Jurnal Teknik Informatika (JUTIF)
Vol. 3, No. 3, Juni 2022, hlm. 763-770

DOI: https://doi.org/10.20884/1.jutif.2022.3.3.346
p-ISSN: 2723-3863
e-ISSN: 2723-3871

"SIASAT" UKSW (UNIVERSITAS KRISTEN SATYA WACANA) WEBSITE SECURITY ANALYSIS USING OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

Amanda Calvina Izumi[*1], Indrastanti Ratna Widiasari[2]

[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Indonesia
Email: [1]672018303@student.uksw.edu, [2]indrastanti.widiasari@uksw.edu

(Naskah masuk: 28 Mei 2022, Revisi : 06 Juni 2022, diterbitkan: 28 Juni 2022)

Abstract

Satya Wacana Christian University (UKSW) is one of the private higher education institutions in Indonesia that utilizes the internet network, namely the web as a medium for conveying information, connecting the academic community and others. UKSW has many webs that are used, one of which is the SIASAT web. SIASAT is Satya Wacana Academic Information System. SIASAT contains important information about the community. Web SIASAT provides information in a private manner or only those with an account can view the information. However, not only people who have access can access the information, but other irresponsible parties can access it in the wrong way and misuse the existing information. So that it can cause harm to the person or organization. SIASAT often experiences security problems with SQL Injection, brute force, and so on but there has never been a hacker who can penetrate the SIASAT web, therefore the SIASAT web needs to be tested for security. Factors that need to be considered in determining security are confidentiality is maintaining the confidentiality of information from unauthorized people, integrity maintaining changes in information from unauthorized people, and availability keeping information accessible. Therefore, in overcoming this problem, one of the steps that can be taken is to analyze the UKSW web where the web to be analyzed is the SIASAT web with the Open Web Application Security Project (OWASP) method. The hope is that with the OWASP, the handling of an attack can be carried out earlier and prevent fatal consequences.

Keywords: *Keamanan Informasi, OWASP, Open Web Application Security Project*.

ANALISIS KEAMANAN WEBSITE "SIASAT" UKSW (UNIVERSITAS KRISTEN SATYA WACANA) MENGGUNAKAN OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

Abstrak

Universitas Kristen Satya Wacana (UKSW) merupakan salah satu lembaga perguruan tinggi swasta di Indonesia yang memanfaatkan jaringan internet yaitu *web* sebagai media menyampaikan informasi, penghubung civitas-civitas akademik dan lain sebagianya. UKSW memiliki banyak *web* yang dipakai salah satunya *web* SIASAT. SIASAT merupakan Sistem Informasi Akademik Satya Wacana. Di dalam *web* SIASAT terdapat banyak informasi-informasi penting para civitas. Web SIASAT memberikan informasi secara privasi atau hanya yang memiliki akun yang bisa melihat informasi tersebut. Namun hal ini tidak hanya orang yang memiliki akses saja yang dapat mengakses informasi tersebut, tetapi pihak-pihak lain yang tidak bertanggung jawab dapat mengakses dengan cara yang salah dan menyalahgunakan informasi yang ada. Sehingga dapat menyebabkan kerugian bagi pribadi atau organisasi. SIASAT pernah mengalami masalah keamanan dengan *SQL Injection*, *brute force*, dan lain sebagainya tetapi belum pernah ada *hacker* yang dapat menembus *web* SIASAT maka dari itu *web* SIASAT perlu diuji keamanannya. Salah satu faktor yang perlu diperhatikan dalam menentukan keamanan yaitu *confiedentiality* (kerahasiaan) merupakan menjaga kerahasiaan informasi dari orang-orang yang tidak berwenang, *integrity* (intergritas) menjaga perubahan informasi dari orang-orang yang tidak berwenang, dan *availability* (ketersediaan) menjaga agar informasi selalu dapat diakses. Tiga faktor tersebut disingkat dengan CIA TRIAD. Maka dari itu dalam mengatasi masalah ini salah satu langkah yang dapat ditempuh adalah melakukan analisis terhadap *web* UKSW yang dimana *web* yang akan dilakukan analisis yaitu *web* SIASAT dengan metode *Open Web Application Security Project* (OWASP). Harapannya dengan adanya OWASP, penanganan atas sebuah serangan bisa dilakukan lebih awal dan mencegah akibat yang fatal.

Kata kunci: *Keamanan Informasi, OWASP, Open Web Application Security Project.*.

