Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan *OWASP*

Analysis of Bina Darma University Academic Information System Security Vulnerabilities Using the OWASP

Tamsir Ariyadi[1] ,Tantri Langgeng Widodo[2], Nely Apriyanti[3] , Febriani Sasti Kirana[4]
[1,2, 3, 4] Program Studi Teknik Komputer, Universitas Bina Darma
email: [1]tamsirariyadi@binadarma.ac.id,[2]tantrilanggengwidodo@gmail.com,
[3]nelyapriyanti712@gmail.com, [4]febrianisastikirana@gmail.com

Abstrak

Sistem Keamanan Informasi Akademik Universitas Bina Darma ialah suatu sistem berbasis web yang mengolah semua data ataupun informasi dan melakukan berbagai proses kegiatan akademik dimana melibatkan tenaga pendidik dan peserta didik, administrasi akademik, data nilai mahasiswa dan masih banyak lagi yang berkaitan dengan akademik. Pastinya data akademik tersebut sangat penting dan harus dijaga keamanannya. Oleh kareena itu, perlu dilakukan analisis kerentanan keamanan . Pada penelitian ini peneliti menggunakan metode *Action Research* yang menitikberatkan pada hasil scan yang berkaitan dengan celah keamanan dari website tersebut dan juga Framework *OWASP* dalam pengujian. Hasil dari penelitian ini sendiri yakni memberi informasi mengenai port-port mana yang saja yang terbuka dan juga solusi untuk meningkatkan keamanan website dan meminimalisir terjadinya *Attack* yang dilakukan oleh *Hacker*.

Kata kunci : Kerentanan, Keamanan, Sistem Informasi, *OWASP, Action Research*

Abstract

The Bina Darma University Academic Information Security System is a web-based system that processes all data or information and carries out various academic activity processes which involve teaching staff and students, academic administration, student grade data and much more related to academics. Certainly the academic data is very important and must be kept secure. Therefore, it is necessary to analyze security vulnerabilities. In this study, researchers used the Action Research method which focused on scan results related to security vulnerabilities on the website and also the OWASP method in testing. The results of this research itself are to provide information about which ports are open and also solutions to improve website security and minimize attacks by hackers. As well as experiments using the OWASP method.

***Keywords** : Vulnerability, Security, Information Systems, OWASP, Action Research*

1. PENDAHULUAN

Diera globalisasi, teknologi mengalami perkembangan yang pesat dikarenakan kebutuhan akan sarana komunikasi dan informasi [1]. Bahkan teknologi yang ada saat ini dapat dikatakan semakin canggih sehingga memberikan kemudahan kepada kita dalam berbagai aktivitas sehari-hari [2]. Meski demikian, ancaman dalam bidang digital menjadi permasalahan tersendiri yang berdampak pada suatu sistem, semisalnya pada sebuah *Website*. *Website* ialah sebuah halaman data berbasis web yang menyediakan berbagai informasi, dokumen ataupun tautan yang menghubungkan halaman data satu dengan halaman data lainnya yang dapat kita akses saat terkoneksi dengan internet kapanpun dan dimanapun melalui *browser* [3]. Selain itu, *website* sangatlah dibutuhkan dalam penyampaian informasi yang begitu luas dan tanpa batas [4]. Terkhususnya pada Institusi Pendidikan, contohnya Sistem Informasi Akademik.

Sistem informasi akademik merupakan suatu sistem berbasis *web* yang mengolah berbagai data ataupun informasi dan melakukan berbagai proses kegiatan akademik dimana melibatkan tenaga pendidik dan peserta didik, administrasi akademik, data nilai mahasiswa dan lain sebagainya yang berkaitan mengenai akademik [5]. Melalui sistem informasi akademik ini tentunya memberikan kemudahan kepada mahasiswa dalam mengakses hal yang berkaitan dengan akademik. Namun disisi lain ada beberapa permasalahan yang masih perlu diperhatikan salah satunya yakni kerentanan keamanan dari sistem informasi itu sendiri. Pada dasarnya keamanan sistem informasi tentunya akan terus menjadi permasalahan utama ditengah perkembangan teknologi informasi dan komunikasi dimana dalam hal ini ada beberapa aspek yang perlu diperhatikan untuk melindungi informasi atau data secara terstruktur dan komprehensif, aspek itu sendiri dikenal dengan *CIA TRIAD* yang terdiri dari *Confidentiality* (Kerahasian) yakni menjaga kerahasian informasi dengan pembatasan hak akses sehingga hanya pihak yang diizinkan yang dapat mengakses suatu informasi atau data. *Integrity* (Keaslian) yakni keakuratan data dan informasi yang diterima dimana dalam hal ini data terjaga keasliannya dan tidak dimodifikasi oleh pihak manapun. Dan *Availability* (Ketersedian) yakni ketersedian data dan informasi ketika dibutuhkan dalam hal ini informasi atau data harus tersedia untuk pihak yang memiliki akses tanpa terhambat ataupun kesulitan [6], [7].

