AITI: Jurnal Teknologi Informasi, Volume 21 No. 1 Maret 2024, 44-57
ISSN 1693-8348 E-ISSN 2615-7128

JURNAL TEKNOLOGI INFORMASI

Uji kerentanan keamanan pada aplikasi berbasis web menggunakan metode *Vulnerability Assessment*

Rissal Efendi [1)], Teguh Wahyono [2)], Indrastanti R. Widiasari [3)]
[1,2,3)]Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
Jl. O Notohamidjojo 1-10, Salatiga, Jawa Tengah
Email: rissal.efendi@uksw.edu

Riwayat Artikel		
Diterima:	Direvisi:	Disetujui:
05-01-2024	20-02-2024	22-02-2024

Abstract

Vulnerability assessment is a process to look for system security gaps that can cause information technology process system failure. In carrying out a vulnerability assessment there are three main stages, namely information collection, assessment and exploit using the Greybone Openvas tool with a Full Scan template on the object and several credentials provided by a website. From the vulnerability assessment process, five vulnerabilities were found on assets, namely critical risk with a few 0, high risk with a few 2, medium risk with a few 2, and low risk with a few 1. Based on the conclusions from the vulnerability analysis the website and the results of identity verification, it was concluded that the website had a few weaknesses and vulnerabilities that needed to be fixed to maintain the security and quality of the website. Corrective actions on website configuration need to be taken such as setting cookies, SSL, HTTP headers, and others. SSL/TLS services do not accurately limit the renegotiation stage of the system, making it easier for attackers to carry out Denial of Service attacks by carrying out many renegotiations in one connection.

Keywords: *Vulnerability assessment, Greybone, security*

Abstrak

Vulnerability assessment merupakan proses untuk mencari celah keamanan sistem yang dapat menyebabkan kegagalan sistem pada proses teknologi informasi. *Vulnerability assessment* terdapat tiga tahapan utama yaitu Pengumpulan informasi, *Assessment* dan *Exploit* dengan menggunakan *tool Greybone Openvas* dengan *template Full Scan* pada obyek, dan beberapa kredensial yang diberikan oleh sebuah aplikasi berbasis web. Proses *vulnerability assessment* ditemukan lima kerentanan pada aset yaitu yang bersifat risiko kritis sejumlah 0, risiko tinggi sejumlah 2, risiko menengah sejumlah 2, dan risiko rendah sejumlah 1. Kesimpulan berdasarkan analisis kerentanan situs web serta hasil verifikasi identitas diperoleh bahwa situs web tersebut memiliki sejumlah kelemahan dan kerentanan yang perlu diperbaiki demi menjaga keamanan dan kualitas situs web. Tindakan perbaikan pada konfigurasi *website* perlu dilakukan seperti pengaturan *cookie*, SSL, *header* HTTP, dan lainnya terutama layanan SSL/TLS. Layanan yang tidak membatasi secara akurat pada tahap negosiasi ulang pada sistem mempermudah penyerang untuk melakukan serangan *Denial of Service* dengan melakukan negosiasi ulang dalam satu koneksi.

Kata kunci: *Vulnerability assessment*, *Greybone*, Keamanan

Pendahuluan

Aplikasi *website* merupakan media penyampaian informasi mengenai profil, visi, misi, jenis produk, dan data perusahaan [1]. Aplikasi berbasis web berorientasi pada tugas aplikasi yang digunakan di web server, hal ini diperlukan untuk menjaga dan melindungi integritas informasi yang disampaikan kepada pengguna *website* [2].

Penggunaan situs web yang semakin banyak semakin mengancam keamanan situs web tersebut, peningkatan serangan dunia maya dan pencurian data *sensitive* merupakan topik utama yang sering dibicarakan saat ini. Laporan *Global* oleh *Cyber Imperva* sepanjang tahun 2020, web keamanan server di dunia meningkat 33% dari tahun 2019 [3]. Pengembang web perlu mempertimbangkan data tersebut dari sisi keamanan dan penilaian risiko dalam merancang sebuah aplikasi berbasis web [4], [5]. Situs web saat pertama kali diluncurkan menjadi target yang menarik untuk penyerang [6]. Pengguna yang menggunakan aplikasi ini juga rentan menjadi target *hacker* untuk mendapatkan data pribadi dan informasi rahasia yang terdapat di dalamnya [7].

Mengidentifikasi dan meminimalkan keamanan ancaman yang dapat menimbulkan risiko, maka perlu dilakukan pengukuran terhadap risiko tersebut. *Vulnerability assessment* merupakan rangkaian kegiatan untuk menilai keamanan aplikasi web. Penilaian dilakukan terhadap keamanan penilaian berorientasi pada risiko [8]. Penilaian ini bertujuan untuk mengidentifikasi celah keamanan dan risiko yang timbul melalui percobaan serangan dalam aplikasi web. Risiko yang ditimbulkan dapat berupa pengambilan informasi esensial atau upaya untuk menggagalkan proses teknologi informasi yang sedang berlangsung. Kegiatan ini dipandang perlu untuk menjaga dan menyempurnakan mekanisme perlindungan keamanan informasi rahasia. Tindakan yang akan dilakukan dalam penilaian ini berupa pencegahan, deteksi, dan penanggulangan [9].

