Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web

Bella Tasya Kumala Dewi
Program Studi Informatika
Fakultas Tenologi Industri
Universitas Islam Indonesia
Jl. Kaliurang, Sleman, Yogyakarta
18523305@students.uii.ac.id

Mukhammad Andri Setiawan
Program Studi Informatika
Fakultas Tenologi Industri
Universitas Islam Indonesia
Jl. Kaliurang, Sleman, Yogyakarta
andri@uii.ac.id

***Abstrak*— *Website* sebagai salah satu sumber informasi dapat diakses oleh semua orang di seluruh dunia. Namun, tidak semua informasi dapat diakses dan diketahui secara bebas. Oleh karena itu, diperlukan upaya menjaga keamanan informasi untuk menghindari akses dari pihak yang tidak berwenang. Pengujian celah keamanan diperlukan sebagai upaya melindungi *website* dari serangan. Tulisan ini berisi pemaparan studi literatur mengenai metode, tahapan, dan *tools* yang digunakan dalam pengujian celah keamanan *website*. Literatur yang dikumpulkan, dipilih, dan dianalisis merupakan jurnal ilmiah yang memiliki International Standard Serial Number (ISSN) dan diterbitkan sejak tahun 2017 hingga 2021. Literatur dikelompokkan berdasarkan jenis metode yang digunakan dalam menguji celah keamanan *website*. Tujuan dari kajian literatur ini diharapkan memberikan hasil yang dapat dijadikan sebagai acuan dalam menentukan metode dan *tools* yang digunakan untuk pengujian celah keamanan aplikasi berbasis web. Hasil kajian literature ini menunjukkan bahwa sebagian besar penelitian menggunakan metode OWASP serta dalam pengujiannya menerapkan sepuluh daftar kerentanan teratas OWASP. Selain itu, terdapat kesamaan urutan tahapan dalam setiap metode analisis celah keamanan dengan tahap awal yaitu mendapatkan informasi mengenai target yang hendak di uji coba hingga tahap akhir pelaporan pengujian dengan menggunakan kombinasi beberapa *tools*.**

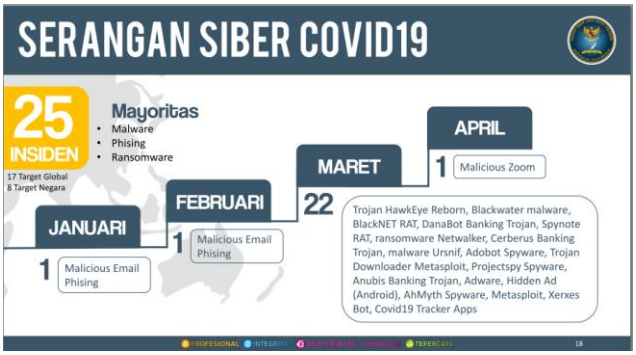
Kata kunci—Keamanan informasi; Website; Pengujian Celah Keamanan

I. PENDAHULUAN

Perkembangan Ilmu Pengetahuan Teknologi dan Komunikasi (IPTEK) semakin pesat pada era sekarang ini. Berbagai macam aktivitas dapat dilakukan melalui media internet. Dengan adanya internet semua orang dapat mengakses informasi tanpa terbatas ruang dan waktu. Salah satu akses informasi dapat diperoleh melalui *website*. *Website* adalah sekumpulan halaman web yang saling berhubungan, dapat diakses oleh semua orang melalui *browser* dan jaringan internet sebagai media membaca dan memperoleh informasi yang berupa gambar, audio, video, teks, atau animasi, tanpa terbatas ruang dan waktu [1].

Selain itu, pada masa pandemi seperti saat ini penggunaan internet semakin meningkat. Hal ini dikarenakan adanya pembatasan aktivitas untuk mengurangi penyebaran kasus *covid-19* sehingga hampir seluruh aktivitas dilakukan dari rumah dan mengandalkan media internet. Namun, angka kejahatan *cyber security* juga ikut meningkat seiring dengan peningkatan penggunaan internet.

Berdasarkan data yang diperoleh dari BSSN (Badan Siber dan Sandi Negara) [2] pada bulan Januari hingga April 2020 terdapat tiga mayoritas serangan selama pandemi *covid-19* diantaranya: *malware*, *phishing*, *ransomware* (Gambar 1).



Gambar 1 Serangan Siber *Covid19* [2]

Melakukan analisis celah keamanan merupakan salah satu bentuk deteksi dini terhadap ancaman di masa mendatang serta untuk menjamin *confidentiality* (kerahasiaan), *integrity* (konsistensi, akurasi, dan validitas data), *availability* (ketersediaan) atau biasa disebut dengan *CIA Triad* yang merupakan komponen dasar keamanan informasi [3]. Celah keamanan dapat dijumpai dalam sebuah sistem maupun jaringan, salah satunya sistem aplikasi berbasis web. Dalam melakukan analisis celah keamanan suatu *website* diperlukan metode pengujian yang memuat kerangka pengujian sesuai standar keamanan yang ada.

II. METODE

Penyusunan langkah-langkah dalam penelitian ini menggunakan metode pendekatan *Systematic Literature Review* untuk menjawab *research question* dengan tahapan meliputi: identifikasi, menilai, dan interpretasi topik penelitian dalam seluruh temuan. Metode ini dipilih karena

penerapannya secara sistematis sesuai dengan tahapan yang membuat proses dalam *literature review* terindar dari pemahaman subyektif.