1. PENDAHULUAN

Perkembangan teknologi dan informasi di era sekarang begitu sangat pesat, internet menjadi salah satu bagian penting dalam keberlangsungan aktivitas yang dilakukan oleh masyarakat sekarang. Hal ini dilihat dengan semakin banyak pengguna media sosial dan internet saat ini. Dengan semakin bertambahnya pengguna internet, maka semakin banyak informasi yang dapat diperoleh dari internet. Informasi yang bisa didapatkan seperti ekonomi, sosial, budaya, kehidupan sehari-hari dan lain sebagainya. Namun informasi-informasi tersebut tidak semuanya bebas dikonsumsi oleh masyarakat umum, terdapat juga informasi yang bersifat rahasia dan hanya orang berwenang yang dapat mengaksesnya. Data-data rahasia tersebut biasanya tersimpan di dalam *storage* dari aplikasi yang dilengkapi keamanan, sehingga data tersebut tetap aman dari akses yang diinginkan. Tingkat keamanan ini yang nantinya harus diuji untuk menentukan sejauh mana data-data rahasia ini aman dari serangan-serangan pihak luar yang tidak bertanggung jawab. Serangan-serangan keamanan informasi bisa datang dalam bentuk apapun. Penyadapan dokumen atau data merupakan hal yang paling ditakuti oleh pengguna jaringan komunikasi pada saat ini [1]. Maka dari itu semakin banyaknya masyarakat memberikan informasi maka semakin menipisnya privasi yang dimiliki oleh masyarakat. Sehingga dari itu masyarakat harus mulai memperhatikan resiko keamanan dari informasi yang diberikan di internet agar tidak memberikan dampak buruk yang dapat mempengaruhi dalam kehidupan sehari-hari. Evaluasi keamanan suatu sistem pada instansi sektor pendidikan menjadi sangat penting karena ancaman serangan siber pada tahun 2020 menurut Badan Siber dan Sandi Negara [2]. Mereka memanfaatkan celah keamanan demi mencuri data atau mengambil keuntungan dari peretasan ke dalam sistem [3]. Universitas Kristen Satya Wacana (UKSW) merupakan salah satu lembaga perguruan tinggi swasta di Indonesia yang memanfaatkan jaringan internet yaitu web sebagai media menyampaikan informasi, penghubung civitas-civitas akademik dan lain sebagianya. UKSW memiliki banyak web yang dipakai salah satunya web SIASAT. SIASAT merupakan Sistem Informasi Akademik Satya Wacana. Di dalam web SIASAT terdapat banyak informasi-informasi penting para civitas. Web SIASAT memberikan informasi secara privasi atau hanya yang memiliki akun yang bisa melihat informasi tersebut. Namun hal ini tidak hanya orang yang memiliki akses saja yang dapat mengakses informasi tersebut, tetapi pihak-pihak lain yang tidak bertanggung jawab dapat mengakses dengan cara yang salah dan menyalahgunakan informasi yang ada. Sehingga dapat menyebabkan kerugian bagi pribadi atau organisasi. SIASAT pernah mengalami masalah keamanan, berdasarkan hasil wawancara dengan salah satu pihak Bagian Biro Teknologi dan Sistem Informasi (BTSI) yang bertanggung jawab dalam web SIASAT memberikan penjelasan bahwa : (1) Web SIASAT sering mendapatkan serangan dan ancaman misal dengan SQL Injection, brute force, dan lain sebagainya tetapi belum pernah ada hacker yang dapat menembus web SIASAT; (2) Dari awal SIASAT dibangun sudah menggunakan *three-tier system* yaitu *application tier*, *database tier*, *component tier* maka jika ingin masuk harus bertahap tidak ada celah antar server; (3) Banyak yang membobol web SIASAT tetapi dengan mencari email dan password user, namun itu merupakan kesalahan dari user sendiri dikarenakan tidak bisa menjaga kerahasiaan akunnya; (4) Semua serangan yang masuk sudah teridentifikasi karena semua sudah terecord realtime. Sebagaimana yang telah dipaparkan sebelumnya, keamanan sangatlah penting, maka dari itu web SIASAT perlu diuji keamanannya. Salah satu faktor yang perlu diperhatikan dalam menentukan keamanan yaitu *confidentiality* (kerahasiaan) merupakan menjaga kerahasiaan informasi dari orang-orang yang tidak berwenang, *integrity* (integritas) menjaga perubahan informasi dari orang-orang yang tidak berwenang, dan *availability* (ketersediaan) menjaga agar informasi selalu dapat diakses. Tiga faktor tersebut disingkat dengan CIA TRIAD [4]. CIA TRIAD merupakan salah satu parameter yang digunakan dalam menganalisis keamanan dan menjadi acuan keamanan sebuah *website* [5]. Jika faktor-faktor tersebut tidak terpenuhi maka jaringan dapat dikategorikan tidak aman rawan tersusupi oleh pihak tidak bertanggung jawab yang dapat mengeksploitasi keamanan web. Maka dari itu dalam mengatasi masalah ini salah satu langkah yang dapat ditempuh adalah melakukan analisis terhadap web UKSW yang dimana web yang akan dilakukan analisis yaitu web SIASAT dengan metode *Open Web Application Security Project* (OWASP). Metode OWASP (Open Web Application Security Project) merupakan sebuah organisasi nirlaba yang berfokus pada keamanan web [6]. Metode penilaian resiko OWASP adalah suatu cara sederhana yang berguna untuk menghitung dan menilai kerentanan resiko pada website [7]. Pengguna *OWASP* dalam penelitian didasarkan pada alasan yang telah dikemukakan oleh para peneliti keamanan, didorong oleh perangkat lunak *open source* dan dibandingkan dengan alat di pasar yang relatif mahal [8]. OWASP Zed Attack Proxy (OWASPZap) adalah *tools* digunakan untuk menemukan berbagai lubang keamanan aplikasi web saat pengembangan dan pengujian aplikasi web [5].

