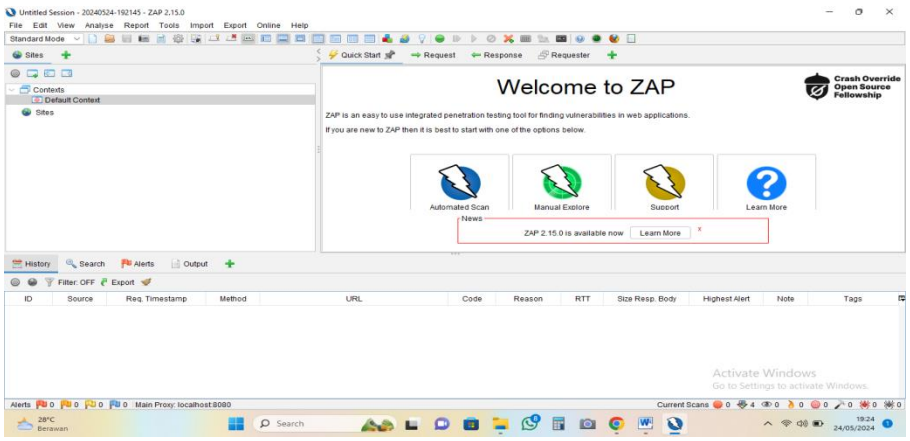
3 HASIL DAN PEMBAHASAN

Berdasarkan tahap awal yang dilakukan, peneliti berhasil menganalisis masalah kerentanan keamanan pada situs web, khususnya situs Sistem Akademik, dari berbagai sumber, termasuk jurnal penelitian, prosiding, dan literatur online. Dari berbagai sumber tersebut dapat diambil kesimpulan bahwa jika seorang Administrator mengabaikan keamanan sistem dari website atau melakukan kesalahan dalam penulisan kode keamanan, tentunya akan terbuka celah yang memungkinkan seorang Hacker atau oknum yang tidak bertanggung jawab melakukan peretasan website untuk keuntungan pribadi pelaku.[16] Untuk mengkaji lebih dalam terkait permasalahan ini, peneliti menjadikan Sistem Akademik Universitas Islam Indragiri atau yang dikenal dengan SIAKAD CLOUD sebagai objek penelitian. Siakad Cloud ini memuat berbagai hal yang berkaitan dengan akademik termasuk dengan Data Pribadi dari Mahasiswa maupun Dosen. Namun disisi lain website ini sering kali mengalami Down karena tingginya tingkat akses sehingga memungkinkan terbukanya celah untuk hacker masuk dan mencuri berbagai data dan informasi penting untuk tujuan tertentu.

Dari permasalahan tersebut, upaya solusi pun mulai direncanakan pada tahap selanjutnya yakni peneliti berencana untuk melakukan Analisis Kerentanan Keamanan Sistem Informasi Akedemik Universitas Islam Indragri (Siakad Cloud) yang bertujuan untuk meningkatkan keamanan dari website tersebut. Untuk terlaksanannya penelitian ini, peneliti membutuhkan aplikasi OWASP ZAP dengan automated scanner atau manual expore yang bertujuan untuk mendapatkan hasil keretanan terhadap website agar dapat menghindari serangan yang tidak diinginkan terjadi pada website tersebut.

Tahap selanjutnya peneliti akan mulai mengeksekusi rencana pengujian kerentanan website dengan menggunakan OWASP ZAP. Pada hal ini peneliti akan melakukan pengujian kerentanan secara menyeluruh pada website *https://siakadcloud.unisi.ac.id/gate/login* secara otomatis.

