INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 2 Tahun 2024 Page 4536-4549
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ

Aryda Fatihah Putri Dinarto[1]✉
Information System, Industrial Engineering Faculty, Telkom University Surabaya
Email : aryda.fatihah.20@student.is.ittelkom-sby.ac.id[1]✉

Abstrak

Berkembangnya teknologi website, semakin banyak pihak yang memanfaatkannya sebagai media pendukung penyampaian informasi, termasuk lembaga daerah di Indonesia. Keamanan aplikasi website penting untuk memastikan integritas, kerahasiaan, dan ketersediaan data dalam lingkungan digital. Perusahaan Daerah XYZ merupakan salah satu unit usaha milik daerah yang bergerak di bidang mendistandaribusikan air bersih di daerah Surabaya, Pasuruan, Sidoarjo dan Gresik. Perusahaan Daerah XYZ mempunyai website yang bernama Customer Information System (CIS). Website sebagai media untuk membantu memberi informasi kepada pelanggan tentang pasang baru, pengaduan, tagihan dan pemakaian, informasi tagihan online, dan sebagainya. Dengan hal ini, keamanan sistem website rentan akan bug maupun virus dan itu perlu diuji menggunakan Penetration Testing. Penetration Testing adalah kegiatan mensimulasikan serangan yang dapat dilakukan terhadap jaringan organisasi atau perusahaan tertentu untuk menemukan kerentanan dan menguji ketahanan dalam sistem website jaringan berdasarkan standar kerangka ISSAF. Standar ini menawarkan beberapa keunggulan dibandingkan fitur keamanan lainnya dan bertindak sebagai penghubung antara perspektif teknis. Kerangka kerja ISSAF terdapat 9 penilaian pengujian yang mencakup Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Sites dan Maintaining Access, Covering Tracks. Tujuan dari tugas akhir ini adalah untuk mengetahui kerentanan keamanan informasi situs website dari bug maupun virus menggunakan Penetration Testing berdasarkan Framework ISSAF untuk membuat rekomendasi peningkatan keamanan pada situs website Perusahaan Daerah XYZ. Hasil penelitian dari tugas akhir ini analisis kerentanan pada situs web Perusahaan Daerah XYZ menunjukkan adanya beberapa kerentanan keamanan, namun situs tersebut masih dapat dianggap aman. Kerentanan yang ditemukan dapat diperbaiki melalui pembaruan server dengan mengupgrade OS pada sistem situs web.

Kata kunci: *Keamanan Sistem Informasi, Aplikasi Website, ISSAF, Penetration Testing, Perusahaan Daerah XYZ*

Abstract

With the development of website technology, more and more parties are using it as a supporting medium for conveying information, including regional institutions in Indonesia. Website application security is important to ensure the integrity, confidentiality and availability of data in a digital environment. XYZ Regional Company is a regionally owned business unit which operates in the field of standardizing clean water in the Surabaya, Pasuruan, Sidoarjo and Gresik areas. Regional Company XYZ has a website called Customer Information System (CIS). Website as a medium to help provide information to customers about new installations, complaints, bills and usage, online billing information, and so on. With this, the security of the website system is vulnerable to bugs or viruses and this needs to be tested using Penetration Testing. Penetration Testing is the activity of simulating attacks that can be carried out against a particular organization's or company's network to find vulnerabilities and test resilience in the network's website system based on the ISSAF Framework standards. This standard offers several advantages over other security features and acts as a link between technical perspectives. The ISSAF Framework contains 9 test assessments which include Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromising Remote Users/Sites and Maintaining Access, Covering Tracks. The aim of this final assignment is to determine the information security vulnerabilities of website sites from bugs and viruses using Penetration Testing based on the ISSAF Framework to make recommendations for improving security on the XYZ Regional Company website. The research results from this final project, vulnerability analysis on the XYZ Regional Company website show that there are several security vulnerabilities, but the site can still be considered safe. The vulnerabilities found can be fixed through server updates by upgrading the OS on the website system.

