Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

Journal Homepage: http://journal.lembagakita.org/index.php/jtik

Analisis Keamanan *Website* SIASAT Menggunakan Teknik *Footprinting* dan *Vulnerability Scanning*

Alvin Kendek Allo [1*], Indrastanti R. Widiasari [2]

[1*,2] *Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Kota Salatiga, Provinsi Jawa Tengah, Indonesia.*

a r t i c l e i n f o

Article history:
Received 31 October 2023
Received in revised form
19 December 2023
Accepted 15 March 2024
Available *online* April 2024

DOI:
https://doi.org/10.35870/jtik.v8i2.1723.

Keywords:
Network Security;
Footprinting; Vulnerability Scanning.

Kata Kunci:
Keamanan jaringan;
Footprinting; Vulnerability Scanning.

a b s t r a c t

Universitas Kristen Satya Wacana (UKSW) is one of the private universities in Indonesia that actively utilizes internet technology and its Website to support academic and non-academic activities. SIASAT (Satya Wacana Academic Information System) provides important information confidentially to the community or makes this information only accessible to users who have an account. Regarding security, SIASAT has experienced problems, and threats such as SQL Injection, brute force, and so on which still happen frequently. Problems related to the security and confidentiality of data in computer networks are Privacy (confidentiality) data must be kept away from unauthorized parties. Integrity (integrity) ensures that the information sent remains intact or without changes. Authenticity (authenticity) is a procedure for knowing that a user is truly authorized to access a system. Authenticity could be password, PIN, fingerprints, or other identification. Non-repudiation (irrefutable proof) is proof to ensure that the user has full access to the services used in a system. A system can be categorized as unsafe if the above issues cannot be met. Therefore, by using Footprinting and vulnerability scanning techniques, analysis can be carried out on the SIASAT Website to overcome this problem. This research was carried out using an approach of ethical Hacking, with an emphasis on level Footprinting and vulnerability scanning. The results of this research have found information related to the SIASAT Website and several vulnerability warnings after scanning with high to low-risk levels.

a b s t r a k

Universitas Kristen Satya Wacana (UKSW) merupakan salah satu perguruan tinggi swasta di Indonesia yang secara aktif memanfaatkan teknologi internet dan situs webnya untuk mendukung kegiatan akademik dan non akademik. SIASAT (Sistem Informasi Akademik Satya Wacana) menyediakan informasi penting secara rahasia kepada civitas atau menjadikan informasi tersebut hanya dapat diakses oleh pengguna yang memiliki akun. Terkait dengan keamanan, SIASAT pernah mengalami kendala, ancaman seperti SQL Injection, brute force, dan lain sebagainya yang masih sering terjadi. Permasalahan yang terkait dengan keamanan dan kerahasiaan data baik itu dalam jaringan komputer adalah Privacy (kerahasiaan) data itu harus dijauhkan dari pihak yang tidak berhak. Integrity (integritas) menjaga bahwa informasi yang terkirim tetap utuh atau tanpa mengalami perubahan. Authenticity (keaslian) merupakan prosedur untuk mengetahui bahwa pengguna benar-benar berwenang untuk mengakses suatu sistem. Authenticity bisa berupa password, PIN, sidik jari, atau identitas lainnya. Non-repudiation (pembuktian yang tak bersangkal) merupakan pembuktian untuk menjaga user bahwa ia telah melakukan akses penuh terhadap layanan yang digunakan dalam suatu sistem. Suatu sistem dapat dikategorikan tidak aman jika isu-isu diatas tidak dapat terpenuhi. Oleh karena itu, dengan menggunakan teknik Footprinting dan vulnerability scanning, dapat dilakukan analisis terhadap Website SIASAT untuk mengatasi permasalahan tersebut. Penelitian ini dilakukan dengan pendekatan ethical Hacking, dengan penekanan pada tahap Footprinting dan vulnerability scanning. Hasil penelitian ini telah menemukan informasi terkait Website SIASAT dan beberapa peringatan kerentanan setelah dilakukan pemindaian dengan tingkat risiko tinggi hingga rendah.

Corresponding Author. Email: 672019141@student.uksw.edu [1].

