Terbit *online* pada laman web jurnal : www.journal.unbara.ac.id/index.php/INTECH
INFORMATIKA DAN TEKNOLOGI (INTECH)
ISSN (Online) : 2722-7367



Implementation of the Jeopardy Capture The Flag Method as a Website-Based Cyber Security Learning Media (Case Study: TJKT Expertise Competencies of SMK Negeri 1 Wanayasa)

Implementasi Metode *Jeopardy Capture The Flag* Sebagai Media Pembelajaran *Cyber Security* Berbasis *Website* (Studi Kasus: Kompetensi Keahlian TJKT SMK Negeri 1 Wanayasa)

Imam Nurfalah[1*], Heni Rahmawati[2*], Purwanto[3*]
[1*,2*,3*]Program Studi Informatika, STIMIK Tunas Bangsa, Banjarnegara, Indonesia
*E-mail: falahimamnur@gmail.com

ABSTRACT

This study addresses the need for practical cybersecurity learning media for vocational students, particularly in the Computer and Network Engineering (TJKT) program. The research aimed to develop and evaluate SkawanCTF, a website-based learning platform that applies the Jeopardy Capture The Flag (CTF) approach. The platform was developed using the Research and Development method with the Four-D model, consisting of Define, Design, Develop, and Disseminate. System requirements and workflows were designed using Unified Modeling Language, while implementation used Next.js, Tailwind CSS, Supabase, and Vercel. Functional testing was conducted using Black Box and White Box approaches. Learning outcomes were evaluated through pre-test and post-test scores, while user perceptions were collected using a five-point Likert questionnaire. The evaluation involved 168 students. The total pre-test score was 995 and the post-test score was 1,602, producing an N-Gain value of 0.8861 (88.61%), categorized as high. User perception reached an average score of 3.88, categorized as agree. The reported functional tests passed all tested scenarios across 37 modules. These findings indicate that SkawanCTF can operate as an accessible practice medium and received positive responses from participating students. Further evaluation with comparison groups and validated instruments is recommended.

Keywords: Cybersecurity, Capture The Flag, Jeopardy, Learning Media, Website

ABSTRAK

Penelitian ini dilatarbelakangi kebutuhan media pembelajaran keamanan siber yang bersifat praktis bagi peserta didik vokasi, khususnya pada program Teknik Jaringan Komputer dan Telekomunikasi (TJKT). Penelitian bertujuan mengembangkan dan mengevaluasi SkawanCTF, yaitu platform pembelajaran berbasis website yang menerapkan pendekatan Jeopardy Capture The Flag (CTF). Pengembangan dilakukan menggunakan metode Research and Development dengan model Four-D yang meliputi Define, Design, Develop, dan Disseminate. Kebutuhan dan alur sistem dirancang menggunakan Unified Modeling Language, sedangkan implementasi memanfaatkan Next.js, Tailwind CSS, Supabase, dan Vercel. Pengujian fungsional dilakukan melalui pendekatan Black Box dan White Box. Hasil pembelajaran dievaluasi menggunakan skor pre-test dan post-test, sedangkan persepsi pengguna dikumpulkan melalui kuesioner skala Likert lima tingkat. Evaluasi melibatkan 168 siswa. Total skor pre-test sebesar 995 dan post-test sebesar 1.602, sehingga diperoleh nilai N-Gain 0,8861 atau 88,61% dengan kategori tinggi. Persepsi pengguna memperoleh nilai rata-rata 3,88 dengan kategori setuju. Pengujian fungsional dilaporkan berhasil pada seluruh skenario yang diuji dalam 37 modul. Temuan ini menunjukkan bahwa SkawanCTF dapat digunakan sebagai media latihan yang mudah diakses dan memperoleh tanggapan positif dari siswa yang berpartisipasi. Evaluasi lanjutan disarankan menggunakan kelompok pembanding dan instrumen yang telah divalidasi.

Kata kunci: Keamanan Siber, Capture The Flag, Jeopardy, Media Pembelajaran, Website

Informasi Artikel
Submit 30 Oktober | Diterima 5 November 2026 | Publish Online 30 November 2026.
This is an open access article under the CC BY-NC 4.0 license.
Published by Universitas Baturaja.

PENDAHULUAN

Perkembangan layanan digital menjadikan keamanan siber sebagai kompetensi penting, termasuk bagi peserta didik pada pendidikan vokasi bidang jaringan komputer. Pembelajaran yang hanya menekankan teori berisiko belum memberi cukup kesempatan kepada siswa untuk berlatih mengidentifikasi masalah dan menyelesaikan tantangan keamanan secara langsung. Kebutuhan pembelajaran praktis menjadi semakin relevan ketika sekolah mengelola infrastruktur dan situs web yang berpotensi menghadapi gangguan keamanan.

Capture The Flag (CTF) merupakan pendekatan latihan keamanan siber berbasis tantangan. Dalam format *Jeopardy*, peserta memilih dan menyelesaikan tantangan yang dikelompokkan berdasarkan kategori atau tingkat kesulitan, lalu mengirimkan *flag* sebagai bukti penyelesaian. Kajian tentang gamifikasi CTF menunjukkan bahwa format ini telah dipelajari sebagai pendekatan untuk pembelajaran keamanan siber [1]. Penelitian tentang pengembangan platform CTF juga menyoroti pentingnya ketersediaan sistem dan konten tantangan yang terstruktur[2]. Implementasi CTF di lingkungan pendidikan tinggi Indonesia turut menunjukkan bahwa penerapannya memerlukan penyesuaian terhadap konteks pembelajaran dan kemampuan peserta [3].

Walaupun penelitian dan platform CTF telah berkembang, kebutuhan media yang sesuai dengan konteks siswa SMK masih perlu diperhatikan. Siswa membutuhkan platform yang tidak hanya menyediakan tantangan, tetapi juga mengatur akun, publikasi tantangan, validasi jawaban, penilaian, dan pengelolaan konten oleh pengajar. Karena itu, penelitian ini berfokus pada pengembangan SkawanCTF untuk Kompetensi Keahlian TJKT SMK Negeri 1 Wanayasa. Tujuan penelitian adalah merancang, mengimplementasikan, dan mengevaluasi media pembelajaran cyber security berbasis *website* dengan metode *Jeopardy* CTF.

TINJAUAN PUSTAKA

Sistem dapat diartikan sebagai suatu kesatuan yang dibentuk oleh sejumlah prosedur maupun komponen yang saling berkaitan. Berdasarkan pendekatan prosedur, sistem merupakan sekumpulan prosedur yang disusun untuk melaksanakan kegiatan tertentu dan mencapai tujuan yang telah ditetapkan. Sementara itu, berdasarkan pendekatan komponen, sistem merupakan kumpulan elemen yang saling berhubungan dan berinteraksi sehingga membentuk suatu kesatuan untuk mencapai tujuan tertentu [4].

1. *Capture The Flag*

CTF mengemas latihan keamanan siber sebagai rangkaian tantangan yang harus diselesaikan peserta. Format *Jeopardy* mengelompokkan tantangan dalam kategori tertentu dan memberikan skor berdasarkan penyelesaian. Pendekatan ini memberi struktur bagi latihan mandiri dan memungkinkan perkembangan peserta ditampilkan melalui skor serta papan peringkat. Syah, Rahma, dan Huda membahas gamifikasi edukasi keamanan siber menggunakan konsep CTF, sedangkan Fadzil dan Abdullah mengkaji pengembangan sistem beserta konten platform CTF [1], [2].