Keywords*: Information System Security, Website Application, ISSAF, Penetration Testing, XYZ Regional Company.*

PENDAHULUAN

Berkembangnya teknologi website telah memunculkan perubahan signifikan dalam pendekatan lembaga daerah/pemerintahan di Indonesia dalam menyampaikan dan mengelola informasi. Sebagai alat pendukung transmisi informasi, website menjadi sarana utama bagi lembaga pemerintah, termasuk Perusahaan Daerah XYZ di Kota Surabaya, untuk memberikan layanan kepada masyarakat. Namun, seiring dengan kemajuan teknologi, ancaman serangan siber yang semakin canggih menjadi perhatian utama, menjadikan keamanan aplikasi website sebagai aspek yang krusial. Keamanan aplikasi website bukan hanya tentang memastikan integritas, kerahasiaan, dan ketersediaan data di lingkungan digital, tetapi juga menghadapi tantangan kompleks dari serangan siber. Dalam konteks ini, Dedy Permadi dari Kementerian Komunikasi dan Informatika (KOMINFO) menyatakan bahwa serangan siber terhadap perusahaan meningkat sebanyak 31% dari tahun 2020 ke

2021, mencapai rata-rata 270 serangan per perusahaan [1]. Oleh karena itu, keberlanjutan layanan online dan interaksi dengan pelanggan memerlukan pemahaman mendalam tentang keamanan aplikasi website. Perusahaan Daerah XYZ, melalui metodologi Penetration Testing berdasarkan Framework ISSAF (Information Systems Security Assessment Framework).

Metode Penetration Testing pendekatan sistematis yang diadopsi peneliti untuk mengidentifikasi dan mengevaluasi celah keamanan dalam aplikasi website. Dengan mensimulasikan serangan oleh pihak yang tidak berwenang, Penetration Testing memungkinkan Perusahaan Daerah XYZ untuk mengidentifikasi dan memperbaiki celah keamanan sebelum diserang oleh pihak yang tidak bertanggung jawab.

Dalam menghadapi tantangan keamanan aplikasi website, Perusahaan Daerah XYZ mungkin menghadapi ancaman serangan siber yang semakin kompleks, termasuk kerentanan keamanan yang belum terdeteksi, masalah dalam sistem otentikasi, konfigurasi yang rentan, atau ketidaktahuan terhadap metode serangan baru. Oleh karena itu, analisis keamanan menggunakan metode Penetration Testing berdasarkan kerangka ISSAF menjadi langkah kritis.

ISSAF singkatan dari Information Systems Security Assessment Framework, merupakan kerangka kerja yang memberikan panduan untuk melakukan penilaian keamanan sistem informasi. Dalam konteks tugas akhir ini, ISSAF digunakan sebagai dasar untuk menganalisis keamanan aplikasi website Perusahaan Daerah XYZ.

Melalui tugas akhir ini, peneliti akan melakukan analisis keamanan aplikasi website Perusahaan Daerah XYZ dengan menggunakan metode Penetration Testing berdasarkan Framework ISSAF. Tujuan utama adalah mengidentifikasi potensi kerentanan atau celah keamanan, menilai tingkat keparahan dan potensi eksploitasi, serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan situs website. Dengan demikian, upaya ini diharapkan dapat memberikan kontribusi positif dalam menjaga keberlanjutan layanan online Perusahaan Daerah XYZ dan melindungi data pelanggan.

PENELITIAN TERKAIT

Sejumlah penelitian sebelumnya telah dilakukan untuk menganalisis keamanan website menggunakan metode Penetration Testing dan Framework ISSAF. Guntoro, Loneli Costaner, dan Musfawati (2020) melakukan penelitian berjudul "Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)." Penelitian ini fokus pada web server Open Journal System Universitas Lancang Kuning, menggunakan Framework ISSAF, dan menunjukkan bahwa

sistem OJS tersebut tergolong aman, meskipun disarankan untuk menerapkan sistem monitoring seperti Firewall.

I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, dan Dewa Made Sri Arsa (2020) juga mengevaluasi keamanan website lembaga X dalam penelitian berjudul "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF." Hasil penelitian menunjukkan adanya celah keamanan berbahaya seperti SQL Injection dan XSS, dengan rekomendasi untuk melakukan validasi pada level php guna mencegah serangan yang merugikan.