ACM Computing Classification System (CCS)
EBSCOhost
Communication and Mass Media Complete (CMMC)

1. Latar Belakang

Saat ini perkembangan teknologi dan informasi sangat pesat, keberlangsungan aktivitas masyarakat tidak lepas dari adanya internet. Internet mempunyai banyak manfaat yang dapat dirasakan oleh masyarakat, seperti sebagai media informasi, media pembelajaran, media transaksi, dan lain sebagainya. Namun terdapat juga informasi yang bersifat rahasia yang tidak dapat diakses oleh setiap orang. Data-data yang bersifat rahasia ini disimpan pada sebuah storage yang dilengkapi keamanan untuk menghindari adanya serangan-serangan yang dapat mengeksploitasi dokumen atau data-data. Masalah keamanan data dan privasi penting dalam organisasi dan individu [1]. Penyadapan dokumen dan data merupakan ketakutan terbesar bagi pengguna jaringan komunikasi saat ini [2]. Penyadapan pada sebuah sistem terjadi karena adanya celah keamanan yang dapat dieksploitasi. Mereka memanfaatkan celah keamanan untuk mencuri data atau meretas sistem [3]. Sebelum peretas melakukan kegiatannya, mereka terlebih dahulu akan mencari informasi target yang akan dibobol sistemnya. Informasi-informasi mengenai celah keamanan inilah yang ingin diketahui kemudian diuji untuk menentukan bagaimana tingkat keamanan informasi rahasia ini dilindungi dari pihak yang tidak bertanggung jawab.

Universitas Kristen Satya Wacana (UKSW) merupakan salah satu perguruan tinggi swasta di Indonesia yang secara aktif memanfaatkan teknologi internet dan situs webnya untuk mendukung kegiatan akademik dan non akademik. Salah satu web yang ada di UKSW ialah SIASAT (Sistem Informasi Akademik Satya Wacana). SIASAT menyediakan informasi penting secara rahasia kepada civitas atau menjadikan informasi tersebut hanya dapat diakses oleh pengguna yang memiliki akun. Tetapi ada juga pihak dengan cara yang salah dapat mengakses web SIASAT dan menyalahgunakan informasi yang ada. Terkait dengan keamanan, SIASAT pernah mengalami kendala, dalam wawancara dengan perwakilan bagian Biro Teknologi dan Sistem Informasi yang bertanggung jawab dengan web SIASAT menjelaskan bahwa: (1) Dari sisi pengelola web SIASAT, belum ada *hacker* yang dapat menembus server database, akan tetapi ancaman seperti SQL *Injection*, *brute force*, dan lain sebagainya yang masih sering terjadi. Kemudian dari sisi *user*, biasanya kebobolan seperti penghapusan mata kuliah terjadi apabila *user* atau mahasiswa tidak menjaga password masing-masing, sehingga teman atau orang lain mencoba melakukan login dengan menebak password mahasiswa. (2) Arsitektur keamanan web SIASAT didesain dengan *Three Tier Architecture*, dimana antara *application tier*, *Business Tier*, dan Database Tier diletakkan secara terpisah di dalam tiga server virtual, koneksi antar server hanya dapat dilakukan dengan koneksi protokol http dengan port tertentu. Untuk dapat melakukan akses ke server database, dari sisi klien tidak dapat dilakukan dan hanya dapat dilakukan melalui aplikasi SIASAT dengan melalui firewall yang terpasang di setiap server. Kerahasiaan data dalam pemanfaatan teknologi dalam pendidikan semakin rumit seiring dengan terus majunya perkembangan teknologi [4]. Ini disebabkan oleh keterlibatan teknologi dalam pengumpulan, pengolahan, dan penyimpanan data yang bersifat sensitif, seperti data pribadi dan data akademik [4]. Institusi pendidikan harus memberikan perhatian serius terhadap tantangan privasi yang muncul dalam penggunaan teknologi pendidikan [4].

Permasalahan yang terkait dengan keamanan dan kerahasiaan data baik itu dalam jaringan komputer adalah *privacy* (kerahasiaan), *integrity* (integritas), *authenticity* (keaslian), *non-repudiation* (pembuktian yang tak bersangkal) [1]. *Privacy* (kerahasiaan) data itu harus dijauhkan dari pihak yang tidak berhak. *Integrity* (integritas) menjaga bahwa informasi yang terkirim tetap utuh atau tanpa mengalami perubahan. *Authenticity* (keaslian) merupakan prosedur untuk mengetahui bahwa pengguna benar-benar berwenang untuk mengakses suatu sistem. Authenticity bisa berupa password, PIN, sidik jari, atau identitas lainnya. *Non-repudiation* (pembuktian yang tak bersangkal) merupakan pembuktian untuk menjaga *user* bahwa ia telah melakukan akses penuh terhadap layanan yang digunakan dalam suatu sistem. Keamanan jaringan merupakan upaya untuk melindungi sumber informasi dari potensi ancaman. Keamanan dan menjaga kerahasiaan data adalah hal yang sangat penting dalam konteks informasi [1]. Pada dasarnya menciptakan sistem jaringan yang aman tidak lepas dari pengelolaan sistem yang baik. Keamanan jaringan memiliki beberapa tujuan, di antaranya adalah menjaga kerahasiaan (*confidentiality*) data, memastikan integritas (*integrity*) data tetap terjaga, serta menjaga ketersediaan (*availability*) data agar selalu

