PAPER NAME

29. MTI-60181103-yudi1.pdf

AUTHOR

Yudi Kurniawan

WORD COUNT

3462 Words

CHARACTER COUNT

20970 Characters

PAGE COUNT

11 Pages

FILE SIZE

203.7KB

SUBMISSION DATE

Apr 4, 2023 3:02 PM GMT+7

REPORT DATE

Apr 4, 2023 3:03 PM GMT+7

24% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 24% Internet database
- 10% Publications database
- Crossref database
- Crossref Posted Content database
- 0% Submitted Works database

Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Manually excluded sources

Analisis Keamanan Website Menggunakan *Information System Security Asessment Framework* (ISSAF)

Herman[1)], Imam Riadi[2)], Yudi Kurniawan[3)*)], Irhash Ainur Rafiq[4)]

[1,3)]Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
[2)]Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan
[*)]Correspondence Author: yudi2007048008@webmail.uad.ac.id, Yogyakarta, Indonesia
DOI: https://doi.org/10.37012/jtik.v9i1.1439

Abstrak

Di zaman ini internet sudah menjadi kebutuhan. Banyak hal yang dapat dilakukan dengan Internet. Mulai dari mendapatkan informasi, belajar, berbelanja, dan yang lainnya dapat dilakukan melalui website. Website adalah web yang berada di dalam web server. Tetapi banyak pengguna atau pemilik website kurang mengetahui tentang pentingnya keamanan dari sebuah website. Misalnya yang berkatian dengan kerentanan terhadap malware maupun terhadap SQL *Injection*. Kerentanan bisa disebabkan oleh berbagai macam, salah satu yang penting adalah di bagian *coding* website tersebut, sehingga menyebabkan *backdoor* yang dapat di eksploitasi oleh penyerang. Analisis kerentanan keamanan sebuah website sangat diperlukan. Pada penelitian ini dipaparkan sebuah proses analisis kerentatan website menggunakan metode *Information Systems Security Assessment Framework* (ISSAF). Dalam melakukan assessment digunakan beberapa tools untuk mencari hingga menganalisis kerentanan sebuah website seperti *WhoIsDomain*, *Subgraph Vega*, dan *Nmap* sehingga pengguna atau pemilik website mengetahui bagaimana kerentanan dari website tersebut. Hasil analisis ini menyimpulkan bahwa website yang di uji masih memiliki beberapa kerentanan seperti XSS, SQL *Injection*, CSRF *Token not set*, dan yang lainnya. Hasil akurasi yang di dapatkan menggunakan *subgraph vega* adalah sebesar 100% untuk kerentanan *Cross Site Scrpting*, dan 77% untuk SQL Injection.

Kata Kunci: ISSAF, Kerentanan, Malware, Eksploitasi, Website

Abstract

In this era the internet has become a necessity. Many things can be done with the Internet. Starting from getting information, studying, shopping, and others can be done through the website. Website is a web that resides on a web server. But many users or website owners do not know about the importance of website security. For example, those related to vulnerabilities to malware and to SQL Injection. Vulnerabilities can be caused by various kinds, one of which is important is in the coding part of the website, causing a backdoor that can be exploited by attackers. Analysis of security vulnerabilities of a website is very necessary. In this study, a website vulnerability analysis process was described using the Information Systems Security Assessment Framework (ISSAF) method. In conducting the assessment, several tools are used to search for and analyze the vulnerabilities of a website, such as WhoIsDomain, Subgraph Vega, and Nmap so that users or website owners know how the vulnerabilities of the website are. The results of this analysis conclude that the tested website still has several vulnerabilities such as XSS, SQL Injection, CSRF Token not set, and others. The accuracy results obtained using the vega subgraph are 100% for Cross Site Scrpting vulnerabilities, and 77% for SQL Injection.