Penelitian oleh Sulis Andriyani, M. Fajar Sidig, dan Bita Parga Zen (2023) dengan judul "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework ISSAF Pada Website SMK Al- Kautsar" menguji penetrasi pada website SMK Al-Kautsar, menunjukkan rentan terhadap serangan DDoS. Penelitian ini juga mencatat penggunaan Framework ISSAF dalam tahapan uji penetrasi pada website.

Esi Putri Silmina, Arizona Firdonsyah, dan Rovalia Adhella Attya Am (2022) melakukan penelitian berjudul "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test dan ISSAF" pada Sistem Informasi MTsN 8 Bantul. Hasil pengujian dengan Kali Linux menunjukkan bahwa tidak ada celah yang terdeteksi, menyoroti keamanan sistem informasi sekolah tersebut.

Terakhir, Firda Nurelia Syah Putri, Yudo Bismo Utomo, dan Harso Kurniadi (2023) melakukan penelitian berjudul "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux." Hasil pengujian penetrasi pada website Pemerintah Kabupaten Kediri menemukan beberapa port terbuka dan eksposur informasi sensitif, menekankan penggunaan beberapa tools pada Penetration Testing sesuai dengan konteks penelitian. Semua penelitian ini menunjukkan bahwa penggunaan Framework ISSAF dalam tahapan uji penetrasi pada website merupakan pendekatan yang efektif dalam mengidentifikasi dan mengatasi celah keamanan.

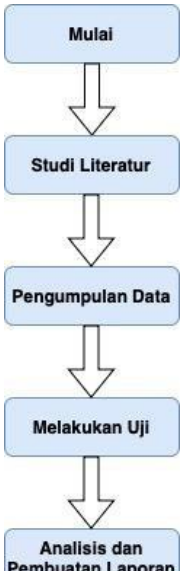
Kesimpulan dari lima penelitian di atas menunjukkan variasi dalam tingkat keamanan sistem informasi pada berbagai web server dan situs yang diteliti yang menekankan pentingnya penggunaan metode Penetration Testing dan Framework ISSAF dalam menilai dan meningkatkan keamanan sistem informasi pada berbagai platform web server dan situs. Temuan celah keamanan dan rekomendasi yang dihasilkan dari penelitian tersebut dapat menjadi acuan bagi pengelola sistem informasi untuk memperkuat pertahanan dan mengurangi risiko terhadap potensi serangan.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode *Penetration Testing* berdasarkan *Framework* ISSAF. *Penetration Testing* ISSAF terletak pada *technical control assessment* yang didesain untuk menguji jaringan, sistem dan kontrol aplikasi. *Penetration Testing*, juga dikenal sebagai *pentesting* atau *ethical hacking* adalah pendekatan untuk menguji keamanan suatu sistem dengan mensimulasikan serangan oleh pihak yang berwenang.

Tujuan dari metode ini adalah untuk mengidentifikasi kelemahan, kerentanan atau celah keamanan pada aplikasi *website* Perusahaan Daerah XYZ. Metodologi *Penetration Testing* ISSAF terdiri dari tiga tahap dan sembilan area *assessment.*

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



Gambar 1. Alur Penelitian

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

Kemudian di tahap selanjutnya yaitu wawancara dan observasi dengan pihak perusahaan daerah XYZ. Kemudian pada tahap pengujian berdasarkan *Framework* ISSAF terdiri dari 9 tahap. Tahap Information Gathering merupakan pengumpulan informasi umum tentang *website* atau *website* sasaran [2]. Tahap *network mapping* adalah tahapan mengumpulkan informasi spesifik tentang jaringan *website* target [2]. Tahap *vulnerability identification* merupakan pemindaian kerentanan pada *website* target Berdasarkan