dapat diakses [5]. *Hacking* merupakan kegiatan memasuki sebuah sistem secara ilegal. Orang atau kelompok yang melakukan kegiatan *Hacking* ada yang bersifat positif (*hacker*) dan negatif (*cracker*). Batasan antara *hacker* dan *cracker* sangatlah tipis [6]. Batasan ini ditentukan oleh etika, moral, dan integritas dari pelakunya sendiri [6]. *Hacker* setelah memasuki sistem tidak melakukan perusakan sistem, tetapi memberitahu atau memberikan solusi kepada pemilik sistem yang dibobol. Sedangkan *cracker* jika telah menguasai sistem maka mereka cenderung merusak. Kegiatan *cracker* ini disebut *cracking*.

Footprinting mengacu pada aktivitas apa pun yang bertujuan mengumpulkan data pada target yang sistemnya akan diretas sebelum melakukan proses pembobolan sistem sesungguhnya [7]. *Footprinting* dibagi menjadi dua macam yaitu *passive Footprinting* dan active *Footprinting*. *Passive Footprinting* proses pengumpulan informasi mengenai suatu target serangan tanpa melibatkan interaksi langsung dengan target serangan. [7]. Kegiatan passive *Footprinting* meliputi analisa informasi perusahaan dan analisa jaringan computer. Analisa informasi perusahaan dilakukan seperti mencari situs *Website* perusahaan, alamat perusahaan, kontak telepon perusahaan, dan lain-lain [7]. Analisa jaringan komputer dilakukan seperti mencari domain name perusahaan, IP Address, jenis router dan server yang digunakan, dan lain-lain [7]. Active *Footprinting* adalah proses pengumpulan informasi tentang target yang diretas melalui interaksi langsung dengan target yang akan diretas. Kegiatan yang dilakukan berupa social engineering, menyelidiki struktur *Website*, E-mail bouncing, DNS zone transfers, dan lain-lain [7].

Alasan mengapa proses *Footprinting* ini penting karena 90% waktu seorang *cracker* digunakan untuk mengumpulkan informasi, dan 10% untuk melakukan percobaan menguasai sistem server [7]. *Vulnerability scanning* adalah proses memperoleh informasi tentang kerentanan jaringan diperoleh dengan menggunakan berbagai alat pemindaian jaringan dan pemindaian kerentanan seperti pencarian *port* terbuka, identifikasi bug dalam aplikasi, serta teknik ini juga membantu dalam memahami potensi serangan yang dapat ditujukan ke kerentanan yang ada di dalam situs web, yang memiliki potensi dampak yang signifikan apabila terjadi serangan [8]. Penelitian terkait yang juga menggunakan Teknik *Footprinting* dan *vulnerability scanning* di lakukan pada *Website* salah satu institusi perguruan tinggi di Indonesia. Hasil penelitian tersebut ditemukan informasi mengenai target, antara lain IP Server, *Operating system* (OS) *version*, *port-port* yang terbuka, topologi jaringan, service version pada server dan lokasi server, juga ditemukan kerentanan keamanan dengan tingkat risiko tinggi hingga rendah [9]. Penelitian selanjutnya dilakukan pada SIAKAD Univesitas XYZ. Pada penelitian tersebut ditemukan kerentanan dengan tingkat risiko tinggi 1, tingkat risiko medium 6 dan tingkat risiko rendah 14 [10].

