ISSN: 2477-0078

Evaluasi Risiko Keamanan Sistem SIREKAP Berbasis STRIDE dan DREAD

Nurul Iflahah[1], Masdukil Makruf[2], Fathorrozi Ariyanto[3]
[123]Teknik informatika,Fakultas Teknik,Universitas Islam Madura
[1]nuruliflahah123@gmail.com, [2]masdukil.makruf@gmail.com, [3]fathorroziariyanto7@gmail.com

ABSTRAK

Sistem Informasi Rekapitulasi (SIREKAP) yang dikembangkan oleh Komisi Pemilihan Umum (KPU) memiliki peran penting dalam menjaga transparansi serta akurasi proses Pemilu. Namun, sifatnya yang digital dan terhubung dengan jaringan internet membuat sistem ini rentan terhadap berbagai ancaman siber seperti spoofing, manipulasi data, maupun kebocoran informasi. Penelitian ini melakukan evaluasi risiko keamanan pada SIREKAP dengan pendekatan *threat modeling* menggunakan metode STRIDE dan DREAD. Analisis difokuskan pada tiga komponen utama, yaitu browser, Web API, dan basis data. Hasil penilaian dengan metode DREAD menunjukkan bahwa browser merupakan titik paling rawan dengan skor 35 (kategori risiko tinggi), sedangkan Web API dan basis data masing-masing berada pada kategori risiko sedang. Temuan ini memperlihatkan bahwa aspek autentikasi pengguna menjadi prioritas dalam mitigasi risiko. Oleh karena itu, penelitian ini mengusulkan beberapa strategi pengamanan, antara lain penerapan autentikasi multi-faktor (MFA), validasi masukan pada Web API, serta pembatasan akses basis data dengan prinsip *least privilege*. Dengan rekomendasi tersebut, diharapkan keamanan sistem SIREKAP dapat ditingkatkan sehingga integritas dan transparansi hasil Pemilu tetap terjaga. Penelitian ini juga memberikan landasan bagi pengembangan langkah mitigasi lanjutan dalam menghadapi potensi serangan siber di masa mendatang.
Kata kunci: SIREKAP, keamanan siber, STRIDE, DREAD, threat modeling.

ABSTRACT

The Election Recapitulation Information System (SIREKAP), developed by the General Elections Commission (KPU), plays a crucial role in maintaining the transparency and accuracy of the election process. However, its digital nature and internet connectivity make it vulnerable to various cyber threats, such as spoofing, data manipulation, and information leaks. This study evaluates SIREKAP's security risks using a threat modeling approach using the STRIDE and DREAD methods. The analysis focused on three main components: the browser, Web API, and database. The DREAD assessment revealed that the browser was the most vulnerable point with a score of 35 (high risk category), while the Web API and database were each in the medium risk category. These findings demonstrate that user authentication is a priority in risk mitigation. Therefore, this study proposes several security strategies, including the implementation of multi-factor authentication (MFA), input validation on the Web API, and limiting database access using the principle of least privilege. These recommendations are expected to improve the security of the SIREKAP system, thereby maintaining the integrity and transparency of the election results. This research also provides a foundation for developing further mitigation measures to address potential future cyber attacks.
Keywords: *SIREKAP, cybersecurity, STRIDE, DREAD, threat modeling.*

1. PENDAHULUAN

Sirekap merupakan sebuah aplikasi berbasis teknologi informasi yang digunakan untuk mempublikasikan hasil penghitungan suara dan proses rekapitulasi Pemilu,keamanan pada sistem rekap pemilu sangat penting dilakukan untuk mencegah manipulasi hasil dan sebagainya. Selain itu, aplikasi ini juga berfungsi sebagai alat bantu dalam pelaksanaan rekapitulasi hasil penghitungan suara. Dengan meningkatnya kompleksitas pemilihan umum dan volume data yang dikelola, memastikan keandalan sistem ini menjadi sangat penting untuk menjaga integritas dan transparansi pemilu (Lestari & Utamajaya,

ISSN: 2477-0078

t.t.2024). Tidak hanya itu, mejaga keamanan data pada sistem tersebut juga harus dilakukan terlebih pada sistem SiRekap[2] ,yang memuat dan menyimpan serta mengelola data dari suara dari pemilihan dikarenakan banyak sistem pemilu mengalami masalah dalam hal keamanan siber, yang dapat mengakibatkan kebocoran data dan potensi manipulasi hasil pemilu[3].

