Jurnal Sosial dan Teknologi (SOSTECH)
Volume 5, Number 12, Desember 2025
p-ISSN 2774-5147 ; e-ISSN 2774-5155

Analisis Risiko Kerentanan Keamanan Aplikasi Gawai Layanan Masyarakat Pt.Xyz Menggunakan Parameter Owasp Mobile Security dan Pembobotan Cvss

Mohammad Afwanul Hakim
Universitas Gunadarma, Indonesia
Email: fanul.doang@gmail.com

Abstrak
Saat ini Perusahaan PT. XYZ tengah dalam masa persiapan pembangunan menuju visi *service excellence.* Dalam rangka mendukung pencapaian visi tersebut perlu diperhatikan terkait berjalannya sistem informasi yang menjadi andalan bisnis Badan PT. XYZ. Seiring dengan visi perusahaan, PT. XYZ membuat aplikasi layanan masyarakat pada gawai baik di android maupun di IOS. OWASP (*Open Web Application Security Project*) *Mobile Security* adalah sebuah paramater dan *guideline* yang secara spesifik dapat digunakan untuk mendeteksi celah keamanan pada suatu aplikasi gawai, OWASP *Mobile Security* menggunakan skenario *Test Case* berkonsep dari "Attack Tree - Bruce Scheiner" yang komprehensif dan mempunyai glossary definitif terhadap *Threat Agents, Attack Vectors, Security Weakness* , *Technical Impacts* dan *Business Impact* yang dapat digunakan sebagai definitif *guideline* dalam pembobotan CVSS. CVSS (*Common Vulnerability Scoring System*) merupakan standar yang digunakan untuk menentukan kerentanan keamanan pada suatu sistem. CVSS banyak digunakan di dunia karena CVSS menyediakan cara untuk menangkap karakteristik utama kerentanan dan menghasilkan skor numerik yang mencerminkan tingkat kerentanan. Skor numerik kemudian dapat diterjemahkan ke dalam representasi kualitatif rendah, sedang dan tinggi untuk menilai dengan benar dan memprioritaskan proses manajemen kerentanan keamanan. Oleh karena itu penulis tertarik melakukan analisis risiko kerentanan pada aplikasi gawai layanan masyarakat PT. XYZ guna mendapatkan keyakinan atas risiko keamanan yang mungkin terjadi, sebagai parameter dan *guideline* penulis menggunakan OWASP *Mobile Security* dan untuk pembobotan skor risiko penulis menggunakan CVSS.
Kata Kunci: OWASP *Mobile Security*, CVSS, Keamanan, Aplikasi Layanan Masyarakat

Abstract
Currently the PT. XYZ is in the midst of preparation for development towards the vision of service excellence. In order to support the achievement of this vision, it should be noted that the information system that is the mainstay of the PT. XYZ. Along with the company's vision, PT. XYZ makes a community service application on devices both on Android and in IOS. OWASP (Open Web Application Security Project) Mobile Security is a parameter and guideline that can specifically be used to detect security holes in a device application, OWASP Mobile Security uses a Scenario Test Case with the concept of Attack Tree - Bruce Scheiner that is comprehensive and has a definitive glossary on Threat Agents, Attack Vectors, Security Weakness, Technical Impacts and Business Impact which can be used as definitive guidelines for weighting CVSS. CVSS (Common Vulnerability Scoring System) is a standard used to determine security vulnerabilities in a system. CVSS is widely used in the world because CVSS provides a way to capture the main characteristics of vulnerability and produce a numerical score that reflects its severity. The numerical score can then be translated into low, medium and high qualitative representations to properly assess and prioritize the security vulnerability management process. Therefore the authors are interested in conducting vulnerability risk analysis in the application of community service devices PT. XYZ in order to get confidence in possible security risks, as a parameter and guideline author uses OWASP Mobile Security and for risk score weighting author uses CVSS.
Keyword: OWASP Mobile Security, CVSS, Security, Public Service Application

PENDAHULUAN

Indonesia mengalami pertumbuhan eksponensial dalam penggunaan internet, di mana pada tahun 2017 tercatat 143,26 juta pengguna dari total 262 juta penduduk, menunjukkan

kenaikan signifikan dari tahun sebelumnya. Tren ini didorong oleh permintaan layanan berbasis data, khususnya melalui layanan mobile broadband (Alanda et al., 2020; Diallo et al., 2025). Peningkatan pasar ini menciptakan arena yang matang bagi konvergensi Teknologi Informasi dan Komunikasi (TIK), namun pada saat yang sama, meningkatkan risiko keamanan siber secara substansial (Alfi et al., 2023; Jaelani et al., 2024; Karim et al., 2024).