Keywords: *ISSAF, Vulnerability, Malware, Exploitation, Website*

PENDAHULUAN

Website adalah kumpulan halaman web yang saling terhubung dan seluruh file saling terkait Web terdiri dari page atau halaman dan kumpulan halaman yang dinamakan homepage (B Kusnandar, 2021). Homepage berada pada posisi teratas dengan halaman-halaman terkait berada di bawahnya. Biasanya, setiap halaman di bawah homepage (*child*

page) berisi *hyperlink* ke halaman lain dalam web. Ada dua jenis website berdasarkan sifatnya yaitu dinamis dan statis. (Prasetyo Eko & Hassanah N, 2021)

Kerentanan dapat terjadi pada aplikasi web karena terdapat suatu kesalahan pada proses pengembangan atau perancangannya. Kerentanan aplikasi web juga disebabkan karena serangan dari dalam maupun dari luar. Kerentanan dalam aplikasi web biasanya terjadi di tingkat database atau tingkat jaringan. Hal tersebut juga mencakup berbagai hal seperti kesalahan input atau input tidak valid, desain aplikasi web yang bermasalah/buruk, dll. Website biasanya rentan terhadap serangan SQL *Injection*, *Cross Site Scripting*, *Brute Force*, dan *Malware* (H Hutagalung et al., 2017).

Pengujian sistem keamanan aplikasi berbasis web adalah hal yang penting di era perkembangan aplikasi berbasis web yang melaju dengan pesat. Semakin berkembangnya aplikasi berbasis web juga diiringi dengan tingginya serangan keamanan dari berbabagai teknik ancaman (S Sanjaya, 2020). Seringkali masalah keamanan berada di urutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Oleh karena itu organisasi perlu melakukan asesmen pada aplikasi berbasis website agar oraganisasi mampu mendeteksi kerentanan dan memahami risiko yang dihadapi.

Beberapa faktor yang menyebabkan kurangnya tingkat keamanan pada aplikasi website, diantaranya adalah kesalahan penulisan kode program dan *misconfigutation*. Kesalahan pada penulisan kode program dalam pembuatan aplikasi berbasis web sering dimanfaatkan oleh penyerang. Serangan yang sering dilakukan oleh penyerang diantaranya adalah SQL *Injection*, *Authentication*, XSS, CSRF Token tidak di set dan session tidak di atur. Dampak yang dapat terjadi jika masih terdapat kerentanan seperti sql *injection*, penyerang dapat menyisipkan query dimana dalam menyisipkan query ini penyerang tidak perlu melakukan login ke dalam database, sehingga penyerang dapat dengan leluasa mengganti data dalam database, dan kerentanan *session cookie not set* (CSRF token) (G Guntoro & Musfawati Muhammad, 2020). Penyerang dapat mengambil alih sesi pengguna, sehingga nantinya penyerang dapat mengambil informasi data pengguna sesi tersebut sehingga faktor kerahasiaan website tersebut menjadi hilang, itulah dampak yang dapat terjadi jika keamanan website tidak menjadi prioritas bagi sebuah website (D Bernadisman, 2019). Begitu Juga dengan web server, kerentanan dalam aplikasi Web server akan memberikan peluang bagi *hacker* untuk melakukan eksploitasi serangan pada sistem secara bertahap dan tidak menutup kemungkinan sistem yang diserang akan diambil alih sepenuhnya (Yunanri et al., n.d.).

Beberapa langkah dalam membuat *assessment* terkait kerentanan sebuah website, metode yang digunakan adalah *Information System Security Assessment* (ISSAF)(B Ratore, 2005), proses *assessment* ISSAF sendiri terbagi menjadi 3 proses besar, pertama phase 1 di mana dalam proses phase 1 mengumpulkan informasi terkait website yang akan dianalisis kerentanannya, phase 2 mencari kerentanan yang ada pada website tersebut, dan yang terakhir phase 3 pihak penguji membuat laporan terhadap website yang di uji (Ramansyah et al., n.d.). Tujuan dilakukannya penelitian ini adalah untuk melakukan assessment keamanan website, mencari apa saja kerentanan yang ada pada website tersebut serta menganalisis dampak apa saja yang dapat terjadi jika kerentanan tersebut ada pada website tersebut, sehingga hasil dari analisa *assessment* dapat membantu pengelola dan pengembang sistem untuk mencegah dan mengatasi dampak resiko yang di temukan di sistem. Assessment kerentanan diharapkan juga berdampak bagi pengguna yaitu memberi wawasan apa saja kerentanan yang ada, dan dampak bagi penggunanya (Hasan Muhammad & S suharmanto, 2021).

METODE

Penerapan *penetration testing* pada sebuah website sangat penting dilakukan (J Ruhiyat, 2018) sebelum website tersebut aktif digunakan agar meminimalisir adanya celah dari berbagai jenis serangan pada website tersebut. Dalam proses *penetration testing* penelitian ini mengunakan beberapa device pendukung seperti pada Tabel 1.

