BAB II. TINJAUAN PUSTAKA

Dengan melakukan pengujian kerentanan menggunakan metode ISSAF, keamanan informasi pada *website* SIKMA Universitas Atma Jaya Yogyakarta dapat diketahui. Serangan-serangan yang dapat merusak sistem dan mengambil informasi dapat diatasi sehingga *website* dapat menjadi lebih aman. Selain itu, dengan menggunakan metode ISSAF dapat membantu keamanan web tanpa membahayakan web tersebut.

Fahmi Fachri, Abdul Fadlil dan Imam Riadi pada tahun 2021 melakukan analisa terhadap sistem keamanan *webserver* menggunakan metode *penetration test* atau pentest. Pengujian tersebut dilakukan dengan harapan agar dapat megetahui kerentanan atau kelemahan yang dimiliki oleh sistem keamanan *webserver* perguruan tinggi agar dapat menghindari serangan *hack* yang dapat dilakukan oleh oknum yang tidak bertanggung jawab. Peneliti menggunakan beberapa teknik pengujian *penetration test* seperti *information gathering, vulnerability assessment, gaining access, maintaining access* dan *clearing tracks* dengan menggunakan beberapa alat seperti Vega, Netparker dan WHOIS. Kesimpulan dari penelitian tersebut adalah terdapat kelemahan pada Sistem Informasi Akademi target, kelemahan tersebut terbagi menjadi tiga kategori yaitu level high, medium dan low dan simulasi serangan berhasil menemukan username dan password sehingga dapat masuk kedalam sistem [1].

Agus Rochman, Rizal Rohian Salam dan Sandi Agus Maulana pada tahun 2021 melakukan pengujian celah keamanan pada *website* sistem untuk mengetahui celah-celah keamanan pada *website* tersebut. Penulis menggunakan dua *framework* pada penelitian ini yaitu ISSAF *(Information System Security Assessment Framework)* dan OWASP (*Open Web Application Security Project*). Pada *framework* ISSAF terdapat beberapa langkah yaitu *fase planning and preparation, fase assessment* dan *fase clean up and destroy artefacts* sedangkan pada *framework* OWASP memiliki langkah *footprinting, scanning fingerprinting and enumeration, exploit* dan *reporting*. Kesimpulan dari penelitian yang dilakukan adalah ditemukannya beberapa kelemahan yang dimiliki oleh *website* seperti target masih mengaktifkan notifikasi error pada penulisan program, mengaktifkan halaman

public html dan memberikan nama file yang mudah ditebak atau umum sehingga memudahkan peretas mengakses hal-hal tersebut [2].

Tio Revolino Syarif dan Didit Andri Jatmiko pada tahun 2019 melakukan pengujian menggunakan tiga macam *framework* yaitu PTES (*Penetration Testing Execution Standard*), ISSAF (*Information System Security Assessment Framework*) dan OWASP (*Open Web Application Security Project*) untuk mengetahui tingkat keamanan *website* dan untuk mengetahui mana *framework* yang terbaik dan tepat untuk menjaga keamanan *website*. Peneliti menggunakan alur penelitian yaitu identifikasi masalah, analisis perbandingan metode, *penetration testing*, dan hasil. Hasil dari penelitian tersebut mengatakan bahwa *framework* yang paling cocok untuk digunakan pada *website* DISKOMINFO kota Bandung adalah PTES dan OWASP. Hal tersebut dikarenakan penilaian pada kedua *framework* tersebut menggunakan bahasa yang dapat dimengerti oleh semua kalangan bukan hanya orang yang berpengalaman dengan *penetration testing* saja [3].

I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita dan Dewa Made Sri Arsa pada tahun 2020 melakukan penelitian untuk mengetahui celah keamanan yang terdapat pada suatu *website* dengan *framework* ISSAF dan memberikan rekomendasi untuk meningkatkan keamanan sistem. Metode penelitian yang dilakukan peneliti sesuai dengan *framework* ISSAF yaitu diawali dengan *information gathering, network mapping, vulnerability identification, penetration, gaining access and privilege escalation, enumerating further, compromise remote user, maintaining access* dan *covering tracks*. Hasil memaparkan bahwa terdapat keamanan yang dapat dibobol seperti SQL Injection dan XSS pada *website* target, terdapat juga *port* TCP yang terbuka. Sedangkan rekomendasi yang diberikan adalah validasi level *php* dan penutupan *port* yang terbuka [4].