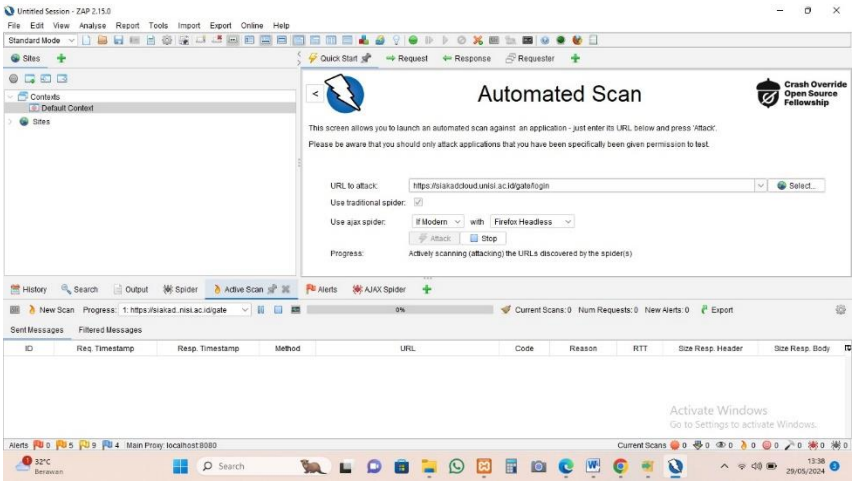
Berikut adalah langkah-langkah dalam mencari celah kerentanan keamanan dengan menggunakan owasp-zap melalui Automated Scanner dan Manual Expore: Pertama silahkan buka apliaksi Owasp-Zap. Jika sudah terbuka maka akan ada 2 pilihan yang disediakan oleh aplikasi owasp-zap yaitu Automated scan dan Manual expore, dapat dilihat pada Gambar 4 dibawah ini.



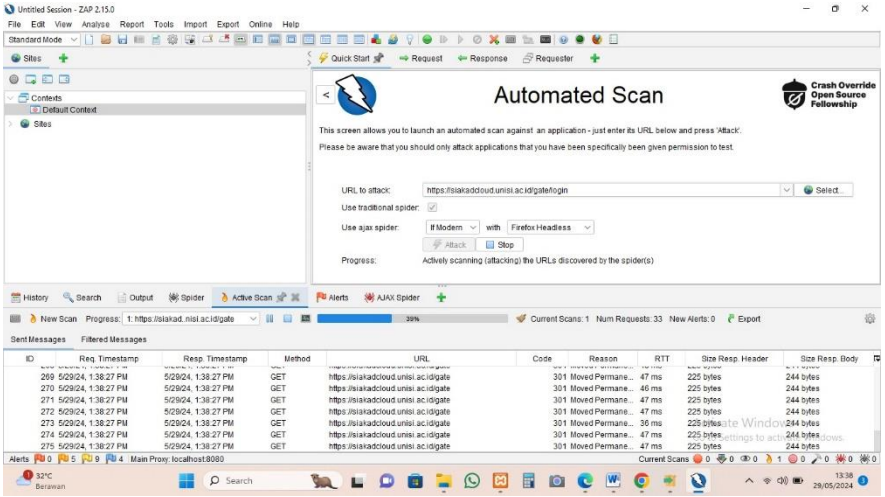
Gambar 4 Tampilan Awal OWASP ZAP

Jiika ingin menggunakan Automated Scan maka klik Automated Scan, lalu masukan link https://siakadcloud.unisi.ac.id/gate/login

Kemudian klik attack maka aplikasi owasp-zap akan langsung otomatis memperoses hasil dari link tersebut, bisa dilihat pada gambar 5 dan 6 dibawah ini.