Perusahaan PT. XYZ, dalam upayanya mencapai visi *service excellence*, sangat bergantung pada sistem informasi yang handal, termasuk pengembangan aplikasi layanan masyarakat pada platform gawai (Android dan iOS) (Haq et al., 2021; Petraityte et al., 2018). Kegagalan sistem atau eksploitasi kerentanan pada aplikasi publik ini dapat berdampak langsung pada operasional bisnis dan kepercayaan pengguna. Laporan *Global Cybersecurity Index* tahun 2017 menempatkan Indonesia di peringkat terbawah (ke-12) di Asia Pasifik, mengindikasikan bahwa sistem informasi nasional, termasuk aplikasi layanan publik, sangat rentan terhadap serangan (Lallie et al., 2021; Technology, 2023).

Oleh karena itu, diperlukan analisis risiko keamanan yang metodis dan terkuantifikasi. Penilaian risiko konvensional seringkali gagal memberikan prioritas yang jelas bagi manajemen teknis (Adrian et al., 2015; Kim et al., 2015; Riskhan et al., 2025). Penelitian ini mengadopsi standar *Global Open Web Application Security Project* (OWASP) *Mobile Security* sebagai parameter kualitatif untuk deteksi celah keamanan, dan *Common Vulnerability Scoring System* (CVSS) sebagai kerangka kuantifikasi untuk menentukan tingkat kerentanan dan prioritas mitigasi (First.Org, 2019; Kadir et al., 2025; Project, 2018, 2024).

Meskipun PT. XYZ telah mengimplementasikan aplikasi gawai layanan masyarakat, keyakinan mengenai tingkat risiko keamanan yang mungkin terjadi masih perlu diuji dan divalidasi secara objektif. Masalah utama yang diidentifikasi adalah kebutuhan untuk memformulasikan hasil pengujian keamanan menjadi metrik risiko yang dapat dipahami dan ditindaklanjuti oleh manajemen (Isnaini et al., 2023). Berdasarkan latar belakang tersebut, penelitian ini fokus pada tiga hal : 1) Kerentanan keamanan apa saja yang terdeteksi pada Aplikasi Gawai PT. XYZ sesuai dengan parameter OWASP *Mobile Security Testing Guide* (MSTG). 2) Berapakah Skor Risiko Base dan Temporal (CVSS) untuk setiap kerentanan yang ditemukan. 3) Berdasarkan skor CVSS, bagaimana prioritas mitigasi risiko yang efektif dapat direkomendasikan kepada PT. XYZ?

Tujuan penelitian disesuaikan dengan definisi masalah yang telah diuraikan : 1) Melakukan pengujian keamanan menggunakan parameter OWASP atas kemungkinan-kemungkinan serangan *cyber* terhadap aplikasi. 2) Mengukur rating risiko kerentanan keamanan (CVSS) aplikasi layanan masyarakat. 3) Memberikan rekomendasi peningkatan keamanan atas risiko kerentanan keamanan yang terpapar.

Setelah penelitian ini dilaksanakan diharapkan PT. XYZ dapat melakukan : 1) Melakukan peningkatan dan perbaikan pada Keamanan Aplikasi Gawai Layanan Masyarakat PT. XYZ. 2) Menjadi Referensi atau Tolak Ukur dalam pengujian keamanan aplikasi-aplikasi gawai PT. XYZ di masa yang akan datang. 3) Sebagai alat menentukan Risiko Prioritas atas kerentanan keamanan yang terpapar bagi PT. XYZ.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode penelitian kualitatif. Penelitian kualitatif adalah penelitian yang menggambarkan atau melukiskan objek penelitian berdasarkan fakta-fakta yang tampak atau sebagaimana adanya. Nawawi dan Martini (1996: 73). Penelitian deskriptif kualitatif berusaha mendeskripsikan seluruh gejala atau keadaan yang ada, yaitu keadaan gejala menurut apa adanya pada saat penelitian dilakukan. Mukhtar (2013: 28).