Vulnerability assessment dilakukan untuk mencari celah keamanan sistem yang dapat menyebabkan kegagalan sistem pada proses teknologi informasi. Penyerang akan menemukan celah kemudian akan menentukan cara mengaksesnya, dengan demikian ancaman terhadap kerahasiaan aplikasi meningkat. Penyerang menggunakan beberapa *tools* untuk mengidentifikasi kerentanan aplikasi [10], [11]. Salah satu alat untuk mengidentifikasi kerentanan aplikasi adalah *burpsuit* yang digunakan untuk menemukan celah keamanan pada perangkat lunak atau halaman web. *Tool* ini memungkinkan penyerang menemukan acara untuk melewati keamanan perangkat lunak atau halaman web [12], [13].

Penyerang telah menemukan celah keamanan, langkah selanjutnya adalah melakukan penetrasi. *Penetration Testing* merupakan cara untuk mengidentifikasi celah keamanan pada implementasi mekanisme keamanan sistem. Kegiatan ini dilakukan dengan menyerang sistem komputer untuk menemukan kelemahan

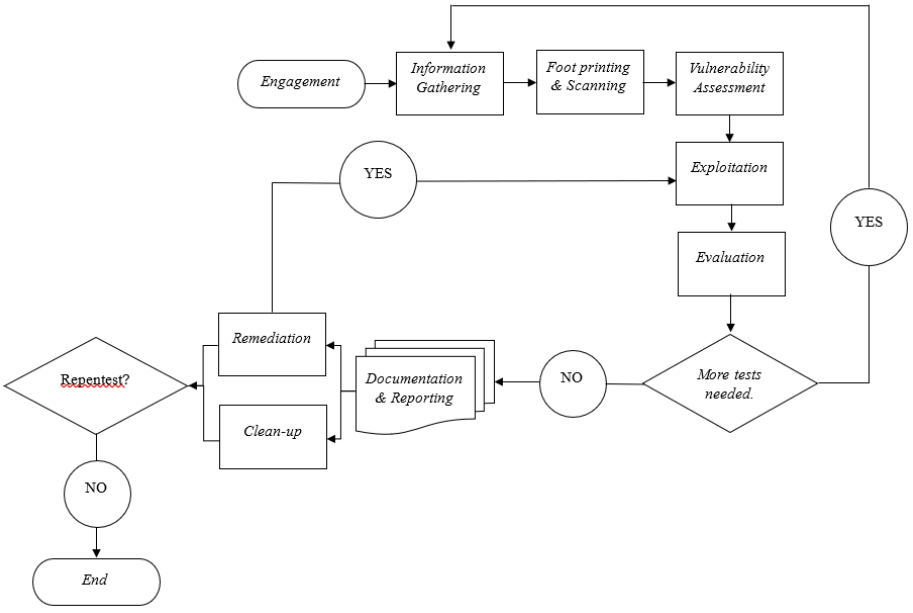
keamanan untuk mendapatkan akses ke fungsi dan datanya [14], [15]. Hasil simulasi penyerangan ini kemudian didokumentasikan dan disajikan sebagai laporan kepada pihak pemangku kepentingan terkait. Lembaga pendidikan dapat menggunakan makalah ini sebagai bahan evaluasi untuk perbaikan keamanan pada aplikasi web repositori mereka.

Menjaga keamanan informasi pada webserver terdapat tiga hal yang harus diperhatikan yaitu kerahasiaan *(confidentiality)*, menjaga kerahasiaan informasi dari orang yang tidak berwenang, integritas data *(integrity)*, yang mencegah data diubah oleh orang yang tidak berwenang dan ketersediaan *(availability)* data yang tersedia. Langkah-langkah dalam melakukan penilaian kerentanan adalah deteksi kerentanan (mengidentifikasi kerentanan dengan membuat daftar kerentanan sistem), analisis (menentukan masalah apa yang didasarkan pada hasil deteksi), prioritas (mengevaluasi risiko yang ditemukan dan kemudian mengklasifikasikannya sebagai tinggi atau lebih serius), remediasi (menerapkan tindakan korektif atau menangani kerentanan yang ditemukan berdasarkan nilai prioritas).

Langkah penilaian kerentanan diharapkan menjadi sebuah awal persiapan serangan untuk menghidanri konsekuensi yang fatal. Adanya aktivitas yang tidak normal pada sebuah aplikasi berbasis web mendorong dilakukannya *Vulnerability Assessment* secara menyeluruh pada aplikasi web tersebut.

Metode Penelitian

Metode penelitian yang dilakukan terlihat pada Gambar 1 Metode Penelitian



Gambar 1 Metode Penelitian

Metodologi standar pengujian yang dilakukan dalam penilitian ini adalah *vulnerability assessment*. *Vulnerability assessment* memiliki beberapa langkah-langkah yang harus dilakukan adalah langkah persiapan, langkah pemindaian, langkah evaluasi, langkah pelaporan dan langkah tindakan perbaikan.