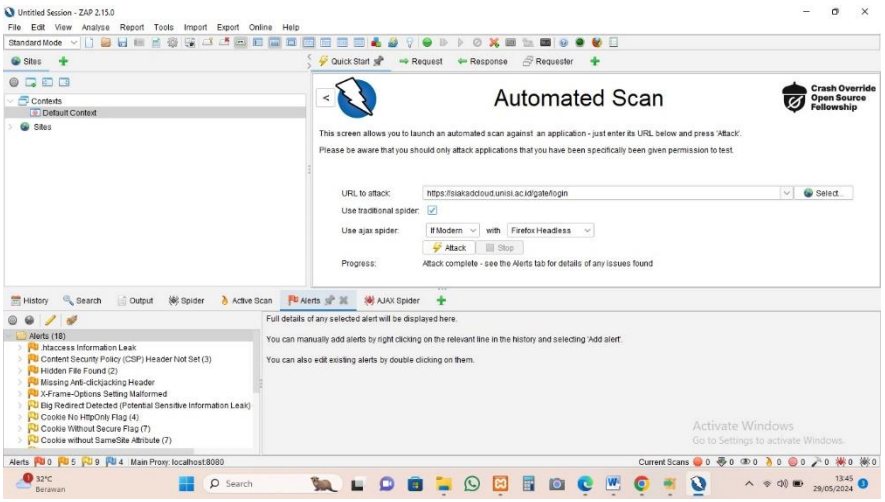


Gambar 5 Proses attack link



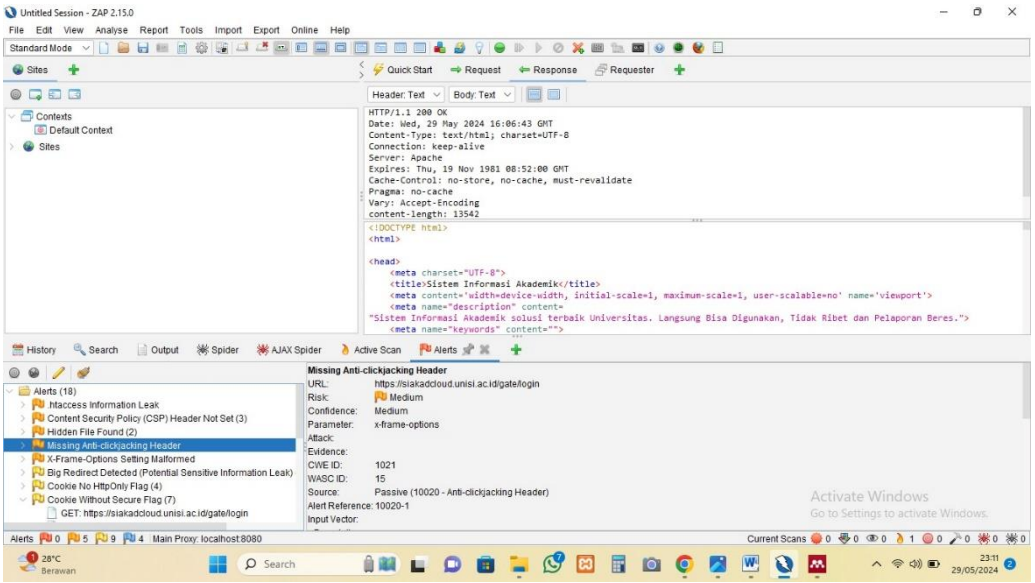
Gambar 6 Tampilan Proses Automated Scan

Setelah proses scanning sudah selesai maka akan terlihat beberapa kerentanan, menurut Owasp-Zap website https://siakadcloud.unisi.ac.id/gate/login memiliki 14 keretanan yang diantaranya 5 kerentanan dengan level medium, 9 kerentanan dengan level low, dan ada juga 4 kerentanan dengan level informational atau aman (bukan kerentanan). Sehingga total yang ter deteksi adalah 18 Bisa dilihat pada gambar 7 dibawah