A. *Pertanyaan Penelitian*

Pertanyaan penelitian ini dijadikan acuan dalam mencari artikel terkait, adapun pertanyaan tersebut meliputi:

- Metode apa yang dapat digunakan dalam pengujian celah keamanan website?
- Tahapan apa saja yang digunakan dalam metode pengujian celah keamanan website?
- Tools apa saja yang digunakan dalam melakukan pengujian celah keamanan website?

B. *Pengumpulan Literatur*

Pengumpulan literatur dilakukan dengan melakukan pencarian terhadap beberapa literatur yang memiliki topik serupa dengan penelitian yaitu membahas tentang metode dalam melakukan pengujian celah keamanan *website*. Pencarian literatur dilakukan melalui *Google Cendekia* menggunakan kata kunci seperti: pengujian celah keamanan, analisis keamanan *website*, standar keamanan *website*, metode dalam analisis celah keamanan *website*, metode *vulnerability scanning*.

C. *Pemilihan Literatur*

Literatur dipilih dan dianalisis sesuai dengan kriteria menggunakan Mendeley pada desktop. Sebanyak 15 literatur terpilih berdasarkan kriteria seperti: kesamaan topik pembahasan yaitu membahas tentang metode pengujian yang digunakan dalam mengidentifikasi celah keamanan *website* dengan tahun penerbitan minimal tahun 2017 dan literatur sudah berstandar internasional yang disertai dengan nomor *ISSN*. 15 literatur tersebut kemudian dikategorikan berdasarkan metode, tahapan, dan *tools* yang digunakan. Literatur yang terpilih dikelompokkan dan dihitung berdasarkan kata kunci yang dicari seperti yang tertuang pada TABEL 1.

TABEL 1. JUMLAH LITERATUR BERDASARKAN KATA KUNCI

Kata kunci	Literatur	Jumlah
Pengujian celah keamanan	[1], [4], [5], [6], [7], [8], [9], [10]	8
Analisis keamanan website	[1], [5], [6], [7], [9], [10], [11], [12], [13]	9
Standar keamanan website	[1], [5], [7], [9], [10], [11], [14], [15],	8
Metode analisis celah keamanan website	[1], [4], [5], [11], [6], [7], [8], [9], [10], [13], [14], [15], [16],	13
Metode *vulnerability scanning*	[1], [4], [5], [6], [7], [10], [15], [16], [17]	9

Berdasarkan tabel di atas dapat dilihat bahwa literatur [1], [5], [7], dan [10] ditemukan pada semua kata kunci yang dicari.

III. HASIL DAN PEMBAHASAN

Hasil dan pembahasan berisi data hasil 15 literatur yang telah dikaji untuk dijadikan sebagai referensi penulis dalam menjawab pertanyaan ilmiah dan memilih metode pengujian untuk menguji celah keamanan *website* dalam penelitian. Setelah dilakukan analisis mendalam pada literature yang terpilih, diperoleh hasil yang menunjukkan bahwa metode *OWASP* lebih sering digunakan dari tujuh metode yang ditemukan. Metode pengujian yang ditemukan penulis untuk menguji celah keamanan website, meliputi:

a. *OWASP* Versi 4 merupakan standar keamanan aplikasi berbasis web dengan sebelas langkah yang dilakukan untuk melakukan pengujian dan menilai keamanan *website* [1], sebelas langkah tersebut berupa: *Information Gathering, Configuration and Deployment Management, Identity Management, Authentication, Authorization, Session Management, Input Validation, Testing for Error Handling, Testing for weak Cryptography, Business Logic,* dan *Client Side Testing* [18]. Sedangkan *OWASP Top* 10 adalah sebuah daftar yang berisikan sepuluh kerentanan teratas yang dapat mengancam *website*, daftar kerentanan ini dirilis oleh komunitas *OWASP* dan dapat berubah seiring dengan perkembangan teknologi [11]. Sepuluh daftar kerentanan tersebut meliputi: *Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XEE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring* [4].

b. *ISSAF (Information System Security Assessment Framework)* merupakan sebuah metode untuk melakukan evaluasi keamanan pada sebuah jaringan komputer, sistem, maupun suatu aplikasi [12]. Metode *ISSAF* memiliki 9 langkah penilaian [1] yang terdiri dari 3 fase pengujian yang meliputi: 1) persiapan dan perancangan, 2) pengujian, 3) pelaporan dan pembersihan jejak serangan [5].

c. *OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)* adalah sebuah kerangka kerja yang digunakan untuk melakukan identifikasi, analisis, pengawasan, serta mengelola risiko berdasarkan pengidentifikasian risiko keamanan yang dilakukan [14].

d. *PTES (Penetration Testing Execution Standard)* yang dikembangkan oleh *Pentest Organisation* merupakan sebuah metode yang digunakan sebagai standar dalam melakukan analisis dan audit keamanan sebuah sistem [15].

e. *DREAD (Damage Potential, Reproducibility, Exploitability, Affected User, Discoverability)* adalah suatu teknik yang berupa kerangka kerja dalam melakukan identifikasi dan analisis kerentanan suatu *website*. DREAD dapat digunakan untuk melakukan perhitungan risiko berupa informasi peringkat pada suatu ancaman [16].

f. *Ethical Hacking* merupakan metode yang digunakan dalam teknik *hacking* menggunakan sebuah aplikasi dan langkah-langkah dalam melakukan identifikasi

kerentanan suatu sistem untuk menganalisis keamanannya [6].

g. *Vulnerability Assessment* merupakan sebuah metode dalam penetration testing yang berfokus dalam penilaian kerentanan suatu sistem [7].

