JIKOM: JURNAL ILMU KOMPUTER
Volume 2 Nomor 1, Juli, 2024
ISSN: 3031-125X (ONLINE)
Penerbit: Program Studi Teknik Informatika S-2 Universitas Pamulang

Analisis Vulnerabilitas Situs Web Universitas Pamulang Menggunakan Nessus

* Asep Herman Nursalam [1], R.P. Fiki Wisnu Subekti [2], Astried Nirmala Safitri [3], Yossy Veifbrian Fitri Prasmono [4], Adila Indriyani Otafiyani [5]

[1,2,3,4,5)] Teknik Informatika, Program Pascasarjana, Universitas Pamulang, Kota Tangerang Selatan, Banten

Email: [1] asephnursalam@gmail.com, [2] fikiwisnu90@gmail.com, [3] astriednirmala@gmail.com, [4] yossyveif@gmail.com, [5] adillaindriyani22@gmail.com

ABSTRACT

The Pamulang University (UNPAM) website is an official website that is used for various purposes. Therefore, website security needs to be maintained so that it is not exploited by irresponsible parties. Vulnerability analysis is one way to find out the vulnerabilities that exist in a system. This research aims to conduct vulnerability analysis on the UNPAM website using Nessus. The research results show that the UNPAM website has a high level of vulnerability. This is indicated by the existence of high and medium levels of vulnerability. These vulnerabilities can be exploited by irresponsible parties to attack the UNPAM website. To mitigate these vulnerabilities, UNPAM website managers can take preventative steps by upgrading to a cipher suite with a key length of 128 bits or more, verifying the authenticity of the SSL certificate, enabling DNSSEC and implementing a DNSSEC-enabled resolver, using a DNS firewall, and disabling TLS 1.0 and enabling TLS 1.2 or higher version.

Keywords: Vulnerability Analysis; *Vulnerability Assesment*; *Nessus; Website*

ABSTRAK

Situs web Universitas Pamulang (UNPAM) merupakan situs web resmi yang digunakan untuk berbagai keperluan. Oleh karena itu, keamanan situs web perlu dijaga agar tidak dimanfaatkan oleh pihak yang tidak bertanggung jawab. *Vulnerability analysis* merupakan salah satu cara untuk mengetahui kerentanan yang ada pada suatu sistem. Penelitian ini bertujuan untuk melakukan analisis kerentanan pada situs web UNPAM menggunakan Nessus. Hasil penelitian menunjukkan bahwa situs web UNPAM memiliki tingkat kerentanan yang tinggi. Hal ini ditunjukkan dengan adanya kerentanan dengan tingkat *high* dan *medium*. Kerentanan-kerentanan tersebut dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan terhadap situs web UNPAM. Untuk mengurangi kerentanan tersebut, pengelola situs web UNPAM dapat melakukan langkah pencegahan dengan meningkatkan ke *cipher suite* dengan panjang kunci 128 bit atau lebih, memverifikasi keaslian sertifikat SSL, mengaktifkan DNSSEC dan menerapkan *resolver* yang diaktifkan DNSSEC, menggunakan *firewall* DNS, dan menonaktifkan TLS 1.0 dan mengaktifkan TLS 1.2 atau versi yang lebih tinggi.

Kata kunci: *Vulnerability Analysis*; *Vulnerability Assesment*; Nessus; Situs Web

1. PENDAHULUAN

Situs web merupakan salah satu sarana komunikasi dan informasi yang penting di era digital saat ini. Situs web digunakan untuk berbagai keperluan, seperti informasi akademik, pengumuman, kegiatan, dan lain-lain. Oleh karena itu, keamanan situs web perlu dijaga agar tidak dimanfaatkan oleh pihak yang tidak bertanggung jawab [1].

Kerentanan (*vulnerability*) merupakan kelemahan atau kekurangan pada suatu sistem yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan. Kerentanan pada situs web dapat berupa celah keamanan pada *software*, konfigurasi yang tidak aman, atau kesalahan desain [2].