Dalam penelitian Iwana[4] yakni threat modeling menggunakan pendekatan STRIDE dan DREAD untuk mengetahui risiko dan mitigasi keamanan pada sistem layanan pendidikan menjelaskan bahwa berhasil mengidentifikasi dan mengevaluasi berbagai ancaman yang terdapat pada sistem layanan pendidikan Universitas X dengan menggunakan pendekatan threat modeling berbasis STRIDE dan DREAD.

Sistem yang rentan untuk disusupi oleh pihak lain akan mengakibatkan keutuhan dan keakuratan datanya dipertanyakan.[5]Oleh karena itu sistem rekapitulasi dijadikan sasaran dalam penelitian yang ingin mencari celah d an kelemahan pada sistem tersebut,dikarenapan pada Sistem REKAPITULASI SUARA pada pemilihan tidak dapat dipungkiri keamanan sistem tersebut aman [3].

Berbagai penelitian menjelaskan tentang penggunakan metode STRIDE dan DREAD yang diterapkan di berbagai sistem untuk keamanan serta melihat tingkat resiko dan juga mitigasinya,salah satu penelitian dari Muhammad Khairul Faridi (2021) dengan judul penelitiannya pemodelan sistem E-Health menggunakan metode[6] STRIDE dan DREAD Berdasarkan hasil identifikasi ancaman menggunakan model STRIDE dan penilaian ancaman menggunakan metode DREAD dapat disimpulkan bahwa tingkat ancaman pada masing-masing bagian seperti pengguna, web server, dan database memiliki tingkat ancaman paling banyak yaitu medium dan low. Sedangkan tingkat ancaman tertinggi high terdapat pada bagian database dengan ancaman denial of servic[7].

Penelitian yang dilakukan oleh Said Akmala (2021) Evaluasi Keamanan Sistem E-Government menggunakan Security Development Lifecycle (SDL) Threat Modelling Tool dengan hasil Berdasarkan hasil pemodelan dan pengujian system e-government (website e monitoring) terdapat 5 kategori potensi risiko ancaman, namun hal itu masih bisa dilakukan langkah mitigasi terhadap potensi risiko ancaman yang mungkin akan terjadi. Adapun langkah mitigasi dapat dilakukan prioritas perbaikan system berdasarkan tingkat ancaman tertinggi hingga terkecil. Beberapa langkah mitigasi ancaman juga sudah diterapkan pada web e-monitoring untuk mengamankan data yang ada seperti pencegahan terhadap DDos menggunakan Cloudflare, menyembunyikan login page dan melakukan enkripsi terhadap direktori yang ada.

Penelitian dari Azis Catur Laksono dan Yudi (2021) dengan npenelitian Threat Modeling Menggunakan Pendekatan STRIDE dan DREAD untuk Mengetahui risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik [8].

Tujuan dari penelitian ini adalah untuk menganalisis sistem SIREKAP pemilu yang mana pada sistem tersebut merupakan sistem yang sangat penting untuk dijaga akan keakuratan hasilmnya,sehigga diharapkan dengan hasil dari penelitiab ini dapat membantu tim IT yang bertugas dalam menjaga keabsahan dari hasil tersebut dengan metode STRIDE dan DREAD [9].

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan *Threat Modelling* yang menggunakan metode *STRIDE* dan *DREAD* yang mana pada pendekatan Threat modelling atau pemodelan ancaman ini dapat membantu perusahaan atau sistem untuk menghindari kebocoran data, informasi, hingga aset penting dalam keamanan siber [10]. Dengan menggunbakan metode STRIDE yaitu singkatan dari *STRIDE* adalah singkatan dari *Spoofing*, Tampering, Repudiation, Information Disclosure, Denial of Service, dan Elevation of

ISSN: 2477-0078

Privilege , yang merupakan ancaman paling umum terhadap aplikasi.Yang kemudian untuk mengkategorikan nilai resiko dari ancaman tersebut yaitu menggunakan metode *DREAD*.Berikut merupakan metode penelitian yang digunakan :

2.1 Identifikasi sistem

Identifikasi sistem dilakukan dengan cara menganalisis sistem web dari SIREKAP [11] yakni https://www.kpu.go.id/cari/sirekap.Website tersebut merupakan sistem yang digunakan untuk mengumpulkan, memproses, dan menyajikan data hasil Pemilu secara resmi.

2.2 Klasifikasi Ancaman berdasarkan STRIDE

Setelah melakukan identifikasi sistem langkah selanjutnya yaitu melakukan klasifikasi dari sistem tersebut dengan mengategorikan atau memetakkan sistem ke metode STRIDE

Proses klasifikasi ancaman dilakukan dengan mengadopsi kategorisasi ancaman pada metodologi STRIDE.