Penelitian ini bertujuan untuk menguji keamanan web SIASAT dengan OWASP dan menganalisis hasil pengujian dengan OWASP.

2. PENELITIAN TERKAIT

Penelitian terkait yang juga menggunakan metode *Open Web Application Security Project* (OWASP) dilakukan di Sistem Informasi Mahasiswa (SIMAS-Online) Perguruan Tinggi XYZ. Hasil penelitian tersebut yaitu ditemukan adanya celah keamanan sebanyak 13 celah pada aplikasi web tersebut [9]. Penelitian berikutnya dilakukan di Domain UII.AC.ID. Hasil penelitian tersebut yaitu keamanan pada 10 web target yang memiliki domain uii.ac.id masih belum memenuhi prinsip *confidentiality* [10]. Penelitian selanjutnya dilakukan di Aplikasi Skripsi Online (SISPO) FTI PERBANAS. Hasil penelitian tersebut yaitu tidak ditemukannya kelemahan *injection, Security Misconfiguration, Missing Function Level Access Control,* dan *Cross-Site Request Forgery* [11]. Penelitian selanjutnya dilakukan di Website beralamat www.xyz.com. Hasil penelitian tersebut yaitu website www.xyz.com beberapa tahap kategori masih belum memenuhi standar keamanan [12]. Penelitian selanjutnya dilakukan pada Aplikasi Berbasis Web. Hasil penelitian tersebut yaitu ditemukannya celah-celah keamanan pada website yang diuji [13]. Penelitian selanjutnya dilakukan di Website SMA Negeri 2 Amlapura. Hasil penelitian tersebut yaitu memperkirakan kemungkinan *vulnerability* yang ditemukan dan dieksploitasi [14]. Penelitian selanjutnya tentang Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode OWASP untuk Penilaian Risk Rating. Hasil penelitian tersebut yaitu menunjukkan penggunaan framework Codeigniter dan PHP Native memiliki kesamaan tingkat keparahan Likelihood di *level medium*, sedangkan untuk impact berada di *level low* [15]. Dengan penelitian-penelitian sebelumnya menunjukkan bahwa adanya keterkaitan dengan penelitian yang akan dilakukan.

Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul (Sarno dan Iffano) [16]. Secara tidak langsung informasi dapat menjamin kelangsungan bisnis dan mengurangi resiko-resiko yang terjadi. Menurut ISO/IEC 17799:2005 tentang *information security management system* bahawa keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman untuk memastikan keberlanjutan bisnis, meminimalisir resiko bisnis, dan meningkatkan investasi dan peluang bisnis. Keamanan informasi memiliki 3 aspek, yaitu *Confidentiality*, *Integrity*, dan *Availability* yang merupakan konsep *information protection* [16].

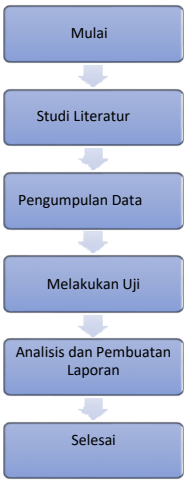
Penetration testing merupakan sebuah metode dalam mengevaluasi keamanan dari sebuah sistem dan jaringan komputer. Evaluasi tersebut dilakukan dengan cara melakukan sebuah simulasi serangan. Menurut Emily Chow (2011) dalam judul "*Ethical Hacking & Penetration Testing*", menyimpulkan bahwa *ethical hacking* dan *penetration testing* dianggap sebagai cara efisien dan efektif dalam mengatasi celah keamanan dan kelemahannya sebelum adanya eksploitasi dari peretas jahat [17].

OWASP memiliki beberapa project yaitu *OWASP Top 10, OWASP Proactive Controls, OWASP Application Security Verification Standard (ASVS), OWASP Software Assurance Maturity Model (SAMM), OWASP Zed Attack Proxy (ZAP), dan OWASP Mod Security Core Rule Set (CRS)*.