Vulnerability analysis merupakan salah satu cara untuk mengetahui kerentanan yang ada pada suatu sistem. Nessus merupakan salah satu alat yang dapat digunakan untuk melakukan *vulnerability analysis*. Nessus dapat digunakan untuk mengidentifikasi berbagai kerentanan, seperti kerentanan keamanan aplikasi, kerentanan keamanan jaringan, dan kerentanan keamanan sistem operasi.

Universitas Pamulang (UNPAM) merupakan salah satu perguruan tinggi swasta terbesar di Banten. UNPAM memiliki situs web yang digunakan untuk berbagai keperluan, seperti informasi akademik, pengumuman, kegiatan, dan lain-lain. Situs web UNPAM memiliki domain www.unpam.ac.id.

Penelitian ini bertujuan untuk melakukan analisis kerentanan pada situs web Universitas Pamulang (UNPAM) menggunakan Nessus, sehingga dapat dilakukan tindakan mitigasi untuk meningkatkan keamanan situs web tersebut. Beberapa penelitian terdahulu yang berhubungan dengan tujuan penelitian ini adalah sebagai berikut:

Penelitian yang dilakukan oleh Hasibuan dan Elhanafi (2022), dengan judul "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box Studi Kasus Web Server Diva Karaoke.co.id" [3]. Penelitian ini dilakukan dengan melakukan analisis dan perancangan dengan menggunakan alat-alat yang ada di Kali Linux. Hasil penelitian ini menunjukkan tingkat kerentanan pada server web Diva Karaoke masih rendah. Penulis bermaksud menggunakan Nessus untuk melakukan penelitian serupa terhadap situs web UNPAM.

Adapun penelitian yang dilakukan oleh Armando, dkk. (2022), membahas "*IT Support Website Security Evaluation Using Vulnerability Assessment Tools*" [4]. Penelitian ini menggunakan metode *Vulnerability Assessment Penetration Testing* (VAPT) Life Cycle yang memiliki enam tahapan yaitu: *Scope*, *Planning*, *Scanning &*

Vulnerability Analysis, *Exploitation*, *Privilege Escalation*, dan *Generating Report*. Hasil penelitian ini diperoleh berbagai kerentanan mulai dari *Low* hingga *Critical* pada website IT Support di institusi XYZ.

Sedangkan, pada penelitian yang dilakukan oleh Adha, dkk. (2023), membahas "*Website Security Test at The University of Mataram Using Vulnerability Assessment*" [5]. Pada penelitian ini, website yang menjadi sasaran adalah unram.ac.id milik Universitas Mataram yang digunakan untuk operasional perusahaan dengan menggunakan beberapa *tools* pengujian yaitu *Hosted Scan* dalam pencarian ulang dan pengujian keamanan *website* sebelumnya. Pada penelitian ini ditemukan beberapa kerentanan pada level tinggi, sedang, dan rendah pada *website* target.

Berikutnya penelitian yang dilakukan oleh Aziz (2021), membahas "Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas XYZ" [6]. Penelitian ini bertujuan untuk melakukan *Vulnerability Assesment* terhadap web aplikasi E-Learning untuk mendeteksi kerentanan, mendeskripsikan kerentanan, menilai kerentanan berdasarkan CVSS (*Common Vulnerability Scoring System*), dan memberikan solusi.

2. TINJAUAN PUSTAKA

2.1. Universitas Pamulang (UNPAM)

Universitas Pamulang (UNPAM) adalah salah satu dari perguruan tinggi swasta yang berada di wilayah Kota Tangerang Selatan Provinsi Banten. UNPAM berdiri dan beroperasi berdasarkan SK MENDIKNAS Nomor: 136/D/O/2001, tentang izin operasional Perguruan Tinggi. Dengan izin operasional dan STATUTA UNPAM, maka UNPAM resmi dan mulai beroperasi melaksanakan fungsinya sebagai lembaga pendidikan yang dilaksanakan dan dikelola oleh non pemerintah. Dari tahun 2001 sampai dengan tahun 2004, UNPAM berada di bawah Yayasan Prima Jaya. Untuk lebih menyatukan kekuatan sumber daya teruatama sumber daya finansial maka pada tahun 2004 sampai dengan saat ini UNPAM berada di bawah Yayasan Sasmita Jaya [7]. UNPAM memiliki situs web resmi yaitu unpam.ac.id yang digunakan untuk berbagai keperluan, seperti informasi akademik, pengumuman, kegiatan, dan lain-lain.