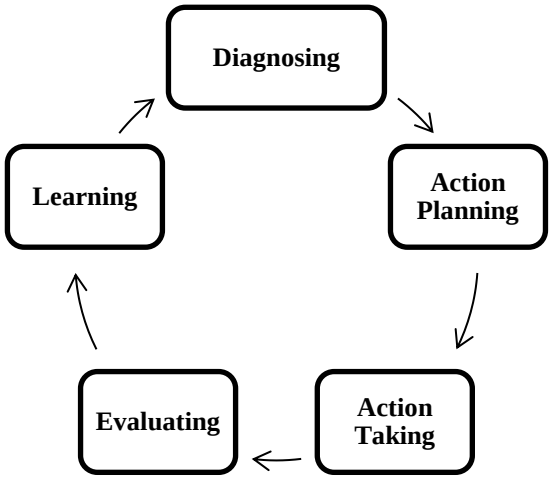
Pada penelitian ini peneliti mengkaji terkait *website* Sisfo Bina Darma yang merupakan Sistem Informasi Akademik Universitas Bina Darma. Dimana dari hasil kajian peneliti, belakangan ini *website* Sisfo Bina Darma sering kali mengalami *Down* karena tingginya tingkat akses yang dilakukan oleh Mahasiswa. Sistem yang *Down* ini tentunya akan berdampak pada terbukanya celah untuk seorang *hacker* atau oknum tak bertanggung jawab melakukan peretasan *website* berlandaskan demi keuntungan pribadi pelaku. Jika Administrator kurang memperhatikan keamanan dari *website* atau melakukan kesalahan dalam penulisan kode keamanan tentunya akan memberikan dampak yang lebih buruk lagi. Maka dari permasalahan tersebut, keamanan sistem informasi perlu ditingkatkan lagi dan untuk meningkatkan hal tersebut peneliti berencana melakukan Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma (Sisfo Bina Darma). Dengan tujuan untuk mengetahui celah mana saja yang terbuka dan memberikan solusi agar terhindar dari serangan yang dilakukan oleh *hacker*.

Penelitian yang telah membahas mengenai analisis keamanan sistem informasi akademik ini pernah dilakukan oleh Hendra dan Eka Budhy dalam jurnal yang berjudul *Peningkatan Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Jakarta Melalui Klasifikasi Serangan Cyber Dalam Menunjang WFH*. Pada penelitian ini peneliti melakukan analisis pada Sistem Informasi Akademik Universitas Bina Muhammadiyah Jakarta (Siakad UMJ) dengan melakukan pengujian celah keamanan atau penetrasi testing terhadap *website* menggunakan OWASP-ZAP. Dari hasil scan, peneliti kemudian melanjutkannya pada tahap pengujian dengan melakukan *attack* pada *website* untuk menjamin keamanan dari *website* Siakad UMJ [8]. Selanjutnya penelitian yang dilakukan oleh Guntoro, Loneli Costaner dan Musfawati dalam jurnal yang berjudul *Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)*. Pada penelitian ini peneliti melakukan analisis keamanan *Web Server Open Jurnal System (OJS)* dengan menggunakan *Framework ISSAF* dan *OWASP* versi 4. Selain itu, peneliti menggunakan *OWASP ZAP* untuk penetrasi *testing* [9]. Penelitian selanjutnya yakni, peneliti melakukan Penetration Testing yang digunakan sebagai metode dalam melakukan analisis keamanan jaringan pada Pay2Home [10]. Lalu penelitian yang dilakukan oleh Albestty Islamyati Rafeli dkk yang melakukan pengujian terakit celah keamanan menggunakan metode OWASP Web Security Testing Guide (WSTG) pada sebuah website. Penelitian ini juga memiliki skema blackbox testing sehingga tidak menggunakan beberapa teknik. Authentication Testing, Authorization Testing, Session Management Testing tidak digunakan dikarenakan fiture login tidak bekerja dengan baik [11]. Terakhir yakni penelitian dari Rahmad Ashar melakukan penelitian yang berkaitan dengan analissi keamanan *Open Website* dengan menggunakan metode OWASP dan ISSAF. Penelitian ini memberikan solusi pada kerentanan keamanan website berdasakan tingkatannya semisalnya jenis kerentanan yang awalnya termasuk kategori High menjadi kategori Low [12].

Didasari dari penelitian terdahulu, pada penelitian Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma, peneliti melakukan analisis terhadap port-port keamanan sistem yang terbuka dengan *Whois. Robtex* yang belum diterapkan pada penelitian terdahulu tersebut. *Whois.Robtex* adalah suatu *website* yang digunakan untuk mengetahui dan menemukan identitas sebuah IP Address pada *Domain Name* pada sebuah website [13]. Penggunaan *Whois.Robtex* ini bertujuan untuk megidentifikasi serta memverifikasi permasalahan pada suatu sistem secara terperinci. Selain itu, peneliti juga menerapkan point-point dalam *Pentesting. Pentesting* atau *Penetration Testing* ialah suatu proses yang berisi prosedur dan teknik yang bertujuan untuk menguji dan melindungi keamanan suatu jaringan atau organisasi dengan cara memberikan beberapa rekomendasi yang dapat digunakan dalam mengatasi dan memperbaiki masalah yang ada selama pengujian[14]. Selain itu pada penelitian ini, peneliti juga mendefinisikan masing-masing masalah dalam tiap alert yang ditampilkan melalui hasil automated scan yang diperoleh dari OWASP ZAP dan dijelaskan sesuai dengan hasil yang terdata. Untuk terlaksananya penelitian ini, peneliti menggunakanan metode *Action Research* yang menitikberatkan pada hasil scan yang berkaitan dengan celah keamanan dari *website* tersebut dengan pengujian yang dilakukan menggunakan Framework *OWASP* yang berfokus pada *Authentication Testing, Authoization Testing, Session Management Testing. OWASP (Open Web Application Security Project)* adalah suatu organisasi non-profit amal yang berdiri sejak tahun 2001 yang dikeluarkan oleh OWASP *Foundation* [15]. Hasil dari penelitian ini sendiri yakni analisis mengenai port-port mana yang saja yang terbuka dan juga solusi untuk meningkatkan keamanan *website* dan meminimalisir terjadinya *Attack* yang dilakukan oleh *Hacker*.

