Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 27128-27137
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Perancangan Sistem Informasi Untuk Deteksi Dini Serangan Social Engineering Berbasis Web

Muhammad Adhif Fajrian[1], Hery Afriyadi[2]
[1 2] Sistem Informasi,Sains dan Teknologi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi
[1] muhammadadhif06@gmail.com [2] hery.afriyadi@uinjambi.ac.id

Abstrak

Perkembangan teknologi informasi yang pesat telah mempermudah berbagai aspek kehidupan manusia, namun juga membuka peluang bagi pelaku kejahatan siber untuk melancarkan serangan terhadap sistem informasi. Salah satu jenis serangan yang sulit diidentifikasi adalah social engineering, yang mengeksploitasi kelemahan manusia melalui manipulasi psikologis. Data dari Indonesia Anti-Phishing Data Exchange (Idadx) menunjukkan peningkatan signifikan dalam laporan phishing pada kuartal keempat 2022 dan kuartal pertama 2023. Penelitian ini bertujuan membangun sistem informasi berbasis web yang mampu mendeteksi dini serangan social engineering sekaligus meningkatkan pemahaman pengguna melalui informasi edukatif. Sistem dirancang untuk mendeteksi serangan social engineering berbasis URL dan interaksi pengguna, seperti phishing, baiting, dan pretexting, dengan fokus pada deteksi dini serta edukasi pengguna. Metodologi Agile digunakan untuk memungkinkan penyesuaian sistem secara fleksibel melalui tahapan perencanaan, perancangan, pengembangan, pengujian, evaluasi, dan pemeliharaan. Hasil pengujian menunjukkan bahwa sistem mampu menjalankan fungsi deteksi sesuai harapan. Pendekatan rule based dinilai efektif dalam mendeteksi serangan social engineering yang umum terjadi serta memberikan peringatan awal kepada pengguna. Sistem ini diharapkan dapat membantu meningkatkan kewaspadaan dan pemahaman pengguna terhadap ancaman social engineering, sekaligus mendukung upaya pencegahan serangan siber secara lebih efektif. Selain itu, sistem dapat menjadi sarana edukasi bagi pengguna dalam mengenali berbagai bentuk manipulasi psikologis dan meningkatkan kesadaran terhadap keamanan informasi dalam penggunaan teknologi digital sehari-hari.

Kata Kunci: *Rekayasa Social, Sistem Informasi, Deteksi Dini, Agile, Phising*

1. Latar Belakang

Banyak aspek kehidupan manusia menjadi lebih mudah berkat perkembangan teknologi informasi yang pesat, khususnya di bidang komunikasi digital dan manajemen data. Akan tetapi, di sisi lain, kemajuan ini juga memberikan peluang bagi pelaku kejahatan siber untuk melancarkan berbagai serangan terhadap sistem informasi. Salah satu jenis serangan yang paling rumit dan sulit untuk diidentifikasi adalah serangan rekayasa sosial atau social engineering.

Di zaman teknologi yang semakin canggih dan meluas seperti saat ini, keterampilan dan perasaan rasa ingin tahu manusia untuk menguasai teknologi juga semakin tumbuh. Ini sejalan dengan munculnya berbagai jenis kejahatan online. Kejahatan dunia maya (cybercrime) adalah istilah singkat untuk aktivitas ilegal yang dilakukan melalui penyalahgunaan teknologi digital dan jaringan komputer [1].

Serangan pada perlindungan sistem informasi seringkali terjadi serangan saat ini. Kejahatan siber (cybercrime) di dunia maya sering kali dilakukan oleh sekelompok individu yang berusaha menerobos suatu sistem keamanan sebuah sistem. Kegiatan ini dimaksudkan untuk menemukan, mendapatkan, merubah, dan bahkan menghapus data yang terdapat dalam system itu jika memang benar-benar dibutuhkan [2].

Bahaya signifikan, seperti pelanggaran privasi, penyalahgunaan uang, dan kerugian finansial, terkait dengan phishing. Bahaya ini memengaruhi banyak aspek kehidupan internet di seluruh dunia, tidak hanya di Indonesia [3]. Dengan 6.106 pengaduan pada kuartal keempat tahun 2022 dan 26.675 laporan pada kuartal pertama tahun 2023, data dari Indonesia Anti-Phishing Data Exchange (Idadx) menunjukkan peningkatan yang cukup besar dalam laporan phishing [4].