OWASP Top 10 berisikan 10 daftar celah keamanan yang dapat mengancam keamanan suatu web, tetapi daftar ini terus berkembang dan berubah-ubah mengikuti perkembangan teknologi. OWASP Top 10 dibuat dengan tujuan meningkatkan kesadaran tentang keamanan aplikasi dengan mengindentifikasi resiko celah keamanan yang sering dihadapi dalam banyak kasus [18]. Kasus yang dihadapi seperti berikut: *Injection, Broken Authentication, Cross-Site Scripting (XSS), Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross-Site Request Forgery (CSRF), Using Known Vulnerable Components, dan Unvalidated Redirects and Forwards*.

3. METODE PENELITIAN

Dalam melakukan penelitian *web* siasat.uksw.edu menggunakan metode OWASP. OWASP merupakan organisasi non-profit yang berdedikasi membuat pengujian keamanan yang *open-source* yang bebas digunakan oleh siapa saja [6].



Gambar 1. Alur Penelitian

Pada penelitian ini, akan dilakukan beberapa alur penelitian yang dapat dilihat pada Gambar 1.

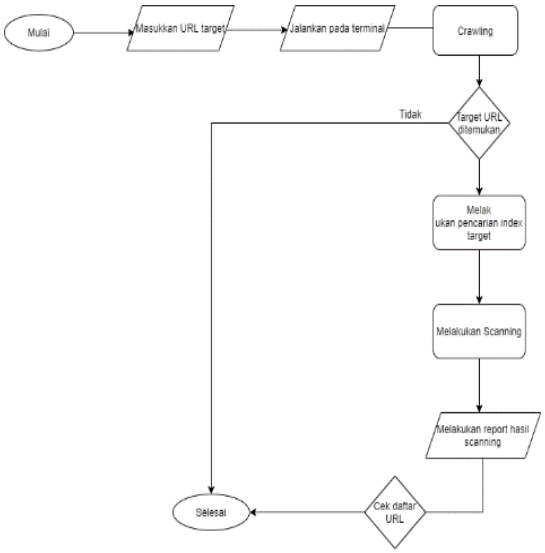
Tahap awal yang dilakukan dengan melakukan studi literatur yang didapatkan dari membaca jurnal dan skripsi dengan penelitian serupa.

Kemudian di tahap kedua yaitu pengumpulan data dengan cara mengumpulkan data target yang akan dilakukan pengujian. Pengumpulan data

dilakukan dengan mengidentifikasi *web* SIASAT UKSW.

Tahap ketiga ini dilakukan pengujian terhadap data yang telah ditemukan pada *web* SIASAT UKSW dengan OWASP. Tahap terakhir hasil dari pengujian tersebut dilakukan analisis dan pengambilan kesimpulan. Selanjutnya pada tahap ini juga dilakukan penulisan laporan hasil penelitian berupa artikel ilmiah.

Otomatisasi OWASPZap membantu dalam proses melakukan pengujian dan ditulis seperti pada *flowchart* Gambar 2. Hal pertama yang dilakukan memasukan *URL* target (*web* target), kemudian menjalankan pada terminal. Selanjutnya akan melakukan tahap dimana mesin pencarian menemukan *web* tersebut (*crawling*). Setelah target ditemukan akan melakukan tahap pencarian semua *index* yang terdapat pada web tersebut. Setelah itu dilakukan tahap *scanning* pada *index* tersebut untuk mencari celah keamanan, kemudian setelah tahap *scanning* selesai akan menghasilkan *report*. Selanjutnya dilakukan pengecekan terhadap daftar *URL* target jika semua daftar target selesai dieksekusi maka tahap pengujian sudah selesai.

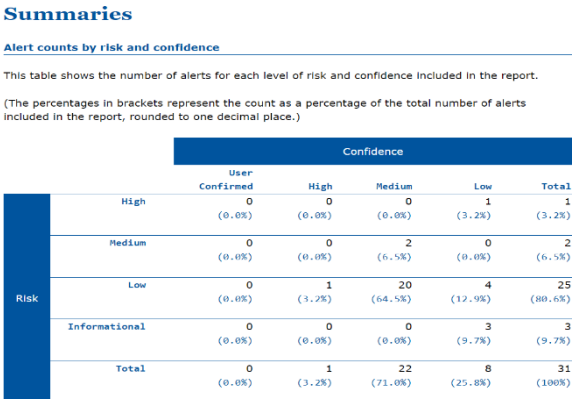


Gambar 2. Flowchart Otomatisasi OWASPZap [10]

4. HASIL DAN PEMBAHASAN

Hasil report yang dikeluarkan aplikasi dalam format .html akan berupa tabel. Tabel paling atas berisikan risk level celah keamanan, jumlah celah yang dapat dideteksi dan tabel berisikan level risk celah, kategori atau nama celah, lokasi celah berada, method, parameter dan juga yang terakhir solusi untuk menghadapi celah keamanan tersebut seperti yang ditunjukan pada Gambar 3, Gambar 4 dan Gambar 5.