2. Media Pembelajaran

Media pembelajaran berbasis web dapat diakses melalui peramban tanpa bergantung pada instalasi aplikasi khusus pada setiap perangkat. Dalam pengembangan sistem, pemodelan UML membantu menjelaskan aktor, proses, dan struktur sebelum implementasi. Penelitian ini menggunakan Next.js untuk pengembangan aplikasi web, Tailwind CSS untuk penyusunan antarmuka, serta Supabase untuk autentikasi dan penyimpanan data. Sistem dipublikasikan menggunakan Vercel. Teknologi tersebut dipilih sebagai komponen implementasi, sedangkan keberhasilan sistem dievaluasi melalui pengujian fungsional dan tanggapan pengguna.

3. Jeopardy

Jeopardy merupakan salah satu format dalam kompetisi *Capture The Flag* (*CTF*) yang berfungsi untuk mengukur tingkat pemahaman peserta terhadap konsep-konsep keamanan komputer yang dirancang untuk menguji penguasaan mereka terhadap berbagai aspek keamanan informasi [1]. *Jeopardy* merupakan salah satu format dalam kompetisi *Capture The Flag* (*CTF*) yang memanfaatkan *server* sebagai media penyimpanan berbagai soal. Tantangan yang disajikan dapat mencakup beragam kategori, seperti *web exploitation*, forensik digital, maupun *kriptografi*. Tujuan utama dari

format ini adalah agar peserta mampu menemukan *string* khusus atau *flag* yang disembunyikan dalam sistem, sehingga keterampilan analisis dan pemahaman konsep keamanan siber [5]. Pada format *Jeopardy* setiap peserta diberikan serangkaian tantangan atau pertanyaan dengan bobot poin tertentu sesuai tingkat kesulitannya. Peserta berupaya menyelesaikan tantangan tersebut untuk memperoleh poin. Pemenang ditentukan berdasarkan akumulasi skor tertinggi yang dicapai hingga akhir kompetisi [2]. *Kriptografi* dalam *Jeopardy Capture The Flag* merupakan salah satu kategori tantangan yang dalam memecahkan kode dan menganalisis algoritma *enkripsi* [6]. *Digital forensics* merupakan cabang ilmu forensik yang bertujuan untuk memperoleh bukti digital terkait pelaku kejahatan dengan melakukan proses identifikasi, menjaga keutuhan bukti, menganalisis data, serta menyusun laporan hasil temuan secara sistematis [7]. Proses ini menuntut keahlian teknis khusus, penggunaan alat canggih, dan prosedur ketat agar integritas bukti tetap terjaga [8]. Web exploitation sering muncul sebagai masalah keamanan *web* di mana peserta harus mengeksploitasi *bug* untuk mendapatkan hak akses yang lebih tinggi [2] *Reverse engineering* adalah proses menganalisis dan membongkar produk, sistem, atau perangkat lunak untuk memahami fungsi serta strukturnya [9].

4. Pengujian *Black Box* dan *White box*

Black Box Testing merupakan metode pengujian yang tidak meninjau detail internal sistem seperti kode program maupun struktur data. Fokus utama pendekatan ini adalah pada fungsi dan fitur yang disediakan sistem, dengan menilai bagaimana sistem merespons masukan serta menghasilkan keluaran, tanpa memperhatikan proses internal yang digunakan untuk mencapai fungsionalitas tersebut [10].

White Box Testing adalah metode pengujian perangkat lunak yang menelaah struktur internal kode yang digunakan deteksi dini kesalahan logika, optimasi kinerja, serta identifikasi potensi celah keamanan. Dengan cakupan pengujian yang menyeluruh terhadap jalur, cabang, dan pernyataan dalam kode, White Box Testing tidak hanya menilai fungsionalitas tetapi juga kualitas dan konsistensi kode. Integrasinya dengan proses pengembangan menjadikan metode ini penting dalam memastikan perangkat lunak yang lebih efisien, aman, dan andal, sehingga layak dijadikan landasan teori dalam penelitian pengujian perangkat lunak [10]

METODE PENELITIAN

1. Metode Penelitian RND

Penelitian menggunakan pendekatan *Research and Development* (R&D) dengan model Four-D, yang terdiri atas *Define*, *Design*, *Develop*, dan *Disseminate*. Tahap *Define* mengidentifikasi kebutuhan pembelajaran dan masalah yang ditemukan pada konteks TJKT. Tahap *Design* menerjemahkan kebutuhan ke rancangan proses, peran pengguna, basis data, dan antarmuka. Tahap *Develop* mencakup implementasi platform serta pengujian fungsional. Tahap *Disseminate* dilakukan melalui penerapan platform kepada siswa dan pengumpulan data evaluasi [11].

Sistem dimodelkan menggunakan UML, meliputi Use Case Diagram, Activity Diagram, Class Diagram, dan *Deployment* Diagram. Sistem mempunyai dua peran utama, yaitu *admin* dan *user*. *Admin* dapat mengelola level dan kategori, mengatur tantangan, meninjau pengajuan tantangan, menangani laporan, serta mengelola akun. *User* dapat melihat tantangan yang telah dipublikasikan, mengirimkan *flag*, melihat *leaderboard*, menyimpan tantangan, melaporkan masalah, dan mengajukan tantangan untuk ditinjau *admin*. Tantangan yang dibuat *user* tidak langsung dipublikasikan, melainkan melalui proses verifikasi [12], [13], [14], [15], [16].

Implementasi menggunakan Next.js sebagai *framework* aplikasi, Tailwind CSS untuk antarmuka, Supabase sebagai layanan *backend* dan basis data, serta Vercel untuk *deployment* [17]. Pengelolaan kode sumber dilakukan menggunakan GitHub [18]. Sistem menerapkan autentikasi pengguna dan pengaturan hak akses agar fungsi *admin*istrasi dibedakan dari fungsi peserta.

2. Metode Pengumpulan Data

a. Observasi

Observasi merupakan metode pengumpulan data yang dilakukan melalui pengamatan langsung dengan memanfaatkan seluruh panca indera. Teknik ini dapat dilaksanakan menggunakan berbagai instrumen, seperti tes, angket, gambar, maupun rekaman suara [19].

b. Wawancara

Wawancara merupakan metode pengumpulan data melalui kegiatan tanya jawab langsung antara peneliti dan responden untuk memperoleh informasi atau ide terkait topik tertentu.

c. Studi pustaka

Studi pustaka merupakan kegiatan penting dalam penelitian yang berfungsi mengembangkan aspek teoretis maupun praktis. Melalui telaah literatur, peneliti dapat membangun landasan teori, menyusun kerangka berpikir, serta merumuskan hipotesis dengan memadukan pendekatan deduktif dan induktif [20].

d. Metode Analisi Data

Analisis data adalah proses mengorganisasikan, mengurutkan, mengelompokkan, memberi kode, dan mengkategorikan data agar dapat ditemukan tema dan dirumuskan hipotesis kerja yang sesuai dengan data tersebut. Proses ini dimulai sejak pengumpulan data dan dilakukan secara intensif setelah pengumpulan selesai, bertujuan mengangkat teori substansif dari pola yang ditemukan. Analisis data memerlukan konsentrasi fisik dan pikiran serta pendalaman literatur untuk mengonfirmasi atau membenarkan teori baru yang mungkin muncul [19]. Analisis kualitatif dilakukan dengan mereduksi, menyajikan, dan menarik kesimpulan dari data wawancara serta observasi. Analisis Hasil Tes (*Pre-test* dan *Post-test*) dilakukan untuk mengukur peningkatan pemahaman siswa sebelum dan sesudah menggunakan platform SkawanCTF. Analisis peningkatan dihitung menggunakan rumus *Normalized Gain* (*N-Gain*). Analisis kuantitatif dilakukan dengan mengolah data kuesioner kepuasan siswa yang diukur menggunakan skala *Likert*, melalui perhitungan persentase dan rata-rata

3. Populasi Penelitian

Populasi penelitian adalah 209 siswa TJKT yang aktif mengikuti pembelajaran. Perhitungan Slovin dengan margin of error 10% menghasilkan kebutuhan sampel minimum 68 responden. Penelitian melaporkan data evaluasi dari 168 siswa. Oleh karena itu, artikel ini menggunakan jumlah responden aktual yang dilaporkan pada bagian hasil; jumlah tersebut lebih besar daripada sampel minimum hasil perhitungan.