Di era digital yang semakin maju, ancaman serangan social engineering (rekayasa social) terus berkembang dan menjadi salah satu tantangan utama dalam keamanan informasi. Serangan ini tidak hanya memanfaatkan celah teknis, tetapi juga lebih focus pada aspek manusia melalui manipulasi psikologis, seperti menciptakan kepercayaan, menimpulkan ketakutan, atau mengeksloitasi ketidak tahuan korban. Serangan social

engineering mengeksploitasi kelemahan manusia sebagai titik lemah utama. Akibatnya, identifikasi terhadap tipe serangan ini menjadi lebih menantang dan sering kali luput dari perhatian sistem keamanan umum. Berbagai bentuk umum dari serangan ini mencakup phishing, pretexting, baiting, dan tailgating, yang sering ditemukan di lingkungan organisasi maupun individu.

2. Metode Penelitian

Pendekatan penelitian kualitatif ini menekankan pada pengamatan langsung dan penggalian makna di baliknya. Dalam penelitian kualitatif, pilihan kata dan frasa memiliki dampak signifikan pada kejelasan dan analisis. Dengan demikian, Basri menyimpulkan bahwa dalam penelitian kualitatif, prosedur dan interpretasi temuan menjadi pusat perhatian. Untuk lebih memahami suatu peristiwa, aktivitas, atau fenomena, penelitian kualitatif lebih banyak bergantung pada aspek manusia, objek, dan institusi, serta hubungan atau interaksi antara hal-hal tersebut [5].

2.1. Metode Pengumpulan Data

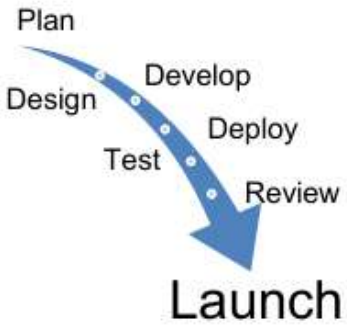
1. Observasi
   Pada tahap proses penelitian ini, para peneliti mengumpulkan data yang andal dan akurat melalui pengamatan atau peninjauan langsung. Pengamatan langsung di lokasi penelitian, yaitu Kantor Komunikasi dan Informatika Provinsi Jambi, digunakan untuk mengumpulkan data observasi.
2. Wawancara
   Wawancara tatap muka adalah metode pengumpulan informasi, penilaian keterampilan, atau mendapatkan sudut pandang seseorang tentang suatu subjek melalui percakapan. Penulis berbicara dengan Direktur dan karyawan terkait lainnya.
3. Studi Literatur
   Metodologi penelitian mencakup membaca materi tentang suatu subjek, mengidentifikasi literatur yang relevan, dan mensintesis temuan-temuan tersebut.

2.2 Metode Perancangan

1. UseCase Diagram
   Use Case Diagram Salah satu cara untuk menggambarkan dampak fungsional yang diharapkan dari sistem adalah melalui Diagram Kasus Penggunaan. Diagram Kasus Penggunaan menggambarkan bagaimana sistem akan berinteraksi dengan sekelompok pengguna atau entitas lain [6].
2. Activity Diagram
   Activity Diagram Pihak-pihak yang berkepentingan dapat memperoleh manfaat dari pengoperasian sistem ini, menurut diagram ini. Urutan proses suatu sistem ditunjukkan secara vertical [7].
3. Class Diagram
   Class Diagram Salah satu contoh diagram struktur UML adalah diagram kelas, yang memberikan representasi visual dari kelas, properti, metode, dan koneksi suatu objek [8].

2.3. Metode Pengembangan Sistem

Metodologi Agile digunakan dalam penelitian ini. Agile adalah metodologi untuk menciptakan perangkat lunak yang memprioritaskan rilis produk iteratif dan inkremental, kerja tim yang kuat, dan kemampuan beradaptasi [9]. Dalam hal pengembangan perangkat lunak, teknik Agile efektif dan lincah. Meskipun ada teknik untuk menjadi pemodel yang baik, pendekatan ini tidak memberikan proses yang tepat untuk membangun tipe model tertentu [10].