2.3 Penilaian Ancaman

Merupakan tahap penerapan metode DREAD [12] untuk menilai, membandingkan, dan memprioritaskan tingkat risiko yang ditimbulkan dari setiap ancaman. Istilah DREAD merupakan singkatan dari setiap kategori risiko yaitu Damage potential, Reproducibility, Exploitability, Affected user, dan Discoverability.

Tabel 4.1 merupakan skema pengertisn Dread serta penjelasan Penilaian[8] pada ancaman yang biasa digunakan dalam memebrikan nilai Ancaman dengan peringkat tinggi dinilai sama dengan 3, peringkat sedang dinilai sama dengan 2, dan peringkat rendah dinilai sama dengan 1 [5].

Dengan rumus sebagai berikut :

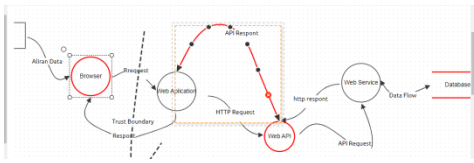
` $Rs_{(t)} = \frac{D_{(T)}+R_{(t)}+E_{(t)}+A_{(t0}+D_{(t)}}{5}$.

3. HASIL DAN PEMBAHASAN

Hasil dari pengumpulan informasi tentang sistem SIREKAP dalam bentuk dokumen threat model selanjutnya digunakan untuk bahan penyusunan Data Flow Diagram yang menggunakan aplikasi *OWASP THREAT DRAGON*. Pada tabel 5 dibawah ini merupkan Penilaian ancaman hasil analisis dari 3 komponen Sirekap.

Pengurain Pemodelan Sistem SIREKAP

Gambar di bawah menunjukkan hasil analisis Streat Dragon OWASP yang menjelaskan beberapa sistem yang mengalami ancaman:



Gambar 1. Pemodelan sistem Sirekap

Dari hasil analisis tersebut menggunakan Owasp treat dragon dapat diketahui bahwa beberapa sistem tersebut mengalami ancaman diantaranya Browser,Web Api,Database.

Dibawah merupakan tabel hasil threats atau pemodelan ancaman pada sistem yang dianalisis menggunakan OWASP THREAT DRAGON.Dari beberapa threat tersebut beberapa yang dijadikan sampel dan dimitagsi berikut merupakan threat yang termasuk pada kategori metode yang digunakan.

1) Browser

Browser disini merupakan salah satu sistem yang menjadi komponen ancaman dengan memodelkan pada manajemen sistem sirekap maka bisa digambarkan seperti dibawa ini:



Gambar 2. Threat Browser

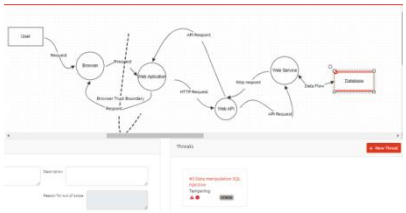
Pada browser menjadi sistem yang terancam pada Sirekap setelah di analisis dengan OWASP Threat Dragon ,browser menjadi akses dan konten pada internet,dan menjadi titik utama masuknya bagi petugas KPPU,KPPS sehingga ancaman yang

ISSN: 2477-0078

terjadi pada browser meliputi penyerang menyamar sebagai entitas yang sah untuk mendapatkan akses tidak sah ke sistem.

2) Web API

Gambar dibawa ini merupakan penjambaran pada analisis Web API.

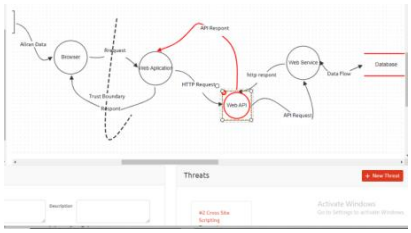


Gambar 3. Threat Web API

Serangan skrip lintas situs (Cross-Site Scripting atau XSS) merupakan serangan keamanan yang memanfaatkan kelemahan pada aplikasi web untuk menyisipkan skrip berbahaya ke dalam halaman yang dilihat oleh pengguna.

3) Database

Gambar dibawah ini merupakan penjabaran pada analisis Database.



Gambar 4. Threat Database

Manipulasi data merupakan ancaman serius terhadap integritas sistem, khususnya dalam database. Jika dibiarkan, ancaman ini dapat mengakibatkan kehilangan kepercayaan pengguna, kerugian finansial, dan gangguan operasional.