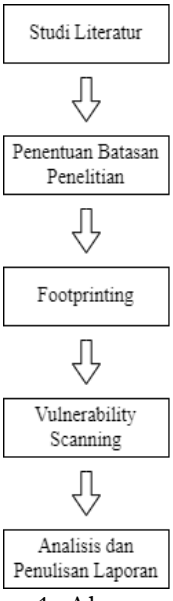
Penelitian berikutnya dilakukan di *Website* lembaga pendidikan di salah satu kota di Indonesia. Hasil pada pada penelitian trsebut ditemukan 11 kerentanan keamanan dengan tingkat risiko medium hingga rendah, seperti *Application error message*, *HTML form without CSRF protection*, *Host header attack*, *User credentials are sent in clear text*, *Multiple vulnerabilities fixed in PHP*, *Clickjacking: X-Frame-Options header missing*, *Documentation file*, *Cookie without Http Only flag set*, *Login page password-guessing attack*, *Possible sensitive files*, *Possible sensitive directories* [8]. Penelitian selanjutnya dilakukan pada *Website* Institut Teknologi Padang. Hasil penelitian tersebut ditemukan *Website* ITP mendapatkan hasil skor pada level tiga, yang berarti *Website* ini tidak dalam kondisi aman [11]. Dari perbandingan tersebut, dapat disimpulkan bahwa keempat penelitian tersebut memiliki fokus yang berbeda dalam menganalisis keamanan *Website*. Mereka mengidentifikasi informasi mengenai target, seperti IP server, sistem operasi, *port-port* yang terbuka, dan topologi jaringan. Selain itu, mereka juga menemukan celah keamanan dengan tingkat risiko yang bervariasi, mulai dari risk level *high* hingga *low*.

Keamanan data dan privasi bukan lagi sekadar prioritas, tetapi suatu keharusan. Dalam dunia yang semakin terkoneksi dan terpapar oleh teknologi, keamanan adalah fondasi yang tidak dapat diabaikan. Keamanan adalah kunci untuk menjaga kerahasiaan data, memastikan integritas informasi, dan memverifikasi keaslian pengguna. Tanpa keamanan yang memadai, risiko terhadap kebocoran data dan peretasan sistem semakin meningkat. Suatu sistem dapat dikategorikan tidak aman jika isu-isu diatas tidak dapat terpenuhi, sehingga keamanan sistem tersebut dapat dieksploitasi oleh orang yang tidak bertanggung jawab. Seperti yang telah dijelaskan sebelumnya,

pentingnya keamanan menjadi alasan mengapa perlu untuk menguji keamanan *Website* SIASAT. Oleh karena itu, dengan menggunakan teknik *Footprinting* dan *vulnerability scanning*, dapat dilakukan analisis terhadap *Website* SIASAT untuk mengatasi permasalahan tersebut. Tujuan penelitian ini adalah untuk menguji keamanan web SIASAT dengan teknik *Footprinting* dan menganalisis hasil pengujian dengan *vulnerability scanning*.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan ethical *Hacking*, dengan penekanan pada tahap *Footprinting* dan *vulnerability scanning*. Objek atau target yang menjadi fokus penelitian adalah *Website* SIASAT Universitas Kristen Satya Wacana. Adapun tahapan penelitian ini dapat dilihat pada gambar 1.