DOI: https://doi.org/10.31004/riggs.v5i2.13456

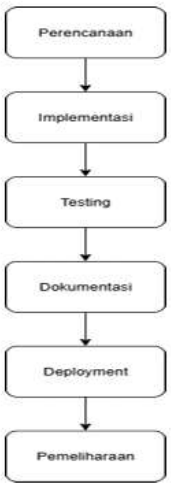
Gambar 2.1 Tahapan Metode Agile

Gambar diatas merupakan tahapan umum dari proses metode agile, Adapun penjelasan dari masing-masing tahapan yaitu sebagai berikut :

1. Planning (Perancanaan)
   Tahap ini dilakukan identifikasi kebutuhan sistem berdasarkan studi literatur dan hasil observasi terhadap ancaman social engineering yang umum terjadi.
2. Design (Perencangan)
   Setelah perencanaan selesai, dilakukan perancangan sistem yang meliputi wireframe antarmuka, arsitektur basis data, dan pemetaan alur kerja berdasarkan proses deteksi dini serangan social engineering, seperti phishing, rekayasa psikologis, dan anomali perilaku pengguna.
3. Develop (Pengembangan)
   Tahap pengembangan dilakukan dengan menerjemahkan desain menjadi bentuk nyata berupa kode program. Dalam konteks sistem ini, pengembangan dilakukan menggunakan teknologi berbasis web, dengan Bahasa pemrograman seperti PHP, Javascript, serta basis data MySQL.
4. Test (Pengujian)
   Agar suatu sistem dapat berfungsi dengan baik, langkah ini sangat penting. Pengujian unit, pengujian integrasi, dan UAT adalah alat yang digunakan untuk menjalankan pengujian ini.
5. Deploy (Penerapan Sementara)
   Fitur yang telah diuji dan dinyatakan layak, akan dipasang (deploy) ke lingkungan pengujian (staging environment) atau server internal. Tujuannya agar stakeholder dapat mencoba sistem secara langsung dan memberikan masukan tambahan. Stabilitas sistem dan pencegahan kesalahan fatal memerlukan proses implementasi yang metodis dan progresif.
6. Review
   Di sini, penulis mengevaluasi hasil sprint yang telah selesai. Mengevaluasi fungsi sistem hanyalah permulaan, review juga mencakup proses refleksi tim terhadap hambatan atau kekurangan selama proses sprint.
7. Launch (Peluncuran Akhir)
   Tahapan terakhir adalah peluncuran sistem secara penuh kepada pengguna akhir. Setelah melalui beberapa iterasi dan proses evaluasi, sistem dinyatakan siap digunakan. Peluncuran dilakukan dalam bentuk rilis sistem ke server produksi, yang dapat diakses secara resmi. Sistem ini akan menjadi alat bantu untuk mendeteksi dan memitigasi potensi serangan social engineering secara dini.

2.4. Tahapan Penelitian

Pada penelitian ini peneliti menerapkan metode Agile, ada beberapa tahapan penelitian yang digunakan yaitu sebagai berikut:



DOI: https://doi.org/10.31004/riggs.v5i2.13456

Gambar 2.2 *Tahap Penelitian*

1. Perencanaan
   Pada tahap awal pengembangan sistem dengan metodologi Agile, dilakukan perencanaan melalui studi literatur, observasi, dan konsultasi dengan pihak terkait, yaitu Kantor Komunikasi dan Informatika Provinsi Jambi. Kebutuhan sistem didokumentasikan dalam product backlog yang mencakup fitur input konten, deteksi frasa manipulatif, dan tampilan hasil risiko. Selanjutnya, rencana kerja dibagi ke dalam beberapa sprint dengan prioritas fitur dan target tiap iterasi agar pengembangan lebih terarah dan adaptif terhadap perubahan.
2. Implementasi
   Tahap implementasi merupakan proses realisasi backlog dalam setiap sprint. Peneliti menggunakan PHP dan MySQL untuk membangun sistem deteksi dini berbasis web. Pengembangan dilakukan bertahap, mulai dari form input, deteksi frasa berisiko, hingga tampilan hasil analisis. Setiap sprint menghasilkan fitur yang siap diuji dan dievaluasi untuk dikembangkan pada sprint berikutnya.
3. Testing
   Setelah implementasi tiap sprint selesai, dilakukan pengujian fitur menggunakan metode black box untuk memastikan sistem bekerja sesuai harapan. Pengujian dilakukan melalui berbagai kasus, seperti memasukkan konten mencurigakan dan memeriksa hasil deteksi risiko. Jika ditemukan kesalahan atau ketidaksesuaian, sistem diperbaiki kembali pada tahap implementasi sebelum melanjutkan ke tahap berikutnya.
4. Dokumentasi
   Dokumentasi dilakukan selama proses pengembangan dan pengujian sebagai pencatatan aktivitas proyek. Dokumentasi mencakup skenario dan hasil pengujian, perubahan sistem, antarmuka, serta struktur basis data. Dokumentasi digunakan sebagai bahan laporan skripsi, referensi pengembangan, dan bentuk pertanggungjawaban atas keputusan teknis berdasarkan hasil pengujian.
5. Deployment
   Setelah seluruh fitur diuji dan berfungsi dengan baik, sistem di-deploy ke lingkungan uji coba atau server lokal untuk memastikan integrasi antarfitur berjalan lancar. Sistem kemudian diuji dengan skenario nyata untuk menilai performa dan penggunaannya sebelum dilakukan validasi akhir
6. Pemeliharaan
   Setelah sistem digunakan, dilakukan pemeliharaan untuk menjaga stabilitas dan menyesuaikan kebutuhan baru. Jika ditemukan bug, dilakukan perbaikan dan pengujian ulang. Permintaan fitur baru atau penyesuaian dari pengguna akan dimasukkan ke backlog dan dikembangkan kembali dalam siklus Agile. Pemeliharaan memungkinkan sistem terus beradaptasi dengan kebutuhan yang berkembang.