Pada tahap awal ini mencari informasi tentang *web* SIASAT yang akan dilakukan uji *pentest*. Dengan menggunakan *search engine* yaitu Google seperti terlihat pada Gambar 6. Kemudian dilakukan cek ping terhadap *web* SIASAT sehingga didapatkan IP yang akan digunakan.



Summaries

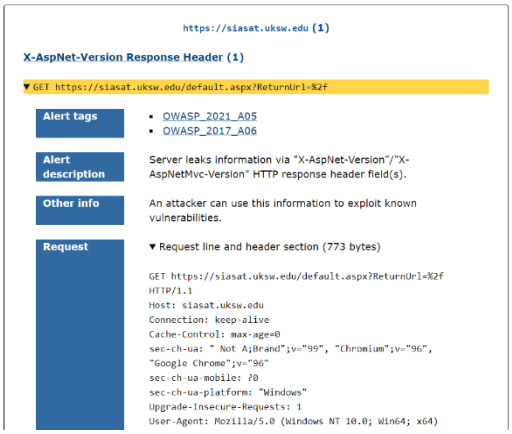
Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (3.2%)	1 (3.2%)
	Medium	0 (0.0%)	0 (0.0%)	2 (6.5%)	0 (0.0%)	2 (6.5%)
	Low	0 (0.0%)	1 (3.2%)	20 (64.5%)	4 (12.9%)	25 (80.6%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 (9.7%)	3 (9.7%)
	Total	0 (0.0%)	1 (3.2%)	22 (71.0%)	8 (25.8%)	31 (100%)

Gambar 3. *Report* Celah Keamanan



https://siasat.uksw.edu (1)

X-AspNet-Version Response Header (1)

▼ GET https://siasat.uksw.edu/default.aspx?ReturnUrl=%2f

Alert tags
- OWASP_2021_A05
- OWASP_2017_A06

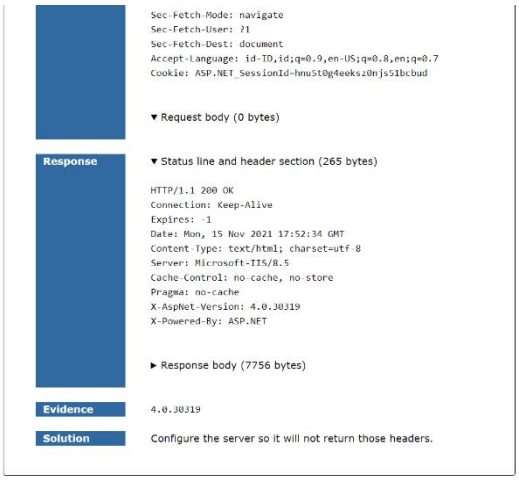
Alert description
Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).

Other info
An attacker can use this information to exploit known vulnerabilities.

Request
▼ Request line and header section (773 bytes)

```
GET https://siasat.uksw.edu/default.aspx?ReturnUrl=%2f
HTTP/1.1
Host: siasat.uksw.edu
Connection: keep-alive
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96",
"Google Chrome";v="96"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

Gambar 4. Detail Report Celah Keamanan



```
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: ASP.NET_SessionId=hnu5t0g4eeksz0njs51bcbud
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (265 bytes)

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Expires: -1
Date: Mon, 15 Nov 2021 17:52:34 GMT
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
Cache-Control: no-cache, no-store
Pragma: no-cache
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

▶ Response body (7756 bytes)

Evidence 4.0.30319

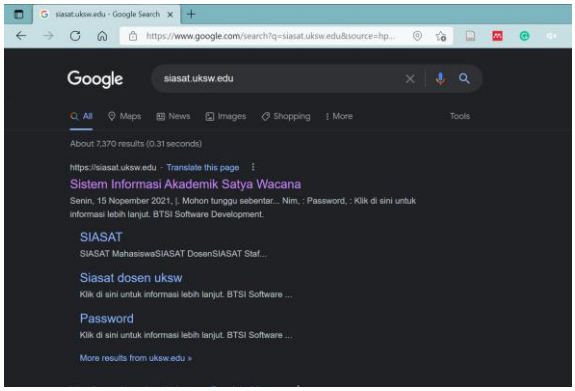
Solution Configure the server so it will not return those headers.

Gambar 5. Solusi Celah Keamanan

Selanjutnya menggunakan *tool* whois terlihat bahwa siasat.uksw.edu memiliki *block IP adders* dari 103.9.183.0 sampai dengan 103.9.183.255. Selain *block* alamat IP juga didapatkan nama, *email* dan kontak pengelola *server*. Dengan menggunakan perintah host didapatkan nama *server* dari UKSW yaitu ariel.uksw.edu seperti Gambar 7.