Langkah pertama adalah persiapan (identifikasi sumber daya, alat dan metode). Identifikasi sumber daya pada tahap ini dilakukan untuk menentukan apa yang akan dievaluasi, hal ini bisa mencakup jaringan, aplikasi, sistem operasi, perangkat keras, dan perangkat lunak yang ada. Alat dan metode pada tahap ini dilakukan untuk menentukan alat yang akan digunakan untuk penilaian kerentanan. Alat populer termasuk *Nessus*, *OpenVAS*, *Nmap*, selain itu dimungkinkan juga dapat menggunakan pendekatan manual atau kombinasi dari kedua metode.

Langkah kedua adalah pemindaian (pemindaian dan identifikasi kerentanan). Pemindaian dilakukan dengan cara menggunakan *tool* yang telah dipilih untuk melakukan pemindaian terhadap sumber daya yang telah diidentifikasi. Pemindaian dapat dilakukan secara internal (dari dalam jaringan) atau eksternal (dari luar jaringan). Identifikasi kerentanan dilakukan setelah pemindaian selesai, identifikasi kerentanan yang ada dalam sistem, seperti celah keamanan, versi perangkat lunak yang kadaluwarsa, konfigurasi yang rentan, atau kelemahan dalam jaringan.

Langkah ketiga adalah evaluasi (prioritas kerentanan, Analisis dan verifikasi). Prioritaskan kerentanan berdasarkan hasil pemindaian, tentukan kerentanan mana yang paling kritis atau memiliki potensi dampak terbesar. Pada tahap ini, kerentanan diberi peringkat berdasarkan tingkat risiko dan dampaknya terhadap keamanan. Analisis dan verifikasi, langkah ini untuk memastikan bahwa kerentanan yang diidentifikasi adalah valid serta melakukan verifikasi untuk memastikan bahwa kerentanan yang dilaporkan benar-benar ada dan dapat dieksploitasi.

Langkah keempat pelaporan (dokumentasi hasil dan komunikasi hasil). Pada tahap ini dilakukan pendokumentasian hasil, membuat laporan yang merinci semua kerentanan yang ditemukan beserta rekomendasi perbaikan yang diperlukan. Tahap selanjutnya yaitu komunikasikan hasil, laporan hasil *vulnerability assessment* disampaikan kepada pemangku kepentingan yang relevan. Hal ini bisa termasuk tim keamanan, manajemen TI, atau pemilik sistem yang terpengaruh.

Langkah kelima tindakan perbaikan (perbaiki kerentanan dan lakukan pemantauan dan ulangi). Perbaiki kerentanan yang dilakukan adalah perbaikan terhadap kerentanan yang telah diidentifikasi, dapat berupa pembaruan perangkat lunak, konfigurasi ulang, atau penerapan tindakan korektif lainnya. Lakukan Pemantauan dan ulangi, setelah melakukan perbaikan monitor sistem untuk

memastikan bahwa kerentanan telah ditangani. Lakukan evaluasi ulang secara berkala untuk memastikan tidak ada kerentanan baru yang muncul.

Hasil dan Pembahasan

Tujuan yang ingin dicapai dalam kegiatan *vulnerability assessment* ini yaitu untuk mengidentifikasi kerentanan apa saja yang saat ini masih ada pada *network environment* organisasi perusahaan sehingga prinsip CIA (*Confidentiality, Integrity, Availability*) dapat terjaga. Secara spesifik tujuan dari dilakukannya kegiatan ini yaitu pertama untuk mengidentifikasi dan dalam usaha menutup celah keamanan yang terdapat pada aplikasi, infrastruktur maupun sistem sebelum ditemukan oleh pihak yang tidak berwenang. Kedua dapat mengidentifikasi risiko yang ditimbulkan akibat dari celah keamanan aplikasi, infrastruktur maupun sistem terhadap bisnis perusahaan serta memberikan rekomendasi mitigasinya dan ketiga dapat menerapkan keamanan informasi dengan standar yang telah diakui secara internasional.

Langkah pertama yang dilakukan untuk mencapai tujuan tersebut yaitu mendapatkan *List* Aset *vulnerability assessment*. *Vulnerability assessment* yang dilakukan mencakup sejumlah aset yang penting bagi kegiatan operasional dan bisnis yang dimiliki. Metode yang digunakan adalah penggunaan *tool vulnerability assessment*: *Greybone Openvas* dengan *template Full Scan*. Hasil yang diperoleh dari Aktivitas Vulnerability *Assessment* yang dilakukan yaitu didapatkan nilai dengan tingkat keparahan yang tinggi, menengah dan rendah.

Hasil *vulnerability assessment* dengan tingkat keparahan tinggi ditunjukkan pada Tabel 1 Masalah dengan tingkat keparahan tinggi MS15-034 HTTP.sys kerentanan eksekusi remote codedan Tabel 2 Masalah dengan tingkat keparahan tinggi SSL/TLS: report vulnerable cipher suites for HTTPS.