2.2. Keamanan Situs Web

Situs web merupakan salah satu media informasi yang paling banyak digunakan saat ini. Situs web dapat digunakan untuk berbagai keperluan, seperti informasi akademik, pengumuman, dan kegiatan lainnya. Oleh karena itu, keamanan situs web perlu dijaga agar tidak dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Keamanan situs web adalah suatu konsep dan langkah-langkah yang diambil untuk melindungi situs web dari ancaman dan serangan yang dapat merusak Integritas (*Integrity*), Kerahasiaan (*Confidentiality*), dan Ketersediaan (*Availability*). Keamanan situs web penting untuk menjaga data dan pengalaman pengguna tetap aman [8].

2.3. *Vulnerability Analysis*

Secara umum, *Vulnerability analysis* dianggap mirip dengan *vulnerability assessment*. Namun, ada sedikit perbedaan antara keduanya. *Vulnerability analysis* adalah bagian dari siklus *vulnerability assessment*, di mana Anda mengidentifikasi kerentanan, mengukur risiko, dan memprioritaskan risiko. *Vulnerability analysis* menyelidiki kerentanan yang terdeteksi oleh alat *vulnerability assessment* [9].

Risk severity adalah tingkat keparahan risiko yang terkait dengan setiap kerentanan, bergantung pada lingkungan dan sifat bisnis. Risiko dapat dikategorikan menjadi lima, yaitu :

1. *Critical severity*. Kerentanan yang teridentifikasi pada tingkat kritis harus segera diselidiki. Kerentanan pada tingkat ini mengasumsikan eksploitasi kelemahan dapat menyebabkan kompromi sistem atau data secara penuh.
2. *High severity*. Kerentanan dengan tingkat keparahan tinggi dapat dikategorikan sebagai kelemahan yang dapat menyebabkan penyerang mengakses sumber daya aplikasi atau pemaparan data yang tidak disengaja.
3. *Medium severity*. Kerentanan dengan tingkat keparahan sedang biasanya timbul karena kesalahan konfigurasi sistem atau kurangnya kontrol keamanan. Eksploitasi kerentanan ini dapat menyebabkan akses terhadap data dalam jumlah terbatas atau dapat digunakan bersama dengan kelemahan lain untuk mendapatkan akses yang tidak diinginkan ke sistem atau sumber daya.
4. *Low severity*. Kerentanan dengan tingkat keparahan rendah mengandung kelemahan yang mungkin tidak dapat dieksploitasi secara langsung namun

menimbulkan kelemahan yang tidak perlu pada aplikasi atau sistem. Kelemahan ini biasanya disebabkan oleh hilangnya kontrol keamanan, atau pengungkapan informasi yang tidak perlu tentang lingkungan aplikasi.

5. *Info severity*. Kerentanan tingkat keparahan informasi berisi informasi yang mungkin memiliki nilai, namun belum tentu terkait dengan cacat atau kelemahan tertentu.

Vulnerability scanning dapat dikategorikan menjadi enam jenis berdasarkan kategori aset yang dipindai, yaitu [10]:

1. *Port scanning*. Permintaan koneksi dikirimkan kepada mereka, dan respons permintaan dipantau untuk menentukan apakah mereka aktif atau tidak. Jika pemindaian menemukan kerentanan port terbuka, peretas kemungkinan besar dapat mengidentifikasinya juga.
2. *Network vulnerability scanning*. Pemindaian kerentanan jaringan dapat dilakukan melalui pemindaian *brute force* yang memeriksa kata sandi yang lemah, pemindaian kredensial, dan pemindaian eksploitasi yang memeriksa kerentanan dan mengeksploitasinya hingga terjadi gangguan jaringan.
3. *Application vulnerability scanning*. Pemindaian kerentanan aplikasi menguji jaringan, situs web, aplikasi web, dan aplikasi seluler untuk mendeteksi kesalahan konfigurasi dan kerentanan perangkat lunak yang diketahui.
4. *Host-based vulnerability scanning*. Pemindaian kerentanan berbasis *host* menilai konfigurasi dan sistem operasi server, mesin lokal, dan host jaringan lainnya.
5. *Database vulnerability scanning*. Pemindaian kerentanan basis data mengidentifikasi titik lemah dalam basis data dengan memindai kerentanan seperti kurangnya enkripsi, konfigurasi keamanan yang salah, dan banyak lagi.
6. *Cloud vulnerability scanning*. Pemindaian kerentanan *cloud* memindai penerapan *cloud.*

Vulnerability analysis dibutuhkan dalam Upaya pencegahan risiko. *Vulnerability analysis* mengungkap celah/kesenjangan/kerentanan dalam sistem. Dengan menjalankan pemindaian ini secara berkala, organisasi dapat mengidentifikasi kerentanan yang diketahui pada infrastruktur TI secara tepat waktu.

2.4. Nessus

Nessus adalah salah satu produk *Vulnerability Assessment* yang paling banyak digunakan. Pertama kali dirilis pada tahun 1998 oleh Renaud Deraison, alat ini telah menjadi salah satu alat pemindaian kerentanan paling populer yang digunakan di industri selama 15 tahun terakhir.

2.5. *Common Vulnerability Scoring System* (CVSS)

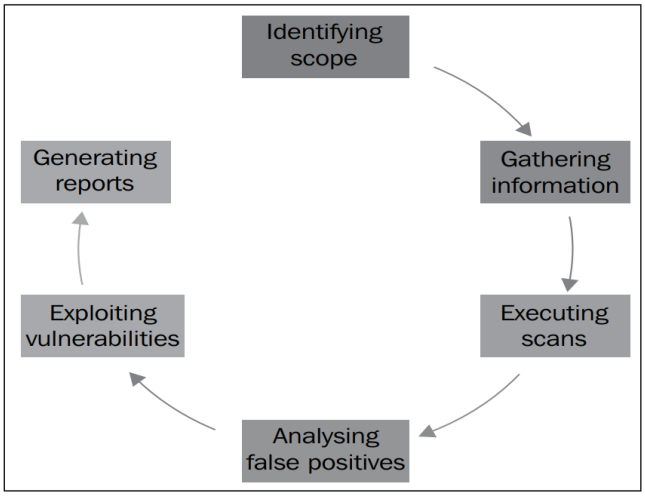
Berdasarkan sistem penilaiannya, Nessus menggunakan *Common Vulnerability Scoring System* (CVSS) untuk menilai kerentanan. Ini adalah sistem pemeringkatan kerentanan *open source* berdasarkan karakteristik dan dampak kerentanan. Ini mencakup parameter seperti ciri-ciri kerentanan yang hakiki, ciri-ciri kerentanan yang berubah seiring waktu, dan ciri-ciri kerentanan yang spesifik pada suatu lingkungan. Tabel 1 berikut mencantumkan skor CVSS berdasarkan peringkat kerentanan yang digunakan oleh Nessus.

Tabel 1. Daftar *Common Vulnerability Scoring System*

CVSS score	Criticality
0	*Info*
<4	*Low*
<7	*Medium*
<10	*High*
10	*Critical*

3. METODE

Metode penelitian yang digunakan mengikuti langkah-langkah dalam *Vulnerability Assesment and Penetration Testing Life Cycle.* VAPT *Life Cycle* terdapat enam langkah yang dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Pada Gambar 1 menggambarkan tahapan-tahapan yang akan dilakukan dalam penelitian, penjelasan dari tahapan-tahapan penelitian tersebut adalah:

1. *Scoping*, adalah untuk mengidentifikasi ruang lingkup penilaian dalam hal infrastruktur yang akan digunakan untuk melakukan penilaian, dalam penelitian ini situs web Universitas Pamulang sebagai objek yang akan dilakukan penilaian.
2. *Information Gathering*, untuk mencari tahu informasi mengenai sistem sasaran
3. *Vulnerability Scanning*, tahap ini melakukan pemindaian protokol TCP, UDP, dan ICMP untuk menemukan port dan layanan terbuka yang berjalan pada mesin target. Keluaran dari fase ini memberikan gambaran keseluruhan tentang jenis kerentanan yang ada pada infrastruktur target yang jika dieksploitasi dapat menyebabkan kompromi system.
4. *False Positive Analysis*, untuk menghilangkan kerentanan apa pun yang dilaporkan secara salah.
5. *Vulnerability Exploitation* (*Penetration Testing*), Pengujian Penetrasi bertujuan untuk menembus sistem target berdasarkan kerentanan yang teridentifikasi.
6. *Report Generation*, pelaporan akhir mencakup detail tentang setiap temuan beserta dampaknya dan rekomendasi untuk memperbaiki kerentanan.

4. HASIL DAN PEMBAHASAN

Pada penelitian ini, *vulnerability analysis* dilakukan terhadap situs web Universitas Pamulang yaitu www.unpam.ac.id, penulis menggunakan bantuan aplikasi Nessus 10.6.3 yang diinstal pada Kali Linux untuk melakukan pengujian *vulnerability scanning* yang akan menghasilkan daftar kerentanan beserta penjelasan terhadap kerentanan, dampak dari kerentanan, persentase kerentanan yang ditemukan, dan solusi untuk mengatasi kerentanan sehingga dapat digunakan untuk mengevaluasi serta meningkatkan keamanan terhadap situs web Universitas Pamulang. Sebagai informasi awal ditemukan *IP Address*, DNS, dan port yang digunakan untuk menjalankan service pada situs web www.unpam.ac.id

4.1. *Vulnerability Scanning*

Vulnerability Scanning dilakukan pemindaian kerentanan situs web www.unpam.ac.id menggunakan Nessus. Hasil pemindaian kerentanan ditunjukkan pada Gambar 2.

Gambar 2. Hasil *Vulnerability Scanning*

Pada Gambar 2 menunjukkan hasil *vulnerability analysis* yang dilakukan pada situs web Universitas Pamulang. Pemindaian ini dilakukan pada tanggal 4 Desember 2023. Berikut jenis kerentanan yang terdapat pada Tabel 2.

Tabel 2. Daftar Kerentanan

No	Nama Kerentanan	*Base Score*	Tingkat Kerentanan
1	*SSL Medium Strength Cipher Suites Supported (SWEET32)*	7.5	*High*
2	*SSL Certificate Cannot Be Trusted*	6.5	*Medium*
3	*SSL Weak Cipher Suites Supported*	5.3	*Medium*
4	*DNS Server Spoofed Request Amplification DDoS*	7.5	*High*
5	*DNS Server Recursive Query Cache Poisoning Weakness*	5.0	*Medium*
6	*TLS Version 1.0 Protocol Detection*	6.5	*Medium*
7	*TLS Version 1.1 Protocol Deprecated*	6.5	*Medium*

Daftar kerentanan pada tabel mempunyai dampak yang berbeda-beda untuk masing-masingnya. Pada daftar kerentanan, tidak ditemukan kerentanan dengan tingkat *Critical*. Namun, tentu lebih baik memberikan perhatian terhadap kerentanan-kerentanan tersebut. Hasil pemindaian kerentanan menunjukkan kerentanan ditemukan pada 3 (tiga) layanan, yaitu: SSL, DNS, dan TLS. Adapun penjelasan dari daftar kerentanan adalah sebagai berikut:

1) *SSL Medium Strength Cipher Suites Supported (SWEET32)*. Host jarak jauh mendukung penggunaan sandi SSL yang menawarkan enkripsi kekuatan sedang. Nessus menganggap kekuatan sedang sebagai enkripsi apa pun yang menggunakan panjang kunci minimal 64 bit dan kurang dari 112 bit, atau yang menggunakan rangkaian enkripsi 3DES.