3. Hasil dan Pembahasan

3.1. Gambaran Umum Dinas Komunikasi dan Informatika Jambi

Statistik, kriptografi, dan komunikasi merupakan wewenang Kantor Komunikasi dan Informatika Jambi, sebuah badan regional yang melapor kepada Pemerintah Provinsi Jambi. Instansi ini bertanggung jawab menyediakan implementasi teknis untuk mendukung tata kelola pemerintahan yang efektif, transparan, dan akuntabel melalui teknologi informasi dan komunikasi.

Kantor Komunikasi dan Informatika Provinsi Jambi mengawasi sistem informasi pemerintah, pengembangan infrastruktur teknologi informasi, pengamanan jaringan, serta penyebaran informasi kepada masyarakat. Selain itu, instansi ini berperan dalam menjaga keamanan informasi dan sistem elektronik di lingkungan Pemerintah Provinsi Jambi, termasuk mencegah berbagai ancaman siber yang dapat mengganggu kinerja pemerintahan.

Seiring meningkatnya penggunaan teknologi digital dan sistem berbasis internet, potensi serangan siber, khususnya social engineering, semakin perlu diperhatikan. Social engineering merupakan tindakan manipulasi psikologis yang bertujuan menipu korban agar mengungkapkan informasi sensitif, seperti kredensial login. Ancaman ini dapat menyebabkan kebocoran data, gangguan layanan, serta menurunnya kepercayaan terhadap sistem informasi pemerintah.

Berdasarkan hasil observasi, pihak instansi jarang mendapatkan serangan social engineering. Namun, kemungkinan pegawai Dinas Komunikasi dan Informatika Provinsi Jambi menjadi korban tetap ada, sehingga dapat membahayakan profil pegawai maupun instansi.

Oleh karena itu, dibutuhkan sistem informasi untuk deteksi dini serangan social engineering sebagai platform daring yang dapat membantu Dinas Komunikasi dan Informatika Jambi memantau, mendeteksi, dan menganalisis aktivitas mencurigakan secara terorganisir. Sistem ini bertujuan mendukung pelaporan insiden, pengelolaan data serangan, serta pemberian peringatan kepada pihak yang tepat. Dengan adanya sistem ini,

DOI: https://doi.org/10.31004/riggs.v5i2.13456

diharapkan kesiapan keamanan informasi meningkat, respons terhadap ancaman menjadi lebih cepat, serta tercipta lingkungan sistem informasi pemerintahan yang lebih aman dan terkontrol.

3.2 Analisa Kebutuhan Sistem

3.2.1 Kebutuhan Fungsional

Untuk mencapai tujuan pengembangan sistem, sistem tersebut perlu memiliki karakteristik atau persyaratan fungsional tertentu. Kebutuhan fungsional sistem tersebut adalah sebagai berikut:

Tabel 3.1 Kebutuhan Fungsional

Pengguna	Kebutuhan Fungsional
Pegawai/karyawan Dinas Komunikasi dan Informatika Provinsi Jambi	Menyediakan form pelaporan Validasi input URL dan alasan pelaporan Menyimpan laporan ke database Memberikan konfirmasi pelaporan berhasil Melihat berita dan konten edukasi
Admin pengelola web Dinas Komunikasi dan Informatika Provinsi Jambi	Login dan Logout Menampilkan daftar laporan Melihat detail laporan Mengubah status laporan Mengubah berita dan konten edukasi