2. METODE PENELITIAN

Berdasarkan penelitian yang dikerjakan oleh peneliti, maka peneliti menggunakan metode *Study Literature*, sebagai teknik untuk mengumpulkan berbagai data dan informasi yang berkaitan dengan penelitian melalui internet dan rata-rata berupa Artikel atau Jurnal Penelitian. Selain itu untuk proses penelitian, peneliti menggunakan Metode *Action Research*.[16] Metode *Action Research* adalah metode yang menjelaskan, menggambarkan dan menginterpretasikan terkait suatu keadaan secara bersamaan dengan proses intervensi yang bertujuan untuk pengembangan dan berfokus pada praktik dibandingkan pengetahuan [17][18]. Metode ini dimulai dari tahap *Diagnosing*, *Action Planning*, *Action Taking*, *Evaluation* dan *Learning*. Pada penelitian ini juga menggunakan framework OWASP untuk pengujian yang mana berfokus pada *Authentication Testing, Authoization Testing, Session Management Testing.*



Gambar 1 Metode *Action Research*

Langkah-langkah dalam Metode Action Research sebagai berikut;

1. *Diagnosing*

Pada tahap ini, peneliti melakukan diagnosa terhadap permasalahan Keamanan Sistem Informasi terkhususnya pada Sistem Informasi Akademik. Dimana dalam hal ini peneliti melakukan *Study Literature* untuk mengetahui dan menambah wawasan mengenai permasalahan tersebut dari berbagai sumber seperti Jurnal Penelitian, Prosiding dan lain sebagainya. Pada tahap ini peneliti juga menemukan berbagai faktor dan solusi apa yang perlu diambil untuk mengatasi permasalahan tersebut.

2. *Action Planning*

Dari diagnosa tersebut, peneliti mencoba mencari upaya solusi yang tepat untuk mengatasi permasalahan yang ada. Dimana peneliti berencana akan melakukan analisis kerentanan keamanan Sistem Informasi Akademik dengan menggunakan Whois.*Robtex, Owasp Zap*

3. *Action Taking*

Setelah perencanaan dibuat peneliti mulai mengeksekusi apa yang telah direncanakan sebelumnya dimana pada bagian ini terdiri dari berbagai tahap, yakni;

1) Tahap Identifikasi *Website* Menggunakan Whois.*Robtex*.
2) Tahap Verifikasi Menggunakan *Pentest-tools.*
3) Tahap Validasi Menggunakan *OWASP ZAP*.

4. *Evaluation*

Pada tahap ini, peneliti melakukan evaluasi terhadap hasil dari penelitian. Dimana peneliti akan melakukan pengujian terhadap *website* Sistem Informasi Akademik.

5. *Learning*

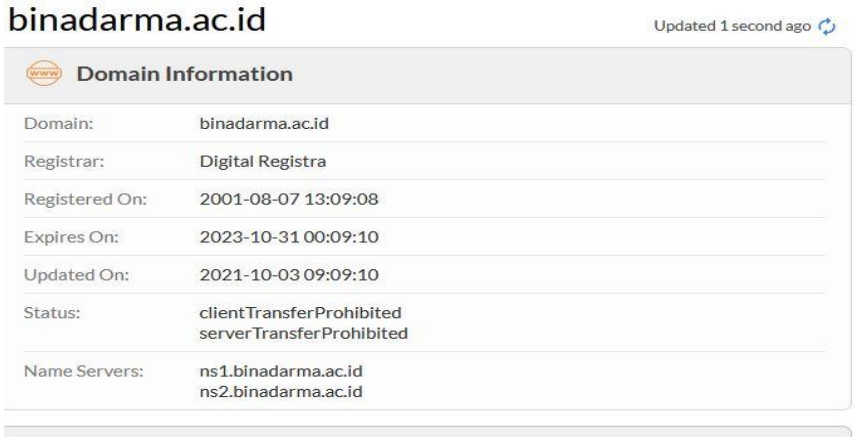
Pada langkah ini adalah langkah terakhir dari Metode Penelitian, dimana pada langkah ini peneliti melaksanakan uji coba kembali mengenai hasil penelitian dan pemahaman kembali terkait penggunaan dari hasil penelitian.