Beberapa jenis metode pengujian celah keamanan yang ditemukan di atas dikelompokkan berdasarkan tahun yang disajikan dengan TABEL 2.

TABEL 2. METODE PENGUJIAN YANG DILAKUKAN BERDASARKAN TAHUN

Tahun	Metode						
	OWASP	***ISSAF***	***OCTAVE***	***PTES***	***DREAD***	***Ethnical Hacking***	***Vulnerability Assessment***
2017			[14]		[16]		
2018							[13]
2019	[8]						
2020	[1]	[1], [5]		[9]		[6]	[7]
2021	[4], [11]	[12]	[17]	[15], [10]			

Berdasarkan hasil pengelompokkan di atas dapat disimpulkan bahwa pengujian celah keamanan menggunakan metode *OWASP* lebih banyak digunakan. Pengelompokan lebih lanjut pada literature yang terpilih dilakukan berdasarkan tahapan dan *tools* yang digunakan pada setiap metode pengujian. Metode *OWASP* yang ditemukan pada empat literatur memiliki dua jenis yaitu *OWASP Top 10* dan *OWASP* Versi 4. Pengelompokkan pada metode *OWASP Top 10* dikategorikan berdasarkan tahapan dan *tools* yang digunakan seperti TABEL 3.

TABEL 3. TAHAPAN DAN TOOLS PENGUJIAN MENGGUNAKAN METODE OWASP TOP 10

Tahapan	Tools	
	OWASP ZAP	Tidak disebutkan
Injection	[11]	[4]
Broken Authentication	[11]	[4]
Sensitive Data Exposure	[11]	[4]
XML External Entities (XXE)	[11]	[4]
Broken Access Control	[11]	[4]
Security Misconfiguration	[11]	[4]
Cross-Site Scripting (XSS)	[11]	[4]
Insecure Deserialization	[11]	[4]
Using Components with Known Vulnerabilities	[11]	[4]
Insufficient Logging &Monitoring	[11]	[4]

Temuan yang penulis dapatkan dari literatur yang menggunakan metode OWASP Top 10 dalam analisis celah keamanan website menunjukkkan bahwa tahapan yang digunakan pada kedua literature memiliki kesamaan seperti yang tertuang pada TABEL 3. Namun, dapat dilihat bahwa pada salah satu literatur tidak menjelaskan tools yang digunakan dalam pengujian.

Berdasarkan penelitian menggunakan metode *OWASP Top 10* 2017 yang dilakukan oleh S. Hidayatulloh dan D. Saptadiaji [4] dengan *tools Whois, Host, theHarvester, Ping, Whatweb, Nmap, Uniscan, Nikto* dan tahapan yang dilakukan meliputi: *Scanning and Discovery, Attack*, dan *Reporting* diperoleh kesimpulan bahwa berdasarkan aspek *CIA TRIAD (confidentiality, integrity,* dan *availability)* telah terpenuhi sehingga keamanan pada *website* target tergolong baik.

Menurut A. Elanda dan R. L. Buana [11] dalam penelitiannya menggunakan metode OWASP Top 10 dengan tahapan pengujian meliputi: Identifikasi Kerentanan, Penetrasi *OWASP ZAP*, Penetrasi *OWASP ZAP* Berdasarkan *OWASP TOP 10*, Rekomendasi. *Tools* yang digunakan yaitu *OWASP ZAP* dan *Acunetix*, didapatkan kesimpulan bahwa target memiliki tingkat kerentanan sedang berdasarkan pengujian yang dilakukan menggunakan *OWASP ZAP* mendeteksi 13 kerentanan dan 4 kerentanan berdasarkan *OWASP Top 10* yang meliputi: *Sensitive Data Exposure, Security Misconfiguration, Cross Site Scripting, dan Insecure Deserialization.*

Penulis menemukan temuan bahwa metode *OWASP* Versi 4 terdiri dari 11 tahapan pengujian atau biasa disebut dengan *WSTG (Web Security Testing Guide)*, tahapan tersebut meliputi: *Information Gathering, Configuration and Deployment Management, Identity Management, Authentication, Authorization, Session Management, Input Validation, Testing for Error Handling, Testing for weak Cryptography, Business Logic*, dan *Client Side Testing.* Namun, pada kedua literature tidak menerapkan semua tahapan sehingga penulis mengelompokkan sesuai dengan tahapan dan *tools* yang digunakan pada kedua literatur seperti pada TABEL 4.