Penelitian ini menggunakan metode deskriptif kualitatif-kuantitatif. Pendekatan ini dipilih karena kerentanan teknis harus dideskripsikan (kualitatif) berdasarkan *guideline* OWASP, dan dampak risikonya harus diukur dan diprioritaskan (kuantitatif) menggunakan CVSS.

Tahapan penelitian dilaksanakan secara berurutan:

1. Pengumpulan Data: Dilakukan melalui studi literatur mendalam mengenai OWASP, CVSS, dan riset terkait keamanan mobile.
2. Pengujian Keamanan *(Penetration Testing*): Dilaksanakan terhadap Aplikasi Layanan Masyarakat PT. XYZ pada platform *Android*.
3. Analisis Kerentanan: Pemetaan temuan pengujian ke dalam kategori OWASP dan penentuan vektor CVSS *Base*.
4. Kuantifikasi Risiko: Perhitungan skor numerik CVSS.

Penetration Pengujian keamanan menggunakan pendekatan hibrida, yaitu *Blackbox* Testing dan *Greybox* Testing, dengan mengacu pada OWASP *Mobile Security Checklist*. Justifikasi Metode Hibrida: Dalam keamanan aplikasi gawai, menggunakan *Blackbox* (tanpa akses kode sumber) saja tidak cukup, karena banyak kerentanan kritis (seperti manajemen kunci atau penggunaan algoritma kriptografi usang) tersembunyi di dalam kode aplikasi. Oleh karena itu, *Greybox* Testing diterapkan, yang menggabungkan pengujian eksternal dan fungsional (*Blackbox*) dengan pengetahuan parsial kode atau arsitektur internal.

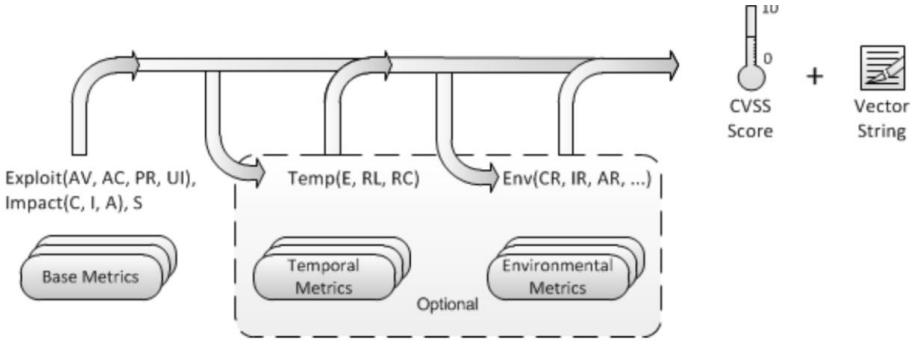
Pendekatan ini diimplementasikan melalui dua komponen utama:

1. *Static Application Security Testing (SAST):* Analisis ini, yang mencerminkan komponen *white-box* dari *Greybox Testing*, melibatkan *reverse engineering* (*disassembling* dan *decompiling*) kode aplikasi menggunakan alat seperti apktool, dex2jar, dan jdgui. SAST bertujuan untuk mengidentifikasi kebocoran informasi (*hardcoded credential*), *misuse* izin aplikasi, dan keberadaan algoritma kriptografi yang tidak aman (*deprecated algorithms*).
2. *Dynamic Application Security Testing (DAST):* Analisis runtime ini, yang mencerminkan komponen *black-box*, dilakukan saat aplikasi berjalan. DAST berfokus pada pengujian perilaku aplikasi terkait manajemen *session, copy/paste buffer caching*, dan kerentanan injeksi. Alat yang digunakan mencakup *adb logcat* dan *proxy* seperti *Burpsuite* untuk menganalisis lalu lintas komunikasi.

Pengujian juga melibatkan analisis komunikasi serta analisis sisi *server* (*Webservices* and API) untuk mengidentifikasi kerentanan seperti *Weak Password Policy* dan *Session Timeout Protection*.

