Penerapan Tanda Tangan Digital dan *Secure Coding* berdasarkan OWASP pada Sistem *E-Control* Tugas Akhir

Dhana Arvina Alwan[1)], Nurul Qomariasih[2)]
(1) Badan Siber dan Sandi Negara, dhana.arvina@bssn.go.id
(2) Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, nurul.qomariasih@poltekssn.ac.id

Abstrak

Teknologi sangat penting dalam kehidupan manusia. Dalam bidang pendidikan, teknologi dapat mempermudah proses pendidikan. Salah satu manfaat teknologi dalam pendidikan adalah sistem e-control tugas akhir. Namun, beberapa sistem yang ada masih memiliki kekurangan dalam hal keamanan aplikasi web. Oleh karena itu, penulis melakukan penelitian untuk memperbaiki sistem dengan menerapkan praktik keamanan berdasarkan panduan OWASP Secure Coding Practices Quick Reference Guide. Penulis juga akan menerapkan tanda tangan elektronik pada mahasiswa melalui API Balai Sertifikasi Elektronik Badan Siber dan Sandi Negara untuk memperbaiki efisiensi penggunaan sistem. Praktik keamanan yang diterapkan meliputi input validation, output encoding, authentication and password management, session management, access control, cryptographic practices, error handling and logging, data protection, communication security, system configuration, database security, file management, memory management, dan general coding practices. Hasil akhir dari penelitian ini adalah terciptanya Sistem E-Control Tugas Akhir yang aman dengan fitur notifikasi, pengajuan topik penelitian, proposal, tugas akhir, tanda tangan elektronik dokumen, broadcast message pada email, unggah-unduh dokumen, dan manajemen pengguna. Penerapan keamanan berdasarkan OWASP Secure Coding Practices Quick Reference Guide yang telah dilakukan terbukti dapat mengurangi risiko kerentanan sebesar 48,15%.

Kata kunci: secure coding; tanda tangan elektronik; tugas akhir

Abstract

Technology is very important in human life. In the field of education, technology can simplify the educational process. One of the benefits of technology in education is the final assignment e-control system. However, some existing systems still have shortcomings in terms of web application security. Therefore, the author conducted research to improve the system by implementing security practices based on the OWASP Secure Coding Practices Quick Reference Guide. The author will also apply electronic signatures to students via the National Cyber and Crypto Agency's Electronic Certification Center API to improve the efficiency of system use. Security practices implemented include input validation, output encoding, authentication and password management, session management, access control, cryptographic practices, error handling and logging, data protection, communication security, system configuration, database security, file management, memory management, and general coding practices. The final result of this research is the creation of a secure Final Assignment E-Control System with notification features, submission of research topics, proposals, final assignments, electronic signature of documents, broadcast messages on email, uploading and downloading documents, and user management. Implementing security based on the OWASP Secure Coding Practices Quick Reference Guide has been proven to reduce the risk of vulnerabilities by 48.15%.

Keywords: secure coding; electronic signature; final assignment

1. PENDAHULUAN

Teknologi merupakan bidang yang paling kritis di kehidupan manusia sehari-hari. Teknologi dinilai sebagai representasi apakah ekonomi di suatu negara berkembang dengan baik [1]. Hal ini dapat terjadi karena dengan teknologi, manusia dapat melakukan pekerjaan dengan efektif dan efisien [1]. Salah satu penerapan dari teknologi adalah pada bidang pendidikan. Di bidang pendidikan, teknologi menjadi suatu harapan bagi seluruh elemen pendidikan untuk dapat mempermudah jalannya proses pendidikan [2]. Salah satu manfaat teknologi dalam bidang pendidikan adalah dikembangkannya sistem *e-control* tugas akhir. Sistem ini merupakan sebuah sistem berbasis web yang dibuat untuk mempermudah pengelolaan tugas akhir mahasiswa mulai dari pengajuan proposal tugas akhir hingga mahasiswa dinyatakan lulus.