3. HASIL DAN PEMBAHASAN

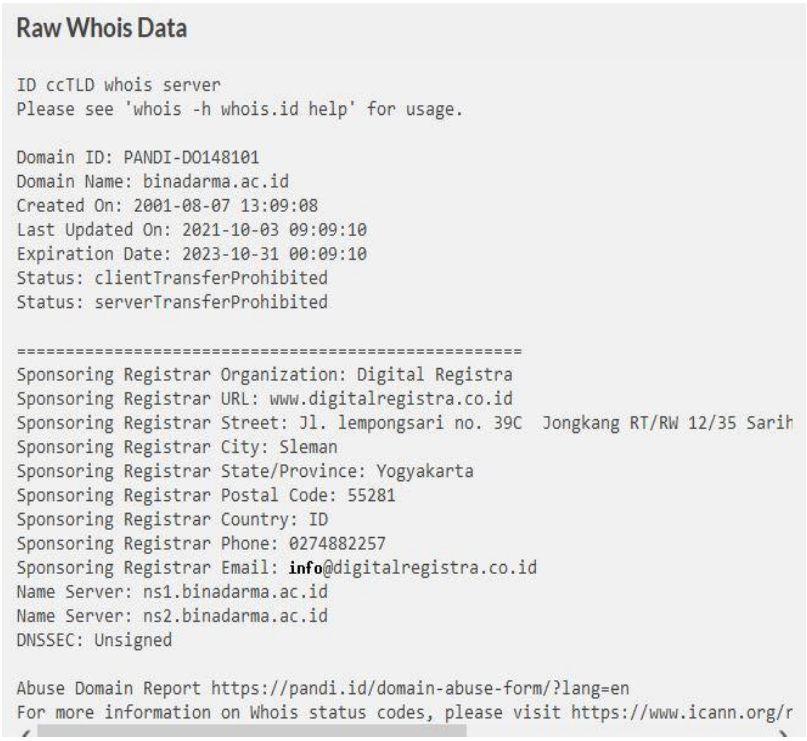
Berdasarkan tahap awal yang dilakukan, peneliti berhasil melakukan analisis permasalahan terkait kerentanan keamanan pada *website* terkhususnya *website* Sistem Akademik dari berbagai sumber seperti jurnal penelitian, *prosiding*, *literature* internet dan lain sebagainya. Dimana dari berbagai sumber tersebut dapat ditarik kesimpulan jika seandainya seorang Administrator kurang memperhatikan keamanan dari *website* atau melakukan kesalahan dalam penulisan kode keamanan tentunya akan berdampak pada terbukanya celah yang memungkinkan seorang *Hacker* atau oknum tak bertanggung jawab melakukan peretasan terhadap *websi*te tersebut dengan berlandaskan demi keuntungan pribadi pelaku. Untuk mengkaji lebih dalam terkait permasalahan ini, peneliti menjadikan Sistem Akademik Universitas Bina Darma atau yang dikenal dengan Sisfo Bina Darma sebagai objek penelitian. Sisfo Bina Darma 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 tahap *Action Planning*. Dimana peneliti berencana untuk melakukan Analisis Kerentanan

Keamanan Sistem Informasi Akedemik Universitas Bina Darma (Sisfo Bina Darma) yang bertujuan untuk meningkatkan keamanan dari *website* tersebut. Untuk terlaksanannya penelitian ini, peneliti membutuhkan beberapa tools seperti *Robtex* adalah sebuah aplikasi footprinting yang dapat digunkan untuk melihat, mengetahui, mencari informas mengenai suatu website secara lengkap. Lalu *Pentens-tools* dan *OWASP ZAP*. Setelah dilakukan perencanaan yang matang, peneliti mulai melanjutkan ketahap selanjutnya yakni tahap *Action taking*. Dimana peneliti akan mulai mengeksekusi rencana tersebut. Peneliti juga menyiapkan berbagai hal yang diperlukan baik *Hardware* maupun *Software*. Untuk tahap pertama peneliti melakukan Identifikasi *Website* Menggunakan *Robtex* atau *Website whois.robtex*. Untuk identifikasi yang peneliti lakukan ini meliputi *Domain*, *Ip Address*, *Mac Address* dan *Name Server*. Hasil dari tahap identifikasi ini diperoleh data pada Gambar. 2 berikut ini.