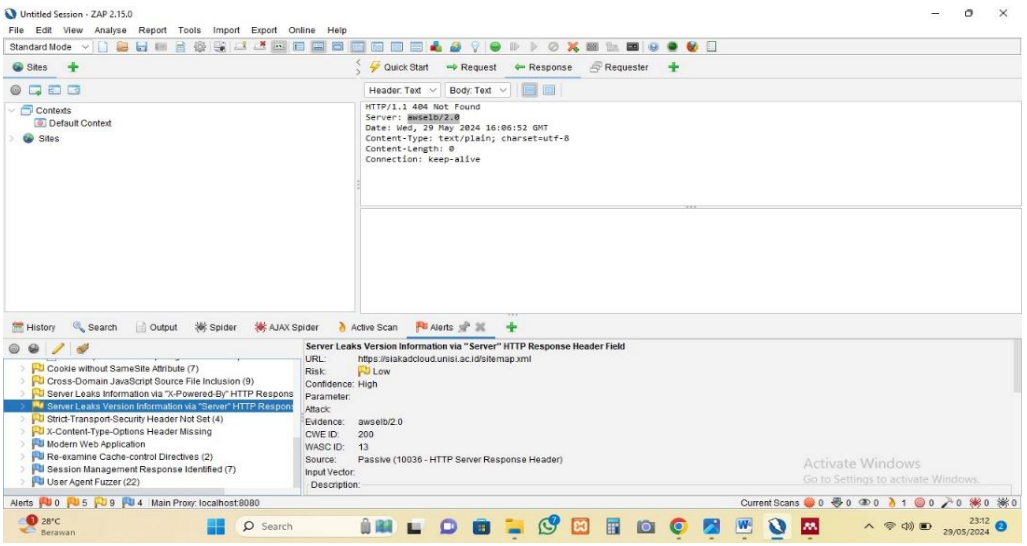


Gambar 7 Tampilan Hasil Kerentanan

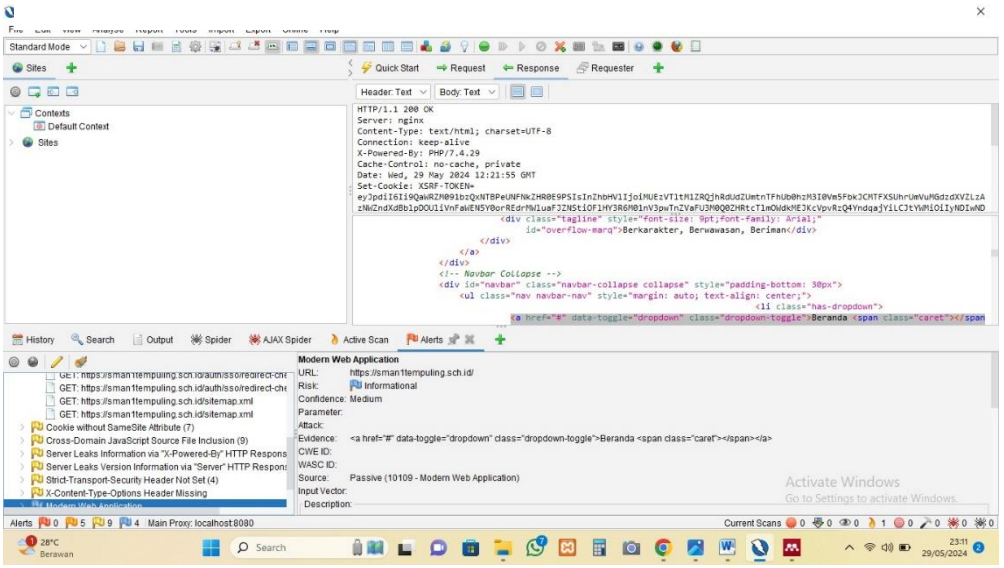
Berikut beberapa hasil pengujian kerentanan website secara menyeluruh dari berbagai tingkatan kerentanan mulai dari sedang, rendah dan informational.