Dr. Raden Teguh Dirgahayu, S.T., M.Sc., Yudi Prayudi, S.Si., M.Kom., Adi Fajaryanto pada tahun 2015 melakukan penelitian mengenai bagaimana cara mengidentifikasi kerentanan sistem dan Analisa kerentanan *webserver* menggunakan metode ISSAF dan OWASP versi 4. Penelitian yang dilakukan menggunakan lima tahapan penelitian yang pertama adalah studi literatur, kemudian pemodelan *webserver*, identifikasi kerentanan sistem, pengujian penetrasi dan yang terakhir analisis dan pelaporan. Hasil dari penelitian tersebut

adalah Analisa dengan metode ISSAF dapat menembus keamanan sistem *webserver* IKIP PGRI Madiun, sedangkan untuk metode OWASP versi 4 mendapatkan hasil bahwa manajemen otentifikasi, sesi dan otorisasi belum dibuat secara baik [5].

Nicolas Ivan Aspriantama pada tahun 2021 melakukan pengujian keamanan sistem pada *website* kuliah.uajy.ac.id milik Universitas Atma Jaya Yogyakarta untuk mengetahui celah-celah keamanan apa saja yang terdapat. Penguji menggunakan beberapa tahapan penelitian yaitu observasi, pengumpulan data, mempersiapkan alat, scanning dan pengujian. Penguji juga menggunakan beberapa tools untuk membantu dalam penelitian seperti Whatweb, Nmap, WHOIS dan Nessus *Web Vulnerability Scanner*. Hasil dari pengujian menggunakan Nessus adalah terdapat dua kerentanan "HIGH", tiga "MEDIUM", satu "LOW" dan 18 "INFO". Sedangkan untuk Metasploit mendapatkan direktori akan tetapi tidak dapat diakses sehingga tidak berhasil. Untuk XSS juga tidak berhasil melakukan injeksi script [6].

Anggi Elanda dan Robby Lintang Buana pada tahun 2020 melakukan pengujian celah keamanan yang ada pada *website* guna mengetahui tingkat keamanan yang dimiliki *website* tersebut dengan menggunakan *framework* ISSAF Versi 4. Metode yang digunakan oleh penulis untuk melakukan penelitian ini berbasis pada *protocol* PRISMA (*Preferred Reporting Item for Systematic Review and Meta-Analysis*). Kesimpulan dari penelitian ini adalah terdapat beberapa kerentanan pada proses otentifikasi, manajemen sesi dan ada juga kerentanan pada proses otorisasi akan tetapi setelah dilakukan pengecekan hanya berupa *false alarm* [7].

Aufan Imron Rosadi pada tahun 2019 melakukan *penetration test* guna mengetahui celah-celah keamanan apa saja yang terdapat pada sistem informasi Universitas XYZ. Metodologi yang dilakukan oleh peneliti adalah dengan perumusan masalah, studi Pustaka, metode Pentest, dan dokumentasi dan laporan. Kesimpulan dari penelitian adalah untuk jenis serangan *sql injection* yang dilakukan aman akan tetapi tidak diketahui untuk jenis-jenis serangan yang lainnya [8].

Fadilla Yulia Fauzan dan Syukhri pada tahun 2021 melakukan *penetration testing* pada aplikasi *e-learning* Universitas Negeri Padang guna mengetahui apakah ada serangan dan kelemahan sistem yang dimiliki oleh aplikasi tersebut.

Metode yang digunakan peneliti adalah dengan menggunakan *Penetration Testing Execution Standard* (PTES) yang mencakup beberapa langkah yaitu *Pre-Engagement Interaction, Intelligence Gathering, Threat Modelling, Vulnerability Testing, Exploitation, Post Exploitation* dan yang terakhir *Reporting*. Kesimpulan dari penelitian tersebut adalah aplikasi *e-learning* memiliki celah keamanan yaitu medium sehingga dapat dikatakan bahwa serangan yang dilakukan tidak terlalu berpengaruh terhadap aplikasi [9].

Yesi Novaria Kunang, Muklis Fatoni dan Siti Sauda pada tahun 2013 melakukan pengujian terhadap *website* berbasis *CMS* (*Content Management System*) guna mencari kerentanan dan solusi yang tepat untuk mengatasi kerentanan tersebut. Metodologi penelitian yang digunakan oleh penulis adalah NIST (*National Institute of Standards and Technology*) yang meliputi langkah diagnosa, rencana tindakan, melakukan tindakan, melakukan evaluasi, dan pembelajaran. Kesimpulan dari penelitian tersebut adalah *CMS* yang memiliki keamanan terbaik adalah *Joomla* dan dapat juga karena tim pengembang *CMS* tersebut lebih responsive dan sering melakukan perbaikan [10].