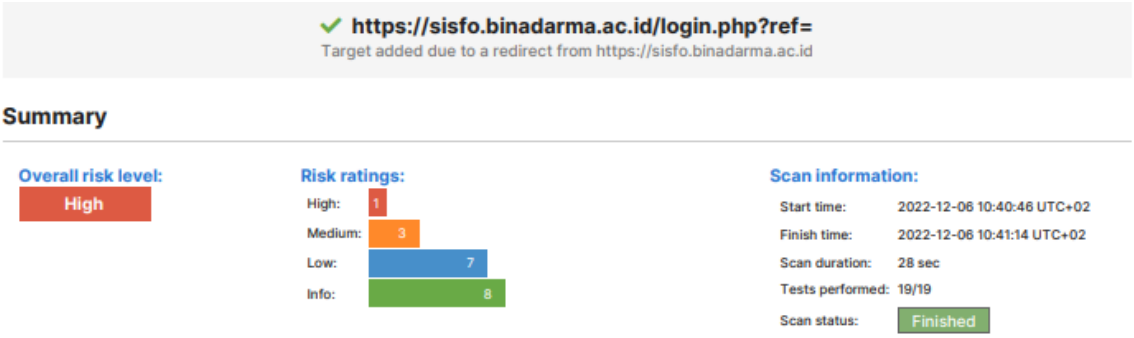
Gambar 2. *Domain Information*



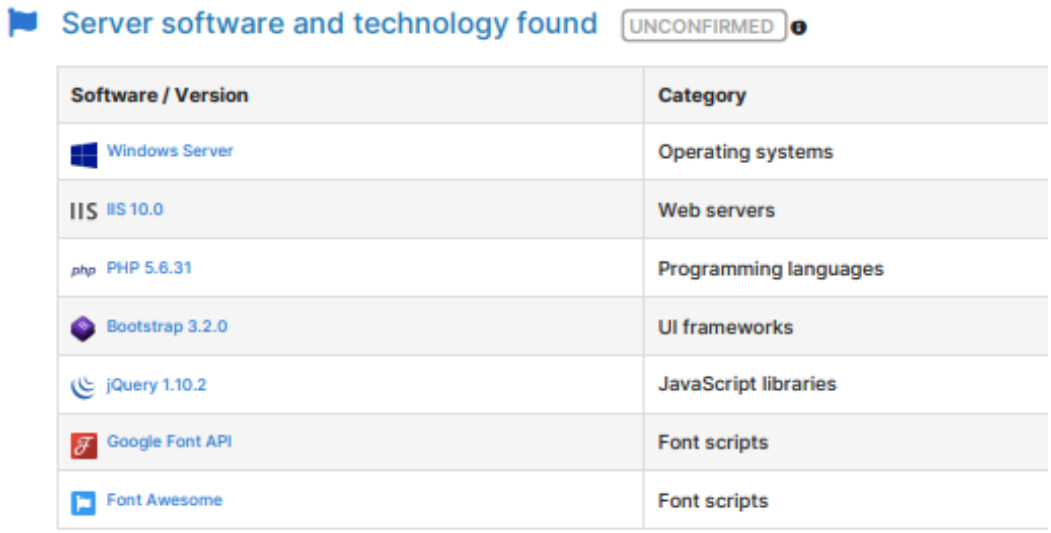
Gambar 3. Verifikasi Menggunakan *Pentest-tool*

Selanjutnya peneliti akan melakukan verifikasi menggunakan *Pentest-tools atau Pentest-tools.com* yang bertujuan untuk memberikan informasi terkait kerentanan pada tingkat minimum

seperti yang terdapat pada Gambar 3 diatas. Ketika sudah ke tahap verifikasi, peneliti kemudian melakukan pengujian pada tahap validasi yang bertujuan untuk menyempurnakan pengujian kerentanan pada *website* Sistem Informasi Akademik Universitas Bina Darma (Sisfo Bina Darma), diperoleh data pada Gambar 4 dan Gambar 5.



Gambar 4. Percobaan Validasi



Gambar 5. Percobaan Validasi

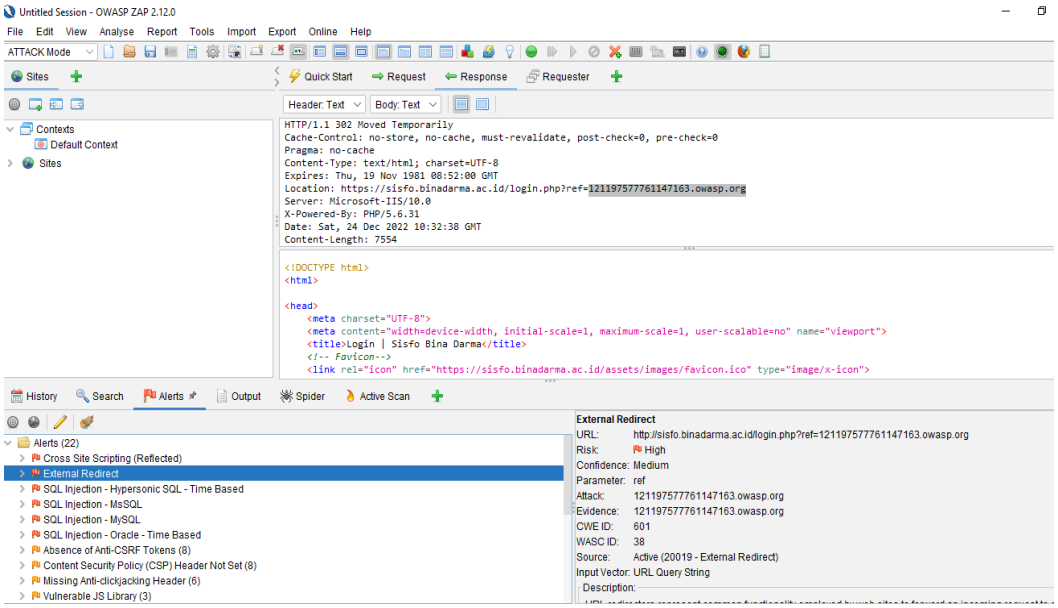
Dalam proses pengujian atau validasi OWASP ZAP menggunakan pemindaian aktif, aturan pemindaian aktif, peringatan, pengujian pada kontrol akses dan aturan kontrol akses dan aturan kontrol pasif. Hasil dari pemindaian ini menemukan kerentanan sedang, dangkal hingga informati. Semisalnya pada formulir HTML, tanpa perlindungan CSRF merupakan kerentanan tingkat tinggi, Dilanjutkan dengan klik tangkap-Header X-Frame-Optins yang hilang disertakan termasuk kerentanan tingkat rendah. Dan terakhir yakni menambahkan keamanan berupa Password dengan perlengkapan otomatis diaktifkan merupakan contoh kerentanan tingkat sedang.

Setelah pengujian validasi, peneliti melakukan validasi menggunakan *OWASP ZAP*. Pada hal ini peneliti akan melakukan pengujian kerentanan secara menyeluruh pada *website sisfo.binadarma.ac.id*. Berdasarkan hasil yang diperoleh, total kerentanan website tersebut berkisar 17 Macam berdasarkan hasil level.