Untuk setiap kerentanan yang ditemukan, skor risiko dihitung menggunakan formulasi CVSS. Penentuan *Vector Base Metrics* (AV, AC, PR, UI, S, C, I, A) didasarkan pada definisi teknis kerentanan yang diperoleh dari pengujian dan *Technical Impacts* yang dijelaskan oleh OWASP *Mobile Security*.

Pemberian penilaian CVSS dilakukan melalui langkah-langkah berikut: 1) Penetapan *Base Metrics*: Vektor ditetapkan berdasarkan karakteristik inheren kerentanan. Misalnya, jika eksploitasi dapat memengaruhi sumber daya di luar hak otorisasi komponen rentan, *Scope* ditetapkan sebagai *Changed* (S:C). 2) Perhitungan Base Score: Skor Base dihitung berdasarkan formulasi resmi CVSS. 3) Penetapan *Temporal Metrics:* Matriks Temporal (E, RL, RC) dinilai untuk merefleksikan kondisi kerentanan saat ini, seperti ketersediaan kode eksploitasi dan perbaikan resmi. Jika *Temporal Metric* tidak ditentukan (X), hal itu tidak memengaruhi skor secara signifikan, setara dengan memberikan nilai tertinggi. 4) Perhitungan *Score*: *Score* yang berfungsi sebagai metrik prioritas risiko yang paling relevan untuk pengambilan keputusan manajemen, dihitung berdasarkan *Base Score* yang dimodifikasi oleh *Temporal Metrics*.
Analisa *Scoring* diilustrasikan sebagai berikut :



Gambar1: Guideline CVSS

Dari *Vector String* yang telah didefinisikan dihitunglah skor numerik dengan rumusan:

The Base Score is a function of the Impact and Exploitability sub score equations. Where the Base score is defined as,

If (Impact sub score <= 0) 0 else,

Scope Unchanged $Roundup\left(Minimum\left[\left(Impact+Exploitability\right),10\right]\right)$

Scope Changed $Roundup\left(Minimum\left[1.08\times\left(Impact+Exploitability\right),10\right]\right)$

and the Impact sub score (ISC) is defined as,

Scope Unchanged $6.42\times ISC_{Base}$

Scope Changed $7.52\times\left[ISC_{Base}-0.029\right]-3.25\times\left[ISC_{Base}-0.02\right]^{15}$

Where,

$$ISC_{Base}=1-\left[\left(1-Impact_{Conf}\right)\times\left(1-Impact_{Integ}\right)\times\left(1-Impact_{Avail}\right)\right]$$

And the Exploitability sub score is,

Gambar 2: Formulasi Skoring CVSS (1)

$$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$$

Temporal
The Temporal score is defined as,

$$Roundup\left(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence\right)$$

Environmental
The environmental score is defined as,

If (Modified Impact Sub score <= 0)	0 else,
If Modified Scope is Unchanged	*Round up(Round up (Minimum [(M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)*
If Modified Scope is Changed	*Round up(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)*

And the modified Impact sub score is defined as,

If Modified Scope is Unchanged	$6.42 \times \left[ISC_{Modified}\right]$
If Modified Scope is Changed	$7.52 \times \left[ISC_{Modified} - 0.029\right] - 3.25 \times \left[ISC_{Modified} - 0.02\right]^{15}$

Where,

$$ISC_{Modified} = Minimum\left[\left[1 - \left(1 - M.I_{Conf} \times CR\right) \times \left(1 - M.I_{Integ} \times IR\right) \times \left(1 - M.I_{Avail} \times AR\right)\right], 0.915\right]$$

The Modified Exploitability sub score is,

$$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$$

Gambar 3: Formulasi Skoring CVSS (2)

untuk setiap kerentanan keamanan, yang kemudian diperoleh CVSS Score dan klasifikasi dari kerentanan keamanan tersebut.