pemetaan jaringan dan informasi yang dikumpulkan selama langkah *network mapping, outputnya* adalah daftar lengkap kerentanan yang ditemukan, beserta tingkat keparahannya [2]. Tahap *penetration* adalah tahapan simulasi serangan, yang tujuannya adalah untuk menemukan kerentanan keamanan informasi di situs *website* atau *website* sasaran. Tahap *gaining access and privilege escalation* merupakan tahapan pengujian akses ke sistem *website* Perusahaan Daerah XYZ atau *website* sasaran. Tahap *gaining access and privilege escalation* merupakan tahapan pengujian akses ke sistem *website* Perusahaan Daerah sasaran. Tahap *enumerating futher* adalah langkah mencari informasi tentang kata sandi di *website* sasaran. Input dari tahap ini adalah akses tersebut memiliki akses yang lebih tinggi daripada Langkah sebelumnya. Tahap *compromise remote user/sites*, adalah langkah untuk mendapatkan akses jarak jauh ke sistem *website* target. Tahap *maintaining access* merupakan tahapan penanaman *backdoor* ke dalam sistem-sistem. dan tahap terakhir *covering tracks*, adalah langkah pengujian terakhir yang menghapus catatan serangan sebelumnya pada sistem target.

HASIL DAN PEMBAHASAN

Hasil dan pembahasan pada penelitian ini meliputi pembahasan hasil pengujian *Penetration Testing* menggunakan *Framework* ISSAF serta rekomendasi yang diberikan berdasarkan hasil pengujian.

1. Hasil *Information gathering*

Hasil proses tahap information gathering yang dilakukan agar mendapatkan informasi berkaitan dengan target yang dianalisa dapat dilihat pada tabel 4.1:

Tabel 4. 1 Tabel Hasil Information gathering

Teknik Pengujian	*Tools*	Hasil
Mencari informasi domain	*Google*	Domain *website* xyz.go.id Tampilan *website*
Identifikasi spesifikasi	*Wappalyzer*	• Bahasa pemrograman PHP • *UI Framework Bootstrap*

		• *Web server Apache HTTP Server* • *Live chat WhatsApp Business* • *JavaScript libraries Stick and JQuery*
Pencarian alamat IP Mencari data informasi tentang domain Database	*Ping* *whois* wawancara	*IP Address:* 1xx.xx.xxx.xx Informasi tentang server website xyz.go.id mysql

2. Hasil *Network Mapping*

Berikut hasil *network mapping, scanning version,* dan *scan* SSL/TLS yang bertujuan untuk *network mapping* (pemetaan jaringan) yang terdapat pda sistem yang dapat dilihat pada tabel 4.2:

Tabel 4. 2 Tabel Hasil Tahapan *Network Mapping*

Teknik Pengujian	*Tools*	Hasil
Network mapping	*Nmap*	• *Port* terbuka

Scanning SSL/TLS	*Ssllabs.com*	Hasil konfigurasi keamanan *website* yaitu Level B

Terdapat tabel melakukan *port scanning* untuk melihat *port* apa saja yang dimiliki *website* xyz.go.id. Pada tahapan ini, menggunakan *tool nmap* yang memiliki keakuratan yang baik. Berikut hasil *scan* xyz.go.id yang menggunakan *tool nmap*.

PORT	STATE	SERVICE
80/tcp	Open	http
443/tcp	Open	https

Lalu pada tahap selanjutnya melakukan uji keamanan *Secure Socket Layer* (SSL) dan *Transport Layer Security* (TLS) yang digunakan pada *website* xyz.go.id dengan menggunakan *tool online* yang bernama *ssllabs.com* dengan hasil sebagai berikut:

Gambar 4. 1 Hasil Scan menggunakan

3. Hasil *Vulnerabiluty Identification*

Berikut hasil *testing vulnerability identification* menggunakan dua fitur dari *tool nessus*, yaitu *basic network scan* dan *web application test* yang dapat dilihat pada tabel 4.3:

Tabel 4. 3 Tabel Hasil *Vulnerability*

Tools		Hasil
Nessus	*Basic network scan*	• 1 info, 1 medium dan 1 high.
	Web application test	• Hanya menampilkan info
Rapidscan		• 2 *low* dan 2 *medium*

4. Hasil *Penetration*

Berikut hasil pada tahap *Penetration Testing* yang diuji berdasarkan hasil analisis diatas. Hasil pada tahap *Penetration Testing* menggunakan dua jenis serangan, yaitu *SQL Injection* dan