Gambar 8 Kerentanan Tingkat Sedang



Gambar 9 Kerentanan Tingkat Rendah



Gambar 10 Kerentanan Tingkat Informational (Aman)

Lalu tahap Terakhir peneliti melakukan uji coba kembali terhadap hasil penelitian dan memahami kembali terkait penggunaan dari hasil penelitian. Pada tahap ini juga, pengujian dilakukan secara menyeluruh dan hasil dari pengujian tersebut dikelompokkan secara bertahap sesuai dengan tipe kerentanan, level kerentanan, dan rekomendasi yang disarankan guna mempermudah pihak administrator dapat mengetahui kerentanan dan berusaha memperbaiki kesalahan pada sistem.

Adapun hasil pengelompokan nya dapat dilihat pada tabel 1 dibawah ini:

Tabel 1 Tabel Pengelompokan Level Kerentanan

No	Kerentanan Website Siakad Cloud Universitas Islam Indragiri	Risk	Confidence
1	.htaccess information leak	Medium	Medium
2	Content Security Policy (CSP) Header Not Set (3)	Medium	High
3	Hidden File Found (2)	Medium	High
4	Missing Anti-clickjacking Header	Medium	Medium
5	X-Frame-Options Setting Malformed	Medium	Medium

6	Big Redirect Detected (Potential Sensitive Information Leak)	Low	Medium
7	Cookie No HttpOnly Flag (4)	Low	Medium
8	Cookie Without Secure Flag (7)	Low	Medium
9	Cookie Without SameSite Attribute (7)	Low	Medium
10	Cross-Domain JavaScript Source File Inclusion (9)	Low	Medium
11	Server Leaks Information via "X-Powered-By" HTTP Respons	Low	Medium
12	Server Leaks Version Information via "Server" HTTP Respons	Low	High
13	Strict-Transport-Security Header Not set (4)	Low	High
14	X-Content-Type-Options Header Missing	Low	Medium
15	Modern web Aplication	Informational (aman)	Medium
16	Re-examine Cache-control Directivies (2)	Informational (aman)	Low
17	Session Management Response Identified (7)	Informational (aman)	Medium
18	User urgent Fuzzer (36)	Informational (aman)	Medium

Selanjutnya Dari 14 kerentanan yang telah didapatkan maka hal yang harus dilakukan adalah memberikan solusi atau rekomendasi terkait keretanan yang dapat menyebabkan website terserang pihak yang tidak bertanggung jawab atau kemungkinan terjadinya kebocoran data. Hasil pengujian secara menyeluruh dan rekomnedasi yang disarankan dapat dilihat pada penjelasan tabel 2 dibawah ini:

Tabel 2 Tabel Hasil Pengujian Menyeluruh

Vulnerability Type	Level Risk	Recommendation
.htaccess information leak	Medium	Pastikan file .htaccess tidak dapat diakses
Content Security Policy (CSP) Header Not Set (3)	Medium	pastikan server web Anda, server aplikasi, penyeimbang beban, dll dikonfigurasi untuk mengatur header kebijakan keamanan konten
Hidden File Found (2)	Medium	Pertimbangkan apakah komponen tersebut benar-benar diperlukan dalam produksi atau tidak, jika tidak maka nonaktifkan. Jika ya, pastikan akses ke sana memerlukan otentikasi dan otorisasi yang sesuai, atau batasi paparan ke sistem internal atau IP sumber tertentu, dll
Missing Anti-clickjacking Header	Medium	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 (misalnya, itu bagian dari FRAMESET)