Langkah selanjutnya setelah melakukan klasifikasi ancaman pada 3 komponen sistem Sirekap [3] tersebut yakni menilai ancaman dan usulan mitigasi pada setiap sistem terhadap keamanan siber [13].

Pada tabel 2 dibawah ini merupakan daftar ancaman pada browser yang menjadi pembuka utama di setiap aplikasi, web API menjadi jembatan pada backend dan frontend sehingga antara keduanya menjaga keamanan data suara yang masuk pada sistem Sirekap,dan Database yang menjadi penyimpanan semua data serta penilaian dengan DREAD menggunakan OWASP Threat Dragon.

Tabel 2. Penilaian pada Browser

No	Komponen	STRIDE	Jenis ancaman	D	R	E	A	D	Total	Jenis ancaman
1	Browser	Spoofing	Sasaran serangan skrip lintas situs	8	7	6	9	5	25	Tinggi
2	Web API	Tampering	Sasaran serangan skrip lintas situs	3	2	2	2	2	11	Sedang
3	Database	Tampering	Manipulasi Data	3	3	2	3	2	13	Sedang

Berdasarkan pengolahan data dengan STRIDE dan DREAD, browser memperoleh skor tertinggi (35), menunjukkan bahwa komponen ini merupakan titik terlemah dalam sistem Sirekap [14]. Web API dan database menunjukkan risiko menengah. Temuan ini memperjelas bahwa ancaman spoofing melalui browser adalah prioritas utama mitigasi.

Mitigasi Setelah melakukan penilain ancaman pada sistem tersebut maka untuk menanggulangi ancaman serta tingkat resikonya perlu pada sistem tersebut dimitigasi , Mitigasi (mitigasi) adalah pengurangan bahaya atau mitigasi. Memitigasi risiko berarti menerima tingkat risiko tertentu[15]. Pada tabel 3 dibawah ini merupakan ususlan mitigasi dari 3 komponen diatas:

Tabel 4. Usulan mitigasi

No	Ancaman	Kategori	Usulan mitigasi
1	Spoofing	Browser Hijacking	Penerapan SSL/TLS:Gunakan SSL/TLS yang valid untuk memastikan pengguna hanya mengakses situs resmi.
2	Tempering	Cross Site Scripting	Validasi & Sanitasi Input Pengodean Output Gunakan Header Keamanan
3	Tempering	Data manipulation	Gunakan ORM seperti SQLAlchemy, Hibernate, menghindari atau Django ORM untuk kueri mentah.

ISSN: 2477-0078

4. KESIMPULAN

Penelitian ini berhasil menerapkan threat modeling dengan metode STRIDE dan DREAD untuk menganalisis risiko pada sistem SIREKAP. Hasilnya menunjukkan komponen browser paling rentan dengan skor DREAD 35 (risiko tinggi), sementara Web API (11) dan Database (13) berada pada kategori risiko sedang. Hal ini menegaskan perlunya penguatan keamanan, terutama pada akses pengguna, komunikasi antar sistem, dan penyimpanan data.Rekomendasi pengembangan mencakup penerapan autentikasi multi-faktor (MFA), penggunaan protokol HSTS, pelatihan pengguna terhadap ancaman spoofing, serta audit lanjutan melalui uji penetrasi dan validasi input ketat. Integrasi alat pemantauan berbasis AI atau SIEM juga disarankan untuk deteksi real-time. Penelitian berikutnya perlu menggunakan data operasional aktual dan memperluas cakupan ke komponen lain seperti server, jaringan, dan deployment.

UCAPAN TERIMA KASIH

Ucapan terimakasih disampaikan kepada Dosen pembimbing baik pembimbing 1 maupun 2 terutama pembimbing 1 yang telah memberikan arahan serta bimbingannya dalam menyelesaikan tugas akhir ini.Tidak lupa pula terhadap teman dan semua dosen yang telah mensuport saya dalam menyelesaikan tugas akhir ini.

DAFTAR PUSTAKA

[1] A. Y. Lestari dan J. N. Utamajaya, “Audit Sistem Informasi Aplikasi Sirekap KPU: Analisis Keamanan dan Efisiensi”.

[2] S. Rochman, Dwi Hastuti, dan Rasyida Shabihah Zukro Aini, “Cybersecurity Measures For Election Information Systems : Sistem Rekapitulasi Suara Pemilu 2024 (siRekap),” *Buana Electrical, Science & Technology*, vol. 6, no. 1, Jun 2024, doi: 10.36456/best.vol6.no1.9182.