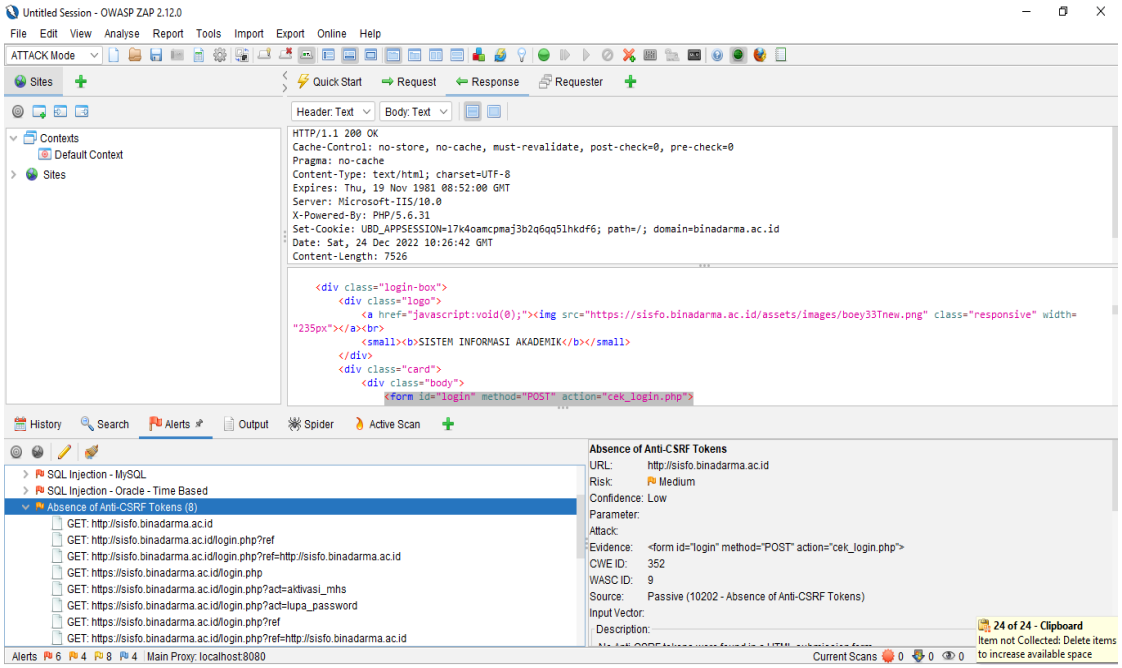
Tabel 1. Kerentanan Berdasarkan Hasil Level Dari Hasil Validasi Menggunakan *OWASP ZAP*

No	Kerentanan *Website Sisfo.binadarma.ac.id.*
1	*Cross Site Scripting (Reflected)*
2	*External Redirect*
3	*SQL injection-Hypersonic MySQL-Time Based*
4	*SQL Injection – MySQl*
5	*SQL injection-Oracle-Time Based*
6	*Absence of Anti-CSRF Tokens*
7	*Content Security Policy (CSP) Header Not Set*
8	*Missing Anti-clickjacking Header*
9	*Vulnerable JS Library*
10	*Big Redirect Detected (Potential Sensitive Information Leak)*
11	*Cookie No HttpOnly Flag*
12	*Cookie Without Secure Flag*
13	*Cookie without SameSite Attribute*
14	*Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*
15	*Server Leaks Version Information via "Server" HTTP Response Header Field*
16	*Strict-Transport-Security Header Not Set*
17	*X-content-type-options header missing*

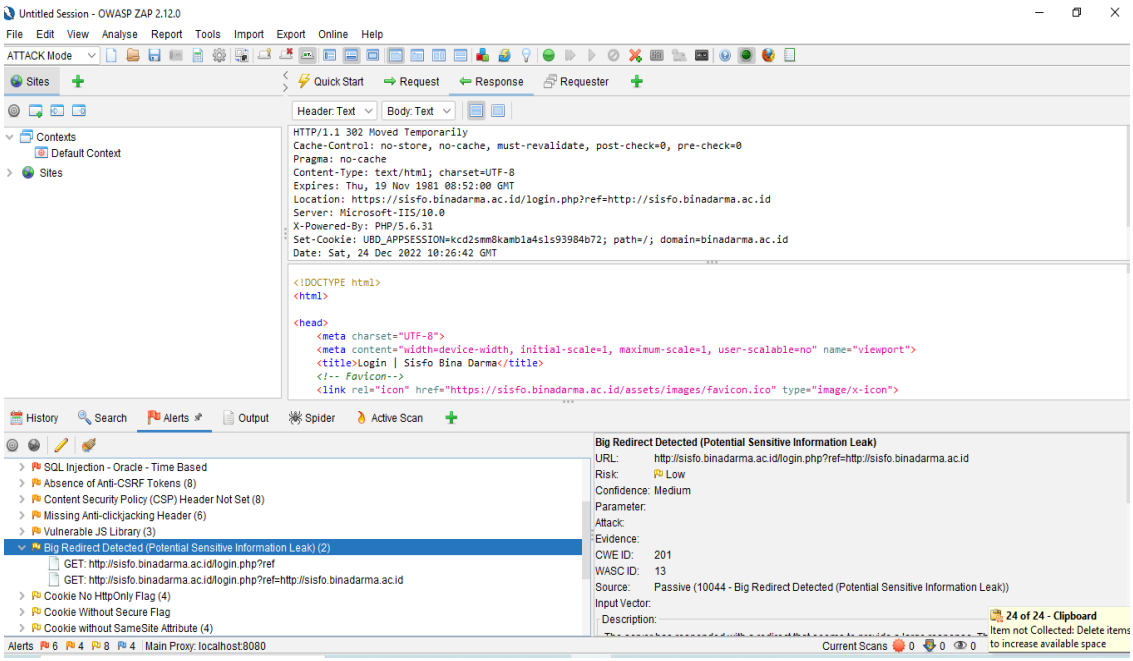
Setelah dilakukannya tahap validasi selanjutnya peneliti melanjutkannya ke tahap penelitian yakni tahap *Evaluating*. Dimana peneliti melakukan evaluasi terhadap hasil dari penelitian. Dengan melakukan pengujian pada *website* ***sisfo.binadarma.ac.id*** **.** Berikut beberapa hasil pengujian kerentanan *website* secara menyeluruh dari berbagai tingkatan kerentanan mulai dari tinggi, rendah dan sedang.