Tabel 1. Kebutuhan Perangkat

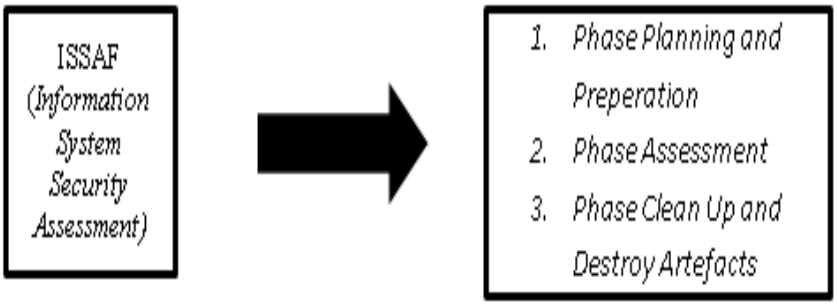
No	Device	Spesifikasi
No	Device	Spesifikasi
1	Laptop/PC	-Asus A455L -RAM 12 GB -SSD 120 GB
2	Sistem Operasi	Windows 10
3	Vulnerabilities Tool	Nmap
4	Penetration Tool	Subgraph Vega
5	Network	Jogja Telkom Net 100 Mbps

Pada penelitian ini terdapat perangkat dan tools yang akan di gunakan sebagai pendukungnya, kebutuhan perangkat dapat dilihat pada tabel 1, yaitu menggunakan laptop dengan RAM 12 GB, SSD 120 GB, sistem operasi menggunakan windows 10, dan menggunakan internet dengan kecepatan 100 mbps. Berikut daftar tools yang digunakan, dapat dilihat pada tabel 2.

Tabel 2. Daftar *Tools*

No	Step	Tool
1	*Phase 1 Planning and Preperation*	-WhoIs Domain -Nmap
2	*Phase2 Assessment*	-SubgraphVega
3	*Phase 3 Clean Up and Destroy Artefacts*	-CCleaner -Shell

Penelitian ini melakukan *penetration testing* (Cyber Security Assessment, 2022) mengikuti *Information System Security Assessment framework* dengan tiga phase di dalamnya seperti pada gambar 1.



Gambar 1. Proses Pengujian

3 Phase Information System Security Assessment adalah sebagai berikut:

1. Phase 1 terdiri dari *information gathering* dan *network mapping*.
   a. *Information Gathering*

      Dalam tahap ini peneliti menggunakan Internet untuk mendapatkan informasi sebanyak-banyaknya dari target (Perusahaan atau Orang) dengan menggunakan metode teknikal (DNS/WHOIS) dan non-teknikal (Search Engine, list E-mail, dan lain-lain). *Information Gathering* tidak membutuhkan peneliti untuk menetapkan hubungan dengan sistem target. Informasi bisa didapatkan melalui sumber-sumber publik seperti internet, dan organisasi-organisasi yang mempunyai informasi publik, seperti perpustakaan dan lain-lain. (G Mahendra, 2021).

   b. *Network Mapping*

      Setelah informasi berhasil didapatkan, pendekatan teknikal yang dapat dilakukan ialah meletakkan "*Footprint*" ke sistem ataupun jaringan yang diinginkan. Untuk lebih efektif, *Network Mapping* sebaiknya dilakukan dengan sesuai dengan rencana. Rencana ini mencakup kemungkinan titik terlemah atau hal-hal yang paling penting dari perusahaan yang akan di nilai.

2. Phase 2 (*assessment*) terdiri dari *vulnerability identification, penetration, gaining access, enumerate further, compromise remote user, maintaining access*.

   a. *Vulnerability Identification*

      Disaat *Vulnerability Identification*, penguji akan melakukan beberapa aktifitas untuk mendapatkan kerentanan yang ada pada sistem.(E Alwi & F Umar, 2020)

   b. *Penetration*

      Penguji akan mencoba untuk mendapatkan akses secara illegal dengan cara mengakali sistem keamanan dan mencoba untuk mencapai akses level seluas-luasnya(Sunyoto A & Pramono Edi, 2021).