		maka Anda sebaiknya menggunakan SAMEORIGIN, sebaliknya jika Anda tidak pernah mengharapkan halaman dibingkai, Anda harus menggunakan DENY. Alternatifnya, pertimbangkan untuk menerapkan arahan "frame-ancestor" Kebijakan Keamanan Konten
X-Frame-Options Setting Malformed	Medium	Pastikan pengaturan yang valid digunakan pada semua halaman web yang dikembalikan oleh situs Anda (jika Anda mengharapkan halaman tersebut hanya dibingkai oleh halaman di server Anda (mis. itu bagian dari FRAMESET) maka Anda sebaiknya menggunakan SAMEORIGIN, sebaliknya jika Anda jangan pernah mengharapkan halaman dibingkai, Anda harus menggunakan DENY. Alternatifnya, pertimbangkan untuk menerapkan arahan "frame-ancestors" dari Content Secunty Policy.
Big Redirect Detected (Potential Sensitive Information Leak)	Low	Pastikan tidak ada informasi sensitif yang bocor melalui respons pengalihan. Respons pengalihan seharusnya hampir tidak memiliki konten. Aktifkan Windows
Cookie No HttpOnly Flag (4)	Low	Pastikan tanda HttpOnly disetel untuk semua cookie.
Cookie Without Secure Flag (7)	Low	Setiap kali cookie berisi informasi sensitif atau merupakan token sesi, maka cookie tersebut harus selalu diteruskan menggunakan saluran terenkripsi. Pastikan tanda aman disetel untuk cookie yang berisi informasi sensitif tersebut.
Cookie Without SameSite Attribute (7)	Low	Pastikan atribut SameSite disetel ke 'longgar' atau idealnya 'ketat' untuk semua cookie.
Cross-Domain JavaScript Source File Inclusion (9)	Low	Pastikan file sumber JavaScript dimuat hanya dari sumber tepercaya, dan sumber tersebut tidak dapat dikontrol oleh pengguna akhir aplikasi
Server Leaks Information via “X-Powered-By” HTTP Respons	Low	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menyembunyikan header "X-Powered-By".
Server Leaks Version Information via “Server” HTTP Respons	Low	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menyembunyikan header "Server" atau memberikan detail umum.
Strict-Transport-Security Header Not set (4)	Low	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda

		dikonfigurasi untuk menerapkan Keamanan Transportasi Ketat
X-Content-Type-Options Header Missing	Low	Pastikan aplikasi/server web menyetel header Tipe Konten 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
Modern web Aplication	Informational (aman)	ini adalah peringatan informasional sehingga tidak diperlukan perubahan.
Re-examine Cache-control Directivies (2)	Informational (aman)	Untuk konten yang aman, pastikan header HTTP kontrol cache disetel dengan "tanpa cache, tanpa penyimpanan, harus divalidasi ulang". Jika suatu aset harus di-cache, pertimbangkan untuk menyetel arahan "publik, usia maksimal, tidak dapat diubah".
Session Management Response Identified (7)	Informational (aman)	Ini adalah peringatan informasional dan bukan kerentanan sehingga tidak ada yang perlu diperbaiki.
User urgent Fuzzer (36)	Informational (aman)	Ini adalah peringatan informasional dan bukan kerentanan sehingga tidak ada yang perlu diperbaiki.

4 KESIMPULAN

Berdasarkan penelitian "Analisis Kerentanan Keamanan Sistem Informasi Akademik Menggunakan Metode OWASP ZAP di Universitas Islam Indragiri" bahwa Website https://siakadcloud.unisi.ac.id/gate/login memiliki sekitar 14 kerentanan keamanan dengan level mulai dari Medium dan Low. Dan juga terdapat 4 kerentanan dengan level Informational atau aman (bukan kerentanan) sehingga didapatkan totak keseluruhan yaitu 18 resiko kerentanan. Dan dapat dikatakan juga jika website tersebut berisiko rendah untuk diserang akan tetapi masih perlu dilakukan perbaikan yang bertujuan untuk memperkuat website tersebut dari beberapa serangan yang berbahaya. Kerentanan keamanan website didominasi pada tahap low (rendah) namun tidak menutup kemungkinan untuk administrator meningkatkan keamanan website tersebut agar tidak mudah di eksploitasi oleh pihak internal maupun eksternal.