1. Halaman Log-in yang dapat dilakukan oleh admin pengelola web Dinas Komunikasi dan Informatika Provinsi Jambi dengan menginputkan username dan password, sementara pengguna bisa langsung masuk dan mengakses sistem untuk langsung digunakan.
2. Halaman dashboard bisa langsung diakses dan digunakan oleh pegawai/karyawan, pada halaman ini menampilkan analisis URL, data, laporkan URL mencurigakan dan konten edukasi, Sedangkan admin dapat melakukan pengecekan laporan terbaru, hasil analisis terbaru, Kelola konten, backup database dan informasi sistem.
3. Halaman Analisis URL dapat diakses untuk melakukan analisis URL yang mencurigakan, dan melihat hasil analisis beserta seluruh search engine yang menganalisisnya, pegawai/karyawan bisa mencetak laporan dan membagikan hasil ataupun langsung melaporkan URL tersebut.
4. Halaman Edukasi dapat diakses untuk mempelajari maksud dari Serangan Social engineering dan agar pegawai/karyawan tercegah dari serangan Social engineering.
5. Halaman Laporkan yang dapat diakses oleh pegawai/karyawan untuk melaporkan laman website yang mencurigakan beserta deskripsi kejadian untuk dilaporkan kepada admin.

3.2.2 Kebutuhan Non Fungsional

Selain fitur utama, sistem juga harus memenuhi aspek teknis yang mendukung peforma dan keamanan sistem, Berikut ialah kebutuhan non-fungsional:

DOI: https://doi.org/10.31004/riggs.v5i2.13456

Tabel 3.2 Kebutuhan Non Fungsional

Jenis kebutuhan	Penjelasan
Performa	Sistem harus merespons permintaan analisis URL dalam waktu ≤ 10 detik, juga harus mampu menangapi 100+ pengguna bersamaan, *database query* harus optimal dengan indeks yang sesuai dan API calls ke VirusTotal harus di-cache untuk performa.
Keamanan	Sistem harus mencegah SQL *injection*, juga harus mencegah XSS *attacks*, password harus di-*hash* dengan *bcrypt*, API key yang harus disimpan secara aman dan akses halaman admin harus diproteksi dengan otentikasi.
Ketersediaan	Sistem harus tersedia 24/7 dan harus memiliki backup *database* harian.
Usability	Antarmuka sistem harus *user-friendly* dan intuitif, juga sistem memiliki petunjuk penggunaan yang jelas, pesan error harus informatif dan membantu, dan sistem harus konsisten dalam design dan navigasinya.
Maintainability	Kode harus modular dan mudah dipahami, dokumentasi harus lengkap untuk *maintenance*, sistem harus mudah untuk di-*extend* dengan fitur baru, *Database schema* harus ter-normalisasi.
Realiability	Sistem harus konsisten dalam memberikan hasil analisis, data tidak boleh hilang atau *corrupt*, sistem harus handle error dengan baik dan backup dan *recovery procedures* harus sudah di tes.
Legal & Compliance	Sistem harus mematuhi kebijakan penggunaan VirusTotal API, dan harus mematuhi privasi data.

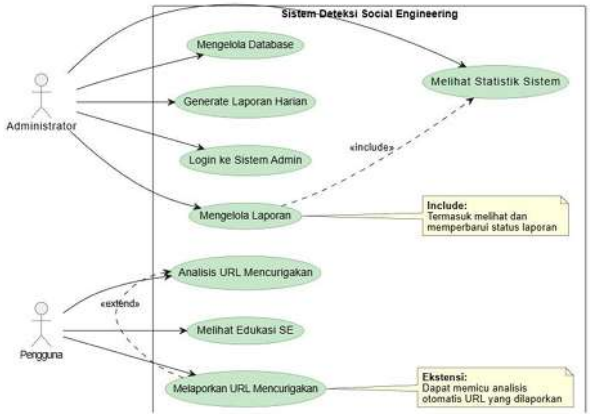
1. Keamanan data, sistem ini menerapkan autentikasi login untuk memastikan hanya admin yang dapat mengkases laman admin, sementara pengguna bisa langsung memakainya.
2. Kemudahan akses, antarmuka sistem dirancang dengan tampilan yang mudah digunakan oleh pengguna.
3. Kecepatan dan efisiensi, Sistem harus memiliki respon yang cepat terhadap analisis URL dan sistem laporan pengguna kepada admin.