Instrumen tes berupa *pre-test* dan *post-test* yang masing-masing terdiri atas 10 soal pilihan ganda tentang dasar keamanan siber dan kategori tantangan *Jeopardy* CTF. Instrumen non-tes berupa kuesioner 10 pernyataan dengan skala Likert lima tingkat. Pengujian perangkat lunak dilakukan melalui *Black Box* dan *White Box* pada modul-modul yang mewakili akses tanpa autentikasi, pengguna terautentikasi, dan *admin*.

N-Gain dihitung dengan membandingkan selisih skor *post-test* dan *pre-test* terhadap selisih skor ideal dan *pre-test*: g = (skor *post-test* − skor *pre-test*)/(skor ideal − skor *pre-test*). Skor Likert dihitung dari total skor jawaban dibagi jumlah seluruh jawaban pada 10 pernyataan..

HASIL DAN PEMBAHASAN

1. Analisis dan Rancangan Sistem

Tabel 1. Tabel Kebutuhan Sistem Pengguna

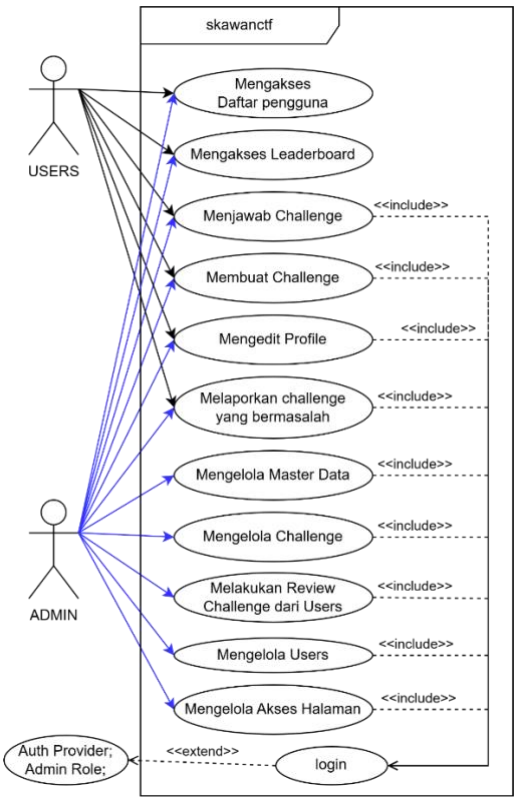
Hardware	***Software***
Laptop/PC	*Web Browser (Brave, Chrome, firefox)*
Ram minimal 4*GB*	*OS (Windows, Macos, Linux)*
SSD / HDD Storage minimal *128GB*	Software tambahan untuk memecahkan soal
Internet	

Tabel 2. Tabel Kebutuhan Pembuatan Sistem

Hardware	***Software***	***Cloud***
Laptop/PC	*Web Browser (Brave)*	Domain *Website* (*skawanctf.my.id*)

Ram min 4	*OS (Windows 11)*	*Serverless (Vercel)*
SSD / HDD Storage minimal *128GB*	*Visual Studio Code* versi *1.106*	*Seo Tools (Google webmaster)*
Internet	*NodeJs v22.18.0*	*Github*
	Figma	*Cloudflare*
		Supabase