Beberapa kerentanan utama yang ditemukan termasuk kebocoran informasi melalui file .htaccess, header Content Security Policy (CSP) yang tidak diatur, Hidden File Found (2) yang tidak sesuai dengan keperluan komponen nya, Missing Anti-clickjacking Header yang tidak sesuai dengan kebijakan keamanan konten, X-Frame-Options Setting Malformed yang tidak valid.

Dengan mengimplementasikan rekomendasi di atas, diharapkan tingkat keamanan website sistem informasi akademik Universitas Islam Indragiri dapat ditingkatkan menjadi lebih aman dan tahan terhadap serangan siber. Saran kepada peneliti selanjutnya, diharapkan mengerjakan penelitian pada orientasi Availability, Karena seirama berkembangnya teknologi, tidak menutup kemungkinan akan ada taktik-taktik peengujian website yang baru. Selain itu apabila terjadi pelanggaran keamanan maka server https://siakadcloud.unisi.ac.id/gate/login harus dikonfigurasi

ulang sehingga hanya orang tertentu yang dapat meminta informasi sensitif yang harus diupdate secara berkala melalui beberapa ekstensi jaringan yang dikelola.

REFERENSI

[1] A. P. Armadhani, D. Nofriansyah, and K. Ibnutama, "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 2, p. 80, 2022, doi: 10.53513/jis.v21i2.6119.

[2] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *J. Komtika (Komputasi dan Inform.*, vol. 5, no. 1, pp. 35–42, 2021, doi: 10.31603/komtika.v5i1.5134.

[3] T. Ariyadi, T. Langgeng Widodo, N. Apriyanti, and F. Sasti Kirana, "Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP Analysis of Bina Darma University Academic Information System Security Vulnerabilities Using the OWASP," *Techno.COM*, vol. 22, no. 2, pp. 418–429, 2023.

[4] R. S. Perdana, "AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK MENGGUNAKAN FRAMEWORK NIST SP 800-26 (Studi Kasus : Universitas Sangga Buana YPKP Bandung)," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 3, no. 1, p. 9, 2018, doi: 10.32897/infotronik.2018.3.1.83.

[5] W. Syafitri, "Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 2, no. 2, p. 8, 2016, doi: 10.24014/coreit.v2i2.2356.

[6] M. A. Mu'min, A. Fadlil, and I. Riadi, "Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework," *J. Media Inform. Budidarma*, vol. 6, no. 3, p. 1468, 2022, doi: 10.30865/mib.v6i3.4099.

[7] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.

[8] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.

[9] B. A. B. Ii, "3_195410193_BAB_II - Machfud 'Machfud' Mubarak," pp. 5–18, 2022.

[10] G. Kusuma, "Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 16, no. 2, pp. 178–186, 2022, doi: 10.47111/jti.v16i2.3995.

[11] S. ÖCAL, "No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title," vol. 3, no. 2, p. 6, 2021.

[12] A. W. Kuncoro and F. Rahma, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," *Automata*, vol. 3, no. 1, pp. 1–5, 2021, [Online]. Available: https://www.sciencedirect.com

[13] M. Nur Fikri, B. Parga Zen, R. Adhitama, and E. Ahmad Firdaus, "Analisis Keamanan Sistem Informasi Website SMA Negeri 1 Sokaraja Menggunakan Metode Penetration Testing Execution Standard (PTES)," *J. Inform.*, vol. 2, no. 2, pp. 19–27, 2023, doi: 10.57094/ji.v2i2.1046.

[14] A. F. Hasibuan and D. Handoko, "Analisis Keretanan Website Dengan Aplikasi Owasp Zap," *J. Ilmu Komput. dan Sist. Inf.*, vol. 2, no. 2, pp. 257–270, 2023, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/51

[15] 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.

[16] B. P. Sembiring, M. F. Sidiq, and W. A. Prabowo, "Analisis Keamanan Sistem Informasi Menggunakan Metode Open Web Application Security Project (Owasp)," vol. 8, no. 3, pp. 3049–3054, 2024.