3.3. Hasil Perancangan Sistem

3.3.1 Use Case Diagram

Use case diagram Bagian ini memberikan ringkasan tingkat tinggi tentang interaksi pengguna-sistem. Jika Anda ingin mengetahui siapa yang memiliki jenis akses apa ke suatu sistem, buat diagram kasus penggunaan. Terdapat dua aktor yang menjadi pengguna sistem ini, yaitu pegawai/karyawan Dinas Komunikasi dan Informatika Provinsi Jambi dan Admin.

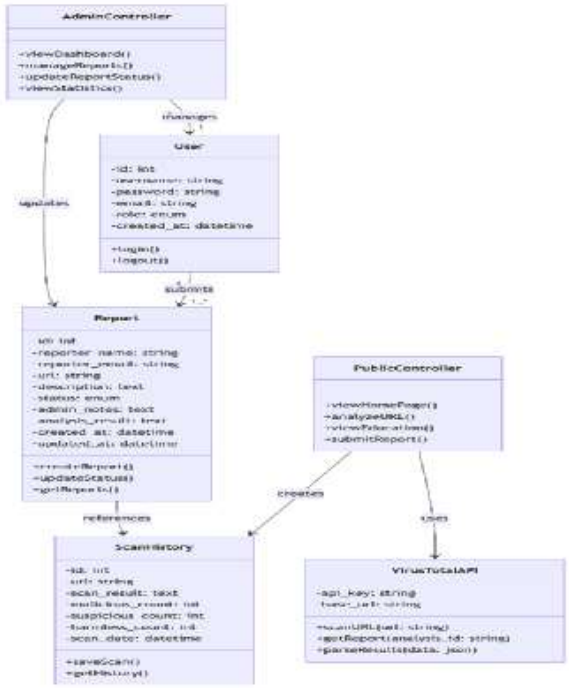
DOI: https://doi.org/10.31004/riggs.v5i2.13456



Gambar 3.1 UseCase Diagram

3.1.2 Class Diagram

Class Diagram memberikan gambaran struktur sistem berdasarkan definisi kelas-kelas yang dirancang untuk membangun sistem informasi deteksi dini serangan social engineering berbasis web. Berikut ini ialah class diagram yang digunakan pada sistem informasi deteksi dini serangan social engineering berbabsis web.



Gambar 3.2 Class Diagram

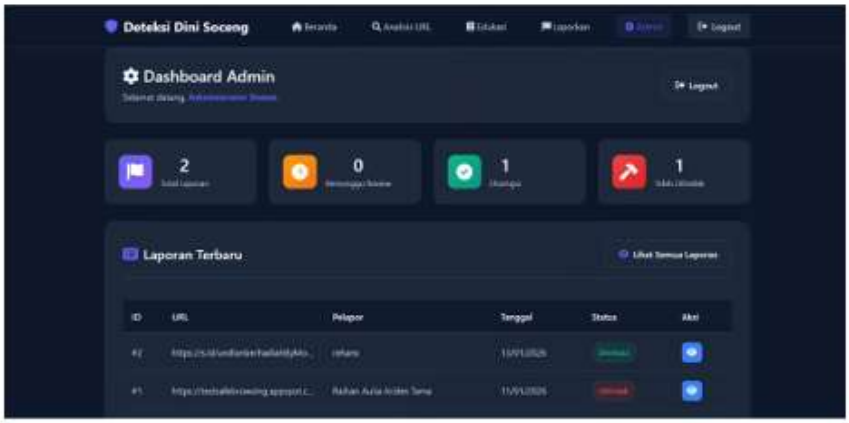
3.4 Implementasi Sistem

1. Tampilan halaman Beranda

DOI: https://doi.org/10.31004/riggs.v5i2.13456

Gambar 3.4 Tampilan Halaman Beranda

2. Tampilan Halaman Dashboard Admin



Gambar 3.5 Tampilan Halaman Dashboard Admin

3.5 Pengujian Sistem

3.6.1 Pengujian Black Box Testing

Sistem diuji dengan memberikan input tertentu dan kemudian mengamati outputnya untuk melihat apakah mengikuti alur yang telah ditentukan. Dengan menggunakan skenario yang telah direncanakan sebelumnya, kita akan menguji setiap fungsionalitas[11]. Black Box Testing merupakan metode pengujian perangkat lunak yang berfokus pada pengujian fungsi sistem tanpa memperhatikan struktur internal, algoritma, maupun kode program yang digunakan. Pengujian dilakukan dengan memberikan masukan (input) tertentu dan kemudian mengamati keluaran (output) yang dihasilkan oleh sistem [12].