Cross Site Scripting (XSS) yang dapat dilihat pada tabel 4.4:

Tabel 4. 4 Tabel Hasil *Penetration*

Jenis Serangan	Hasil
SQL Injection form login user	• Uji *SQL injection* pada *form user login*
XSS Cross Site Scripting	• Uji *XSS pada form* pendaftaran dengan *input manual script.*

Pengujian ini menggunakan alat *SQL Map* sebagai pengujian *SQL injection yang* berdasarkan informasi mengenai *website* xyz.go.id terindentifikasi menggunakan *database mysql.*

Gambar 4. 2 *SQL Injection* dengan *Tool SQL Map*

Berikut tabel penjelasan parameter yang digunakan dalam percobaan diatas:

Parameter	Penjelasan
-u	Menunjukkan URL target yang akan diuji kerentanan oleh SQL Map.

--dbs	Memberikan perintah kepada SQL Map untuk mengidentifikasi dan menampilkan daftar database yang dapat diakses melalui situs web tersebut
--hh	Memberikan instruksi kepada SQL Map untuk menyajikan hasil dalam format yang lebih mudah dibaca atau disajikan.-

5. Hasil *Gaining Access and Privilege Escalation*

Berikut hasil pada tahap *Gaining Access and Privilege Escalation* yang diuji berdasarkan hasil analisis diatas, dapat dilihat pada tabel 4.5:

Tabel 4. 5 Tabel Hasil *Gaining Access*

Jenis serangan	Hasil
Bruteforce attack menggunakan tool metasploit	Uji *bruteforce attack* pada port 21
Eksploitasi	

6. Hasil *Enumerating Further*

Berikut hasil pada tahap diuji berdasarkan hasil analisis diatas, dapat Enumerating Further yang dilihat pada tabel 4.6:

Tabel 4. 6 Tabel Hasil Enumerating Further

Jenis Serangan	Hasil
Burpsuite	
Mendapat request cookie yaitu xyz_session	

7. Hasil *Compromise Remote User/Sites*

Pada tahap ini upaya dilakukan berkali-kali hingga IP yang dimiliki oleh peneliti *terblockir.* Memberi rekomendasi validasi agar orang lain tidak melakukan *bruteforce* untuk

mendapatkan akses istimewa ke di jaringan internal dengan mengeksploitasi kerentanan pengguna atau situs yang ada. Setelah berhasil mengontrol pengguna atau lokasi jarak jauh, bisa mendapatkan akses lebih besar ke jaringan internal. Namun karena sistem Perusahaan Daerah XYZ telah dikonfigurasi dengan benar dan didukung dengan memperoleh ISO/IEC 27001, dan tahap ini tidak dapat dicapai karena tahap peningkatan akses dan hak istimewa gagal sehingga menghalangi akses lebih lanjut.

8. Hasil *Maintaining Access*

Selama tahap ini, berbagai teknik dan strategi digunakan untuk mempertahankan akses yang diperoleh, termasuk mengeksploitasi kerentanan yang belum terselesaikan dan membuat sistem *backdoor* untuk akses jangka panjang guna menghindari deteksi oleh sistem keamanan yang ada.

Namun karena sistem *website* Perusahaan Daerah XYZ telah terkonfigurasi dengan baik atau sesuai dengan yang diperlukan, tahap ini tidak dapat dicapai karena tahap peningkatan akses dan hak istimewa gagal sehingga menghalangi akses lebih lanjut.

9. Hasil *Covering Tracks*

Pada tahap terakhir ini yaitu melakukan serangkaian langkah untuk menghilangkan jejak aktivitas, termasuk menghapus atau mengubah *file log*, menghapus *entri log,* menghapus *file* atau *folder* yang terkait dengan serangan, serta melakukan tindakan lain yang bertujuan

untuk menghapus bukti-bukti yang dapat mengungkap identitas penyerang. Namun tidak dapat sampai ke tahap ini karena gagalnya dalam tahap *gaining access and privillage escalation* dikarenakan sistem yang dimiliki oleh Perusahaan Daerah XYZ telah dikonfigurasi dengan baik sehingga tidak dapat diakses lebih lanjut.