TABEL 4. TAHAPAN DAN TOOLS PENGUJIAN MENGGUNAKAN METODE OWASP VERSI 4

Tools	Tahapan				
	A1	**A2**	**A3**	**A4**	**A5**
OWASP ZAP	[8]	[8]	[1], [8]	[8]	[8]
Mozilla Firefox	[8]	[8]	[1], [8]	[8]	[8]
Google Chrome	[1]	[1]	[8]	[8]	
Netsparker	[8]	[8]	[8]	[8]	[8]
HAVIJ 1.15				[8]	
Brutus	[1]				

Tools	Tahapan				
	A1	A2	A3	A4	A5
WebScarab	[1]	[1]			
WFuzz		[1]			
Dirb		[1]	[1]		
OWASP CSRF Tester			[1]		

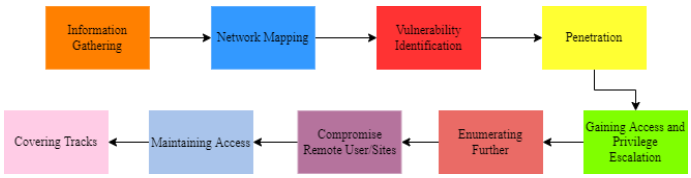
Keterangan:
A1: *Authentication*
A2: *Authorization*
A3*: Session Management*
A4: *Input Validation*
A5: *Testing for Error Handling*

Berdasarkan TABEL 4. dapat dilihat bahwa Kedua literatur menerapkan tahapan serupa yaitu *authentication testing, authorization testing,* dan *session management testing*. Namun, kedua literature ini tidak menerapkan semua tahapan yang dirilis oleh *OWASP* mengenai *WSTG* atau *OWASP* versi 4, hal ini mungkin terjadi karena kebutuhan yang diperlukan setiap *website* berbeda sehingga pengujian hanya menerapkan tahapan yang sesuai dengan yang diperlukan setiap *website*.

Berdasarkan penelitian terdahulu yang dilakukan oleh G. Guntoro, L. Costaner, dan M. Musfawati [1]. diperoleh hasil berdasarkan pengujiannya menggunakan standar pengujian *OWASP* versi 4 dengan *tools google chrome, brutus, webscarab, wfuzz, dirb, OWASP ZAP, OWASP CSRF Tester, Mozilla firefox* dan fokus penelitian *Authentication Testing, Authorization Testing, dan Session Management Testing* menunjukkan bahwa web *server* yang diuji coba tergolong aman, namun terdapat kelemahan pada *login* sistem tidak dapat dilakukan pemblokiran ketika *user* melakukan kesalahan berulang.

Menurut M. Yunus [8] dalam pengujiannya menggunakan *OWASP* versi 4 dengan *tools Mozilla Firefox, Netsparker, OWASP ZAP, Google Chrome, HAVIJ 1.15* dengan fokus pengujian *Authentication Testing, Authorization Testing, Session Management Testing, Input Validation Testing*, dan *Error Handling* menggunakan kombinasi *security tools project* diperoleh kesimpulan bahwa untuk melakukan analisis kerentanan dan keamanan aplikasi berbasis web dapat menggunakan metode *OWASP* versi 4 sebagai standar penilaian.

Sebagaimana pengelompokan dengan kategori tahapan dan *tools* pada metode *OWASP*, dilakukan juga pengelompokkan pada metode *ISSAF* dalam tiga literatur yang berbeda dengan kategori tahapan dan *tools* yang digunakan. Tahapan yang digunakan dalam metode *ISSAF* tertuang pada Gambar 2.



Gambar 2 Tahapan pengujian metode *ISSAF*

Berdasarkan Gambar 2 di atas dapat dilihat tahapan yang digunakan pada metode *ISSAF* meliputi: *Information gathering* yaitu tahapan yang dilakukan untuk mengumpulkan informasi umum mengenai target. Tahapan kedua *network mapping* merupakan tahap pengumpulan informasi target yang lebih spesifik secara spesifik. Tahap ketiga *vulnerability identification* merupakan tahap identifikasi kerentanan dapat berupa *scanning* pada *website* target. Keempat adalah tahap *penetration* yang digunakan untuk mendapatkan celah keamanan target dengan cara mensimulasikan suatu serangan. Tahap kelima *gaining access and privilege escalation* merupakan pengujian dengan cara mencoba akses masuk dalam sistem target. Tahap keenam *enumerating further* dilakukan dengan mengambil dan memecahkan informasi *password* yang diperoleh dari target. Tahap ketujuh *compromise remote user/sites* adalah tahap pengujian yang dilakukan dengan cara mengeksploitasi akses *user root* pada *website* melalui *remote* atau berjarak. Tahap berikutnya *maintaining access* merupakan tahapan penanaman *backdoor*, dapat dilakukan dengan memanfaatkan fitur *file upload* pada suatu sistem target. Tahapan terakhir yaitu *covering tracks* yang dilakukan dengan cara menghapus log *attack* yang sudah dilakukan pada *website* target [5].

Dari tahapan di atas digunakan beberapa *tools* yang dipetakan berdasarkan penelitian di setiap literatur seperti pada TABEL 5.