2) *SSL Certificate Cannot Be Trusted.* Sertifikat X.509 server tidak dapat dipercaya. Hal ini dapat terjadi melalui tiga cara: sertifikat bukan berasal dari otoritas sertifikat publik yang diketahui, sertifikat tidak valid pada saat pemindaian, atau sertifikat berisi tanda tangan yang tidak valid.
3) *SSL Weak Cipher Suites Supported*. Host jarak jauh mendukung penggunaan cipher SSL/TLS yang menawarkan enkripsi lemah (termasuk enkripsi RC4 dan 3DES).
4) *DNS Server Spoofed Request Amplification DDoS*. Server DNS menjawab permintaan apa pun. Dimungkinkan untuk meminta *name server* (NS) dari *rootzone* ('.') dan mendapatkan jawaban yang lebih besar dari permintaan awal. Dengan memalsukan alamat IP sumber, penyerang memanfaatkan 'amplifikasi' ini untuk meluncurkan serangan DDoS terhadap host pihak ketiga menggunakan server DNS.
5) *DNS Server Recursive Query Cache Poisoning Weakness*. Server DNS memungkinkan pengguna untuk mencari informasi tentang nama domain yang dimiliki oleh pihak ketiga.
6) *TLS Version 1.0 Protocol Detection*. *Service* menerima koneksi yang dienkripsi menggunakan TLS 1.0. TLS 1.0 memiliki sejumlah kelemahan desain kriptografi. Implementasi modern TLS 1.0 mengurangi masalah ini, namun versi TLS yang lebih baru seperti 1.2 dan 1.3 dirancang untuk mengatasi kelemahan ini dan harus digunakan bila memungkinkan.
7) *TLS Version 1.1 Protocol Deprecated*. *Service* menerima koneksi yang dienkripsi menggunakan TLS 1.1. TLS 1.1 tidak memiliki dukungan untuk cipher suite saat ini dan yang direkomendasikan. Cipher yang mendukung enkripsi sebelum komputasi MAC, dan mode enkripsi terautentikasi seperti GCM tidak dapat digunakan dengan TLS 1.1

4.2. *Vulnerability Port Service*

Berikut ini merupakan *port service* yang memiliki *vulnerability* pada situs web Universitas Pamulang dapat dilihat pada Tabel 3.

Tabel 3 Vulnerability Port Service

No	Service Port	Threat Level
1	443 / tcp / www	*High*
2	443 / tcp / www	*Medium*
3	443 / tcp / www	*Medium*
4	53 / udp / dns	*High*
5	53 / udp / dns	*Medium*
6	443 / tcp / www	*Medium*
7	443 / tcp / www	*Medium*

Pada Tabel 3 ditemukan bahwa kerentanan situs web pada *port* 443 memiliki 5 (lima) kerentanan, dimana 1 (satu) kerentanan dengan tingkat *high* dan 4 (empat) kerentanan dengan tingkat *medium*. Sedangkan, pada *port* 53 memiliki 2 (dua) kerentanan, dengan masing-masing kerentanan dengan *base score* 7.5 dan 5.0, dengan tingkat kerentanan *high* dan *medium.*

4.3. *Generating Report*

Generating Report merupakan laporan awal hingga akhir sebagai saran langkah perbaikan situs web. Setelah dilakukan proses identifikasi, ditemukan beberapa kerentanan pada situs yaitu *high* dan *medium*, dan tentunya setiap kerentanan memiliki solusi yang berbeda-beda. Oleh karena itu pada tahapan pembuatan laporan akan memberikan rekomendasi solusi berupa laporan pada Tabel 4.