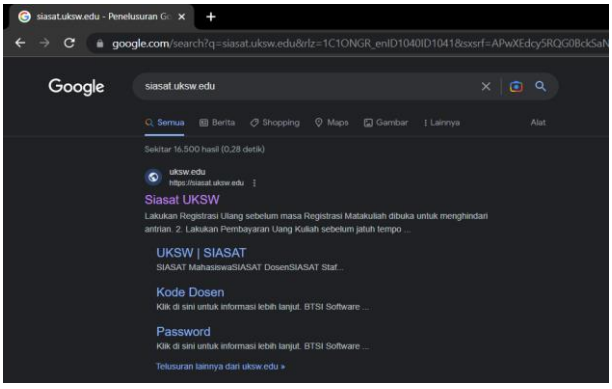


Gambar 1. Alur penelitian

1) Studi literatur
   Tahap awal dilakukan melalui penelitian literatur, membaca buku, jurnal dan disertasi sebagai referensi dalam penelitian ini.
2) Penentuan batasan penelitian
   Batasan-batasan yang diterapkan pada *Website* target yang diuji adalah terbatas pada tahap *Footprinting* dan *vulnerability scanning* tanpa melibatkan tindakan eksploitasi sistem seperti merubah tampilan, melakukan *SQL Injection*, *brute force, DDos*, dan lain-lain.
3) *Footprinting*
   Langkah ini dilakukan untuk memperoleh data atau informasi sebanyak mungkin dari target, termasuk merek, tipe, nomor versi *OS*, perangkat *network address*. Adapun *tools Footprinting* yang digunakan pada penelitian ini yaitu CMD (*command prompt*), CMD merupakan aplikasi berbasis *Command line interpreter* pada system operasi Microsoft Windows. Pada tahap ini, *Command Prompt* digunakan untuk mengidentifikasi alamat *IP* target, dengan menjalankan perintah *ping siasat.uksw.edu*. Kemudian Zenmap, Zenmap adalah antarmuka grafis *(GUI)* untuk Nmap (*Network Mapper*), yang merupakan salah satu alat pemindaian jaringan terkemuka yang digunakan untuk mengevaluasi keamanan jaringan. Selanjutnya Whois Domain, Whois Domain digunakan untuk mendapatkan informasi lebih lanjut tentang *domain* target, seperti alamat, kontak, dan pemilik domain, serta *server name*.
4) *Vulnerability scanning*
   Pada tahap ini, dilakukan pengumpulan informasi tentang kerentanan jaringan dari target seperti *port* yang terbuka, *bugs* aplikasi. Adapun *tools* yang digunakan adalah pentest-tools.com. Dengan mengakses situs web pentest-tools.com dan memasukkan alamat IP target untuk memulai pemindaian kerentanan. Pemindaian ini mencakup pemindaian *port* yang terbuka, mengidentifikasi versi perangkat lunak yang digunakan, dan mencari kerentanan yang mungkin ada.
5) Analisis dan penulisan laporan
   Pada tahap ini, dilakukan analisis dan dokumentasi terhadap informasi kerentanan yang ditemukan setelah melakukan pemindaian terhadap target.

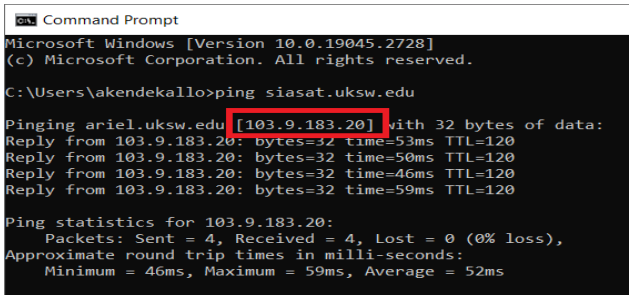
3. Hasil dan Pembahasan

Tahap pertama dari penelitian ini adalah mencari informasi mengenai web SIASAT dengan menggunakan search *engine Google*, sehingga didapatkan hasil yang dapat dilihat pada gambar 2. Dari hasil pencarian tersebut tautan-tautan yang ditemukan mengarah ke berbagai sumber informasi civitas akademika UKSW.



Gambar 2. Hasil pencarian dengan Google

Kemudian melakukan *ping* terhadap web SIASAT menggunakan Command Prompt (CMD). Dalam hal ini, *ping* digunakan untuk menguji koneksi antara komputer dan web SIASAT yang diteliti, sehingga memungkinkan untuk memperoleh informasi tentang *alamat IP* web tersebut, yang dapat dilihat pada gambar 3.

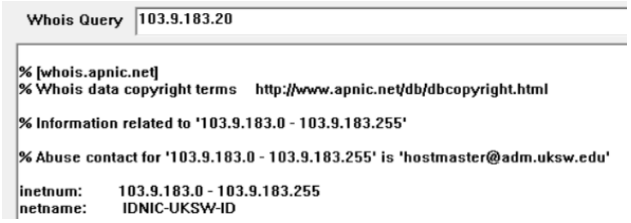


Gambar 3. Hasil *ping* di *Command Prompt*

Selanjutnya adalah melakukan *port scan* untuk mengidentifikasi *port* mana yang terbuka dan aktif. Proses ini menggunakan *tools* Zenmap, sehingga didapatkan hasil yang dapat dilihat pada gambar 4. Zenmap menemukan beberapa *port* yang terbuka, dimana informasi dapat berguna bagi penyerang *(hacker)* untuk melakukan serangan terhadap jaringan target.

Gambar 4. Hasil *Footprinting* dengan Zenmap

Langkah selanjutnya melakukan pengecekan menggunakan *tools Whois*, Pada gambar 5 terlihat siasat.uksw.edu mempunyai blok alamat IP dari 103.9.183.0 hingga 103.9.183.255, juga mempunyai *netname* IDNIC-UKSW-ID.



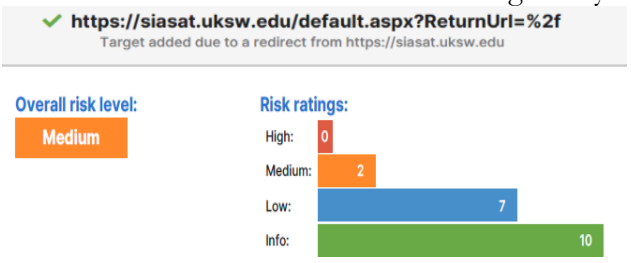
Gambar 5. Hasil *Footprinting* dengan Whois

Selain itu pada gambar 5 informasi seperti nama, *email*, alamat dan kontak pengelola server juga didapatkan.