Dari informasi yang didapatkan tersebut dilanjutkan dengan mencoba melakukan pengujian *Domain Name Server* (DNS) *zone transfer* untuk

seluruh informasi dari siasat.uksw.edu seperti Gambar 8 di bawah ini.



Gambar 6. Hasil Pencarian dengan Google

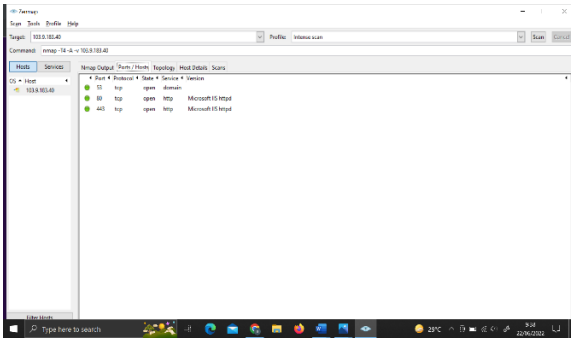
Gambar 7. Hasil Host

Gambar 8. Hasil DNS *Zone Transfer*

DNS zone transfer merupakan proses dimana konten berkas zona DNS disalin dari server DNS utama ke server DNS sekunder sehingga akan didapatkan semua nama domain atau subdomain yang ada pada server DNS utama. Dari hasil DNS zone transfer tidak didapatkan data URL dan IP *Address* dikarenakan kegagalan transfer, sehingga perizinan permintaan transfer pada *DNS server* sudah diseleksi dan dilakukan dengan baik. Lalu dengan perintah host dilakukan pengujian terhadap versi *Berkeley Internet Name Domain* (BIND) yang digunakan. BIND merupakan *server DNS* yang paling umum digunakan. Dari hasil pengujian *BIND server* menjawab permintaan untuk versi BIND yang digunakan. Pengujian selanjutnya menggunakan *tools dnsrecon* menunjukkan hasil seperti pada Gambar 9.

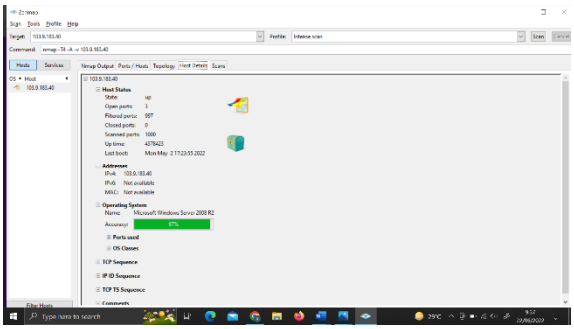
Gambar 9. Hasil Pengujian dengan *dnsrecon*

Tahap selanjutnya adalah melakukan *port scanning* untuk mengetahui port TCP dan UDP apa saja yang ada pada server. Pengujian akan dilakukan dengan *tools* zenmap dengan hasil seperti pada Gambar 10.



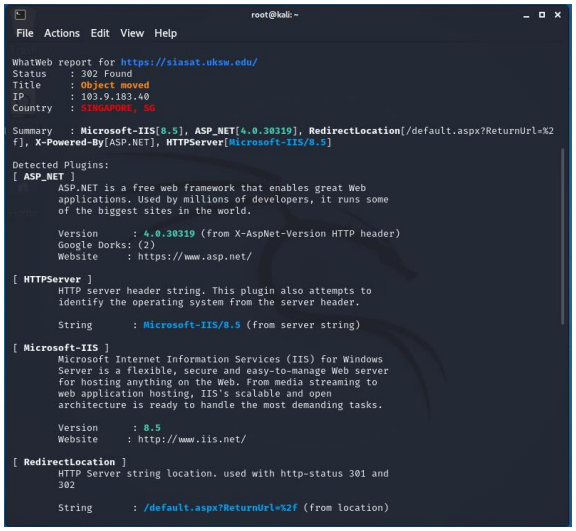
Gambar 10. Hasil *Port Scanning* dengan Zenmap

Tahap selanjutnya akan dilakukan *OS fingerprint* untuk mengetahui jenis sistem operasi yang digunakan pada *server* siasat.uksw.edu. Pengujian *OS fingerprint* akan digunakan *tool* zenmap. Sehingga didapatkan hasil Microsoft Windows Server 2008 R2 dengan tingkat akurasi 97% seperti pada Gambar 11.



Gambar 11. Hasil *Scanning*

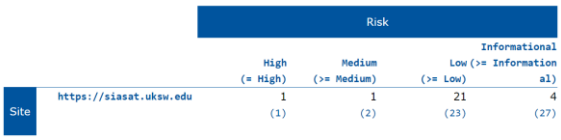
Kemudian untuk mengumpulkan informasi lebih banyak lagi digunakan aplikasi whatweb. Dari hasil whatweb memberikan informasi seperti pada Gambar 12. Hasil dari whatweb menunjukan bahwa HTTP server yang digunakan adalah Microsoft-IIS. Dan pada tahap ini didapatkan informasi penting yang dapat digunakan untuk tahap selanjutnya antara lain *port* dan jenis layanan pada *server*.