TABEL 5. TAHAPAN DAN TOOLS PENGUJIAN MENGGUNAKAN METODE ISSAF

Tools	Tahapan								
	A	B	C	D	E	F	G	H	I
Whois	[1], [5], [12]								
SSL Scan	[1], [12]								
Acunetix			[1], [12]						
Zenmap		[1]							
Low Orbit Ion Canon				[1]					
SQL Map				[1], [12]					
IP lookup Scanner	[5]								
Nmap		[5], [12]							
Vega			[5]		[5]	[5]			
OWASP ZAP					[5]				
LOIC				[12]					
Web Site Analysis					[5]				
Tanpa *tools*				[5]	[5]	[5]	[5]	[5]	[5]

Keterangan:
A: *Information Gathering*
B: *Network Mapping*

C: *Vulnerability Identification*
D: *Penetration*
E: *Gaining Access and Privilege Escalation*
F: *Enumerating Further*
G: *Compromise Remote User/Sites*
H: *Maintaining Access*
I: *Covering Tracks*

Berdasarkan TABEL 5. dapat dilihat bahwa dari tiga literatur yang menggunakan metode *ISSAF* menerapkan tahapan pengujian yang meliputi: *Information Gathering*, *Network Mapping*, *Vulnerability Identification*, dan *Penetration.* Ketiga literatur menggunakan *tools Whois* pada tahap *Information Gathering.* Dari studi literatur terhadap tiga literatur yang menerapkan metode *ISSAF* penulis menemukan hanya satu literatur yang menerapkan semua tahapan secara lengkap, sedangkan dua literatur lainnya hanya menerapkan tahap *Information Gathering*, *Network Mapping*, *Vulnerability Identification*, dan *Penetration.*

Menurut G. Guntoro, L. Costaner, and M. Musfawati [1] dalam pengujiannya menggunakan metode *ISSAF* dengan empat tahap, meliputi: *Information Gathering* dengan *tools Whois* dan *SSL Scan*, *Network Mapping* dengan *tools Zenmap*, *Vulnerability Identification* dengan *tools Acunetix, Penetration* dengan *tools Low Orbit Ion Canon dan SQLMap,* diperoleh kesimpulan bahwa *website* target tergolong aman, namun terdapat kerentanan terhadap serangan *DoS* pada web *server*.

Menurut I. G. A. S. Sanjaya [5] tahapan dan *tools* yang digunakan dalam pengujiannya menggunakan metode *ISSAF* meliputi: *Information Gathering* dengan *tools Whois* dan *IP lookup Scanner*, *Network Mapping* dengan *tools Nmap*, *Vulnerability Identification* dengan *tools Vega*, *Penetration* dengan *manual test, Gaining Access and Privilege Escalation* dengan *tools manual test, Vega, OWASP ZAP, dan Web Site Analysis, Enumerating Further* dengan *tools Vega dan manual test, Compromise Remote User/Sites* dengan *manual test, Maintaining Access* dengan *manual test, Covering Tracks* dengan *manual test.* Kesimpulan yang diperoleh yaitu ditemukan celah keamanan terhadap *SQL Injection* dan *XSS*, serta adanya risiko serangan dan *bug* pada sistem karena terdapat *port TCP* yang terbuka.

Menurut penelitian yang dilakukan Stefanus Eko Prasetyo dan Nurul Hassanah [12] menggunakan metode *ISSAF* dengan tahapan dan *tools* yang digunakan sebagai berikut: *Information Gathering* menggunakan *tools Whois* dan *SSL Scan*, *Network Mapping* menggunakan *tools Nmap*, *Vulnerability Identification* menggunakan *tools Acunetix*, *Penetration* menggunakan *OS Kali Linux* dengan *tools LOIC* dan *SQLMap* diperoleh kesimpulan bahwa *website* target tergolong aman, namun rentan terhadap serangan *DDOS* yang mengakibatkan *down* sementara pada server.

Selain metode *ISSAF* pengelompokkan juga dilakukan berdasarkan metode *PTES* dengan kategori serupa yaitu tahapan pengujian dan *tools* yang digunakan. Tahapan yang digunakan dalam metode *PTES* tertuang dalam Gambar 3 berikut:

Gambar 3 Tahapan pengujian metode *PTES*

Gambar di atas merupakan tahapan yang digunakan dalam metode *PTES*, yang dimulai dari *Pre-Engagement Interaction* dengan tujuan untuk mempersiapkan teknik yang akan digunakan dan *tools* yang dibutuhkan. Tahap kedua *Intelligence Gathering* merupakan tahapan pengumpulan informasi umum mengenai target yang akan dilakukan uji penetrasi. *Threat Modelling* merupakan sebuah teknik dalam melakukan pemodelan ancaman yang diperlukan dalam pengujian penetrasi. *Vulnerability Analysis* adalah proses pengujian celah keamanan yang digunakan untuk menemukan kerentanan suatu sistem. *Exploitation* merupakan fase pengujian penetrasi yang bertujuan melewati batasan keamanan dengan memaksa untuk mengakses sistem maupun sumber daya. *Post Exploitation* merupakan proses menentukan nilai kerentanan sistem dengan tujuan agar sistem dapat mempertahankan kontrol. *Reporting* merupakan langkah pembuatan sebuah laporan yang berisi hasil pengujian secara lengkap [10]. Tahapan penelitian metode *PTES* di atas disebutkan dan digunakan oleh beberapa literatur dalam penelitiannya, seperti yang tertera pada TABEL 6.