Gambar 6. Kerentanan Tingkat Tinggi



Gambar 7. Kerentanan Tingkat Sedang



Gambar 8 Kerentanan Tingkat Rendah

Terakhir peneliti melakukan uji coba kembali terhadap hasil penelitian dan pemahaman 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.

Tabel 2. Hasil Pengujian Kerentanan Secara Menyeluruh

Vulnerability Type	***Level***	***Recommendation***
Cross Site Scripting (Reflected)	*high*	Fase: Arsitektur dan Desain Memakai wacana atau pokok peranan terverifikasi yang tidak memungkinkan ketaksempurnaan ini terjadi atau menyisakan kontruksi yang menciptakan ketaksempurnaan ini lebih mudah dihindari.
External Redirect	*high*	Skema validasi, yaitu memperuntukkan jadwal input yang diizinkan yang cocok sama tambah spesifikasi. Menolak segala sesuatu yang tidak sepenuhnya sesuai spesifikasi, atau mengubahnya menjadi yang sama. Jangan menyandarkan secara distingtif untuk mencari masukan yang berbahaya. Namun, jadwal yang bisa membantu untuk mengetahui kesanggupan pelanggaran atau menetapkan input mana yang cacat sehingga harus ditolak mentah-mentah.
SQL injection-Hypersonic MySQL-Time Based	*high*	Menurut kebanyakan , ketik periksa seluruh data di sisi server. Jika aplikasi menggunakan JDBC, gunakan *PreparedStatemen*t atau *CallableStatement*, dengan parameter yang diteruskan oleh '?' Jika aplikasi menggunakan ASP, gunakan *ADO Command Objects* dengan pemeriksaan tipe yang kuat dan kueri berparameter.
SQL Injection - MsSQl	*high*	Jangan percaya masukan sisi klien, bahkan jika ada validasi sisi klien. Secara umum, ketik periksa semua data di sisi server.
SQL injection-Oracle-Time Based	*high*	Jangan percaya masukan sisi klien, bahkan jika ada validasi sisi klien. Secara umum, ketik periksa semua data di sisi server. Jika aplikasi menggunakan JDBC, gunakan *PreparedStatement* atau *CallableStatement*, dengan parameter yang diteruskan oleh '?' Jika aplikasi menggunakan ASP, gunakan *ADO Command Objects* dengan pemeriksaan tipe yang kuat dan kueri berparameter.
Absence of Anti-CSRF Tokens	*medium*	Fase: Arsitektur dan Desain Gunakan teks atau susunan kerja terverifikasi yang tidak memungkinkan ketaksempurnaan ini terjadi atau menahan desain yang menjalin ketaksempurnaan ini lebih mudah dihindari.

Content Security Policy (CSP) Header Not Set	*medium*	Pastikan bahwa *server web* Anda, *server* aplikasi, penyeimbang beban, dll. dikonfigurasi untuk menyetel tajuk *Content-Security-Policy*, untuk mendapatkan dukungan browser yang optimal: *"Content-Security-Policy"* untuk *Chrome 25+, Firefox 23+*
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 dikembalikan oleh situs/aplikasi Anda.
Vulnerable JS Library	*medium*	Harap tingkatkan ke versi *bootstrap* terbaru.
Big Redirect Detected	*low*	Pastikan tidak ada informasi sensitif yang bocor melalui tanggapan pengalihan. *Redirect* tanggapan seharusnya hampir tidak memiliki konten.
Cookie No HttpOnly Flag	*low*	Pastikan bendera *HttpOnly* disetel untuk semua *cookie*.
Cookie Without Secure Flag	*low*	Setiap kali *cookie* adalah petunjuk sensitif atau mengadakan token sesi, *cookie* harus selalu diteruskan dengan saluran terenkripsi. Pastikan bendera aman disetel kepada cookie yang mengandung petunjuk sensitif tersebut.
Cookie without SameSite Attribute	*low*	Pastikan lambang *SameSite* disetel ke 'longgar' atau idealnya 'ketat' kepada semua *cookie*.
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	*low*	Pastikan *server web*, *serve*r aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menekan header "X-Powered-By".
Server Leaks Version Information via "Server" HTTP Response Header Field	*low*	Pastikan bahwa *server web* Anda, server aplikasi, penyeimbang muatan, dll. dikonfigurasi untuk menyembunyikan tajuk "*Server*" atau memberikan detail umum.
Strict-Transport-Security Header Not Set	*low*	Pastikan bahwa *server web*, *server* aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menerapkan *Strict-Transport-Security*
X-content-type-options header missing	*low*	Pastikan bahwa aplikasi/*server web* menyetel tajuk *Content-Type* dengan benar, dan menyetel tajuk *X-Content-Type-Options* ke "*nosniff'*" untuk semua halaman web.