Tabel 1 Masalah dengan tingkat keparahan tinggi *MS15-034 HTTP.sys* kerentanan eksekusi *remote code*

Title	NVT: MS15-034 HTTP.sys Kerentanan Eksekusi *Remote Code* (Pemeriksaan Aktif)
Risiko	Tinggi
Status	*Open*
Url	*Service cpe:/a: microsoft: internet_information_services*:8.5 Terdeteksi oleh *Microsoft Internet Information Services* (IIS) *Detection* (HTTP)
Deskripsi	• Metode Deteksi Kerentanan: kirim permintaan *HTTP GET* yang dibuat khusus dan periksa responsnya. *Details*: *MS15-034 HTTP.sys* Kerentanan Eksekusi *Remote Code* (Pemeriksaan Aktif) OID:1.3.6.1.4.1.25623.1.0.105257. Versi yang digunakan: 2023-10-10T05:05:41Z. • *Vulnerability Insight*: cacat terjadi karena tumpukan protokol *HTTP 'HTTP.sys'* yang dipicu saat menguraikan HTTP *request*.

Dampak	Eksploitasi yang berhasil akan memungkinkan penyerang jarak jauh menjalankan *arbitrary code* dalam konteks pengguna saat ini dan melakukan tindakan dalam konteks keamanan pengguna saat ini.
Solusi	Tipe solusi: *VendorFix* Vendor telah merilis pembaruan/*update*. Perangkat Lunak/OS yang terpengaruh: MS *Windows* 8 x32/x64, MS *Windows* 8.1 x32/x64, MS *Windows* Server 2012, MS Windows Server 2012 R2, MS *Windows* Server 2008 x32/x64 SP 2 *and prior*, MS *Windows* 7 x32/x64 S P 1 *and prior*
Referensi	cve: CVE-2015-1635 cisa: katalog *Known Exploited Vulnerability* (KEV). url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog url: https://support.microsoft.com/kb/3042553 url: https://technet.microsoft.com/library/security/MS15-034 url: http://pastebin.com/ypURDPc4 cert-bund: CB-K15/0527 dfn-cert: DFN-CERT-2015-0545

Dari Tabel 1 Masalah dengan tingkat keparahan tinggi MS15-034 HTTP.sys kerentanan eksekusi remote codedapat dijelaskan bahwa metode *vulnerability* yang dilakukan dengan cara HTTP *GET Request* dan kemudian mendapatkan *reply* dari server kemudian memeriksa hasil *reply* yang dikirimkan dari server tersebut. Pemeriksaan tersebut didapatkan informasi adanya tumpukan *HTTP.sys* yang dipicu saat *HTTP GET Request* dikirimkan. Hal ini menyebabkan jika terjadi eksploitasi maka akan memungkinkan penyerang menjalankan kode arbitrer dalam konteks pengguna dan melakukan tindakan dalam konteks keamanan pengguna saat ini.

Tabel 2 Masalah dengan tingkat keparahan tinggi SSL/TLS: *report vulnerable cipher suites* for HTTPS

Title	NVT: SSL/TLS: *Report Vulnerable Cipher Suites for* HTTPS
Risiko	Tinggi
Status	*Open*
Url	-
Deskripsi	• Metode Deteksi Kerentanan: Detail: SSL/TLS: Report *Vulnerable Cipher Suites for* HTTPS OID:1.3.6.1.4.1.25623.1.0.108031 Versi yang digunakan: 2023-07-20T05:05:17Z • *Vulnerability Insight*: Aturan ini diterapkan untuk evaluasi rangkaian sandi yang rentan: 64-bit *block cipher* 3DES yang rentan terhadap serangan SWEET32 (CVE-2016-2183).
Dampak	Rutin akan melaporkan *cipher suite* SSL/TLS yang diterima oleh layanan dengan vektor serangan yang hanya ada pada layanan HTTPS. Hasil Deteksi Kerentanan: *'Vulnerable' cipher suites* diterima layanan ini melalui protokol TLSv1.0: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) Rangkaian sandi ' *Vulnerable* ' diterima oleh layanan ini melalui protocol TLSv1.1: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

	Rangkaian sandi ' *Vulnerable* ' diterima oleh layanan ini melalui protokol TLSv1.2: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
Solusi	Tipe Solusi: Mitigasi Konfigurasi diubah agar tidak lagi menerima *cipher suite* yang terdaftar.
Referensi	cve: CVE-2016-2183 cve: CVE-2016-6329 cve: CVE-2020-12872 url: https://bettercrypto.org/ url: https://mozilla.github.io/server-side-tls/ssl-config-generator/ url: https://sweet32.info/

Dari Tabel 2 Masalah dengan tingkat keparahan tinggi SSL/TLS: report vulnerable cipher suites for HTTPS dapat dijelaskan bahwa penggunaan protokol TLSv1.0 dan/atau TLSv1.1 yang tidak digunakan lagi dapat dideteksi pada sistem ini. TLSv1.2+, *service* ini juga menyediakan protokol TLSv1.0 dan TLSv1.1 yang tidak digunakan lagi dan mendukung enkripsi apapun. *Cipher* yang didukung dapat ditemukan di SSL/TLS: Laporan didukung *Cipher Suites*' (OID: 1.3.6.1.4.1 .25623.1.0.802067) VT. Hal tersebut mengakibatkan bahwa Protokol TLSv1.0 dan TLSv1.1 berisi kriptografi yang dikenal seperti: CVE-2011-3389: Eksploitasi *Browser* Terhadap SSL/TLS (BEAST), CVE-2015-0204:

Tabel 3 Masalah dengan keparahan tingkat menengah SSL/TLS: laporan *vulnerable cipher suites* untuk HTTPS

Title	NVT: c
Risk	Medium
Status	*Open*
Url	-
Deskripsi	• Penggunaan protokol TLSv1.0 dan/atau TLSv1.1 yang tidak digunakan lagi dapat dideteksi pada sistem ini. • Selain TLSv1.2+, layanan ini juga menyediakan protokol TLSv1.0 dan → TLSv1.1 yang tidak digunakan lagi dan mendukung satu atau lebih sandi. *Cipher* yang didukung tersebut c →dan dapat ditemukan di 'SSL/TLS: Laporan didukung *Cipher* Suites' (OID: 1.3.6.1.4.1 →.25623.1.0.802067) VT. • *Vulnerability Insight*: Protokol TLSv1.0 dan TLSv1.1 berisi aws kriptografi yang dikenal seperti: CVE-2011-3389: Eksploitasi *Browser* Melawan SSL/TLS (*BEAST*), CVE-2015-0204: Memfaktorkan Serangan pada Kunci RSA-EKSPOR Padding Oracle Pada *Downgraded Legacy Encryption* (FREAK)
Dampak	Rutin ini akan melaporkan semua *cipher suite* SSL/TLS yang diterima oleh layanan vektor serangan yang terdapat pada layanan HTTPS. Hasil Deteksi Kerentanan: *Cipher suite* 'Rentan' diterima oleh layanan ini melalui protokol TLSv1.0: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32) *Cipher suite* 'Rentan' diterima oleh layanan ini melalui protokol TLSv1.1: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

	Rangkaian sandi 'Rentan' yang diterima oleh layanan ini melalui protokol TLSv1.2: TLS_RSA_WITH_3DES_EDE_CBC_SHA (MANIS32)
Solusi	Tipe Solusi: Mitigasi Disarankan untuk menonaktifkan protokol TLSv1.0 dan/atau TLSv1.1 yang tidak digunakan lagi dan mendukung protokol TLSv1.2+.
Referensi	cve: CVE-2011-3389 cve: CVE-2015-0204 url: https://ssl-config.mozilla.org/ url: https://bettercrypto.org/ url: https://datatracker.ietf.org/doc/rfc8996/ url: https://vnhacker.blogspot.com/2011/09/beast.html url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters

Dari Tabel 3 Masalah dengan keparahan tingkat menengah SSL/TLS: laporan vulnerable cipher suites untuk HTTPSdapat dijelaskan bahwa layanan SSL/TLS jarak jauh tidak membatasi dengan akurat negosiasi ulang yang dimulai oleh klien dalam protokol SSL dan TLS. CVE (*Vulnerabilities and Exposures*) yang direferensikan adalah *Open* SSL dan *Mozilla Network Security Services* (NSS) yang bertanggung jawab terhadap penerapan server untuk membatasi negosiasi ulang jika hal tersebut tidak sesuai dalam lingkungan tertentu. Hal ini bisa diatasi dengan adanya pemeriksaan terhadap layanan jarak jauh yang mengizinkan untuk melakukan kembali pertukaran SSL/TLS yang sama (Negosiasi Ulang) melalui koneksi SSL/TLS yang sudah ada atau sudah dibuat.

Tabel 4 Masalah dengan keparahan tingkat menengah SSL/TLS: *renegotiation* DoS *vulnerability* (CVE-2011-1473, CVE-2011-5094)

Title	NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)
Risiko	Medium
Status	*Open*
Url	-
Deskripsi	• *Vulnerability Detection Result*. Berikut ini menunjukkan bahwa layanan SSL/TLS jarak jauh terpengaruh: Protocol *Version* | *Successful* re-*done* SSL/TLS handshakes (*Renegotiation*) melalui → koneksi SSL/TLS yang ada/sudah dibuat • *Vulnerability Insight*: VA ada karena layanan SSL/TLS jarak jauh tidak membatasi dengan benar negosiasi ulang yang dimulai oleh klien dalam protokol SSL dan TLS. Catatan: CVE yang direferensikan memengaruhi *OpenSSL* dan Mozilla *Network Security Services* (NSS) namun keduanya berada dalam status *DISPUTED.* Dapat juga dikatakan bahwa *responsibility* penerapan server, bukan sebuah *security library*, adalah untuk mencegah atau membatasi negosiasi ulang ketika dalam kondisi tidak pantas dalam lingkungan tertentu. Kedua CVE disimpan dalam VT ini sebagai acuan asal usul dari VA ini. • *Vulnerability Detection Method*: Memeriksa apakah layanan jarak jauh mengizinkan untuk melakukan kembali SSL/TLS *handshake* (Re-negosiasi) melalui koneksi SSL/TLS yang sudah ada/sudah dibuat.