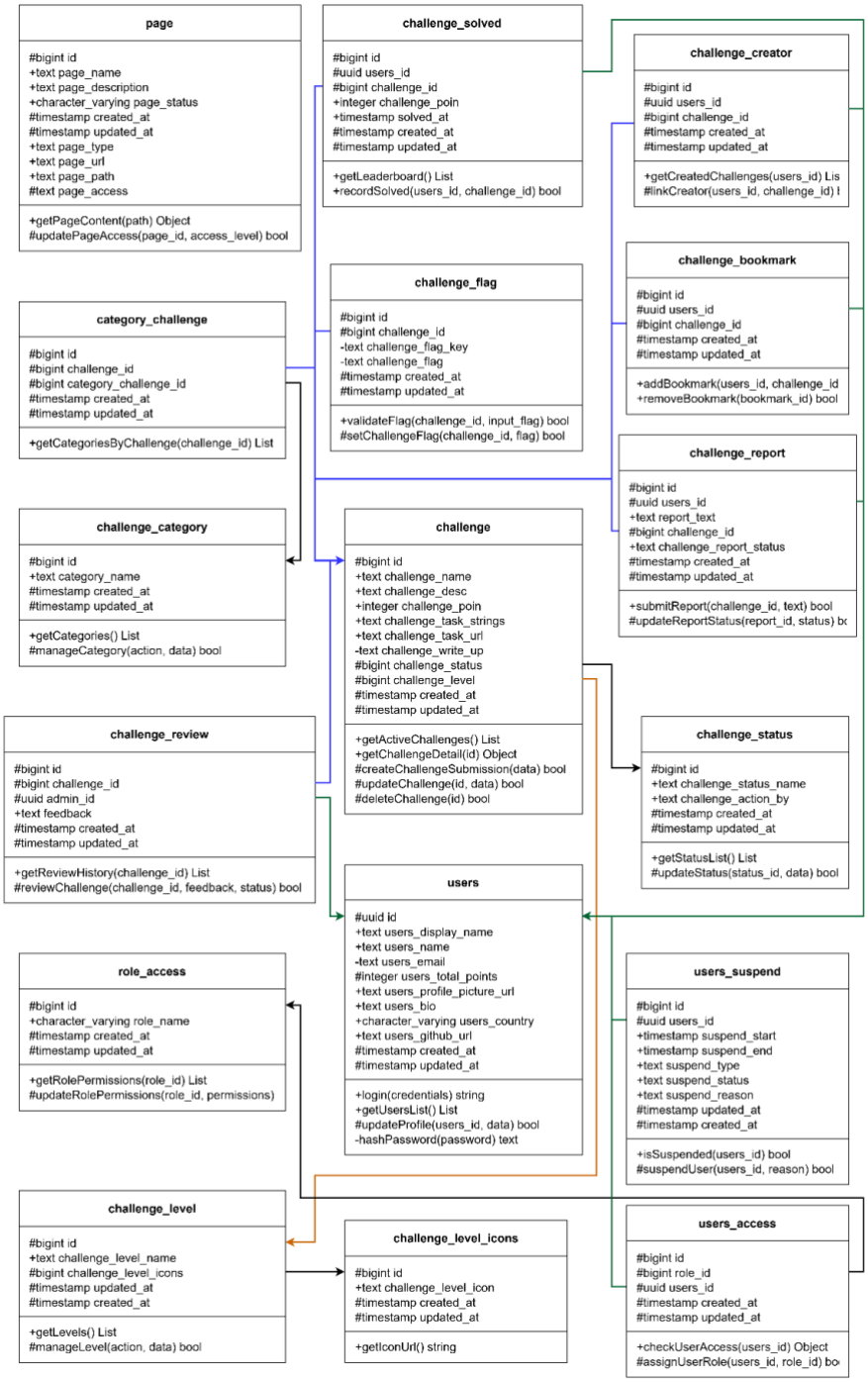
2. Diagram UML



Gambar 1 *Use Case Diagram* skawanctf

SkawanCTF berhasil dikembangkan sebagai platform pembelajaran berbasis *website*. Fitur utama meliputi autentikasi, daftar dan detail tantangan, pengiriman *flag*, perolehan poin, *leaderboard*, *bookmark*, pelaporan tantangan, pengajuan tantangan oleh pengguna, serta proses review oleh *admin*. Pada sisi *admin*istrasi, sistem menyediakan pengelolaan level, kategori, tantangan, laporan, pengguna, status suspend, dan pengaturan halaman. Alur review menjaga agar tantangan buatan pengguna dapat diperiksa sebelum dipublikasikan.

Pemisahan hak akses mendukung pengelolaan konten dan pengalaman latihan siswa dalam satu platform. Fitur *leaderboard* dan poin menyediakan umpan balik berbasis penyelesaian tantangan, sementara alur pengajuan dan verifikasi memungkinkan konten berkembang dengan tetap berada di bawah pengawasan *admin*. Temuan ini menggambarkan implementasi fungsi sesuai ruang lingkup yang ditetapkan; efektivitas setiap fitur secara individual tidak diukur terpisah.



Gambar 2 *Class Diagram*

Alur penggunaan pada sisi user dimulai dari pembuatan akun atau masuk ke sistem. Setelah autentikasi berhasil, pengguna dapat menelusuri daftar tantangan yang telah dipublikasikan, melakukan pencarian, menggunakan filter kategori atau level, lalu membuka detail tantangan. Jika menemukan jawaban yang sesuai, pengguna mengirimkan *flag* melalui form yang tersedia. Sistem memeriksa jawaban; *flag* yang benar menambahkan poin dan mengubah status tantangan menjadi selesai, sedangkan *flag* yang salah menghasilkan pesan bahwa jawaban tidak valid. Hasil penyelesaian tersebut menjadi bagian dari informasi yang ditampilkan pada *leaderboard*.

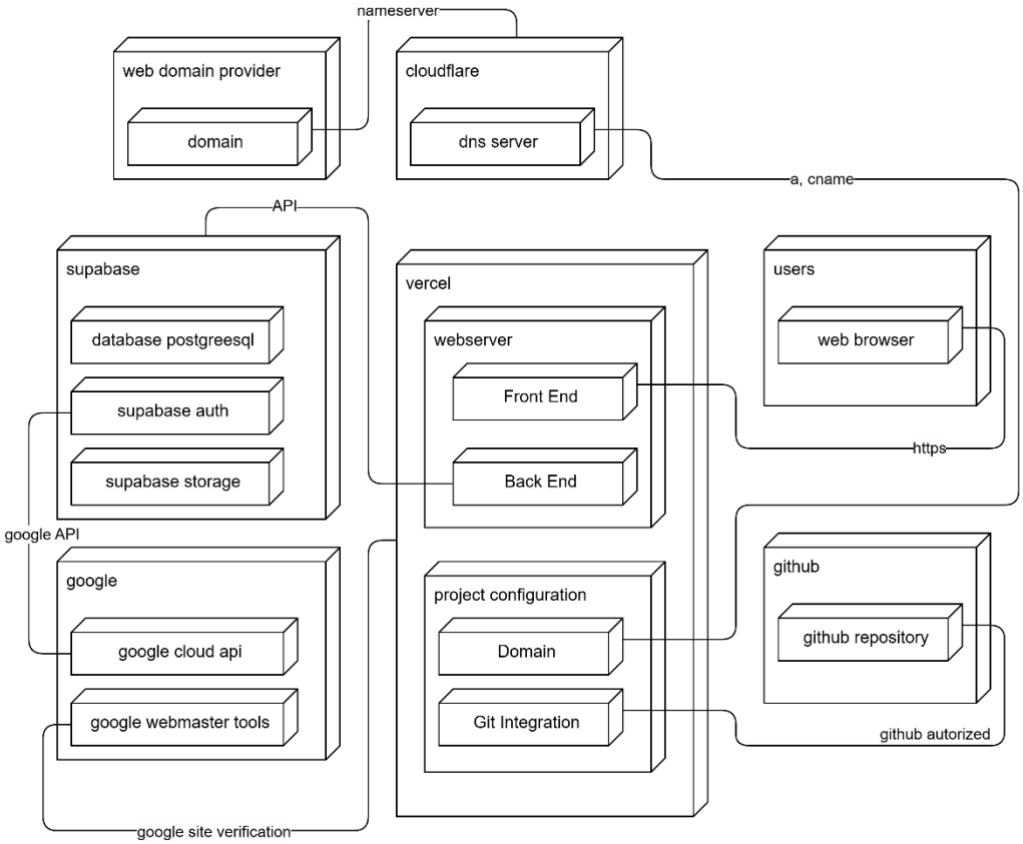
Fungsi tambahan pada sisi *user* meliputi *bookmark* untuk menyimpan tantangan, pelaporan apabila terdapat masalah pada tantangan, serta pengelolaan profil. Pengguna juga dapat mengajukan tantangan buatannya sendiri. Pengajuan tidak langsung muncul sebagai tantangan publik, melainkan masuk ke alur status pengajuan untuk ditinjau *admin*. Mekanisme tersebut penting karena materi

pembelajaran keamanan siber perlu diperiksa sebelum digunakan oleh peserta lain, baik dari segi ketepatan jawaban maupun kejelasan instruksi.

Pada sisi *admin*, sistem menyediakan pengelolaan data level dan kategori, pengelolaan tantangan, antrean review, informasi pembuat tantangan, laporan tantangan, statistik penyelesaian, daftar pengguna, status suspend, daftar *admin*, serta pengaturan halaman. Proses review menyediakan tindakan menyetujui publikasi, meminta revisi, atau menolak pengajuan. Dengan demikian, platform bukan sekadar halaman soal, tetapi juga mencakup fungsi tata kelola konten dan pengguna.

Perancangan antarmuka dibagi menjadi halaman yang dapat diakses sebelum autentikasi, halaman pengguna yang telah masuk, dan halaman *admin*istrasi. Bagian sebelum autentikasi mencakup halaman sambutan, masuk, registrasi, lupa kata sandi, dan reset kata sandi. Area pengguna mencakup dashboard, daftar pengguna, daftar tantangan, detail tantangan, *leaderboard*, daftar tantangan milik pengguna, dan profil. Area *admin* disusun untuk mengakses dashboard *admin*istrasi dan modul pengelolaan data. Pemisahan area ini membantu membatasi kompleksitas tampilan berdasarkan tugas pengguna.

Rancangan data mencakup entitas yang berhubungan dengan tantangan, kategori, level, *flag*, status tantangan, penyelesaian, *bookmark*, laporan, pengguna, akses pengguna, suspend, dan halaman. Struktur tersebut mendukung hubungan antara konten tantangan, pemilik atau pembuatnya, status publikasi, dan aktivitas penyelesaian. Informasi status sangat penting dalam alur moderasi karena pengajuan, revisi, publikasi, dan penolakan merupakan kondisi yang berbeda. Pemisahan entitas juga memberi ruang bagi sistem untuk menyimpan rekam penyelesaian dan menampilkan peringkat pengguna.