Pembuatan Kesimpulan

Penentuan kesimpulan penelitian berdasarkan data-data hasil percobaan dan *Total Estimated Risk* untuk mengetahui tingkat kerentanan aplikasi Layanan Masyarakat dan pemberian rekomendasi peningkatan keamanan yang perlu dilakuk

HASIL DAN PEMBAHASAN

Penelitian ini menemukan empat kerentanan utama yang mempengaruhi prinsip Kerahasiaan (*Confidentiality*) dan Integritas (*Integrity*) pada Aplikasi Gawai Layanan Masyarakat PT. XYZ.

Analisis Kerentanan *Session Timeout Protocol*

Deskripsi Kerentanan

Pada saat pengujian aplikasi gawai saat pengguna telah melakukan login ke Aplikasi, selama pengguna tersebut tidak melakukan logout aplikasi maka pengguna tidak perlu melakukan login kembali jika ingin menggunakan Aplikasi gawai karena tidak ada manajemen *session* untuk otomatis *logout* dalam jangka waktu tertentu.

Pemetaan OWASP dan Dampak

Standard OWASP *Mobile Security Guideline*, V4: *Authentication and Session Management Requirement* (M4), ID standarisasi MSTG-AUTH-7, "Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire."
Terhadap kerentanan jenis ini dalam standard OWASP *Mobile Security* dijelaskan bahwa :

Thread Agent bersifat *Application Specific* dimana *Thread Agent* yang mengeksploitasi kerentanan otentikasi biasanya melakukannya melalui serangan otomatis yang menggunakan alat yang tersedia atau dibuat khusus (Wang & Alshboul, 2015).

Pembobotan CVSS

Penilaian CVSS didasarkan pada skenario penyerang yang mengeksploitasi session aktif melalui jaringan:

Tabel 1. Tabel Pembobotan CVSS Session Timeout Protocol

Metrik	Nilai Vektor	Justifikasi Teknis
Attack Vector (AV)	Network (N)	Penetrasi dapat dilakukan melalui jaringan internet, seringkali melalui serangan otomatis terhadap backend.
Attack Complexity (AC)	Low (L)	*Exploitability* diklasifikasikan OWASP sebagai EASY, menunjukkan keberhasilan yang berulang.
Privileges Required (PR)	High (H)	Penyerang harus terlebih dahulu mendapatkan session atau kredensial pengguna yang sudah login.
Confidentiality Impact (C)	High (H)	Kerahasiaan data terancam secara total selama session aktif.
Remediation Level (RL)	Workaround (W)	Perbaikan memerlukan kustomisasi kode aplikasi gawai (implementasi session management di backend).

Vektor String CVSS : AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:L/E:P/RL:W/RC:X
Base Score: 5.2 (*Medium*), *Temporal Score*: 4.8 (*Medium*).

Analisis Kerentanan *Application Backgrounding* (*Screenshoot*)

Deskripsi Kerentanan

Aplikasi gawai gagal mengimplementasikan fungsi pencegahan *screenshot* saat aplikasi terbuka atau saat diminimalkan (aplikasi *backgrounding*). Hal ini berpotensi mengekspos konten sensitif dalam *snapshot* aplikasi.

Pemetaan OWASP dan Dampak

Standard Kerentanan ini berkaitan dengan penyimpanan data sementara dan privasi, melanggar Standard OWASP Mobile Security Guideline, V2: Data Storage and Privacy Requirements (M9), ID standarisasi MSTG-STORAGE-2. Threat Agent dapat mengeksploitasi ini dengan akses fisik ke perangkat, memungkinkan ekstraksi informasi sensitif melalui alat forensik.

Pembobotan CVSS

Penilaian CVSS didasarkan pada skenario serangan yang membutuhkan akses lokal perangkat:

Tabel 2: Tabel Pembobotan CVSS Session Timeout Protocol

Metrik	**Nilai Vektor**	**Justifikasi Teknis**
Attack Vector (AV)	Local (L)	Eksploitasi utama memerlukan penyerang untuk mengakses data yang tersimpan di perangkat secara lokal (melalui screenshot atau snapshot).
Attack Complexity (AC)	Low (L)	*Exploitability* diklasifikasikan sebagai EASY. Peretas yang memiliki akses fisik perangkat dapat menghubungkannya ke komputer dan menggunakan perangkat lunak yang tersedia secara bebas.
Privileges Required (PR)	High (H)	Kerentanan terjadi setelah pengguna berhasil login dan data sensitif ditampilkan.
Confidentiality Impact (C)	High (H)	Dapat mengakibatkan hilangnya data sensitif dalam konteks terburuk bagi banyak pengguna.
Availability Impact (A)	Low (L)	Dampak pada ketersediaan umumnya kecil, namun eksploitasi berkelanjutan dapat mengganggu ketersediaan data.