   c. *Gaining Access & Privilege Escalation*

      Di beberapa situasi, sebuah sistem dapat dinilai lebih jauh, dalam fase ini mengizinkan penguji untuk memastikan dan mendokumentasikan kemungkinan gangguan, dan penyebaran serangan otomatis. Hal ini memungkinkan hasil dari pengujian yang lebih baik kepada target secara menyeluruh. (J Ruhiyat, 2018)

   d. *Enumerate Further*

      Dalam tahap ini, memungkinkan penguji untuk mendapatkan informasi tambahan berdasarkan proses pada sistem.(C Palmer, 2001)

   e. *Compromise Remote User/Sites*

      Sebuah kerentanan sudah cukup untuk membuka seluruh jaringan, sebagaimanapun amannya sebuah jaringan. Penguji dapat mencoba untuk menggunakan *remote user*. Hal ini dapat memudahkan untuk mendapatkan hak akses untuk ke jaringan yang lebih dalam. (E Stefanus & N Hassanah, 2021)

   f. *Maintaining Access*

      Dengan menggunakan sesuatu seperti *backdoor*, penguji dapat kembali ke dalam sebuah sistem, bahkan jika sistem yang diuji sudah tidak lagi ada. *Backdoor* dapat dibuat dengan beberapa cara, baik dengan menggunakan *root-kit*, dengan mengizinkan sistem target terkoneksi dengan server penguji dan lain-lain. (A Rochman et al., 2021)

3. Phase 3 terdiri dari *covering track, reporting* dan *clean and destroy artefact*

   a. *Covering the Track*

      Pada tahapan ini, penguji akan menghapus jejak-jejak yang ada dengan cara

menyembunyikan file, dan juga menghapus log files. (F Adi, 2015)

b. Reporting

Pada tahap ini, penguji akan melakukan penulisan laporan yang mendeskripsikan hasil pengujian dengan rekomendasi dan penyelesaiannya. (al Azhar Muhammad, 2012)

c. *Clean And Destroy Artifacts*

Semua informasi yang telah dibuat atau diletakkan di sistem sudah harus dihapus pada tahap ini. Jika tidak dapat dilakukan, dengan *remote system*, hal ini harus diberitahukan kepada pihak yang diuji agar para staff IT pada pihak tersebut dapat menghapus informasi ini setelah laporan diterima. (A Raharja, 2019)

HASIL DAN PEMBAHASAN

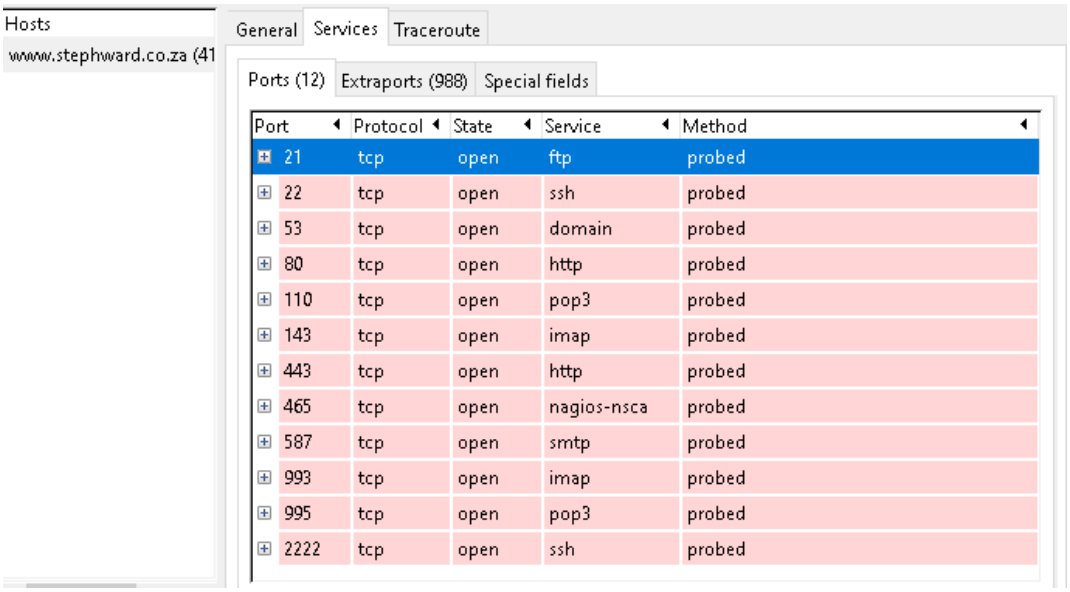
Website yang di gunakan untuk melakukan analisis kerentanan ini adalah www.stephward.co.za pengumpulan informasi website menggunakan WhoIsDomain, di mana informasi ini terkait dengan tanggal dan tahun di buatnya website tersebut, nama server, ip address host server, lokasi server tersebut, dan email admin website terkait, untuk lebih jelas dapat dilihat pada Tabel 3.