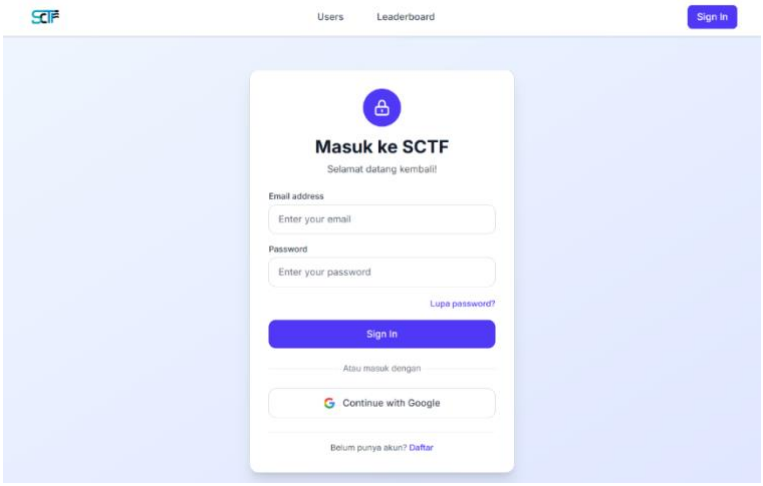
Gambar 3 *Deloyment diagram*

Sistem menggunakan Supabase untuk layanan autentikasi dan basis data serta penggunaan kebijakan *Row Level Security* (RLS) untuk mengatur akses data. Dalam konteks aplikasi yang memiliki peran berbeda, pembatasan akses perlu diterapkan pada lapisan data selain mengandalkan tampilan antarmuka. Meskipun demikian, artikel ini tidak menyimpulkan bahwa konfigurasi keamanan telah

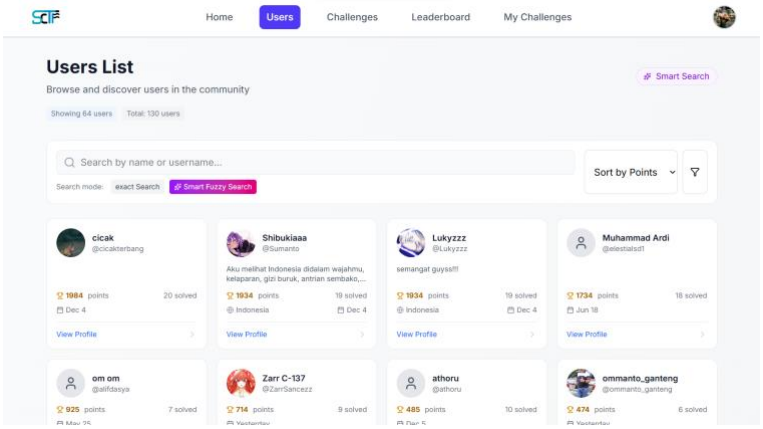
diuji terhadap seluruh jenis serangan; pengujian yang dilaporkan berfokus pada skenario fungsional dan jalur kode yang tercantum dalam dokumen penelitian.

Penggunaan UML memberi cara untuk mendokumentasikan hubungan antara aktor dan fungsi, alur aktivitas, struktur kelas, dan penempatan sistem. Use Case Diagram membantu memetakan batas kemampuan *user* dan *admin*, sedangkan Activity Diagram menjabarkan langkah-langkah pada proses tertentu seperti autentikasi, pengiriman *flag*, dan review tantangan. Class Diagram mendukung pemahaman struktur objek dan hubungan antarkomponen, sementara *Deployment* Diagram menggambarkan lingkungan penerapan. Model ini menjadi acuan saat implementasi sehingga fungsi yang dibangun dapat ditelusuri kembali ke kebutuhan.

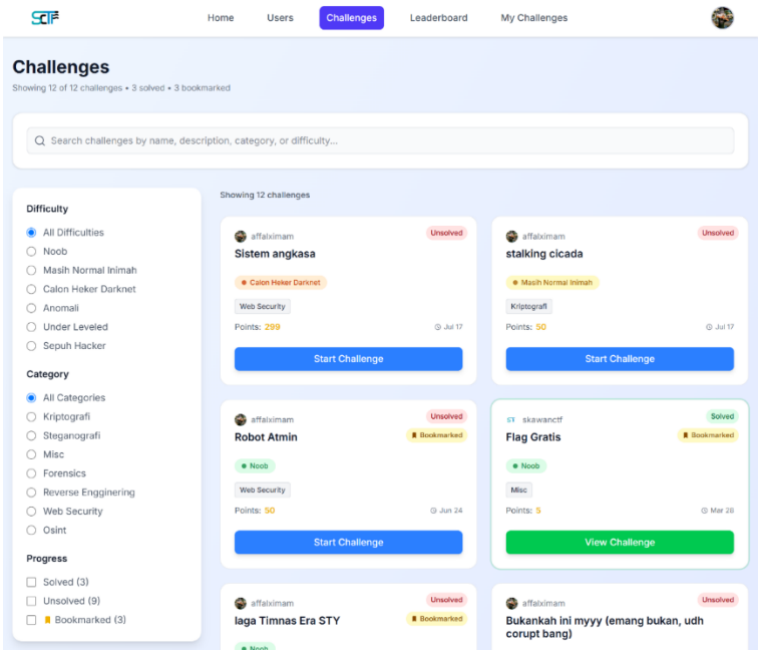
3. Implementasi



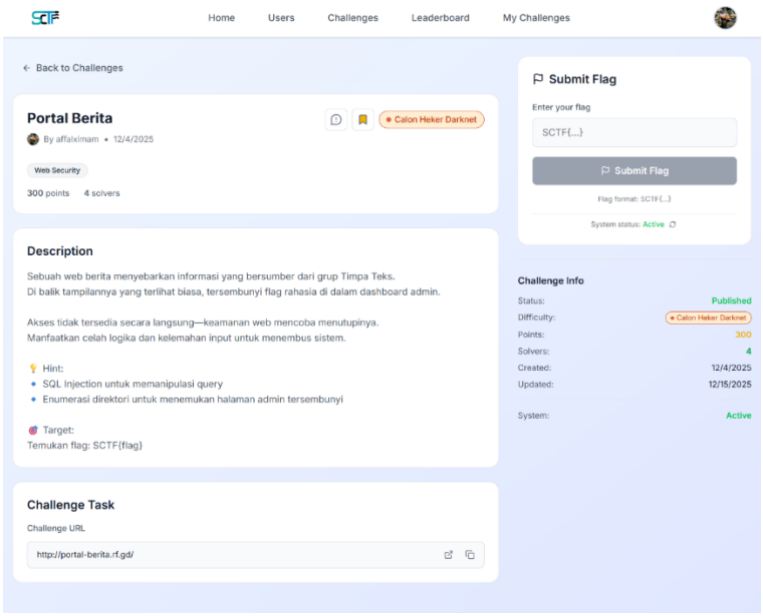
Gambar 4 *Implementasi* halaman *sign-in*