Dampak	Mereka mungkin mempermudah remote a*ttacker* untuk menyebabkan DoS (konsumsi CPU) dengan melakukan banyak negosiasi ulang dalam koneksi tunggal. Layanan *remote* SSL/TLS rentan terhadap *denial of service* (DoS) *vulnerability*.
Solusi	Tipe Solusi: *VendorFix* Pengguna harus menghubungi vendor mereka untuk informasi *patch* tertentu. Solusi umum adalah menghapus/menonaktifkan kemampuan negosiasi ulang dari/dalam layanan SSL/TLS yang terpengaruh.
Referensi	cve: CVE-2011-1473 cve: CVE-2011-5094 url: https://orchilles.com/ssl-renegotiation-dos/ url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/ url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation url: https://www.openwall.com/lists/oss-security/2011/07/08/2 url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation

Tabel 4 Masalah dengan keparahan tingkat menengah SSL/TLS: renegotiation DoS vulnerability (CVE-2011-1473, CVE-2011-5094)dapat dijelaskan bahwa layanan SSL/TLS jarak jauh tidak membatasi dengan akurat negosiasi ulang yang dimulai oleh klien dalam protokol SSL dan TLS. CVE (*Vulnerabilities and Exposures*) yang direferensikan adalah *OpenSSL* dan *Mozilla Network Security Services* (NSS) yang bertanggung jawab terhadap penerapan server untuk membatasi negosiasi ulang jika hal tersebut tidak sesuai dalam lingkungan tertentu. Hal ini bisa diatasi dengan adanya pemeriksaan terhadap layanan jarak jauh yang mengizinkan untuk melakukan kembali pertukaran SSL/TLS yang sama (Negosiasi Ulang) melalui koneksi SSL/TLS yang sudah ada/sudah dibuat.

Tabel 5 Masalah dengan keparahan tingkat rendah

Title	NVT: TCP Timestamps Information Disclosure
Risiko	*Low*
Status	*Open*
Url	-
Deskripsi	• *Vulnerability Detection Result*: Terdeteksi bahwa host mengimplementasikan RFC1323/RFC7323. *Timestamps* berikut diambil dengan jeda 1 detik di antaranya: *Packet* 1: 704442284 dan *Packet* 2: 704442420 • *Vulnerability Detection Method*: Paket IP khusus dipalsukan dan dikirim dengan sedikit penundaan di antara IP target. Responsnya dicari *timestamp*-nya. Jika ditemukan, *timestamp*-nya dilaporkan. • *Vulnerability Insight*: *Remote host* mengimplementasikan TCP *timestamp*, sebagaimana ditentukan oleh RFC1323/RFC7323.
Dampak	*A side e ect of this feature is that the uptime of the remote host can sometimes be computed. The remote host implements TCP timestamps and therefore allows to compute the uptime.*

Solusi	*Solution type*: Mitigation Men-*disable* TCP *timestamps* pada Linux tambahkan baris 'net.ipv4.tcp_timestamps = 0' ke /etc/sysctl.conf. Execute 'sysctl -p' untuk menerapkan settings pada *runtime*. Men-*disable* TCP timestamps pada Windows, jalankan 'netsh int tcp set global *timestamps=disabled'* Dimulai pada Windows Server 2008 dan Vista, *timestamp* tidak dapat di-*disable* sama sekali. Perilaku *default* pada TCP/IP *stack* pada *System* ini adalah tidak menggunakan opsi *Timestamp* Ketika memulai koneksi TCP tetapi menggunakannya jika TCP *peer* yang memulai komunikasi memasukkannya ke segmen *synchronize* (SYN).
Referensi	url: https://datatracker.ietf.org/doc/html/rfc1323 url: https://datatracker.ietf.org/doc/html/rfc7323 url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

Dari Tabel 5 Masalah dengan keparahan tingkat rendahdapat dijelaskan proses *vulnerability assessment* ini mendeteksi bahwa server mengimplementasikan RFC1323/RFC7323 yang merupakan pengembangan protocol TCP tentang timestamp untuk meningkatkan kinerja dan keandalan saat transmisi data. *Timestamp* diambil dengan jeda 1 detik di antaranya: paket 1: 704442284 dan paket 2: 704442420, Deteksi pada tahap ini dilakukan dengan cara mengirimkan dan memalsukan IP dari paket data dengan sedikit penundaan menuju IP target. Hal ini mengakibatkan *uptime* dari *host* target dapat dihitung kemudian *host* target mengimplementasikan *timestamp* TCP sehingga memungkinkan untuk menghitung waktu aktif pengiriman paket data. Solusi yang bisa diambil adalah dengan men-*disable timestamp* namun lebih menggunakan TCP *peer* untuk memulai komunikasi data mulai dari inisiasi pengiriman *(SYN)* pada proses *three-way handshake.*

Pekerjaan yang dilakukan selalu disertakan nilai risiko untuk setiap temuan yang telah berhasil diidentifikasi. Terkait dengan penilaian nilai risiko, setiap aset akan memiliki nilai risiko yang berbeda-beda. Hal tersebut menjadi penentu untuk menyusun beberapa faktor berdasarkan *best practice* yang dapat menjadi perhitungan untuk menilai risiko keamanan yang terdapat pada suatu system.

Arah serangan *(Path of Attack)* pada bagian ini arah serangan menjadi salah satu penentu dalam perhitungan risiko suatu serangan. Semakin jauh seorang *attacker* mengeksekusi serangannya, maka semakin tinggi pula nilai risiko yang ditimbulkannya. Bagian yang menjadi penilaian pada poin ini adalah arah serangan melalui jaringan eksternal (*external network*), jaringan internal (*internal network*), akses lokal (memerlukan *credential* dalam mengeksploitasi), dan terakhir adalah serangan melalui akses fisik (*physical access*).