Gambar 12. Hasil WhatWeb

Tahap selanjutnya adalah *vulnerability indentification* dimana akan dimulai mencari celah keamanan yang ada pada sistem dan server dari 10 target yang ada berdasarkan informasi yang diperoleh sebelumnya secara manual dan dengan *menggunakan automated vulnerability scanner* yaitu tools otomatisasi OWASPZap yang dikembangkan penulis guna mempermudah dalam melakukan *pencarian vulnerability target*.

Selanjutnya dari hasil *scanning* menggunakan *tools* otomatisasi OWASPZap yang dikembangkan menunjukkan terdapat 27 jenis kemungkinan ancaman dengan 1 kategori memiliki tingkat ancaman High, 1 kategori memiliki tingkat ancaman Medium, 21 kategori lainya memiliki tingkat ancaman Low dan 4 Informational seperti pada Gambar 13 dan jenis-jenis kemungkinan ancaman dari hasil scanning terdapat dalam Tabel 1.



Gambar 13. Hasil *Scanning* OWASPZap

Tabel 1. Kategori Ancaman Hasil *Scanning* OWASP ZAP

Tingkat Ancaman	Jenis Ancaman	Jumlah
HIGH	Viewstate without MAC Signature (Unsure)	1
MEDIUM	X-Frame-Options Header Not Set	1
LOW	Absence of Anti-CSRF Tokens	2
LOW	Cookie Without Secure Flag	1
LOW	Cookie without SameSite Attribute	1
LOW	Incomplete or No Cache-control Header Set	1
LOW	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	6
LOW	X-AspNet-Version Response Header	5
LOW	X-Content-Type-Options Header Missing	5
INFORMATIONAL	Information Disclosure - Suspicious Comments	4

Dari hasil *scanning* yang telah dilakukan pada proses sebelumnya ditemukan bahwa web target terdapat beberapa celah keamanan yang dapat membahayakan keamanan *web* yang dikelola oleh UKSW sehingga perlu segera dilakukan tindakan pencegahan lebih dini dan rata-rata kemungkinan celah keamanan yang ditemukan pada hasil scanning menggunakan aplikasi otomatisasi OWASPZap terdeteksi pada plugin yang terdapat dalam *web*. Kebanyakan plugin belum dilakukan pembaruan oleh pengelola sehingga terdapat *query* tertentu yang terindikasi sebagai celah keamanan oleh aplikasi scanning akan tetapi web target yang memiliki domain siasat.uksw.edu tertolong dengan *firewall* yang dimiliki karena serangan yang dilakukan terhadap celah keamanan yang ditemukan terhalang dan dapat langsung dicegah oleh *firewall*. Dari hasil *scanning* menggunakan otomatisasi OWASPZap juga terdapat *false positive* dimana peringatan keamanan yang ditemukan tidak terbukti atau palsu hal ini terjadi karena aplikasi mendeteksi *query* yang mungkin menjadi ciri-ciri dari sebuah celah keamanan sehingga aplikasi memberikan peringatan. Selain itu juga perlu dilakukan konfigurasi kembali terhadap pengaturan server yang dimiliki web target karena terdapat celah keamanan yang cukup sensitif yang tertampil pada OWASP ZAP. Dari semua proses yang telah dilakukan pada tahap sebelumnya penulis memiliki beberapa rekomendasi sesuai Tabel 2.

Tabel 2. Rekomendasi Mengatasi Celah Keamanan

Celah Keamanan	Solusi
Open DNS Server	Melakukan konfigurasi kembali pada *DNS server* agar mengijinkan IP addres yang sudah ditentukan saja yang dapat melakukan permintaan *zone transfer*.
Sensitive Data Exposure	Melakukan pengamanan dengan melakukan *encryption* pada data penting seperti *user login*.
Directory Browsing	Melakukan *disable directory browsing* dan melakukan pemblokiran dengan menggunakan file htacces.

5. KESIMPULAN

Dari pengujian tersebut disimpulkan hasil *scanning* yang telah dilakukan pada proses sebelumnya ditemukan bahwa web target terdapat beberapa celah keamanan yang dapat membahayakan keamanan *web* yang dikelola oleh UKSW sehingga perlu segera dilakukan tindakan pencegahan lebih dini dan kebanyakan plugin belum dilakukan pembaruan oleh pengelola sehingga terdapat *query* tertentu yang terindikasi sebagai celah keamanan oleh aplikasi *scanning* akan tetapi

web target yang memiliki domain siasat.uksw.edu tertolong dengan *firewall* yang dimiliki karena serangan yang dilakukan terhadap celah keamanan yang ditemukan terhalang dan dapat langsung dicegah oleh *firewall*.