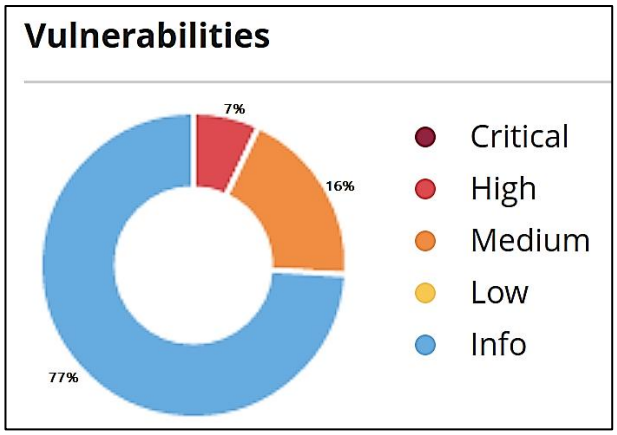
Tabel 4. Laporan *Vulnerability Assesment*

Nama Kerentanan	Dampak	Solusi
SSL Medium Strength Cipher Suites Supported (SWEET32)	Memungkinkan penyerang untuk memulihkan sebagian kecil dari *plaintext* saat dienkripsi dengan cipher blok 64-bit	*Upgrade* ke *cipher suite* dengan panjang kunci 128 bit atau lebih.
SSL Certificate Cannot Be Trusted	Menghalangi *browser* atau perangkat untuk memverifikasi keaslian sertifikat SSL situs web	Verifikasi keaslian sertifikat SSL, hubungi pemilik situs web jika perlu, atau gunakan *browser* atau perangkat lain.
SSL Weak Cipher Suites Supported	Memungkinkan penyerang untuk mendekripsi dan membaca data terenkripsi	*Upgrade* ke *cipher suite* dengan panjang kunci 128 bit atau lebih.
DNS Server Spoofed Request Amplification DDoS	Memungkinkan penyerang untuk membanjiri server DNS dengan permintaan palsu, yang mengakibatkan serangan DoS	Aktifkan DNSSEC dan terapkan *resolver* yang diaktifkan DNSSEC.
DNS Server Recursive Query Cache Poisoning Weakness	Memungkinkan penyerang untuk mengarahkan pengguna ke situs web berbahaya	Aktifkan DNSSEC, terapkan *resolver* yang diaktifkan DNSSEC, gunakan *firewall* DNS, dan mendidik pengguna tentang pencemaran *cache* DNS.
TLS Version 1.0	Menunjukkan adanya protokol TLS	Nonaktifkan TLS 1.0 dan aktifkan TLS

Protocol Detection	1.0 yang sudah usang, yang dianggap tidak aman	1.2 atau versi yang lebih tinggi.
TLS Version 1.1 Protocol Deprecated	Menunjukkan adanya protokol TLS 1.1 yang sudah usang, yang dianggap tidak aman	Nonaktifkan TLS 1.1 dan aktifkan TLS 1.2 atau versi yang lebih tinggi.

4.4. Persentase *Vulnerability Scanning*

Persentase ini diperoleh dari banyaknya kerentanan yang ditemukan pada saat melakukan pemindaian kerentanan menggunakan Nessus, dan persentase ini untuk memudahkan dalam mencari tingkat kerentanan pada situs web Universitas Pamulang sehingga persentase pemindaian kerentanan tersebut dapat dijadikan bahan untuk penilaian keamanan situs web. Persentase kerentanan ditunjukkan pada Gambar 3.



Gambar 3. Persentase *Vulnerability Scanning*

Gambar 3 menggambarkan bahwa persentase pemindaian kerentanan berasal dari jumlah kerentanan yang ditemukan. Tidak ditemukan kerentanan dengan tingkat kerentanan *critical* dan *low*. Berdasarkan hasil *vulnerability asessment* yang dilakukan bahwa *risk level* pada situs web Universitas Pamulang adalah *High*, dikarenakan pada *threat level score* yang paling tinggi ditunjukkan oleh kerentanan *high* yaitu 7.5. Sehingga, dapat disimpulkan bahwa situs web Universitas Pamulang memiliki tingkat kerentanan yang tinggi.