Vektor String CVSS : AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:L/E:P/RL:W/RC:X
Base Score: 5.2 (*Medium*), *Temporal Score*: 4.8 (*Medium*).

Analisis Kerentanan *Weak Password Policy Implementation*

Deskripsi Kerentanan

Aplikasi gawai mengizinkan penggunaan kata sandi lemah (hanya numerik) tanpa ketentuan kompleksitas yang ketat, dan kebijakan ini tidak diverifikasi secara memadai di sisi server (backend), melanggar prinsip defense-in-depth.

Gambar 4. Password Numeric

Pemetaan OWASP dan Dampak

Hal ini melanggar Standard OWASP *Mobile Security Guideline, V1: Architecture, Design and Thread Modelling Requirements* (M1), ID standarisasi MSTG-ARCH-2, yang menekankan bahwa kontrol keamanan tidak boleh hanya diterapkan di sisi klien. Kegagalan ini memungkinkan penyerang melakukan serangan *brute-force* atau *dictionary attack* secara *incremental*.

Pembobotan CVSS

Penetapan skor mencerminkan kompleksitas serangan dan dampak terhadap kerahasiaan kredensial:

Tabel 3. Tabel Pembobotan CVSS Session Timeout Protocol

Metrik	Nilai Vektor	Justifikasi Teknis
Attack Vector (AV)	Network (N)	Serangan (misalnya *brute-force*) dilakukan melalui jaringan internet terhadap API otentikasi.
Attack Complexity (AC)	High (H)	Meskipun password lemah, serangan *penebakan (brute-force atau dictionary attack*) secara *incremental* memerlukan investasi upaya terukur oleh penyerang untuk mencapai keberhasilan (misalnya, mengatasi mekanisme *lockout*). Ini mewakili kondisi di luar kendali penyerang.
Privileges Required (PR)	High (H)	Asumsi penyerang adalah pengguna yang sah yang mencoba merusak kredensial lain, atau penyerang membutuhkan *session* otorisasi dasar.
Confidentiality Impact (C)	High (H)	Jika serangan berhasil, terjadi total kehilangan kerahasiaan kredensial pengguna.
Attack Vector (AV)	Network (N)	Serangan (misalnya *brute-force*) dilakukan melalui jaringan internet terhadap API otentikasi.

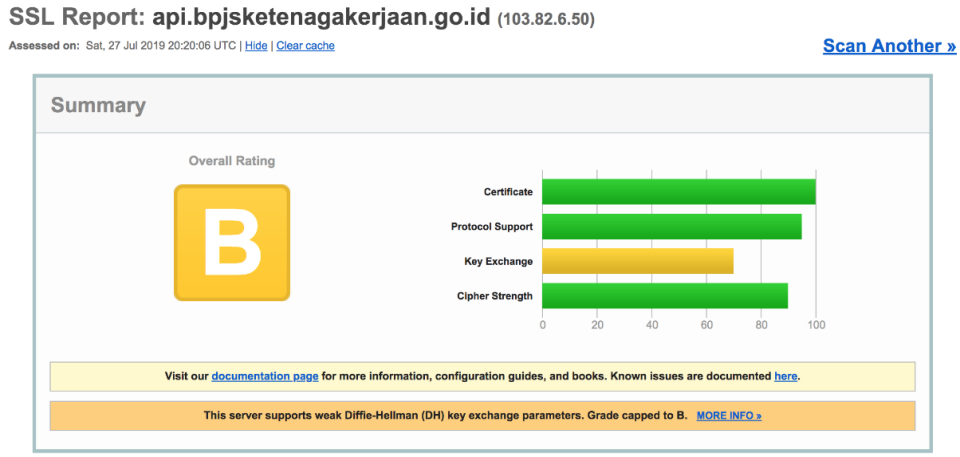
Vektor String CVSS : AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N/E:P/RL:W/RC:X

Base Score: 4.8 (*Medium*), *Temporal Score:* 3.9 (*Low*).