Pengujian penetrasi menggunakan metode OWASP bertujuan untuk menguji tingkat keamanan sistem *web* yang menggunakan domain siasat.uksw.edu yang berasal dari Universitas Kristen Satya Wacana, berdasarkan semua aktivitas yang dilakukan disimpulkan bahwa OWASP 10 Tahun 2021 masih menjadi dasar yang baik untuk menjalankan uji penetrasi pada website dengan domain siasat.uksw.edu, keamanan sistem pada web target dengan domain siasat.uksw.edu belum sesuai dengan prinsip keamanan CIA-TRIAD yaitu kerahasiaan. Hal ini terlihat dalam memanfaatkan celah keamanan yang ada untuk memperoleh informasi penting yang seharusnya memiliki hak akses khusus. siasat.uksw.edu memiliki *firewall* yang cukup bisa diandalkan dalam menanggulangi serangan-serangan yang tidak bertanggung jawab.

Berdasarkan penelitian tersebut ada beberapa saran yaitu semua sistem dengan domain siasat.uksw.edu harus diuji sehingga celah keamanan dapat segera ditangani dan beberapa plugin yang dikelola web perlu diperbaharui secara berkala.

6. UCAPAN TERIMA KASIH

Ucapan terima kasih penulis kepada Universitas Kristen Satya Wacana yang membantu ataupun memberikan dukungan terkait dengan penelitian yang dilakukan.

DAFTAR PUSTAKA

[1] B. E. Widodo and A. S. Purnomo, "IMPLEMENTASI ADVANCED ENCRPYTION STANDARD PADA ENKRIPSI DAN DESKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY," *Jurnal Teknik Informatika (JUTIF)*, vol. 1, pp. 69-77, 2020.

[2] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *Jurnal Komtika (Komputasi dan Infromatika)*, vol. 5, pp. 35-42, 2021.

[3] M. A. Al Hilmi and E. K. , "NETWORK SECURITY MONITORING WITH INTRUSION DETECTION SYSTEM," *Jurnal Teknik Informatika (JUTIF)*, vol. 3, pp. 249-253, 2022.

[4] A. Ramadhani, "KEAMANAN INFORMASI," *JILS (Journal of Information and Library Studies)*, vol. 1, pp. 39-51, 2018.

[5] G. L. Costaner and M. , "ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 05, pp. 45-55, 2020.

[6] PDF Archive Files, 2021. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP_Top_10_-_2010_FINAL_Indonesia_v1.0.1.pdf. [Diakses 22 Juni 2021]

[7] D. Aryanti, N. and J. N. Utamajaya, "ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA," *Jurnal Nasional Indonesia*, vol. 1, pp. 15-25, 2021.

[8] A. Kurniawan, "Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injekasi di Sisi Host-Basec," *Jurnal Telematika*, vol. 14, pp. 9-18.

[9] R. D. Aji, "Evaluasi Risiko Celah Keamanan Menggunakan Metodologi Open Web Application Security Project (OWASP) Pada Aplikasi WEB Sistem Informasi Mahasiswa (STUDI KASUS: Perguruan Tinggi XYZ)," pp. 1-124, 2016.

[10] A. P. Dewanto, "Penetration Testing Pada Domain UII.AC.ID Menggunakan OWASP 10," pp. 1-162, 2018.

[11] F. Hardiansyah and I. M. M.Kom, "Vulnerability Assesment Dan Kajian Aspek Application Security Pada Aplikasi Skripsi Online (SIPSO) FTI PERBANAS," *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)*, pp. 1-9, 2020.

[12] M. Y. "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework OWASP Versi 4," *Jurnal Ilmiah Informatika Komputer Volume 24 No. 1*, pp. 38-48, 2019.

[13] A. M. P. M. T, "Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis WEB," pp. 1-69, 2018.

[14] I. M. E. Listartha, I. M. A. P. Mitha, M. W. A. Arta and I. K. W. Y. Arimika, "ANALISIS KERENTANAN WEBSITE SMA NEGERI 2 AMLAPURA MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT)," *Jurnal Sistem Informasi dan Sistem Komputer*, vol. 7, pp. 23-27, 2022.

[15] B. Ghozali, K. and S. , "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating," *Citec Journal*, vol. 4, pp. 264-275, 2017.

[16] K. H. Dewantara, "Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi Berdasarkan Standar ISO 27001 : 2005 Dan ISO 27002 : 2013 Menggunakan Metode FMEA (Studi Kasus : ISNET)," pp. 1-122, 2016.

[17] E. Chow, 2011. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.475.3877&rep=rep1&type=pdf. [Diakses 14 Juli 2021]

[18] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security (OWASP)," *Jurnal Algoritma*, vol. 19, pp. 77-86, 2021.