5. KESIMPULAN

Berdasarkan hasil *vulnerability assesment* menggunakan Nessus, ditemukan bahwa situs web Universitas Pamulang memiliki beberapa kerentanan; yaitu, 7% bersifat tinggi dan 16% bersifat sedang. Kerentanan-kerentanan yang ditemukan antara lain: *SSL Medium Strength Cipher Suites Supported (SWEET32), SSL Weak Cipher*

Suites Supported, SSL Certificate Cannot Be Trusted, DNS Server Spoofed Request Amplification DdoS, DNS Server Recursive Query Cache Poisoning Weakness, TLS Version 1.0 Protocol Detection, dan TLS Version 1.1 Protocol Deprecated. Untuk mengurangi kerentanan tersebut, pengelola situs web dapat melakukan langkah pencegahan dengan meningkatkan ke *cipher suite* dengan panjang kunci 128 bit atau lebih, memverifikasi keaslian sertifikat SSL, mengaktifkan DNSSEC dan menerapkan *resolver* yang diaktifkan DNSSEC, menggunakan *firewall* DNS, dan menonaktifkan TLS 1.0 dan mengaktifkan TLS 1.2 atau versi yang lebih tinggi. Dengan demikian, maka pihak Universitas Pamulang harus segera melakukan perbaikan dan evaluasi terhadap situs web Universitas Pamulang agar risiko kerentanan pada situs web Universitas Pamulang dapat dikurangi.

6. DAFTAR PUSTAKA

[1] Mohamad Fathurahman, Zulhelman, and Abdul Aziz, "Vulnerability Assessment Dan Penetration Test Pada Website MA/MTs Husnul Khatimah Kuningan," *Pros. Semin. Nas. Terap. Ris. Inov.*, vol. 8, no. 3, pp. 138–145, Jan. 2023.

[2] Riyan Farismana and Dian Pramadhana, "Vulnerability Assessment Untuk Analisis Tingkat Keamanan Pada Sistem Informasi Repositori Karya Ilmiah Politeknik XYZ," *J. Tek. Inform. dan Teknol. Inf.*, vol. 3, no. 1, pp. 26–33, Apr. 2023, doi: 10.55606/jutiti.v3i1.2208.

[3] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box: Studi Kasus Web Server Diva Karaoke.co.id," *Sudo J. Tek. Inform.*, vol. 1, no. 4, pp. 171–177, Dec. 2022, doi: 10.56211/sudo.v1i4.160.

[4] R. Armando, I. G. A. K. Melyantara, R. Elfariani, D. F. Latuconsina, and M. Nasrullah, "IT Support Website Security Evaluation Using Vulnerability Assessment Tools," *J. Inf. Syst. Informatics*, vol. 4, no. 4, pp. 949–957, Nov. 2022, doi: 10.51519/journalisi.v4i4.330.

[5] M. Adha, Z. D. KWA, and A. H. Muhammad, "Website Security Test at The University of Mataram Using Vulnerability Assessment," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 8, no. 2, pp. 647–655, 2023, doi: 10.29100/jipi.v8i2.3830.

[6] M. Aziz, "Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas XYZ," *J. Eng. Comput. Sci. Inf. Technol.*, vol. 2, no. 1, pp. 101–109, 2022, doi: 10.33365/jecsit.v1i1.13.

[7] E. Ruhiyat, "Analisis Faktor Yang Menjadi Penentu Mahasiswa Dalam Memilih Perguruan Tinggi," *INOVASI*, vol. 3, no. 1, pp. 78–96, Apr. 2017, doi: 10.32493/Inovasi.v3i1.p%p.293.

[8] S. Farizy and E. S. Eriana, *Keamanan Sistem Informasi, Tangerang Selatan: Unpam Press, 2022.* Tangerang Selatan: Unpam Press, 2022.

[9] H. Kumar, *Learning Nessus for Penetration Testing*. Birmingham: Packt Publishing, 2014.

[10] S. Graph, "6 Types of Vulnerability Scanning," *Strike Graph, Inc.*, 2023. https://www.strikegraph.com/blog/6-types-of-vulnerability-scanning (accessed Dec. 04, 2023).