Kompleksitas serangan *(Complexity of Attack)* poin ini merupakan poin yang terbilang subyektif jika dilihat secara global. Umumnya, hal yang menjadi pembeda antara sulit dan mudahnya kompleksitas serangan ini adalah dibutuhkan atau tidaknya kemampuan pemrograman di dalam mengeksekusi serangan. Poin ini sendiri dapat dihasilkan dari berbagai sudut pandang, yaitu dari sudut padang kacamata auditor secara umum, atau dapat juga dari sudut pandang internal yaitu yang dinilai oleh auditor independen.

Kebutuhan Hak Akses *(Privileges Required)* poin ini mengambil bagian dari sisi keperluan akses untuk mengeksploitasi sistem tertentu. Bagian yang menjadi penilaian di dalam poin ini adalah tidak dibutuhkannya akses, dibutuhkannya akses level rendah, dan juga dibutuhkannya akses level tinggi.

Interaksi dari pengguna *(Interaction from Users)*, beberapa celah keamanan baru dapat dieksekusi oleh *attacker* ketika mereka memperoleh interaksi dari *user* seperti model serangan Java Applet. Bagian yang dapat mempengaruhi suatu nilai risiko pada poin ini yaitu diperlukannya interaksi dan tidak diperlukannya interaksi dari pengguna *(user).*

Perubahan area hasil serangan *(Scope of Attack),* faktor ini dikhususkan untuk melihat perubahan yang dapat dilakukan oleh *attacker* ketika telah berhasil memasuki suatu sistem. Contoh dalam hal ini, yaitu seorang *attacker* dapat masuk kedalam segmen lain yang seharusnya telah dibatasi di dalam konfigurasi yang ada. Bagian yang berpengaruh di dalam penilaian risiko untuk point ini yaitu terkait dengan berhasil tidaknya attacker melompat ke dalam area yang tidak ditempati oleh target.

Confidentiality, Integrity, dan *Availability* (CIA), sama seperti halnya poin nomor dua (2) pada faktor penentu nilai risiko ini. Jika diukur dari sudut pandang auditor poin ini bersifat subyektif tanpa data yang pasti. Bagian ini memerlukan koordinasi dari klien untuk mengetahui lebih lanjut mengenai kategori data/informasi yang termasuk *confidential*, kategori lama waktu untuk *downtime*, serta definisi gangguan integritas dari setiap klien.

Tabel 6 Model risiko

Risk Factor	***Path of Attack***	***Complexity of Attack***	***Privileges Required***	***Interaction from Users***	***Scope of Attack***	**CIA**
First Situation	*External Network*	*Low*	*None*	*No*	*Changed*	*High*
Second Situation	*Internal Network*	*High*	*Low*	*Yes*	*Unchanged*	*Low*
Third Situation	*Local Access*	*N/A*	*High*	*N/A*	*N/A*	*None*
Fourth Situation	*Physical Access*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*

Model risiko seperti Tabel 6 Model risiko, maka klien pun dapat menentukan prioritas dari setiap temuan berdasarkan risiko yang ada yang telah diperoleh selama hasil pengujian. Skala penilaian yang digunakan adalah nilai dari skala 0–10. Masing-masing nilai skor ditunjukkan pada Tabel 7 Skor penilaian. Deskripsi tentang skor pada Tabel 7 Skor penilaian, dapat dijelaskan pada Tabel 8 Risk level description.

Tabel 7 Skor penilaian

	High	***Moderate to High***	***Moderate***	***Low to Moderate***	***Low***
Scores	9.0–10.0	7.0–8.9	4.0–6.9	0.1–3.9	0

Tabel 8 *Risk level description*

Level Risiko	**Deskripsi**
LOW	Konfigurasi yang tidak sesuai dengan *best practice security* yang ada.
LOW TO MODERATE	Seorang *attacke*r dapat mengumpulkan informasi yang sensitif seperti versi *software* yang ter*install*. Memakai informasi ini, a*ttacker* dapat dengan mudah meng-eksploitasi kerentanan versi *software* tersebut.
MODERATE	Seorang *attacker* dapat memperoleh akses terhadap informasi yang spesifik pada *host*, termasuk konfigurasi keamanan yang ada di dalamnya. Hal ini berpotensi untuk penyalahgunaan *host*. *Severity* level ini diantaranya, dapat diaksesnya file pada sebuah *host*, *directory browsing*, *filtering rules* dari konfigurasi keamanan, serangan *denial-of-service*, dan penggunaan *service* oleh pihak yang tidak mempunyai otorisasi seperti *mail-relaying*.
MODERATE TO HIGH	Seorang *attacker* dapat memperoleh kontrol terhadap *host* dan menyebabkan kebocoran informasi yang sangat sensitif, akses "*read*" penuh terhadap sebuah *file*, *backdoors*, dan mendapatkan daftar *user* pada sebuah *host*.
HIGH	Seorang *attacker* dapat dengan mudah mengambil alih *host*. *Severity* level ini dapat menyebabkan terkomprominya seluruh jaringan infrastruktur, akses *"read"* dan *"write"* terhadap sebuah *file*, *backdoors*, dan mengeksekusi c*ommand* secara *remote.*