SIMPULAN

Dalam bab kesimpulan ini, merangkum hasil dan analisis penelitian ini untuk memberikan gambaran tentang topik yang sedang diteliti, berikut beberapa poin kesimpulan:

1. Hasil analisis kerentanan pada situs web Perusahaan Daerah XYZ menunjukkan adanya beberapa kerentanan keamanan, namun situs tersebut masih dapat dianggap aman. Pemindaian menggunakan alat *Nessus* dan *RapidScan* mengidentifikasi kerentanan yang dapat diperbaiki melalui pembaruan server dengan meng*upgrade* OS pada sistem situs web.

2. Metode *Penetration Testing* berdasarkan *Framework* ISSAF untuk mengukur keamanan aplikasi *website* Perusahaan Daerah XYZ melibatkan beberapa langkah. *Information gathering* dilakukan untuk pemahaman menyeluruh tentang sasaran, diikuti dengan *network mapping* untuk mengidentifikasi *port* terbuka. *Vulnerability identification* dilakukan melalui pengujian otomatis, tetapi dua teknik uji (*SQL Injection* dan XSS) yang diimplementasikan tidak berhasil. Upaya *gaining access and privilege escalation* tidak berhasil karena kegagalan mendapatkan hak akses, sementara *enumerating further* terhambat oleh proteksi *protocol* TLS.
3. Rekomendasi perbaikan keamanan berdasarkan hasil analisis *Penetration Testing* dengan menggunakan *Framework* ISSAF pada aplikasi *website* Perusahaan Daerah XYZ dapat mencakup sejumlah Tindakan menutup akses untuk melakukan *scan* terhadap *port-port* yang ada didalam sistem. Implementasi langkah mitigasi pada tingkat keamanan jaringan juga direkomendasikan untuk mengurangi risiko kerentanan yang terkait dengan *port* yang terbuka. Selanjutnya, diperlukan pembaruan pada TLS ke versi yang lebih baru atau TLS versi 1.3. Semua perbaikan ini seharusnya sejalan dengan pembaruan perangkat lunak, serta pemantauan dan pemeliharaan rutin untuk memastikan tingkat keamanan yang optimal pada *website* Perusahaan Daerah XYZ.

DAFTAR PUSTAKA

Biro Humas Kementrian Kominfo, "Tantangan Keamanan Siber Makin Besar, Indonesia Dorong Tata Kelola Data Lintas Negara,"KOMINFO,28July2022. [Online]. Available:https://www.kominfo.go.id/content/detail/43363/siaran-pers-no-306hmkominfo072022-tentang-tantangan-keamanan-siber-makin-besar-indonesia-dorong-tata-kelola-data-lintas-negara/0/siaran_pers [Accessed 30 June 2023].

I. G. A. S. Sanjaya, G. M. A. Sasmita And D. M.S. Arsa, "Evaluasi Keamanan *Website* Lembaga X Melalui *Penetration Testing* Menggunakan *Framework* ISSAF," Jurnal Ilmiah Merpati, Vol. 8, No. 2, Pp. 1-12, 2020.

I. U. Haq And A. T. Khan, "Kelebihan Dan Kekurangan Kali OS Kali Linux Dirancang Khusus Untuk Pengujian Keamanan Dan Digunakan Oleh Profesional Keamanan Untuk Menguji Keamanan Sistem Dan Jaringan. Kelebihan Dan Kekurangan OS Kali Linux Adalah Sebagai Berikut: Tambahan Terintegras.," Vol. 9, 2021.

Z. A. Khan, N. S. H, M. Irsyad And T. Darmizal, "1593*Penetration Testing* Information System Security Assessment*Framework* (ISSAF)," Kajian Ilmiah Informatika Dan Komputer, Vol. 4, No. 3, Pp. 1-9, 2023.

Herman, I. Riadi, Y. Kurniawan And I. A. Rafiq, "Analisis Keamanan *Website* Menggunakan Information System Security Assessment *Framework* (ISSAF)," Jurnal Teknologi Informatika Dan Komputer, Vol. 9, No. 1, Pp. 1-10, 2023.