TABEL 6. TAHAPAN DAN TOOLS PENGUJIAN MENGGUNAKAN METODE PTES

Tools	**Tahapan**						
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**
Whois		[9], [15], [10]					
Nmap		[9], [15]					
Acunetix				[15], [10]			
Zenmap		[10]					
Kali Linux					[15], [10]		
Google							
theHarvester		[9]					
Nesus VS				[9]			
Pentest-tools.com				[9]	[9]		
OWASP ZAP				[9]	[9]		
Wireshark					[9]		
SQLMap					[9], [10]		
Tanpa *tools*	[9], [15], [10]		[9], [15]			[9], [15]	[9], [15], [10]

Keterangan:
P1: *Pre-Engagement Interaction*
P2: *Intelligence Gathering*
P3: *Threat Modelling*
P4: *Vulnerability Analysis*
P5: *Exploitation*
P6: *Post Exploitation*
P7: *Reporting*

Berdasarkan tabel di atas dapat dilihat bahwa pengujian menggunakan metode *PTES* dengan tiga literatur yang berbeda menggunakan *tools Whois* pada tahap *Intelligence Gathering*. Dari ketiga literatur yang menggunakan metode pengujian *PTES* penulis menemukan temuan berupa hampir seluruh literatur menerapkan semua tahapan yang digunakan dalam metode *PTES*, seperti halnya penelitian yang dilakukan oleh F. Y. Fauzan dan S. Syukhri [10] tidak semua tahapan diterapkan, terdapat dua tahapan yang tidak dilakukan yaitu tahap *threat model* dan *post explanation*.

Menurut penelitian yang dilakukan F. Y. Fauzan dan S. Syukhri [10] menggunakan metode PTES dengan dan tahapan meliputi: *Pre-Engagement Interaction, Intelligence Gathering, Vulnerability Analysis, Exploitation,* dan *Reporting* dengan Sistem Operasi *Kali Linux* dan *tools Whois, Acunetix, Zenmap, SQLMap*. Kesimpulan yang diperoleh dari pengujian menggunakan metode *PTES* ini yaitu ditemukan celah keamanan dengan kategori *medium* pada *website* target dan kegagalan pada pengujian *SQL injection* dikarenakan *website* target telah menggunakan *SSL (Secure Socket Layer).*

Berdasarkan pengujian yang dilakukan oleh S. Utoro, B. A. Nugroho, M. Meinawati, dan S. R. Widianto [9] menggunakan metode *PTES* dengan tahapan *Pre-Engagment Interaction, Intelligence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting*. *Tools* yang digunakan meliputi: Sistem operasi *KALI Linux, TheHarvester, Nessus Vulnerability Scanner, NMAP (Network Mapper), WHOIS, Wireshark,* dan *OWASP Zed Attack Proxy (ZAP)* diperoleh kesimpulan berdasarkan pengujian yang dilakukan bahwa metode *PTES* dapat digunakan sebagai standar penilaian dalam analisis celah keamanan *website*, serta risiko keamanan yang ditemukan pada *website* target berupa *Cross Site Scripting, Cross Site Request Forgery* dan *Eavesdropping*.

Menurut Yosua Ade Pohan, Yuhandri Yunus, dan Sumijan [15] dalam penelitiannya menggunakan metode *PTES* dengan tahapan yang meliputi: *Pre-Engagement Interaction, Intelligence Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting*. Kesimpulan yang diperoleh dari pengujian menggunakan Sistem Operasi *Kali Linux* dan *tools Whois, Nmap, Acunetix* yaitu metode *PTES* dapat digunakan dalam pengujian terhadap *website* target, kategori celah keamanan yang semula sedang dengan tujuh jenis kerentanan dapat diturunkan menjadi rendah dengan satu jenis kerentanan.

Sama halnya dengan pengelompokkan pada pengujian yang menggunakan metode *PTES*, dua literatur yang menggunakan metode *Vulnerability Assessment* juga dikelompokkan berdasarkan tahapan dan *tools* yang digunakan seperti yang tertuang pada TABEL 7.

TABEL 7. TAHAPAN DAN TOOLS PENGUJIAN MENGGUNAKAN METODE VULNERABILITY ASSESSMENT

Tools	Tahapan							
	T1	T2	T3	T4	T5	T6	T7	T8
Whois	[7]							
Nslookup	[7]							
Central OPS	[7]							
Nmap	[7]							
Http Recon	[7]							
OWASP ZAP		[7]						
Wpscan							[13]	
Metasploit-Framework							[13]	
THC-Hydra							[13]	
Slowloris							[13]	
Webscarab							[13]	
Exploit wp_find_password							[13]	
Tanpa *tools*			[7]	[7]	[13]	[13]		[13]

Keterangan:
T1: *Footprinting and Network Discover*
T2: *Scanning Vulnerability*
T3: *Reporting Analysis*
T4: *Countermeasure*
T5: *Asset Identification*
T6: *Asset Value*
T7: *Vulnerability Identification*
T8: *Mitigation*

Berdasarkan tabel di atas penulis menemukan bahwa kedua literatur dengan metode yang sama yaitu metode *Vulnerability Assessment* memiliki tahapan dan *tools* yang berbeda. Namun, memiliki tujuan yang sama yaitu untuk melakukan pengujian celah keamanan terhadap *website*.