Hasil pengumpulan informasi WhoIsDomain di kodekan menjadi STP.01, diketahui, alamat *server host* yang di pakai oleh target, alamat IP address host, email admin website, dan tanggal website tersebut dibuat maupun tanggal website tersebut akan habis, pada tabel 1 berisi informasi terkait website target, seperti nama website tersebut adalah www.stephward.co.za, hosting website tersebut dibuat pada tanggal 25 bulan 9 tahun 2005, dan akan expired pada tanggal 25 bulan 9 tahun 2022, alamat email admin website tersebut di ketahui ber-email mail.stephward.co.za. dan alamat IP host 41.2003.18.163, dan berlokasi di GautengJohannsenburg.

Tabel 3. Informasi Website

No	Jenis	Keterangan
1	Date	-Dibuat pada 2002-09-25 -Expired pada 2022-09-25
2	Nama Server	-NS1.DNS-H.COM -NS1.HOST-H.NET -NS2.HOST-H.NET
3	IP address host	41.203.18.163
4	Lokasi	Gauteng-Johannsenburg
5	Email Admin	mail.stephward.co.za

Pada tahap *network mapping* atau pemetaan jaringan fisik jaringan menggunakan Nmap, hasil dari Nmap dapat dilihat pada Gambar 2.



Gambar 2. *Network Mapping*

Pengumpulan informasi melalui Nmap di ringkas dan di kodekan menjadi STP.02. Port dengan kondisi yang terbuka rentan akan serangan dari penyerang web tersebut, oleh karna itu pada gambar 2 dapat di simpulkan bahwa website rentan terkena serangan *sql injection* di karenakan port 3306/tcp kondisinya terbuka (P Sitorus & A Habibi, 2020).

Pada hasil ini menggunakan Subgraph Vega untuk proses analisis kerentanan website, kerentanan di bagi menjadi 3 level, yaitu level *high*, *medium*, dan *low*. Level high seperti pada Tabel 4.

Tabel 4. Kerentanan Tingkat *High*

No	Level	Jenis	Keterangan	Jumlah Kerentanan
1	*High*	*Cross Site Scripting*	XSS merupakan salah satu jenis serangan injeksi code. XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs.	1
2	*High*	*SQL Injection*	SQL Injection merupakan jenis serangan yang memungkinkan penyerang dapat memperoleh database website	11

Ringkasan pada Tabel 4 menunjukan terdapat kerentanan pada level *high*, pada level ini, website memiliki kerentanan dengan level *high* dengan jenis kerentanan *Cross Site Scripting*, dan SQL *Injection*. Sedangkan pada level *medium* dapat dilihat pada Tabel 5.

Tabel 5. Kerentanan Tingkat *Medium*

No	Level	Jenis	Jumlah Kerentanan
1	Medium	Vulnerable JS Library	2
2		Absence of anti CSRF Token	2009
3		Cookie No HttpOnly Flag	1
4		Cookie without secure flag	1
5		Cookie without Samesite attribute	1
6		Cross domain JavaScript Source File Inclusion	1174
7		Incompete or No Cahce Control	263
8		X-Content-Type Option Header Missing	6313

Pada Tabel 5 menunjukan terdapat 8 kerentanan pada level *medium*, keterangan setiap kerentanan adalah sebagai berikut:

1. *Vulnerable JS Library : Java Script library* rentan
2. *Absence of anti CSRF Token* : Merupakan sebuah *random string* yang di-generate setiap kali halaman form muncul, target tidak memiliki anti CSRF Token, penyerang dapat menyusupkan sebuah tautan, dimana pengguna mengkliknya, penyerang dapat mengambil alih *session* dari pengguna (Bahrun Ghozali, 2019).
3. *Cookie No HttpOnly Flag* : Penyerang dapat dengan mudah mengakses *session user*, dan dengan mudah mengambil data yang sensitif (A Kristianto, 2009).
4. *Cookie without secure flag* : Cookie Bisa di akses dari *unencrypted* koneksi
5. *Cookie without samesite attribute* : Semua cookie tanpa atribut "*SameSite*" akan ditambahkan ke setiap permintaan yang diinisialisasi ke situs web lain mana pun. Ini memungkinkan penyerang untuk menyalahgunakan sesi milik pengguna yang berwenang (R Widianto, 2020).
6. *Cross Domain JavaScript Source File Inclusion* : Terdapat file dari pihak ke 3 yang tidak dipercaya (K Pertiwi, 2019).
7. *Incompete or No Cache Control* : Header kontrol cache belum disetel dengan benar atau tidak ada, memungkinkan browser dan proxy untuk menyimpan konten dalam cache.
8. *X-Content-Type Option Header Missing* : Tidak adanya *header* memungkinkan untuk penyerang mengendus media atau konten bertipe MIME (*Multi Purpose Internet Mail Extension*)(A Raharja, 2019).