Berdasarkan penelitian-penelitian yang telah dilakukan sebelumnya, penulis akan melakukan pengujian keamanan pada *website* sikma.uajy.ac.id milik Universitas Atma Jaya Yogyakarta menggunakan *framework* ISSAF. Tidak seperti penelitian sebelumnya, peneliti akan menggunakan beberapa *tools* yang berbeda dengan penelitian sebelumnya dan pengujian akan dilakukan secara lebih lengkap. Penulis berharap agar penelitian ini dapat digunakan Universitas Atma Jaya Yogyakarta untuk mengevaluasi Kembali.

Tabel 2. 1. Tabel Perbandingan Peneliti Terdahulu dengan Saat Ini

Pembanding	**Fahmi Fachri, dkk [1]**	**Agus Rochman, dkk [2]**	**Tio Revolino Syarif, dkk [3]**	**I Gede Ary Suta Sanjaya, dkk [4]**	**Adi Fajaryanto, dkk [5]**
Judul Penelitian	Analisis Keamanan *Webserver* Menggunakan Penetration Test	Analisis Keamanan Website Dengan *Information System Security Assessment Framework (ISSAF)* dan *Open Web Application Security Project (OWASP)* di Rumah Sakit XYZ	Analisis Perbandingan Metode *Web Security* PTES, ISSAF dan OWASP di Dinas Komunikasi dan Informasi Kota Bandung	Evaluasi Keamanan Website Lembaga X Melalui *Penetration Testing* Menggunakan Framework ISSAF	Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server
Tujuan Penelitian	Menguji kelemahan dan kerentanan *webserver* perguruan tinggi	Mengetahui apakah terdapat celah pada keamanan *website* sistem HRD dengan	Mengetahui seberapa tinggi tingkat keamanan *website* dan *Framework* apa yang tepat digunakan untuk	Mengetahui celah keamanan pada *website* dengan menggunakan pengujian *penetration testing* dengan	Mengetahui cara mengidentifkasi kerentanan sistem dan analisis keamanan *webserver*

	agar menghindari resiko terkenanya serangan *hacking system* oleh pihak yang tidak bertanggung jawab	menggunakan *framework* ISSAF dan OWASP	menjaga keamanan *website*	*framework* ISSAF dan memberikan rekomendasi peningkatan keamanan	menggunakan metode ISSAF dan OWASP versi 4
Tahun Terbit	2021	2021	2019	2020	2015
Metode	*Penetration Testing*	ISSAF, OWASP	PTES, ISSAF, OWASP	ISSAF	ISSAF, OWASP
Platform	*Web Server*	*Website*	*Website*	*Website*	*Web Server*

Pembanding	**Nicolas Ivan Aspriantama [6]**	**Anggi Elanda, dkk [7]**	**Aufan Imron Rosadi [8]**	**Fadilla Yulia Fauzan, dkk [9]**	**Yesi Novaria Kunang, dkk [10]**
Judul Penelitian	Pengujian Keamanan Sistem Informasi UAJY Menggunakan *Penetration Testing*	Analisis Keamanan Sistem Informasi Berbasis *Website* Dengan Metode *Open Web Application Security Project*	ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN *WEB PENETRATION TESTING*	Analisis Metode *Web Security* PTES (*Penetration Testing Execution and Standart*) Pada Aplikasi E-Learning Universitas Negeri Padang	PENGUJIAN CELAH KEAMANAN PADA CMS (*Content Management System)*

		(OWASP) Versi 4: *Systematic Review*			
Tujuan Penelitian	Mengetahui celah keamanan yang terdapat pada *website* kuliah.uajy.ac.id	Mengetahui celah keamanan yang ada pada *website* dengan menggunakan *framework* OWASP Versi 4	Mengetahui tingkat keamanan sistem informasi akademik dan solusi dari kerentanan yang ditembus	Mengetahui apakah ada serangan pada aplikasi *E-learning* Universitas Negeri Padang menggunakan *penetration testing*	Mengetahui mana *website* berbasis *CMS* yang terbaik dengan melakukan uji kerentanan
Tahun Terbit	2021	2020	2019	2021	2013
Metode	*Penetration Testing*	OWASP	*Penetration Testing*	*Penetration Testing*	NIST
Platform	*Website*	*Website*	*Website*	Aplikasi	*Website*

Pembanding	**Cornelius Phillipo Julianto (*)**

Judul Penelitian	Pengujian Celah Keamanan Pada Website Menggunakan *Framework* ISSAF
Tujuan Penelitian	Mengetahui celah keamanan apa saja yang dimiliki oleh *website* dengan menggunakan *framework* ISSAF dan membandingkan aplikasi yang digunakan untuk mencari celah keamanan tersebut
Tahun Terbit	2022
Metode	ISSAF
Platform	*Website*

(*)Penelitian yang dilakukan