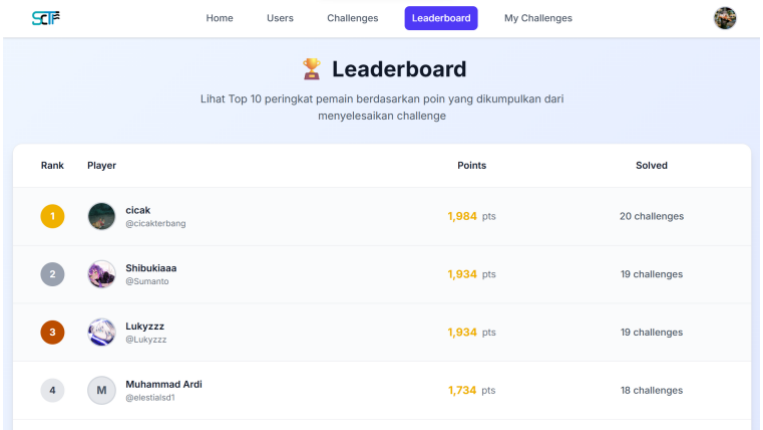
Gambar 5 *Implementasi* halaman daftar *users*



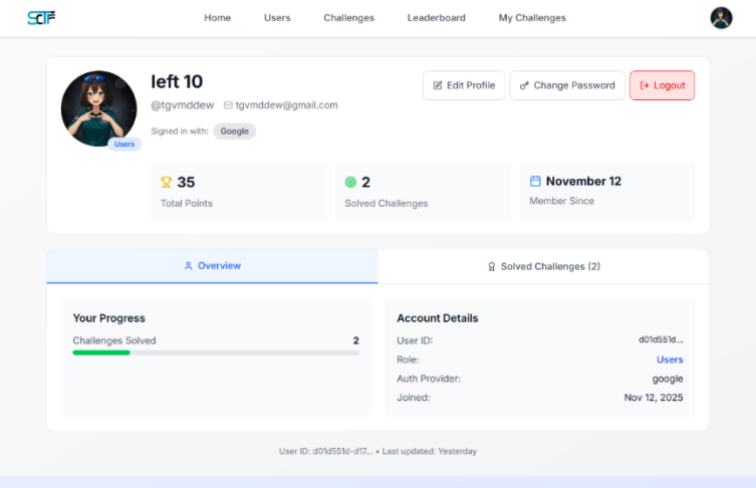
Gambar 6 Implementasi halaman *challenge*



Gambar 7 Implementasi halaman detail *challenge*



Gambar 8 Implementasi halaman *leaderboard*



Gambar 9 Implementasi halaman profil pengguna

4. Pengujian *Black box dan White box*

Pengujian *Black Box* pada mencakup skenario autentikasi, navigasi, pencarian dan penyaringan tantangan, pengiriman *flag* benar maupun salah, pengelolaan profil, fungsi *admin*, dan pengelolaan konten. Seluruh kasus uji yang dicantumkan dinyatakan berhasil. Skenario pengujian *Black Box* disusun berdasarkan tindakan yang dilakukan pengguna dan hasil yang diharapkan. Contoh skenario meliputi penggunaan kredensial yang benar dan salah, validasi kolom kosong, registrasi dengan email atau *user*name yang sudah digunakan, reset kata sandi, pencarian tantangan, pemilihan filter, pengiriman *flag*, perubahan profil, serta fungsi pengelolaan *admin*.

Tabel 3. Hasil Pengujian *Black Box*

No	Halaman	Skenario Pengujian	Hasil yang Diharapkan	Hasil
1	Home	Mengakses halaman Home	Halaman Home berhasil ditampilkan beserta menu navigasi.	Berhasil
2	Sign In	Login menggunakan email dan password yang benar	Pengguna berhasil masuk ke sistem dan diarahkan ke halaman utama.	Berhasil
3	List Users	Membuka halaman daftar users	Sistem menampilkan seluruh daftar pengguna.	Berhasil
4	Challenge	Membuka halaman challenge	Daftar seluruh challenge ditampilkan.	Berhasil
5	Detail Challenge	Mengirim flag yang benar	Sistem menerima flag, menambahkan poin, dan mengubah status menjadi Solved.	Berhasil
6	Leaderboard	Membuka halaman leaderboard	Sistem menampilkan peringkat pengguna berdasarkan poin.	Berhasil
7	Profil Pengguna	Membuka halaman profil	Informasi profil pengguna ditampilkan dengan benar.	Berhasil

Tabel 4. Hasil Pengujian *white Box*

Modul	Komponen dan Jalur Eksekusi yang Diperiksa	Hasil
Sign In	SignInForm dan autentikasi; validasi kredensial, pembuatan sesi, sanitasi input, serta redirect ke halaman utama.	Berhasil
List Users	UsersList dan API GET /users; pengambilan daftar pengguna serta pencarian nama.	Berhasil
Challenge List	ChallengesList; pengambilan daftar challenge serta pemrosesan pencarian dan filter kategori/level.	Berhasil

Detail Challenge	ChallengeDetail dan submitFlag; verifikasi flag, penambahan poin, penyimpanan status solved, bookmark, dan report.	Berhasil
Leaderboard	Leaderboard dan API GET /leaderboard; pengambilan data ranking berdasarkan poin dan penampilan tabel peringkat.	Berhasil
Profil Pengguna	ProfilePage; pengambilan data akun pengguna dan penampilan informasi profil.	Berhasil

Pengujian *White Box* memeriksa jalur eksekusi pada 37 modul, mencakup modul tanpa autentikasi, modul pengguna, dan modul *admin*; hasil yang dilaporkan juga menyatakan seluruh jalur yang diuji berhasil. Pengujian *White Box* memeriksa jalur eksekusi pada modul-modul yang diidentifikasi dalam implementasi. Daftar tersebut mencakup halaman tanpa autentikasi, area pengguna, serta area *admin*. Pemeriksaan berfokus pada komponen, fungsi *backend*, validasi, pengambilan data, perubahan status, dan penjagaan rute. Pengujian melaporkan hasil berhasil untuk modul-modul yang diuji. Artikel ini mempertahankan interpretasi sesuai data tersebut dan tidak menambahkan klaim tentang jumlah kerentanan yang ditemukan atau standar keamanan yang tidak dilaporkan.

5. Analisa hasil Implemenasi

Penlitian melaporkan tingkat keberhasilan pengujian fungsional sebesar 100%. Hasil ini mendukung kesimpulan bahwa fungsi yang diuji berjalan sesuai ekspektasi pada skenario pengujian yang disusun. Namun, angka 100% harus dibaca dalam batas cakupan kasus uji yang dilakukan, bukan sebagai jaminan bahwa sistem bebas dari seluruh kerentanan keamanan atau masalah pada kondisi penggunaan lain.

Data tes berasal dari 168 siswa dengan 10 soal dan skor ideal maksimum 1.680. Total skor *pre-test* adalah 995, sedangkan total skor *post-test* adalah 1.602. Selisih skor sebesar 607 dibandingkan dengan ruang peningkatan sebesar 685 menghasilkan *N-Gain* 0,8861 atau 88,61%. Berdasarkan kriteria yang digunakan, nilai tersebut termasuk kategori tinggi.