Simpulan

Hasil penelitian yang telah dilakukan maka dihasilkan data *vulnerability assessment* beserta dengan rekomendasi dan cara mitigasi terhadap kerentanan baik yang bersifat kritis, tinggi, menengah dan rendah pada asset yang dimiliki. Proses *vulnerability assessment* tersebut ditemukan empat kerentanan pada asset yaitu yang bersifat memiliki risiko tinggi sejumlah 2, risiko menengah sejumlah 2, dan risiko

rendah sejumlah 1. Berdasarkan kesimpulan dari analisis kerentanan situs dan hasil verifikasi identitas, diperoleh kesimpulan bahwa situs web tersebut memiliki sejumlah kelemahan dan kerentanan yang perlu diperbaiki demi menjaga keamanan dan kualitas situs web tersebut. Tindakan perbaikan pada konfigurasi website perlu dilakukan seperti pengaturan *cookie*, SSL dan *header* HTTP. Selain itu, layanan SSL/TLS yang tidak membatasi secara akurat pada setiap tahap negosiasi ulang pada komunikasi data akan mempermudah penyerang untuk melakukan serangan *Denial of Service* dengan melakukan banyak negosiasi ulang dalam satu koneksi

Daftar Pustaka

[1] D. Arnaldy and A. R. Perdana, "Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack," in *2019 2nd International Conference of Computer and Informatics Engineering (IC2IE)*, IEEE, Sep. 2019, pp. 188–192. doi: 10.1109/IC2IE47452.2019.8940872.

[2] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack," *Journal of Computer Networks and Communications*, vol. 2019, pp. 1–10, Jan. 2019, doi: 10.1155/2019/1283472.

[3] V. K. Malviya, S. Rai, and A. Gupta, "Development of web browser prototype with embedded classification capability for mitigating Cross-Site Scripting attacks," *Appl Soft Comput*, vol. 102, p. 106873, Apr. 2021, doi: 10.1016/j.asoc.2020.106873.

[4] S. M. Toapanta, O. A. Escalante Quimis, L. E. M. Gallegos, and M. R. Maciel Arellano, "Analysis for the Evaluation and Security Management of a Database in a Public Organization to Mitigate Cyber Attacks," *IEEE Access*, vol. 8, pp. 169367–169384, 2020, doi: 10.1109/ACCESS.2020.3022746.

[5] R. U. Surian, N. A. A. Rahman, and Y. Nathan, "Nscanner: Vulnerabilities Detection Tool for Web Application," *J Phys Conf Ser*, vol. 1712, 2020, [Online]. Available: https://api.semanticscholar.org/CorpusID:234543649

[6] S. M. T. Toapanta, I. N. C. Ochoa, R. A. N. Sanchez, and L. E. G. Mafla, "Impact on Administrative Processes by Cyberattacks in a Public Organization of Ecuador," in *2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4)*, IEEE, Jul. 2019, pp. 270–274. doi: 10.1109/WorldS4.2019.8903967.

[7] Q. Chen, "Research on the Implementation Method of Database Security in Management Information System Based on Big Data Analysis," *E3S Web of Conferences*, vol. 185, p. 02033, Sep. 2020, doi: 10.1051/e3sconf/202018502033.

[8] A. K. Priyanka and S. S. Smruthi, "WebApplication Vulnerabilities:Exploitation and Prevention," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, IEEE, Jul. 2020, pp. 729–734. doi: 10.1109/ICIRCA48905.2020.9182928.

[9] D. Dalalana Bertoglio and A. F. Zorzo, "Overview and open issues on penetration test," *Journal of the Brazilian Computer Society*, vol. 23, no. 1, p. 2, 2017, doi: 10.1186/s13173-017-0051-1.

[10] A. Jamil, K. Asif, R. Ashraf, S. Mehmood, and G. Mustafa, "A comprehensive study of cyber attacks & counter measures for web systems," in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, New York, NY, USA: ACM, Jun. 2018, pp. 1–7. doi: 10.1145/3231053.3231116.

[11] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," in *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, IEEE, Aug. 2017, pp. 1–6. doi: 10.1109/ICCUBEA.2017.8463920.

[12] C. O. N. Susanto, K. N. F. Rizko, and D. Purbohadi, "Security Assessment Using Nessus Tool to Determine Security Gaps on the Repository Web Application in Educational Institutions," *Emerging Information Science and Technology*, vol. 1, no. 2, 2020, doi: 10.18196/eist.128.

[13] E. A. Altulaihan, A. Alismail, and M. Frikha, "A Survey on Web Application Penetration Testing," *Electronics (Basel)*, vol. 12, no. 5, p. 1229, Mar. 2023, doi: 10.3390/electronics12051229.

[14] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," in *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, IEEE, Aug. 2017, pp. 1–6. doi: 10.1109/ICCUBEA.2017.8463920.

[15] A. Ifeyinwa, A. Sunday, and E. Pater, "Network Vulnerability Analysis," *International Journal of Computer*, [Online]. Available: http://ijcjournal.org/