Analisis Kerentanan *Use Of Insecure And Deprecated Algorithm*

Deskripsi Kerentanan

Aplikasi Pengecekan kualitas lapisan komunikasi (SSL/TLS) API aplikasi gawai melalui *Qualys SSL Labs* mengidentifikasi penggunaan algoritma "Diffie-Hellman" (DH) yang lemah, yang rentan terhadap serangan Logjam. Skor ketahanan kerentanan yang didapat adalah B (Labs, 2015).



Gambar 5. Penilaian Skor SSL

Pemetaan OWASP dan Dampak

Standard OWASP Mobile Security Guideline, V3: *Cryptography Requirement* (M10), ID standarisasi MSTG-CRYPTO-2, yang mewajibkan aplikasi menggunakan implementasi kriptografi yang terbukti aman. Algoritma DH yang lemah terekspos terhadap serangan *man-in-the-middle* (MITM) Logjam, memungkinkan penyerang membaca dan memodifikasi data yang melewati koneksi.

Pembobotan CVSS

Penetapan skor mencerminkan kompleksitas serangan istemik yang dapat ditimbulkan, meskipun serangan tersebut kompleks:

Tabel 6. Tabel Pembobotan CVSS Session Timeout Protocol

Metrik	Nilai Vektor	Justifikasi Teknis
Attack Vector (AV)	Network (N)	Eksploitasi terjadi melalui saluran komunikasi jaringan.
Attack Complexity (AC)	High (H)	Serangan *Logjam* membutuhkan upaya yang terukur dan persiapan yang canggih oleh penyerang.
Privileges Required (PR)	None (N)	Serangan ini ditujukan pada konfigurasi SSL/TLS server, tidak memerlukan otentikasi pengguna.
Scope (S)	Changed (C)	Kerentanan ini tidak terbatas pada aplikasi gawai saja; eksploitasi yang berhasil dapat memengaruhi sumber daya API Server yang

Metrik	Nilai Vektor	Justifikasi Teknis
		terikat (*resource* di luar komponen rentan), sehingga lingkup serangan meluas.
Exploit Code Maturity (E)	Functional (F)	Terdapat laporan eksploitasi kerentanan *Logjam* yang berhasil dilakukan, meskipun serangan canggih.

Vektor String CVSS : AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:F/RL:O/RC:X
Base Score: 6.8 (*Medium*), *Temporal Score:* 6.3 (*Medium*).

KESIMPULAN

Hasil Analisa yang dilakukan berhasil melaksanakan analisis risiko kerentanan keamanan Aplikasi Gawai Layanan Masyarakat PT. XYZ pada platform Android menggunakan metodologi *Greybox* Testing dengan standarisasi *OWASP Mobile Security Testing Guide.* Kuantifikasi risiko dilakukan menggunakan *Common Vulnerability Scoring System* (CVSS), menjamin interpretasi yang terstruktur dengan penentuan prioritas yang jelas. Ditemukan empat kerentanan utama yang memengaruhi Kerahasiaan dan Integritas: 1) *Session Timeout Protocol. 2) Application Backgrounding,* 3) *Weak Password Policy Implementation* dan 4) *Use Of Insecure Deprecated Algorithm*.

Skor risiko kerentanan aplikasi gawai secara keseluruhan berada dalam kategori MEDIUM, dengan Skor Temporal rata-rata 4.9. Kerentanan yang memiliki prioritas mitigasi tertinggi adalah (*Insecure Deprecated Algorithm,* Temporal Score 6.3), berdasarkan pada potensi dampak sistemik (*Scope Changed*) yang dapat memengaruhi infrastruktur API *server*,. Dengan Nilai keseluruhan *Average Score* Aplikasi Gawai PT. XYZ adalah 4,9. Kerentanan keamanan aplikasi gawai pada umumnya mendapatkan predikat MEDIUM. Sehingga perlu dilaksanakan perbaikan keamanan agar tidak disalahgunakan atau dimanfaatkan oleh pengguna yang tidak bertanggung jawab untuk mendapatkan informasi-informasi yang ada di dalam Aplikasi gawai layanan publik PT. XYZ.