L. C. A. M. Guntoro, "Analisis Keamanan Web Server Open Leumal System (Lis) Menggunakan Metode Issaf Dan OAWSP (Studi Kasus Lis Universitas Lancang Kuning," Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika, Vol. 5, No. 1, Pp. 1-11, 2020.

A. Lubis And Tarigan A, "Security Assessment Of Web Application Through Penetration System Techniques," International Jeunal Of Recent Trends In , Engineering & Research, Vol. 3, No. 1, Pp. 1- 10, 2017.

T. A. Hanafi, C. Iswahyudi And R. Y. Rachmawati , "Aplikasi Pendeteksi Celah Keamanan Aplikasi Web Dengan *Penetration Testing* Menggunakan Metode • Input Validation Testing," Jurnal SCRIPT, Vol. 7, No. 2, Pp. 1-10, 2019.

I. M. Raazi, I. Dwitawati And P. Nabila, "Uji Vulnerability Assessment Dalam Mengetahui Tingkat Keamanan Web Aplikasi Sistem Informasi Laporan Diskominfo Dan Sandi Aceh," JINTECH: Journal Of Information Technology, Vol. 4, No. 1, Pp. 1-15, 2023.

K. A. Suputri, M. D. Maharani, G. A. Pratama, N. D. I. S. Putri , I. M. E. Listartha And G. A. J. Saskara, "Perbandingan Tools Vulnerability Scan Ning Pada Pengujian Sebuah *Website*," Jurnal Informatik, Vol. 18, No. 3, Pp. 1-9, 2022.

R. Ashar, "Analisis Keamanan Open *Website* Menggunakan Metode OWASP Abstandaract Dan ISSAF," Jurnal Informasi Dan Teknologi, Vol. 4, No. 4, Pp. 1-8, 2022.

S. F. Y. Fauzan, "Analisis Metode Web Security PTES (*Penetration Testing* Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang," Jurnal Voteteknika, Vol. 9, No. 2, Pp. 1-7, 2021.

S. Utoro, A. B. Nugroho And M, "Analisis Keamanan *Website* E-Learning SMKN 1 Cibatu Menggunakan Metode *Penetration Testing* Executian Standard," Jurnal Multimedia Networking Informatics, Vol. 6, No. 2, Pp. 1-10, 2020.

A. P. Nofriansyah, A. Armandhani And K. Ibnutama , "Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab Testing Menggunakan *Penetration Testing* Standart OWASP," Jurnal Saintikom, Vol. 21, No. 2, Pp. 1-9, 2022.

R. K. Siregar, "Keamanan Informasi," Kementerian Keuangan, 20 May 2020. [Online]. Available: Https://Www.Djkn.Kemenkeu.Go.Id/Kanwil- Rsk/Baca-Artikel/13120/Keamanan- Informasi.Html.. [Accessed 3 July 2023].

H. Azis And F. Fattah, "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing," ILKOM Jurnal Ilmiah, Vol. 11, No. 2, Pp. 1-8, 2019.

H. R. P. Sailellah, "Kali Linux: Pengertian, Sejarah, Kelebihan, Kekurangan & Jenisnya," Puti, 3 May 2023. [Online]. Available: Https://It.Telkomuniversity.Ac.Id/Kali-Linux- Pengertian-Sejarah-Kelebihan- Kekurangan- Jenisnya/.. [Accessed 3 July 2023].

R. Fikriyadi And B. A. Prakosa, "Security Analysis At Wireless Local Area Network (WLAN) Network With The Penetratien Testing Method," Jurnal Mantik, Vol. 4, No. 3, Pp. 1-5, 2020.

A. Rochman, R. R. Salam And S. A. Maulana, "Analisis Keamanan Website Dengan Informatien System Secuat Assessment Examewerk (Ossaf Dan Open Web Application Security Project (Owasp) Di Rumah Sakit Xyz," Jurnal Indonesia Sosial Teknologi, Vol. 3, No. 4, Pp. 1-14, 2021.

E. P. Silmina, A. Firdonsyah And R. A. A. Amanda, "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf," Jurnal Ilmiah Teknik Elektro, Vol. 24, No. 3, Pp. 1-10, 2022.