Gambar 6. Hasil *Footprinting* dengan Whois

Hasil pengujian *Footprinting* pada *Website* SIASAT menggunakan *tools* Command Prompt, Whois, dan Zenmap menunjukkan bahwa beberapa informasi terkait target ditemukan, antara lain *IP Server, Block IP Address, netname, email,* lokasi server, kontak pengelolah server, dan *port-port* yang terbuka. Pengelolah *Website* direkomendasikan untuk melakukan perlindungan terhadap informasi-informasi yang sensitif dari *Website*, memastikan bahwa *hacker* atau pihak yang tidak berkepentingan tidak dapat mengakses atau mengeksploitasi data tersebut.

Tahap selanjutnya adalah melakukan *vulnerability scanning* dengan menggunakan *tools* pentest-tools.com. Hasil pemindaian mencakup kerentanan yang terdeteksi beserta rekomendasi untuk mengatasinya.



Gambar 7. Hasil *vulnerability scanning* dengan pentest-tools.com

Gambar 7 merupakan hasil yang didapatkan setelah melakukan *vulnerability scanning*. *Website* SIASAT berada pada level medium untuk tingkat keamanannya. Rincian kerentanan yang telah ditemukan mencakup dua medium risk, tujuh low risk, dan terdapat 10 *informational*.

Tabel 1. Hasil *vulnerability scanning* dengan pentest-tools.com

No	Kerentanan	Solusi	Tingkat risiko
1	*Insecure cookie setting: missing Secure flag*	Pastikan bahwa *flag* aman *(secure flag)* diatur untuk *cookie* yang mengandung informasi sensitif tersebut.	Medium
2	*Vulnerabilities found for server-side software*	Melakukan *upgrade (web server internet_information_services 8.5)* ke versi terbaru.	Medium
3	*Missing security header: X-XSS-Protection*	Mengatur *header X-XSS-Protection* menjadi *X-XSS-Protection: 1; mode=block*.	Low
4	*Missing security header: X-Frame-Options*	Menambahkan *header HTTP X-Frame-Options* dengan nilai *DENY* atau *SAMEORIGIN* ke setiap halaman yang ingin dilindungi dari serangan *Clickjacking*.	Low
5	*Missing security header: Strict-Transport-Security*	*Header HTTP Strict-Transport-Security* harus dikirimkan bersama setiap respon *HTTPS*.	Low
6	*Missing security header: Referrer-Policy*	*Header Referrer-Policy* harus dikonfigurasi di sisi server untuk menghindari pelacakan pengguna dan kebocoran informasi yang tidak disengaja. Nilai *no-referrer* pada *header* ini memerintahkan *browser* untuk mengabaikan *header Referer* sepenuhnya.	Low
7	*Missing security header: X-Content-Type-Options*	Mengatur *header X-Content-Type-Options* seperti *X-Content-Type-Options: nosniff*.	Low
8	*Missing security header: Content-Security-Policy*	Konfigurasikan *header Content-Security-Header* untuk dikirimkan bersama setiap respon *HTTP* guna menerapkan kebijakan tertentu yang dibutuhkan oleh aplikasi.	Low
9	*Server software and technology found*	Menghapus informasi yang dapat memudahkan identifikasi platform perangkat lunak, teknologi, server, dan sistem operasi: *header* server *HTTP*, informasi meta *HTML* dan sebagainya.	Low

Tabel 1 menunjukan kerentanan yang telah teridentifikasi meliputi kurangnya pengaturan keamanan seperti *flag* aman pada *cookie*, *Secure flag* pada *cookie* seharusnya digunakan untuk mengamankan *cookie* yang dikirim melalui koneksi *HTTPS*, tanpa *Secure flag*, cookie dapat disadap melalui koneksi *HTTP* yang tidak aman. Kerentanan pada perangkat lunak *server-side*, kerentanan yang memungkinkan pengeksploitasi sistem, atau kerentanan yang dapat mengakibatkan kebocoran data. Ketidakhadiran *header* keamanan seperti *X-XSS-Protection, X-XSS-Protection* adalah header keamanan yang dapat digunakan untuk melindungi situs web dari serangan *Cross-Site Scripting (XSS)*. Jika header ini hilang, situs web mungkin rentan terhadap serangan *XSS*. Serta *X-Frame-Options*, ini melindungi situs web dari serangan *framing* yang tidak diinginkan. Jika *header* ini hilang, situs web dapat rentan terhadap *framing*

