BAB V

KESIMPULAN DAN SARAN

V.I Kesimpulan

Untuk menjaga keamanan sistem sebaiknya pihak *team* IT perlu melakukan konfigurasi ulang terhadap sistem, agar celah kerentanan terhadap serangan yang masuk bisa diatasi. Identifikasi kerentanan pada sistem manajemen data sumber terbuka *Ckan website* diskominfo kota bandung menggunakan metode *National Institute of Standards and Technology Special Publicaiton* 800-115, hasil eskploitasi dari uji penetrasi yaitu 5 kerentanan dengan tingkat keparahan Medium dan 2 kerentanan dengan tingkat keparahan low .

Probability Impact Matrix adalah salah satu metode untuk menganalisis risiko secara kualitatif kemungkinan suatu risiko muncul. Penilaian risiko dilakukan berdasarkan peluang probabilitas dan konsekuensinya/dampaknya (Dalam Fatimah, 2021). penilaian risiko merupakan hasil kali antara nilai keparahan suatu risiko. Hasil dari kerentanan yang ditemukan diantaranya adalah

Tabel V. 1 Faktor Faktor yang mempengaruhi nilai matriks

No.	Nama Kejadian Risiko		Frekuensi Risiko yang Terjadi				Tingkat Keparahan Terhadap Pengaruh Risiko			
1			1	2	3	4	1	2	3	4
	A1	*HTTP TRACE/TRACK Methods Allowed* (Medium)	x					x		
	A2	*Web Application Potentially Vulnerable to Clickjacking* (Medium)	x					x		
	A3	*SSL Medium Strength Cipher Suites Supported (SWEET32)* (Medium)	x					x		
	A4	*SSL RC4 Cipher Suites Supported (Bar Mitzvah)* (Medium)	x					x		
	A5	*TLS Version 1.0 Protocol Detection* (Medium)	x					x		
	A6	*php < 1.17.7 Information Disclosure* (Low)	x				x			

	A7	*Unencrypted Password Form* (Low)	x				x			

Untuk menentukan kategori suatu risiko apakah itu rendah, sedang, tinggi ataupun ekstrim dapat menggunakan metode matriks risiko seperti pada tabel matriks risiko dibawah ini:

Tabel V. 2 Tabel Matriks Risiko

Tabel Matriks Risiko		Tingkat Keparahan			
		1	2	3	4
Frekuensi	4	*Medium*	*High*	*Critical*	*Critical*
	3	*Medium*	*High*	*High*	*Critical*
	2	Low	*Medium*	*High*	*High*
	1	A6,A7	A1,A2,A3,A4,A5	*Medium*	*Medium*

Tabel matriks V.2 menjelaskan tentang matriks yang digunakan selama penilaian risiko untuk menentukan tingkat risiko dengan mempertmbangkan kategori keparahan konsekuensi. Ini adalah mekanisme sederhana untuk meningkatkan visibilitas risiko dan membantu pengambilan keputusan(Lemmens, 2022). Angka 1-4 pada kolom frekuensi adalah kerentanan yang muncul , dan angka 1-4 pada kolom tingkat keparahan adalah tingkat keparahan pada kerentanan.

Frekuensi kerentanan yang paling banyak muncul adalah A1, A2, A3, A4 dan A5 dengan manajemen risiko rendah dan frekuensi kerentanan A6, A7 dengan manajemen risiko rendah. konklusi dari seluruh kerentanan yang ditemukan dan dihitung dengan menggunakan tabel matriks adalah jenis serangan yang bisa dikatergorikan dengan tingkat keparahan yang rendah.

Program untuk melakukan validasi konsep (*Proof of Concept)* dari segi fungsional, penerapan, teknis. Beberapa kerentanan yang ditemukan ada diantaranya tidak rentan dikarenakan ada port yang sudah ditutup dan akses yang

tidak ditemukan. Celah kerentanan yang ditemukan dapat dimitigasi dengan banyak cara yag berbeda. Peneliti memberikan saran yang dapat dilakukan untuk memitigasi celah kerentanan yang ditemukan. Penerapan dari saran yang diserahkan sepenuhnya kepada pihak *team* IT yaitu diskominfo kota Bandung.

V.II Saran

Berdasarkan hasil analisis juga pembahasan yang sudah dijelaskan, maka penulis memberikan beberapa saran untuk perbaikan agar sistem menjadi aman yaitu sebagai berikut.

1.Eksploitasi tahap selanjutnya agar dapat dilakukan Kembali dengan menambahkan metode pada pengujiannya agar dapat menemukan celah kerentanan yang lebih mendalam

2. Sebaiknya sistem diuji Kembali jika sudah berhasil diremediasi oleh team IT terkait.

3. Dijadikan bahan acuan untuk memberikan tambahan keamanan pada sistem manajemen data tersebut.