DAFTAR PUSTAKA

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., & Zimmermann, P. (2015). Imperfect forward secrecy: How Diffie-Hellman fails in practice. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 5–17. https://doi.org/10.1145/2810103.2813707

Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020). Mobile application security penetration testing based on OWASP. *IOP Conference Series: Materials Science and Engineering*, *846*(1), 12036. https://doi.org/10.1088/1757-899X/846/1/012036

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5.

Diallo, A., Samhi, J., Bissyandé, T. F., Bodden, E., & Klein, J. (2025). (In)Security of mobile

apps in developing countries: A systematic literature review. *Empirical Software Engineering*, *30*, 131. https://doi.org/10.1007/s10664-025-10689-z

First.Org, I. (2019). *Common Vulnerability Scoring System version 3.1: Specification document*. Forum of Incident Response and Security Teams. https://www.first.org/cvss/v3.1/specification-document

Haq, I., Khan, T., Ahmad, M., & Alam, M. (2021). Penetration frameworks and development issues in secure mobile application development: A systematic literature review. *IEEE Access*, *9*, 79857–79882. https://doi.org/10.1109/ACCESS.2021.3084842

Isnaini, K., Sari, G. J. N., & Kuncoro, A. P. (2023). Analisis Risiko Keamanan Informasi Menggunakan ISO 27005: 2019 pada Aplikasi Sistem Pelayanan Desa. *Jurnal Eksplora Informatika*, *13*(1), 37–45.

Jaelani, W. L., Monellia, I., & Mutoffar, M. M. (2024). Analisis Dan Perancangan Keamanan Aplikasi Manajemen Layanan Sistem Pemerintahan Berbasis Elektronik. *Seminar Nasional Penelitian (Semnas Corisindo 2024)*, 235–241.

Kadir, F. M., Irsan, M., & Putrada, A. G. (2025). Benchmarking mobile apps security in universities: An OWASP Mobile Top 10 framework perspective. *IJoICT (International Journal on Information and Communication Technology)*, *11*(1), 1–15. https://doi.org/10.29099/ijct.v11i1.9094

Karim, A., Umam, M. N., Fatahillah, M. L., & Hadi, M. A. F. (2024). Identifikasi Kerentanan dan Upaya untuk Melindungi Data Pada Aplikasi Seluler. *JUSTIFY: Jurnal Sistem Informasi Ibrahimy*, *2*(2), 178–181.

Kim, H., Lee, S., & Kim, J. (2015). Analyzing user awareness of privacy data leak in mobile applications. *Mobile Information Systems*, *2015*, 369489. https://doi.org/10.1155/2015/369489

Labs, Q. S. S. L. (2015). *SSL Labs grading methodology*. Qualys, Inc. https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Petraityte, M., Dehghantanha, A., & Epiphaniou, G. (2018). A model for Android and iOS applications risk calculation. In *Cyber Threat Intelligence* (pp. 107–126). Springer. https://doi.org/10.1007/978-3-319-73951-9_6

Project, O. W. A. S. (2018). *Mobile Security Testing Guide*. OWASP Foundation.

Project, O. W. A. S. (2024). *OWASP Mobile Top 10 2024*. OWASP Foundation. https://owasp.org/www-project-mobile-top-10/

Riskhan, B., Zakariyah, A. A., Farman Ali, M., Amin Ullah Sheikh, M., & Verma, R. (2025). Current security issues and vulnerabilities associated with mobile application. In *Proceedings of 4th International Conference on Mathematical Modeling and Computational Science* (pp. 27–40). Springer. https://doi.org/10.1007/978-3-031-90998-6_3

Technology, N. I. of S. and. (2023). *National Vulnerability Database: Vulnerability metrics*.

U.S. Department of Commerce. https://nvd.nist.gov/vuln-metrics/cvss

Wang, Y., & Alshboul, Y. (2015). Mobile security testing approaches and challenges. *1st Conference on Mobile and Secure Services (MOBISECSERV)*, 1–5. https://doi.org/10.1109/MOBISECSERV.2015.7073704