berbahaya. Selain itu, ada juga kerentanan terkait dengan *header* keamanan seperti *Strict-Transport-Security*, *Strict-Transport-Security (HSTS)* adalah *header* yang memastikan bahwa koneksi ke situs web selalu dilakukan melalui *HTTPS*, mengurangi risiko penyadapan data. Jika *header* ini hilang, situs web mungkin rentan terhadap serangan *Man-in-the-Middle (MiTM)* atau serangan penyadapan. *Referrer-Policy*, *Header Referrer-Policy* mengontrol informasi yang dikirim oleh *browser* kepada situs web lain saat pengguna mengklik tautan. Jika *header* ini hilang, informasi yang berlebihan dapat bocor ke situs web lain. *X-Content-Type-Options*, *header* yang mencegah *browser* dari melakukan *sniffing* tipe konten *(content type sniffing)* yang dapat digunakan oleh penyerang untuk menyisipkan skrip berbahaya. *Content-Security-Policy*, *header* yang digunakan untuk mengontrol sumber daya yang dapat dimuat pada halaman web. Ini membantu melindungi situs web dari serangan *XSS* dan injeksi skrip lintas situs *(CSRF)*.

Terdapat juga informasi mengenai *platform* perangkat lunak dan teknologi yang ditemukan. Pengelolaan dan perbaikan kerentanan-kerentanan ini sangat penting untuk mengurangi risiko keamanan. Selain solusi yang terdapat pada Tabel 1, berikut beberapa pencegahan yang dapat dilakukan untuk melindungi sistem dari kerentanan yang teridentifikasi. Selalu menjaga *server-side software* terbaru dengan menginstal pembaruan keamanan terbaru. Selain mengatur header X-XSS-Protection, selalu pastikan bahwa aplikasi memvalidasi input pengguna dan menghindari penyisipan skrip yang tidak sah. Selain mengatur *header X-Frame-Options*, pastikan aplikasi menggunakan kontrol akses *CORS (Cross-Origin Resource Sharing)* untuk mengontrol permintaan sumber daya lintas domain. Pastikan bahwa seluruh situs web hanya dapat diakses melalui koneksi *HTTPS* dengan *header HTTP Strict-Transport-Security*. Ini akan mencegah serangan *MITM (Man-in-the-Middle)* dan penyerangan protokol. Selain mengatur *header Referrer-Policy*, pastikan untuk menghindari tautan ke sumber daya yang tidak dikenal atau tidak tepercaya yang dapat mengungkapkan informasi pengguna. Memastikan bahwa sumber daya yang terkirim adalah tipe *MIME* yang tepat untuk mencegah serangan *MIME sniffing*. Selain dari pencegahan di atas melibatkan praktik keamanan terbaik, seperti menjalankan pemindaian keamanan rutin, melakukan pengujian penetrasi, dan mengedukasi tim tentang praktik keamanan *IT* adalah upaya berkelanjutan yang dapat dilakukan untuk melindungi atau menghindari sistem dari serangan.

Software / Version	Category
Windows Server	Operating systems
IIS 8.5	Web servers
Microsoft ASP.NET 4.0.30319	Web frameworks
DigiCert	SSL/TLS certificate authorities

Gambar 8. *Server software* dan teknologi yang ditemukan

Gambar 8 merupakan informasi mengenai *platform* perangkat lunak dan teknologi yang digunakan web SIASAT, dengan sistem operasi Windows Server, *web server* Microsoft IIS 8.5, *web frameworks* Microsoft ASP.NET 4.0.30319, dan sertifikat SSL/TLS dari Digicert.