Ringkasan keseluruhan kerentanan *website* yang diuji dapat dilihat pada tabel 6. Tabel 6 menunjukkan tingkat kerentanan website, di bagi menjadi 3 tingkatan, pertama *high*,

kedua *medium*, dan ketiga *low*, tingkat kerentanan *high* memiliki 2 kerentanan, dan 8 jumlah kerentanan berada di tingkat *medium*.

Tabel 6. Tingkat Kerentanan

No	Tingkat Kerentanan	Jumlah
1	High	2
2	Medium	8
3	Low	0

Selanjutnya untuk mengevaluasi *tools* dan *website* yang di uji kerentanannya, dilakukan *precision rate* berdasarkan tools dan hasil yang di dapatkan dalam website tersebut. Penghitungan *precision rate* menggunakan *tools Subgrraph Vega* dan kerentanan yang di uji adalah *Cross Site Scripting* dan SQL *Injection*, kerentanan dengan tingkat *high*. Hasil dari analisa dapat dilihat pada tabel 7.

Tabel 7. *Precission Rate Scanner*

Scanner	CSS		SQL Injection	
Subgraph Vega	TP	FP	TP	FP
	1	0	10	3

Berdasarkan tabel 7, dapat dilihat perhitungan *precision tools vega*, *True positive* adalah kerentanan di dapatkan dalam hasil *vulnerability scanning* menggunakan subgraph vega, sedangkan *False Positive* adalah adalah kerentanan yang sudah terbukti tidak ada dengan cara check secara manual kerentanan tersebut menggunakan *SQL Map Cross Site Scripting*. Didapatkan *True positive* 1, *False Positive* 1, dan *SQL Injection* di dapatkan *True positive* 10, dan *False Positive* 6. Perhitungan precision / akurasi dapat menggunakan persamaan 1 berikut.

$$Akurasi = \frac{TP}{TP+FP} \quad (1)$$

Akurasi tools *subgraph vega* pada kerentanan *Cross Site Scripting* adalah 100%, sedangkan pada *SQL Injection* adalah 77%.

KESIMPULAN DAN REKOMENDASI

Berdasarkan hasil yang di dapatkan dari proses penelitian pada website www.stephward.co.za menggunakan framework/metode ISSAF maka di temukan hasil kerentanan dengan 2 level, yaitu *high* dengan 2 kerentanan, dan tingkat medium dengan 8 kerentanan. Hasil penelitian yang diperoleh sesuai dengan tujuan penelitan yang di harapkan.

Dari setiap tahap pengujian, di ketahui bahwa website dinilai masih tidak aman untuk digunakan karena masih memiliki kerentanan XSS atau *Cross Site Scripting* dan SQL *Injection*. Kerentanan ini sangat fatal bagi pengguna website tersebut, karena dapat diserang oleh pihak yang tidak bertanggung jawab, dan mengambil informasi pribadi pengguna. Hasil akhir *security assessment* menggunakan *subgraph vega* didapatkan hasil yang bagus dengan tingkat akurasi CSS sebesar 100% dan SQL *Injection* 77%. Untuk melakukan *assessment security* sebaiknya menggunakan lebih dari 1 tools, di karenakan tidak semua hasil scanning tools sama.

REFERENSI

A Kristianto. (2009). Analisis Keamanan Terhadap SQL injection pada web service berbasis representational state transfer.

A Raharja. (2019). Analisis Kerentanan pada Aplikasi E-Voting Menggunakan OWASP Framework.

A Rochman, R Salam, & A Maulana. (2021). Analisis Keamanan Website Dengan Information System Security Assesment Framework dan Open Web Application Security Project. 2.

al Azhar Muhammad. (2012). Digital Forensic Panduan Praktis Investigasi Komputer, Jakarta: Salemba Infotek.