4. KESIMPULAN DAN SARAN

Berdasarkan penelitian "Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan Metode OWASP" bahwa *Website* sisfo.binadarma.ac.id memiliki sekitar 17 kerentanan keamanan dengan level mulai dari *High*, *Medium* dan *Low*. 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 *medium* (sedang) namun tidak menutup kemungkinan untuk administrator meningkatkan keamanan *website* tersebut agar tidak mudah di eksploitasi oleh pihak internal maupun eksternal. Solusi atas permasalahan yang terjadi pada sistem keamanan yang rentan untuk pihak administrator. Kerentanan Cross Site *Scripting (Reflected)* yang termasuk level tinggi, dengan mengaktifkan *Session Cookie HttpOnly Flag Jilid* dan *Session Cookie Secure Flag Jilid*, agar *Session Cookie* tidak bisa dibaca oleh *klien* atau *server* lain menerapkan Teknik enkripsi setiap mengerjakan pergeseran dan persinggungan masukan antar server agar sulit dibaca penyusup. Saran kepada peneliti selanjutnya, diharapkan mengerjakan penelitian pada orientasi *Availability*, Karena seirama berkembangnya teknologi, tidak menutup akan ada taktik-taktik peengujian *website* yang baru. Selain itu apabila terjadi pelanggaran keamanan maka server sisfo.binadarma.ac.id harus dikonfigurasi ulang sehingga hanya orang tertentu yang dapat meminta informasi sensitif yang harus diupdate secara berkala melalui beberapa ekstensi jaringan yang dikelolah.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada semua pihak yang telah membantu peneliti dalam mengerjakan penelitian. Terkhususnya kepada dosen kami Tamsir Ariyadi, M.Kom selaku pengampuh Mata Kuliah Keamanan Sistem Informasi yang membantu peneliti, pada penelitian yang kami lakukan ini dengan judul *"Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan Metode OWASP".*

DAFTAR PUSTAKA

[1] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," *Jurnal Sistem Informasi Bisnis*, vol. 1, pp. 1–8, Feb. 2019.

[2] T. Ariyadi, "Mitigasi Keamanan Dynamic Host Control Protocol (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN)," *Jurnal Inovtek Polbeng - Seri Informatika*, vol. 3, no. 2, pp. 147–154, Nov. 2018.

[3] A. W. Wardhana and H. B. Seta, "Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ," *Jurnal Informatik*, vol. 17, no. 3, pp. 226–237, Dec. 2021.

[4] S. E. Prasetyo and N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF," *Jurnal Ilmiah Informatika (JIF)*, vol. 9, no. 2, pp. 82–86, Sep. 2021.

[5] K. Anam and A. T. Muharram, "Analisa dan Perancangan Sistem Informasi Akademik Berbasis Web Pada MI Al-Mursyidiyyah Al-'Asyirotussuafi'yyah," *Jurnal Teknik Informatika*, vol. 11, no. 2, pp. 207–217, Oct. 2018.

[6] N. Hayaty, *Buku Ajar : Sistem Keamanan*. Tanjungpinang: Universitas Maritim Raja Ali Haji, 2020.

[7] Muh. A. Mu'min, A. Fadlil, and I. Riadi, "Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 3, pp. 1468–1475, Jul. 2022.

[8] Hendra and E. Budhy, "Peningkatan Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Jakarta Melalui Klasifikasi Serangan Cyber Dalam Menunjang WFH,"

in *Seminar Nasional Sains dan Teknologi 2021 Fakultas Teknik Universitas Muhammadiyah Jakarta*, Jakarta: Jurnal Universitas Muhammadiya Jakarta (Jurnal UMJ), Nov. 2021, pp. 1–6.

[9] Guntoro, L. Costaner, and Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning) KUNING)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 05, no. 01, pp. 45–55, Jun. 2020.

[10] S. E. Prasetyo and R. C. Lee, "Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing," 2021. [Online]. Available: https://journal.uib.ac.id/index.php/combines

[11] A. I. Rafeli, H. B. Seta, and W. Widi, "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ".

[12] R. Ashar, "Jurnal Informasi dan Teknologi Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF," vol. 4, pp. 187–194, 2022, doi: 10.37034/jsisfotek.v4i4.233.

[13] R. Novrianda Dasmen, T. Langgeng Widodo, dan Muhammad Tio Farizky, and Kundari, "Pengujian Penetrasi Pada Website Elearning2.binadarma@ac.id Dengan Metode Ptes (Penetration Testing Execution Standard)," *J-ICON*, vol. 11, no. 1, pp. 91–95, 2023, doi: 10.35508/jicon.v11i1.9809.

[14] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)." [Online]. Available: http://jurnal.itg.ac.id/

[15] T. Raden, S. T. Dirgahayu, Y. Prayudi, S. Si, M. Kom, and A. Fajaryanto, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," 2015.

[16] T. Ariyadi, "Desain Keamanan Dhcp Snooping Untuk Mengurangi Serangan Local Area Network(Lan)," *Jusikom*, vol. 2, no. 1, pp. 1–9, 2017.

[17] M. Yaumi and M. Damopolii, *Action Research: Teori, model dan aplikasinya*, 1st ed. Jakarta: Kencana Prenamedia Group, 2016.

[18] T. Ariyadi and M. A. Prabowo, "Perbandingan Kinerja Virtual Private Network Antara Vpn Tunnel Dan Internet Protocols Security," *INOVTEK Polbeng - Seri Informatika*, vol. 6, no. 1, p. 80, 2021, doi: 10.35314/isi.v6i1.1698.