Tabel 5. Rekapitulasi Hasil *Pre-test* dan *Post-test*

Indikator	Hasil
Jumlah responden	168
Jumlah soal	10
Skor ideal maksimum	1.680
Total skor pre-test	995
Total skor post-test	1.602
N-Gain	0,8861
Persentase N-Gain	88,61%
Kategori	Tinggi

Peningkatan skor menunjukkan bahwa hasil tes setelah penggunaan platform lebih tinggi dibandingkan hasil tes awal. Nilai *N-Gain* yang tinggi memberikan indikasi positif terhadap potensi SkawanCTF sebagai media latihan. Meski demikian, karena ringkasan data yang tersedia tidak menyertakan kelompok kontrol, peningkatan ini tidak dapat diatribusikan secara eksklusif kepada platform tanpa mempertimbangkan faktor lain, seperti pembelajaran reguler, latihan mandiri, atau pengaruh pengulangan tes.

Kuesioner diberikan kepada 168 responden dan terdiri atas 10 pernyataan yang mencakup kemudahan penggunaan, antarmuka, variasi tantangan, gamifikasi, minat menggunakan media, kesesuaian materi, pemecahan masalah, sistem penilaian, performa akses, dan keterlibatan siswa dalam pembaruan tantangan. Total skor seluruh pernyataan yang dilaporkan adalah 6.520, sehingga

skor rata-rata per respons adalah 3,88 dari skala 1–5. Nilai ini berada pada interval 3,41–4,20 dan dikategorikan Setuju.

Tabel 6. Ringkasan Evaluasi Persepsi Pengguna

Aspek	Hasil
Jumlah responden	168
Jumlah pernyataan	10
Skala penilaian	Likert 1–5
Rata-rata	3,88
Interpretasi	Setuju

Tanggapan tersebut menunjukkan penerimaan pengguna yang cenderung positif. Skor rata-rata bukan berarti seluruh responden memilih jawaban setuju pada setiap pernyataan; terdapat variasi jawaban antar-aspek. Evaluasi persepsi melengkapi hasil tes dan pengujian teknis, tetapi tidak menggantikan pengukuran langsung atas keterampilan praktik jangka panjang.

Analisis *N-Gain* menggunakan skor total *pre-test* dan *post-test* dengan skor *pre-test* sebesar 995 dan *post-test* sebesar 1.602. Dengan skor ideal 1.680, selisih peningkatan aktual adalah 607, sedangkan peluang peningkatan maksimum dari skor awal adalah 685. Pembagian kedua nilai menghasilkan 0,8861. Ketika dinyatakan sebagai persentase, nilai tersebut menjadi 88,61%. Karena skor *N-Gain* berada di atas 0,70, hasil dikategorikan tinggi berdasarkan kriteria yang digunakan.

Setiap pernyataan kuesioner memiliki rentang skor 1 sampai 5 dengan Sepuluh pernyataan mengukur pengalaman yang berbeda, mulai dari kemudahan antarmuka hingga relevansi materi dan performa akses. Total skor yang dilaporkan adalah 6.520 untuk 1.680 respons item (168 responden dikalikan 10 pernyataan). Pembagian total skor dengan jumlah respons menghasilkan nilai rata-rata sekitar 3,88. Nilai ini termasuk interval Setuju pada interpretasi yang digunakan. Karena data merupakan tanggapan mandiri, hasil tersebut menggambarkan persepsi siswa, bukan pengukuran objektif atas seluruh dimensi kualitas sistem.

SkawanCTF berpotensi melengkapi kegiatan pembelajaran dengan menyediakan tempat latihan yang terstruktur. Guru dapat menggunakan tantangan yang telah diverifikasi sebagai aktivitas latihan, sementara siswa dapat mencoba menyelesaikan tantangan dan melihat umpan balik melalui status serta poin. Papan peringkat dapat menambah unsur kompetisi, tetapi penerapannya perlu diarahkan sebagai sarana motivasi dan pemantauan proses belajar, bukan satu-satunya indikator kompetensi. Keberhasilan dalam CTF juga perlu dipadukan dengan penjelasan konsep, refleksi, dan pembahasan setelah tantangan selesai.

Alur pengajuan tantangan oleh siswa dapat membantu mendorong partisipasi aktif. Dalam proses tersebut, siswa tidak hanya menjawab soal, tetapi berpeluang menyusun materi tantangan untuk ditinjau. Kegiatan merancang tantangan dapat menuntut siswa memahami konsep, merumuskan petunjuk, menentukan jawaban yang valid, dan mempertimbangkan tingkat kesulitan. Namun, manfaat pembelajaran dari proses pembuatan tantangan belum diukur secara terpisah dalam penelitian ini; hal tersebut dapat menjadi fokus evaluasi lanjutan.

Platform web juga memungkinkan materi dikelola secara terpusat. Pengajar dapat memperbarui atau meninjau konten tanpa perlu memasang aplikasi terpisah pada setiap perangkat siswa. Di sisi lain, keberlangsungan pemanfaatan platform memerlukan pengelolaan konten secara berkala, pemantauan akun, pengujian setelah perubahan, dan perhatian terhadap perlindungan data pengguna. Aspek-aspek operasional ini perlu dijadikan bagian dari rencana pemeliharaan sistem jika platform digunakan secara rutin.

Penelitian ini memiliki sejumlah keterbatasan berdasarkan data yang dilaporkan. Pertama, evaluasi *pre-test* dan *post-test* disajikan dalam bentuk skor agregat dan tidak disertai kelompok kontrol dalam ringkasan hasil. Kedua, hasil kuesioner menunjukkan persepsi responden, sehingga

tidak dapat menggantikan penilaian performa praktik atau pengukuran retensi pengetahuan. Ketiga, pengujian *Black Box* dan *White Box* dibatasi pada skenario dan modul yang dicantumkan dalam skripsi. Keempat, implementasi dilakukan pada satu kompetensi keahlian di satu sekolah sehingga penerapan di konteks lain memerlukan pengujian ulang.

Selain itu, jumlah sampel minimum berdasarkan perhitungan Slovin adalah 68 siswa, sedangkan hasil evaluasi dilaporkan untuk 168 siswa. Artikel ini mengikuti jumlah aktual yang dinyatakan pada bagian hasil skripsi. Untuk naskah final, penulis sebaiknya memastikan konsistensi penjelasan mengenai teknik sampling, jumlah siswa yang diundang, jumlah respons yang dianalisis, serta apakah seluruh 168 responden mengisi kedua tes dan kuesioner. Penjelasan yang konsisten akan memperkuat transparansi metode dan memungkinkan pembaca menilai keterwakilan data.

Penelitian berikutnya dapat memperluas pengujian dengan kelompok pembanding, tes tindak lanjut, analisis per kategori tantangan, serta pemeriksaan validitas dan reliabilitas instrumen. Evaluasi teknis juga dapat ditambah dengan pengujian keamanan yang terencana dan terdokumentasi. Dengan demikian, penelitian lanjutan dapat membedakan bukti kelayakan fungsional, penerimaan pengguna, dan dampak pembelajaran secara lebih kuat.

KESIMPULAN DAN SARAN

Penelitian ini berhasil mengimplementasikan SkawanCTF sebagai media pembelajaran *cyber security* berbasis *website* dengan metode *Jeopardy Capture The Flag* untuk siswa TJKT SMK Negeri 1 Wanayasa. Sistem dibangun menggunakan Next.js, Tailwind CSS, dan Supabase, serta diterapkan melalui Vercel. Pengujian *Black Box* dan *White Box* pada 37 modul dilaporkan berhasil pada seluruh skenario yang diuji. Evaluasi pada 168 siswa menghasilkan *N-Gain* 0,8861 (88,61%) dengan kategori tinggi, sedangkan persepsi pengguna memperoleh rata-rata 3,88 dengan kategori Setuju. Hasil ini mendukung kelayakan fungsional dan penerimaan positif platform, serta mengindikasikan peningkatan skor tes setelah penggunaan. Pengembangan berikutnya disarankan menambah jenis CTF, fitur petunjuk bertingkat, *write-up* pembahasan, badge, dan riwayat perkembangan pengguna. Evaluasi lanjutan perlu menggunakan kelompok pembanding atau desain pengukuran yang lebih kuat, memeriksa validitas dan reliabilitas instrumen, serta menerapkan platform pada konteks sekolah yang lebih luas.