3.6.2 Pengujian UAT(*User Acceptancce Testing)*

UAT (User Acceptance Testing) didefinisikan sebagai bentuk validasi akhir sebelum sistem diluncurkan, di mana pengguna akan melakukan interaksi langsung dengan sistem dan memberikan umpan balik terkait fungsionalitas, kemudahan penggunaan, serta kelayakan implementasi[13].Tujuan dari pengujian penerimaan pengguna (User Acceptance Testing/UAT) adalah untuk mendapatkan umpan balik tentang sistem yang telah dibuat dari pengguna dengan mengajukan serangkaian pertanyaan kepada mereka. Setiap pertanyaan diberi nilai skala Likert, dan responden dapat memilih sendiri. Angka antara "sangat setuju" dan "sangat tidak setuju" diberikan kepada setiap respons skala Likert [14].

DOI: https://doi.org/10.31004/riggs.v5i2.13456

Berikut adalah tabel yang berisi semua pertanyaan yang diajukan kepada responden.

Tabel 3.3 Hasil Jawaban Responden

No	Pertanyaan	Skala Penilaian				
		SS	S	C	TS	STS
1.	Apakah sistem Deteksi_Socengku mudah dan dipahami oleh pengguna?	4	6			
2.	Apakah tampilan website modern, menarik, dan nyaman dilihat?	7	3			
3.	Apakah fitur analisis URL berfungsi dengan baik dan akurat?	6	4			
4.	Apakah fitur pelaporan URL mencurigakan mudah diakses dan berfungsi dengan baik?	3	6	1		
5.	Apakah konten edukasi tentang *social engineering* bermanfaat dan mudah dipahami?	2	7	1		
Jumlah		22	26	2		

Berdasarkan hasil dari jawaban responden pada tabel diatas, maka selanjutnya adalah menentukan keseluruhan nilai dari skala jawaban para responden yang didasari tabel 4. 14. Kemudian dari tabel ini, jumlah jawaban pada setiap keterangan (SS,S,C,TS,STS) akan dikali dengan skala dari masing-masing keterangan. Berikut dapat dilihat hasil jumlah skor dari setiap keterangan pada tabel dibawah ini[15].

Tabel 3.4 Hasil Persentasi Pengujian UAT

Kode Pertanyaan	Nilai Rata-rata	Persentase	Keterangan
P1	44/10 = 4.4	(4.4 / 5) x 100% = 88%	Sangat baik
P2	47/10 = 4.7	(4.7 / 5) x 100% = 94%	Sangat baik
P3	46/10 = 4.6	(4.6 / 5) x 100% = 92%	Sangat baik
P4	42/10 = 4.2	(4.2 / 5) x 100% = 84%	Sangat baik
P5	41/10 = 4.1	(4.1 / 5) x 100% = 82%	Sangat baik

Secara keseluruhan, Menurut hasil uji coba, sistem informasi peringatan dini berbasis web untuk serangan rekayasa sosial telah disambut dengan antusiasme besar dan tingkat kepuasan pengguna yang tinggi, dengan nilai UAT sebesar 88%, maka dapat disimpulkan bahwa sistem telah memenuhi kriteria kelayakan.

3.6 Pembahasan

Tujuan utama pengembangan sistem ini adalah menyediakan alat bantu bagi pengguna untuk mengenali potensi serangan social engineering sejak dini sebelum menimbulkan dampak seperti kebocoran data atau kerugian. Sistem memiliki beberapa fitur utama yang terintegrasi, salah satunya analisis URL mencurigakan menggunakan API VirusTotal dengan lebih dari 90 engine keamanan untuk mendeteksi potensi ancaman.

Selain sebagai alat deteksi, sistem ini bertujuan meningkatkan security awareness melalui informasi edukatif dan rekomendasi pencegahan. Metode Agile dipilih karena fleksibel dan dapat menyesuaikan kebutuhan berdasarkan umpan balik lembaga selama proses penelitian dan pengembangan.

Antarmuka sistem dirancang sederhana, bersih, dan intuitif agar mudah digunakan oleh pengguna umum yang tidak memiliki latar belakang teknis di bidang keamanan informasi. Sistem dibangun menggunakan PHP dan MySQL, dengan HTML dan CSS untuk antarmuka serta XAMPP sebagai server lokal dalam proses pengembangan dan pengujian.

Berdasarkan hasil pengujian, sistem mampu menjalankan fungsi deteksi sesuai yang diharapkan. Pendekatan rule-based cukup efektif dalam mendeteksi serangan social engineering umum dan dapat berfungsi sebagai mekanisme peringatan awal bagi pengguna.