B Kusnandar. (2021). Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di Asia. Https://Databoks.Katadata.Co.Id/Datapublish/2021/10/14/Pengguna-Internet-Indonesia.

B Ratore. (2005). Information System Security Assessment Framework (ISSAF).

Bahrun Ghozali. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode OWASP untuk penilaian Risk Rating.

Cyber Security Assessment. (2022, April 19). Www.Itgid.Org.

D Bernadisman. (2019). Analisis Forensik Basis Data Menggunakan Framework Open WeApplication Security Project (OWASP).

E Alwi, & F Umar. (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning.

E Stefanus, & N Hassanah. (2021). Analisis Keamanan Website Universitas International Batam Menggunakan Metode ISSAF. 9.

F Adi. (2015). Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Sebuah WebServer,. 1.

G Guntoro, & Musfawati Muhammad. (2020). Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF Dan OWASP (Studi Kasus OJS Universitas Lancang Kuning. 5.

G Mahendra. (2021). Penetration Testing Menggunakan Framework ISSAF dan OWASP pada Aplikasi Desa Digital Diskominfo Kabupaten Gianyar. 4.

H Hutagalung, E Nugroho, & R Hidayat. (2017). Analisis Uji Penetrasi Menggunakan ISSAF.

Hasan Muhammad, & S suharmanto. (2021). Keamanan Sistem Perangkat Lunak dengan Secure Software Development Lifecycle. 12.

J Ruhiyat. (2018). Sistem Monitoring Website dengan Metode ISSAF Di Dinas Komunikasi dan Informatika Kabupaten Tanggerang.

K Pertiwi. (2019). Analisa Keamanan Website Dari Serangan Cross Site - Scripting (XXS) Menggunakan Framework OWASP.

OWASP Top 10 : The ten most Critical Web Application Security Risk. (2003).

P Sitorus, & A Habibi. (2020). Teknik Pencegahan Penetrasi SQL Injeksi Dengan Pengaturan Input Type Number dan Batasan Input Pada Form Login Website. 4.

Prasetyo Eko, & Hassanah N. (2021). Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF. 9.

R Widianto. (2020). Analisis Keamanan Website E-Learning SMKN 1 Cibatu.

Ramansyah, Prayudi Yudi, & Riadi Imam. (n.d.). Deteksi Bukti Digital Game Online Pad Platform Skyegrid Menggunakan Framework FRED. JATISI, 8.

S Sanjaya. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. 8.

Sunyoto A, & Pramono Edi. (2021). Deteksi Serangan SQL Injection Menggunakan Hidden Markov Model. 5.

Yunanri, Riadi Imam, & Yudhana Anton. (n.d.). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST). 2.

24% Overall Similarity

Top sources found in the following databases:

- 24% Internet database
- Crossref database
- 0% Submitted Works database
- 10% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	researchgate.net Internet	4%
2	repository.thamrin.ac.id Internet	4%
3	opac.wsb.torun.pl Internet	3%
4	fittechinova.com Internet	2%
5	teknologipintar.org Internet	2%
6	media.neliti.com Internet	1%
7	ejournal.upnvj.ac.id Internet	1%
8	ejurnal.stmik-budidarma.ac.id Internet	1%

9	core.ac.uk Internet	<1%
10	digilib.esaunggul.ac.id Internet	<1%
11	id.wikipedia.org Internet	<1%
12	tugastkj015paisaljega.blogspot.com Internet	<1%
13	easycounter.com Internet	<1%
14	jurnal.stmikroyal.ac.id Internet	<1%
15	ojs.unud.ac.id Internet	<1%
16	ejournal.undiksha.ac.id Internet	<1%
17	eprints.utdi.ac.id Internet	<1%
18	perpustakaansidodadi.com Internet	<1%
19	download.garuda.ristekdikti.go.id Internet	<1%
20	ejournal.akprind.ac.id Internet	<1%

21	pt.scribd.com Internet	<1%
22	Dimas Febriyan Priambodo, Asep Dadan Rifansyah, Muhammad Hasbi.... Crossref	<1%

Excluded from Similarity Report

- Bibliographic material
- Cited material
- Quoted material
- Manually excluded sources

EXCLUDED SOURCES

journal.thamrin.ac.id Internet	98%
elibrary.unikom.ac.id Internet	13%