Menurut pengujian yang dilakukan A. M. Tania, D. Setiyadi, dan F. N. Khasanah [13] menggunakan metode *Vulnerability Assessment* dengan empat tahapan meliputi: *Asset Identification, Asset Value, Vulnerability Identification, Mitigation.* Tahap *Vulnerability Identification* menggunakan *tools* yang terdapat pada Sistem Operasi *Kali Linux*, meliputi: *Wpscan, Metasploit-Framework, THC-Hydra, Slowloris, Webscarab, Exploit wp_find_password.* Kesimpulan yang diperoleh dalam penelitian ini yaitu terdapat dua kategori pengujian yang berstatus tidak aman, serta dapat dilakukan pengembangan penelitian menggunakan metode *Hacking Methodology*.

Menurut I. Riadi dan A. Y. Y. W [7] dalam pengujiannya menggunakan *Vulnerability Assessment* dengan tahapan pengujian yang meliputi: *Footprinting and Network Discover, Scanning, Reporting Analysis, Countermeasure*, memakai *tools Whois, Nslookup, Central OPS, Nmap, Http Recon, OWASP ZAP*. Diperoleh kesimpulan bahwa *tools OWASP* dapat

menguji celah keamanan *website* target dengan total celah yang ditemukan sebanyak 6049 sehingga *website* tersebut direkomendasikan untuk tidak digunakan.

Adapun metode *OCTAVE* tidak dilakukan pengelompokkan dikarenakan tidak adanya kategori yang dapat dikelompokkan berdasarkan kedua literatur. Berdasarkan penelitian yang dilakukan N. Nelmiawati, F. R. Destrianto, dan M. A. R. Sitorus [14] dalam manajemen risiko ancaman *website* menggunakan metode *OCTAVE* dengan proses pengujian meliputi: *Secure Transmission, Authentication, Session Management, Cryptography, Data Validation, Denial of Service, Specific Risk of Functionality, Configuration Management*, dan *Error Handling* diperoleh kesimpulan bahwa metode *OCTAVE* dapat dijadikan panduan yang sistematik dalam manajemen risiko, terdapat tujuh jenis ancaman pada *website* target yaitu: s*niffing, cookie replay, cracking, session hijacking, session replay, man-in-the-middle,* dan *clickjacking*.

Berdasarkan R. Ichsan, A. Falach, L. Abdurrahman, I. Santoso, dan S. Si [17] dalam melakukan analisis risiko dan perancangan kontrol keamanan menggunakan metode *OCTAVE Allegro* dengan delapan tahapan pengujian, meliputi: Membangun Kriteria Pengukuran Risiko, Mengembangkan Profil Aset Informasi, Mengidentifikasi Kontainer dari Aset Informasi, Mengidentifikasi *Area of Concern*, Mengidentifikasi Skenario Ancaman, Mengidentifikasi Risiko, Menganalisis Risiko, Memilih Pendekatan Mitigasi. Kesimpulan yang diperoleh bahwa terdapat dua jenis penanganan terhadap *website* target yaitu *mitigate* dan *defer*. Risiko yang diberikan memiliki dampak besar sehingga direkomendasikan untuk melakukan kontrol agar mengurangi dampak yang muncul.

Sama halnya dengan metode *OCTAVE*, metode *DREAD* dan *Ethical Hacking* tidak dilakukan pengelompokkan dikarenakan pada kajian literatur ini hanya terdapat satu literatur yang menggunakan metode tersebut. Menurut A. Saputra, N. Nelmiawati, dan M. A. R. Sitorus [16] dalam penelitiannya menggunakan metode *DREAD* untuk menilai ancaman suatu *website* dengan proses pengujian yang meliputi: *Secure Transmission, Authentication, Session Management, Cryptography, Data Validation, Denial of Service, Specific Risk of Functionality, Error Handling*. Kesimpulan yang diperoleh dalam pengujian ini bahwa *website* target memiliki kerentanan berupa: akun pengguna dapat ditebak, *dictionary attack, cookie replay attack, sniffing, unencrypted login request, session hijacking, session replay*, dan akun pengguna dapat diambil alih. Selain itu, metode *DREAD* dapat memberikan informasi berupa nilai dari jenis kerentanan.

Menurut penelitian yang dilakukan E. I. Alwi, H. Herdianti, dan F. Umar [6] dalam analisis keamanan suatu *website* menggunakan metode *Ethical hacking* dengan tahapan yang meliputi: 1) *Footprinting & Information Gathering* menggunakan *tools Google, Ping, Nmap-Zenmap, Whois.* 2) *Vulnerability Scanning* menggunakan *tools Pentest-tools.com, Acunetix, OWASP ZAP*. 3) *Vulnerability Analysis. 4) Report.* Dalam pengujian menggunakan metode ini diperoleh kesimpulan berupa ditemukan celah keamanan *CORS (Cross-Origin Resource Sharing) origin validation failure* pada *website* target dengan kategori level tinggi, X-*Frame-Options Header Not Set* dengan level sedang, *Directory listing is enabled* dengan level sedang, *HTML form without CSRF protection* dengan level sedang, *WordPress username enumeration* dengan level sedang, dan *Cookie No HttpOnly Flag* dengan level rendah.