DOI: https://doi.org/10.31004/riggs.v5i2.13456

4. Kesimpulan

Hasil dari proses desain menunjukkan bahwa sistem informasi untuk deteksi dini serangan perlu dibangun social engineering berbasis web ini dikembangkan menggunakan metode agile, yang memungkinkan penyesuaian sistem lebih fleksibel. Rancangan dilakukan melalui beberapa tahapan, mulai dari tahap perencanaan, perancangan, pengembangan, pengujian, evaluasi, dan maintanace. Selain itu, sistem ini akan memudahkan para pegawai untuk menganalisis web yang beresiko berbahaya, Berdasarkan hasil pengujian menggunakan Black Box Testing, seluruh fungsi sistem berjalan dengan baik, serta hasil User Acceptance Testing (UAT) memperoleh nilai rata-rata 88% hingga layak digunakan.

Referensi

1. Wahyuni, S., Raazi, I. M., & Dwitawati, I. (2022). Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit. Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI), 5(1), 49–55.
2. Maya Safitri, E., Ameilindra, Z., & Yulianti, R. (2023). Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. Jurnal Ilmiah Teknologi Informasi Dan Robotika, 2(2), 21–26.
3. Alkhairi, M. G., Alkadri, S. P. A., & Utami, P. Y. (2024). Implementasi Unit Testing Dan End-To-End Testing Pada Sistem Informasi Akademik Teknik Informatika. JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika),
4. Idadx. (2023). Laporan Aktivitas Phishing Domain ~.ID Indonesia Anti-Phishing Data Exchange. 1–8.
5. Safarudin, R., Kustati, M., & Sepriyanti, N. (2023). Penelitian Kualitatif. 3, 9680-9694
6. Larasati, I., Yusril, A. N., & Zukri, P. Al. (2021). Systematic Literature Review Analisis Metode Agile Dalam Pengembangan Aplikasi Mobile. Sistemasi, 10(2), 369.
7. Hidayah, N. A., & Nur Muhammad Asnadi. (2024). Penerapan Metode Agile Dalam Manajemen Proyek: Systematic Literature Review. Jurnal Perangkat Lunak, 6(1), 43–53.
8. Mintarsih, M. (2023). Pengujian Black Box Dengan Teknik Transition Pada Sistem Informasi Perpustakaan Berbasis Web Dengan Metode Waterfall Pada SMC Foundation. Jurnal Teknologi Dan Sistem Informasi Bisnis, 5(1), 33–35.
9. Mahmud, A. F., & Wirawan, S. (2024). Phishing Website Detection Using Machine Learning Classification Method. Sistemasi, 13(4), 1368.
10. Linda Khoirul Inayah, N. . 22206052006. (2024). Perbandingan Deteksi Web Phishing Dengan Fitur Menggunakan Svm, Random Forest, Dan Gradient Boosting Classifier.
11. Almaheri, R., Pratama, A., Aprizal, Y., Jhonsen, M., Sarjana, I. P., Teknologi, I., Informasi, S., Diploma, P., & Teknologi, I. (2023). Penerapan Metode Black Box dalam Pengujian Aplikasi Informasi Stok Barang pada PT . Trimega Jaya Medika Berbasis Web PENDAHULUAN saat ini . Website dapat membantu khususnya dalam mencari informasi yang dibutuhkan dijabarkan maka dibangunlah sebuah Aplikas. 9(1), 174–183.
12. Kulkarni, S. (2024). The Necessity of System Integration Testing (SIT) and User Acceptance Testing (UAT) in Project Lifecycle. Interantional Journal of Scientific Research in Engineering and Management, 08(11), 1–7.
13. Wulandari, W., Nofiyani, N., & Hasugian, H. (2023). User Acceptance Testing (Uat) Pada Electronic Data Preprocessing Guna Mengetahui Kualitas Sistem. Jurnal Mahasiswa Ilmu Komputer, 4(1), 20–27.
14. Gustiani, W., & Sepriano, S. (2022). Perancangan Website Berita Menggunakan HTML dan CSS.
15. Fatiha, M. R., Setiawan, I., Ikhsan, A. N., & Yunita, I. R. (2024). Optimisasi Sistem Deteksi Phishing Berbasis Web Menggunakan Algoritma Decision Tree. Jurnal Ilmiah IT CIDA, 10(2), 97.

DOI: https://doi.org/10.31004/riggs.v5i2.13456