[3] Amelia Yoga Lestari dan Joy Nashar Utamajaya, “Audit Sistem Informasi Aplikasi Sirekap KPU: Analisis Keamanan dan Efisiensi,” *Switch*, vol. 2, no. 4, hlm. 23–32, Agu 2024, doi: 10.62951/switch.v2i4.178.

[4] A. A. Iwana, R. B. Huwae, A. H. Jatmika, dan J. Majapahit, “THREAT MODELING MENGGUNAKAN PENDEKATAN STRIDE DAN DREAD UNTUK MENGETAHUI RISIKO DAN MITIGASI KEAMANAN PADA SISTEM LAYANAN PENDIDIKAN,” Vol. 7, no. 1, 2025.

[5] A. C. Laksono dan Y. Prayudi, “Threat Modeling Menggunakan Pendekatan STRIDE dan DREAD untuk Mengetahui Risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik,” *j.sist.teknol.inf.*, vol. 6, no. 1, hlm. 9–20, Jun 2021, doi: 10.32528/justindo.v6i1.3944.

[6] F. Luo, Y. Jiang, Z. Zhang, Y. Ren, dan S. Hou, “Threat Analysis and Risk Assessment for Connected Vehicles: A Survey,” *Security and Communication Networks*, vol. 2021, hlm. 1–19, Sep 2021, doi: 10.1155/2021/1263820.

[7] A. A. Nasution dan M. I. P. Nasution, “Analisis Keamanan Informasi dalam Sistem Informasi Manajemen: Tantangan dan Solusi di Era Cybersecurity,” vol. 02, no. 02, 2024.

[8] M. G. Br Sitorus, N. Maria, dan Y. N. Safa, “Tinjauan Literatur Manajemen Risiko Cyber dalam Proyek: Identifikasi, Evaluasi, dan Mitigasi Ancaman,” *JAMIKA*, vol. 14, no. 2, hlm. 187–198, Jul 2024, doi: 10.34010/jamika.v14i2.12887.

[9] A. S. Mubah, S. Anabarja, P. D. Yakti, dan A. Pratamasari, “DEVELOPING CRITICAL THINKING AND CYBERSECURITY LITERACY SKILLS AHEAD OF THE 2024 ELECTION FOR STUDENTS AT VOCATIONAL HIGH SCHOOL OF AL BADAR IN TULUNGAGUNG,” *JLM*, vol. 8, no. 3, hlm. 357–365, Sep 2024, doi: 10.20473/jlm.v8i3.2024.357-365.

[10] Angel Aurelia dan Andini Egista Maheswari S., “ANALISIS PENGIMPLEMENTASIAN ‘ASEAN CYBER SECURITY

ISSN: 2477-0078

FRAMEWORK' DI SINGAPURA TAHUN 2020," *JSER*, vol. 6, no. 1, hlm. 2168–2179, Sep 2024, doi: 10.54783/jser.v6i1.587.

[11] A. Hartomo, "Perencanaan Strategis Sistem Informasi Dan Sistem Manajemen Keamanan Informasi Berbasis ISO / IEC 27001 : 2013 Menggunakan Ward & Peppard Pada Perusahaan Transshipment," *JTIIK*, vol. 10, no. 1, hlm. 141, Feb 2023, doi: 10.25126/jtiik.20231015604.

[12] B. Branco, J. Silvestre Serra Silva, dan M. Correia, "Cyber Attacks on Commercial Drones: A Review," *IEEE Access*, vol. 13, hlm. 9566–9577, 2025, doi: 10.1109/ACCESS.2025.3527698.

[13] P. Das, Md. R. A. Asif, S. Jahan, K. Ahmed, F. M. Bui, dan R. Khondoker, "STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Treatment of an In-Vehicle Infotainment System," *Vehicles*, vol. 6, no. 3, hlm. 1140–1163, Jun 2024, doi: 10.3390/vehicles6030054.

[14] N. Inzana, A. A. Maulana, dan P. M. Sari, "Inovasi Sirekap dalam Meningkatkan Partisipasi Politik," *Villages*, vol. 5, no. 2, Mei 2024, doi: 10.47134/villages.v5i2.106.

[15] S. Sutrisno, L. Panggalo, M. Asir, M. Yusuf, dan P. A. Cakranegara, "Literature Review: Mitigasi Resiko dan Prosedur Penyelamatan pada Sistem Perkreditan Rakyat," *COSTING*, vol. 6, no. 2, hlm. 1154–1167, Jan 2023, doi: 10.31539/costing.v6i2.4879.

[16] F. Indah, A. Sidabutar, dan N. Annisa, "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)," vol. 1, no. 1, 2022.