Setelah dilakukan analisis mendalam berdasarkan pengelompokan metode sesuai dengan tahapan dan *tools* yang digunakan penulis mendapatkan bahwa metode *OWASP* dinilai lebih lengkap, hal ini terlihat dari langkah-langkah yang tertuang pada dokumen pengujian aplikasi berbasis web *(WSTG).* Dokumen *WSTG (Web Security Testing Guide)* yang dirilis oleh OWASP ini berisikan langkah pengujian secara detail sesuai dengan kebutuhan *website* yang disertai dengan *tools* yang dapat digunakan di setiap pengujian yang dilakukan. Selain itu, *OWASP* juga dilengkapi dengan daftar kerentanan teratas yang diperbaharui secara berkala mengikuti perubahan teknologi.

IV. KESIMPULAN

Berdasarkan studi literatur yang telah dilakukan, penulis memperoleh temuan bahwa metode pengujian celah keamanan *website* yang sering digunakan dalam analisis kerentanan adalah *OWASP*. Sebagian besar penelitian menggunakan sepuluh daftar kerentanan teratas *OWASP*. Hampir seluruh metode menggunakan *tools Whois* dalam pengujian celah keamanan. Terdapat tahapan pengujian yang berbeda pada metode yang sama. Namun, memiliki tujuan yang sama dalam melakukan analisis celah keamanan. Berdasarkan data dari seluruh literatur dapat disimpulkan bahwa urutan tahapan dalam analisis celah keamanan memiliki kesamaan dari tahap awal yaitu mendapatkan informasi mengenai target yang hendak di uji coba hingga tahap akhir pelaporan pengujian. Kajian literatur ini belum membahas mengenai *framework CWE/SANS* yang berisi 25 daftar kerentanan teratas serta metode lain dalam melakukan analisis celah keamanan suatu *website* sehingga sebagai saran dapat dilakukan kajian literatur mengenai analisis celah keamanan menggunakan *framework CWE/SANS Top* 25 dan penggunaan metode *penetration testing* yang lainnya.

DAFTAR PUSTAKA

[1] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.

[2] Victor Tobing, "Rekapitulasi Insiden Web Defacement," *Badan Siber dan Sandi Negara*, vol. Juni 2020, no. Maret, pp. 1–27, 2020, [Online]. Available: https://bssn.go.id/rekap-serangan-siber-januari-april-2020.

[3] W. Abidian and M. A. Setiawan, "Implementasi Splunk dalam Membangun Security Information and Event Management Berdasarkan Log Firewall (studi kasus : Jaringan UII)," 2020.

[4] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[5] I. G. A. S. Sanjaya, "Evaluasi Keamanan Website Lembaga X

Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati*, vol. 8, no. 2, pp. 113–124, 2020.

[6] E. I. Alwi, H. Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *INFORMAL Informatics J.*, vol. 5, no. 2, p. 43, 2020, doi: 10.19184/isj.v5i2.18941.

[7] I. Riadi and A. Y. Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Security Analysis Open Journal System Website Using," vol. 7, no. 4, pp. 853–860, 2020, doi: 10.25126/jtiik.202071928.

[8] M. Yunus, "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4," *J. Ilm. Inform. Komput.*, vol. 24, no. 1, pp. 37–48, 2019, doi: 10.35760/ik.2019.v24i1.1988.

[9] S. Utoro, B. A. Nugroho, M. Meinawati, and S. R. Widianto, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," *Multinetics*, vol. 6, no. 2, pp. 169–178, 2020, doi: 10.32722/multinetics.v6i2.3432.

[10] F. Y. Fauzan and S. Syukhri, "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang," *Voteteknika (Vocational Tek. Elektron. dan Inform.*, vol. 9, no. 2, p. 105, 2021, doi: 10.24036/voteteknika.v9i2.111778.

[11] A. Elanda and R. L. Buana, "ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10," vol. 6, no. 2, pp. 37–43, 2021.

[12] U. I. Batam *et al.*, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF," 2021.

[13] A. M. Tania, D. Setiyadi, and F. N. Khasanah, "Keamanan Website Menggunakan Vulnerability Assessment," *Keamanan Website Menggunakan Vulnerability Assess.*, vol. 2, no. 2, pp. 171–180, 2018.

[14] N. Nelmiawati, F. R. Destrianto, and M. A. R. Sitorus, "Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE," *J. Integr.*, vol. 9, no. 1, p. 35, 2017, doi: 10.30871/ji.v9i1.284.

[15] Y. A. Pohan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *J. Sistim Inf. dan Teknol.*, vol. 3, pp. 1–6, 2021, doi: 10.37034/jsisfotek.v3i1.36.

[16] A. Saputra, N. Nelmiawati, and M. A. R. Sitorus, "Penilaian Ancaman pada Website Transkrip Aktifitas Mahasiswa Politeknik Negeri Batam Menggunakan Metode DREAD," *J. Integr.*, vol. 9, no. 1, p. 53, 2017, doi: 10.30871/ji.v9i1.281.

[17] R. Ichsan, A. Falach, L. Abdurrahman, I. Santoso, and S. Si, "Octave Allegro Risk Analysis and Information Security Control Design in Hospital Management Information System Billing Module Using Octave Allegro," vol. 8, no. 2, pp. 2709–2722, 2021.

[18] OWASP, "4.0 Testing Guide," *OWASP Found.*, no. Cc, p. 224, 2014, [Online]. Available: https://www.owasp.org/images/1/19/OTGv4.pdf.