Setelah melakukan *footprinting* dan *vulnerability scanning*, ditemukan bahwa web target yang dikelola oleh UKSW memiliki beberapa kerentanan yang berpotensi mengancam keamanan web tersebut. Maka dari itu, langkah-langkah pencegahan lebih awal diperlukan, dan rata-rata kerentanan yang ditemukan melalui alat-alat seperti pentest-tools.com terletak pada *plugin* yang terintegrasi dalam situs web. Sebagian besar *plugin* belum diperbarui oleh pengelola, menyebabkan beberapa *query* yang diidentifikasi sebagai masalah keamanan oleh aplikasi *scanning*. Namun demikian, *firewall* yang dimiliki oleh situs target dengan domain siasat.uksw.edu berhasil melindunginya, sehingga *firewall* dapat mencegah serangan langsung terhadap celah keamanan yang ditemukan. Selain itu, hasil *scanning* yang dihasilkan oleh pentest-tools.com otomatis menunjukkan adanya *false positive*. Ini adalah peringatan atau indikasi kesalahan yang diberikan oleh sistem keamanan atau aplikasi keamanan, yang sebenarnya tidak sesuai dengan fakta atau tidak valid. Dalam konteks keamanan siber, *false positive* dapat terjadi ketika sebuah sistem keamanan atau aplikasi keamanan menganggap sebuah aktivitas atau tindakan tertentu sebagai ancaman atau serangan keamanan, yang kemungkinan tidak ada ancaman atau serangan yang terjadi sehingga memberikan peringatan. Misalnya, alat pemindaian mungkin menemukan port yang terbuka dan menganggapnya sebagai kerentanan, padahal port tersebut sebenarnya dibuka untuk tujuan yang sah.

4. Kesimpulan

Setelah dilakukan *footprinting* dan *vulnerability scanning* pada website SIASAT, dapat disimpulkan bahwa terdapat beberapa celah keamanan yang berpotensi membahayakan website tersebut. Kerentanan yang ditemukan ialah *Insecure cookie setting: missing Secure flag (medium), Vulnerabilities found for server-side software (medium), Missing security header: X-XSS-Protection (low), Missing security header: X-Frame-Options (low), Missing security header: Strict-Transport-Security (low), Missing security header: Referrer-Policy (low), Missing security header: X-Content-Type-Options (low), Missing security header: Content-Security-Policy (low), Server software and technology found (low)*. Prinsip-prinsip keamanan seperti *privacy* (kerahasiaan), *integrity* (integritas), *authenticity* (keaslian), dan *non-repudiation* (pembuktian yang tak bersangkal) dalam jaringan komputer menjadi sangat penting untuk diperhatikan, karena informasi sensitif dapat dicuri oleh pihak yang tidak berwenang jika tidak dijaga dengan baik. Oleh karena itu, perbaikan keamanan pada website SIASAT harus segera dilakukan untuk mengurangi risiko serangan *cyber* dan pencurian data. Pentingnya menjaga kerahasiaan data dalam dunia yang terus terhubung dan serba digital. Informasi pribadi, bisnis, atau akademis dapat menjadi sasaran serangan siber jika tidak dijaga dengan ketat. Untuk itu, selalu perhatikan praktik keamanan seperti penggunaan kata sandi yang kuat, enkripsi, dan penggunaan akses yang bijak. Berpartisipasi dalam pelatihan keamanan dan meningkatkan kesadaran tentang risiko siber adalah langkah penting untuk melindungi data dan mencegah kemungkinan pencurian atau penyalahgunaan. Dengan berkomitmen pada kerahasiaan data, dapat membantu memastikan bahwa informasi sensitif tetap aman dan terlindungi dalam era digital yang terus berkembang.

5. Daftar Pustaka

[1] Kristanto, A. (2003). Keamanan Data pada Jaringan Komputer. *Gava Media, Yogyakarta*.

[2] Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69-77.

[3] Al Hilmi, M. A., & Khujaemah, E. (2022). Network Security Monitoring With Intrusion Detection System. *Jurnal Teknik Informatika (JUTIF)*, *3*(2), 249-253.

[4] Cahyanto, I. (2023). Privacy Challenges in Using Wearable Technology in Education Literature Review. *Formosa Journal of Applied Sciences*, *2*(6), 909-928. DOI: https://doi.org/10.55927/fjas.v2i6.4272.

[5] Ariyus, D., & Kom, M. (2007). Intrusion detection system. *Yogyakarta: Andi*.

[6] Fatkhurozzi, M. (2021, November). Analisa Keamanan Website Menggunakan Metode Footprinting dan Vulnerability Scanning pada Website Kampus. In *Prosiding Seminar Nasional Informatika Bela Negara* (Vol. 2, pp. 144-148).

[7] Herdianti, H., & Umar, F. (2020). Analisis keamanan website menggunakan teknik footprinting dan vulnerability scanning. *INFORMAL: Informatics Journal*, *5*(2), 43-48. DOI: https://doi.org/10.19184/isj.v5i2.18941.

[8] Alwi, E. I., & Ilmawan, L. B. (2021). Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment. *INFORMAL: Informatics Journal*, *6*(3), 131-135. DOI: https://doi.org/10.19184/isj.v6i3.27053.

[9] Zirwan, A. (2022). Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner. *Jurnal Informasi dan Teknologi*, 70-75.