DECLARATIONS

Statement on the Use of Artificial Intelligence.

Artificial Intelligence (AI) was used as an assisting tool during the system development process, particularly in implementing the system based on the previously established Unified Modeling Language (UML) designs. The research design, system requirements, and development decisions were determined by the authors.

Author contribution statement.

All authors contributed collaboratively to the research and preparation of the article. Their contributions included research planning, system design and development, data collection, data analysis, manuscript preparation, and final review of the article. All authors participated in the research process and approved the final manuscript.

Funding statement.

This research received no external funding or grant support. All research and development expenses were personally funded by the authors as part of their academic and scientific contribution.

Conflict of interest.

The authors declare that there are no conflicts of interest related to the research, authorship, or publication of this article.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada SMK Negeri 1 Wanayasa, para siswa TJKT yang berpartisipasi serta pihak-pihak yang mendukung pelaksanaan penelitian.

DAFTAR PUSTAKA

[1] H. N. R. Syah, F. Rahma, dan S. N. Huda, "Kajian Literatur: Gamifikasi Edukasi Keamanan Siber dengan Konsep Capture the Flag," *Pros. Semin. Nas. Tek. Elektro Sist. Inf. Dan Tek. Inform. SNESTIK*, 2024, doi: https://doi.org/10.31284%2Fp.snestik.2024.5860.

[2] M. A. M. Fadzil dan Z. Abdullah, "The Development of System and Content of Capture the Flag (CTF) Platform," *Appl. Inf. Technol. Comput. Sci.*, vol. 6, no. 1, hlm. 486–504, 2025, doi: https://doi.org/10.30880/aitcs.2025.06.01.027.

[3] D. G. Kartasasmita dan F. G. C. Timur, "Capture the Flag (CTF) Implementation in The Informatics Engineering Study Program Indonesia Defense University," *J. Eng. Educ. Transform.*, vol. 38, no. 4, hlm. 36–44, Apr 2025, doi: 10.16920/jeet/2024/v38i4/25094.

[4] A. N. Kholili, "RANCANG BANGUN SISTEM INFORMASI RAPORT SISWA BERBASIS WEB PADA SEKOLAH MENENGAH KEJURUAN," *INTECH*, vol. 3, no. 1, hlm. 1–7, Apr 2022, doi: 10.54895/intech.v3i1.1285.

[5] M. H. Maulana, S. J. I. Ismail, dan M. F. Rizal, "Membangun Server CTF (Capture the Flag) Untuk Komunitas Security Di Telkom University," *E-Proceeding Appl. Sci.*, vol. 9, no. 5, hlm. 2332–2338, Oktober 2023.

[6] J. T. Santoso, *TEKNOLOGI KRIPTOGRAFI MODERN*. Yayasan Prima Agus Teknik, 2023.

[7] I. Riadi dan B. F. Muthohirin, *Forensik Email*. Jl. Melati No. 171 Sambilegi Baru Kidul, Maguwoharjo, Depok, Sleman, Yogyakarta: Diandra Kreatif (Kelompok Penerbit Diandra), 2022.

[8] Hanafi, *DASAR CYBER SECURITY DAN FORENSIC*. Jl.Rajawali, G. Elang 6, No 3, Drono, Sardonoharjo, Ngaglik, Sleman Jl.Kaliurang Km.9,3 – Yogyakarta 55581: PENERBIT DEEPUBLISH (Grup Penerbitan CV BUDI UTAMA), 2022.

[9] T. A. Kovács dan I. Fürstner, Ed., *Critical Infrastructure Protection: Advanced Technologies for Crisis Prevention and Response*. dalam NATO Science for Peace and Security Series C: Environmental Security. Dordrecht: Springer Netherlands, 2025. doi: 10.1007/978-94-024-2308-2.

[10] S. R. Wicaksono, *Pengujian Perangkat Lunak*. CV. Seribu Bintang, 2023.

[11] A. Rahayu, "Metode Penelitian dan Pengembangan (R&D) : Pengertian, Jenis dan Tahapan," *DIAJAR J. Pendidik. Dan Pembelajaran*, vol. 4, no. 3, hlm. 459–470, Jul 2025, doi: 10.54259/diajar.v4i3.5092.

[12] R. R. Ayuni, S. Rahayu, dan D. Triwahyuningtyas, "Pengembangan dan Uji Efektivitas E-Modul Interaktif Berbasis Scratch Menggunakan Model ADDIE pada Materi Penjumlahan dan Pengurangan Bilangan Cacah Siswa Kelas II SD," *Efektor*, vol. 13, no. 1, hlm. 1–16, Mei 2026, doi: 10.29407/e.v13i1.28237.

[13] A. F. M. Nasuttion, E. Irwansyah, S. Sugara, T. Firmansyah, dan I. Gunawan, "Penerapan UML dalam Analisis dan Perancangan Sistem Informasi di STIKOM Tunas Bangsa," *J. Inov. Artif. Intell. Komputasional Nusant.*, vol. 3, no. 1, hlm. 14–16, Jun 2025, doi: 10.260396/gyk64z07.

[14] C. Nisa, A. Wijaya, dan F. Rizal, *TEORI UML DAN IMPLEMENTASI PRAKTEK: Panduan Untuk Pengembangan Perangkat Lunak*. CV BRAVO PRESS INDONESIA, 2024.

[15] S. W. Ramdany, S. A. Kaidar, B. Aguchino, C. A. A. Putri, dan R. Anggie, "Penerapan UML Class Diagram dalam Perancangan Sistem Informasi Perpustakaan Berbasis Web," 2024.

[16] J. T. Santoso dan Migunani, *DESAIN ANALISIS & Sistem Berorientasi Obyek dengan UML*. Yayasan Prima Agus Teknik, 2021.

[17] A. Libby, *Practical Next.js for E-Commerce: Create E-Commerce Sites with the Next.js Framework*. Berkeley, CA: Apress, 2023. doi: 10.1007/978-1-4842-9612-7.

[18] A. R. Faqih, A. Taufiqurrahman, J. H. Husen, dan M. K. Sabariah, "Empirical Analysis of CI/CD Tools Usage in GitHub Actions Workflows," *J. Inform. Web Eng.*, vol. 3, no. 2, hlm. 251–261, Jun 2024, doi: 10.33093/jiwe.2024.3.2.18.

[19] S. Widodo *dkk.*, *Buku Ajar Metode Penelitian*. CV Science Techno Direct, 2023.

[20] Magdalena, B. Endayana, A. I. Pulungan, Maimunah, dan N. D. Dalimunthe, *METODE PENELITIAN UNTUK PENULISAN LAPORAN PENELITIAN DALAM ILMU PENDIDIKAN AGAMA ISLAM*. Kantor: Jl. Pemancar TVRI Tasik Malaya, Curup Utara Kabupaten Rejang Lebong, Provinsi Bengkulu, Kode Pos: 39125, Provinsi Bengkulu.: Penerbit Buku Literasiologi, 2021.