Dalam pengembangan aplikasi web, keamanan merupakan hal krusial yang menjadi perhatian bagi para pengembang aplikasi [3]. Hal tersebut dikarenakan banyak terjadi ancaman keamanan siber di bidang aplikasi web. Para ilmuwan mencoba untuk menganalisis frekuensi kemunculan kerentanan siber pada berbagai sumber, yaitu *Open Web Application Security Project* (OWASP), *National Institute of Standards and Technology* (NIST), dan MITRE. Didapati isu terpenting berkaitan dengan keamanan siber di bidang aplikasi web yang diidentifikasi dari kesamaan kerentanan siber berbagai sumber tersebut, diantaranya adalah *authentication, buffer, code injection, cross site scripting forgery,* dan *cross-site scripting* [4]. Dari data tersebut, dapat disimpulkan bahwa masih banyak terjadi kerentanan yang ditemukan pada aplikasi web dan OWASP dapat dipercaya sebagai acuan strategi manajemen risiko

keamanan. Berdasarkan dokumen OWASP *Secure Coding Practices Quick Reference Guide* dikatakan bahwa penerapan seluruh *checklist* merupakan serangkaian praktik keamanan pemrograman secara umum yang dapat diintegrasikan pada *software development lifecycle* [5]. Ketika praktik-praktik ini diimplementasikan, maka dapat mencegah terjadinya kerentanan perangkat lunak yang paling umum terjadi. Maka dari itu, sebaiknya pengembang aplikasi dapat menerapkan seluruh praktik yang ada.

Berbagai penelitian terdahulu telah membahas masalah keamanan aplikasi web dan penerapan praktik *secure coding*. Penelitian yang dilakukan oleh Lala *et al*. menunjukkan pentingnya penggunaan pedoman OWASP dalam pengembangan aplikasi web yang aman, yaitu penerapan praktik *secure coding* mampu mengurangi kerentanan terhadap serangan siber [3]. Selain itu, Sołtysik-Piorunkiewicz dan Krysiak juga menyoroti berbagai ancaman siber yang sering ditemukan pada aplikasi web dalam konteks Industri 4.0, yang menunjukkan bahwa keamanan siber adalah elemen krusial dalam pengembangan sistem berbasis web [4].

Penelitian-penelitian ini memberikan dasar yang kuat bagi pengembangan sistem *E-Control* Tugas Akhir dengan menerapkan OWASP *Secure Coding Practices* untuk meningkatkan keamanan dan efisiensi sistem. Studi ini melanjutkan upaya tersebut dengan menambahkan implementasi tanda tangan elektronik menggunakan *API (Application Programming Interface)* milik Balai Sertifikasi Elektronik (BSrE), sebuah langkah yang belum secara luas diterapkan dalam penelitian sebelumnya. Untuk memastikan sisi keamanan sistem, penulis akan menerapkan *secure coding* berdasarkan 14 daftar periksa OWASP *Secure Coding Practices Quick Reference Guide* berupa *input validation, output encoding, authentication and password management, session management, access control, cryptographic practices, error handling and logging, data protection, communication security, system configuration, database security, file management, memory management,* dan *general coding practices.*

2. TINJAUAN PUSTAKA

2.1 Tugas Akhir Jurusan Kriptografi Politeknik Siber dan Sandi Negara

Penelitian ini akan diimplementasikan pada proses tugas akhir di Jurusan Kriptografi Politeknik Siber dan Sandi Negara (Poltek SSN). Berdasarkan Keputusan Ketua Sekolah Tinggi Sandi Negara Nomor 1 Tahun 2011 tentang Pedoman Tugas Akhir, tugas akhir adalah karya ilmiah hasil penelitian dan/atau percobaan yang disusun oleh taruna dengan bimbingan dosen pembimbing dan dipertanggungjawabkan dalam bidang untuk memenuhi persyaratan memperoleh gelar lulusan [6].

Tahapan Tugas Akhir di lingkungan Politeknik Siber dan Sandi Negara dimulai dari pengajuan *Idea Concept Paper* (ICP), penyusunan proposal, seminar proposal, penyusunan laporan 70%, seminar 70%, penyusunan laporan 100%, dan sidang tugas akhir. Mahasiswa akan dibimbing oleh satu orang dosen pembimbing untuk mendampingi mahasiswa dalam melakukan bimbingan tugas akhir. Di setiap seminar, mahasiswa akan diuji oleh tiga orang penguji, satu diantaranya adalah pembimbing. Dari keseluruhan tahap tugas akhir, akan dilakukan penilaian baik pada laporan yang ditulis ataupun seminar tugas akhir. Penilaian akan ditulis pada lembar khusus yang tersedia dengan menggunakan angka 0-100 berdasarkan peraturan Direktur Poltek SSN yang berlaku.

2.2 Bahasa Pemrograman PHP

Bahasa pemrograman *Hypertext Preprocessor* (PHP) merupakan bahasa pemrograman yang digunakan secara luas dan bersifat *open-source* yang secara khusus sesuai dengan pengembangan aplikasi web dan dapat digunakan bersama dengan *Hypertext Markup Language* (HTML) [7]. Bahasa pemrograman PHP ini diekseskusi pada sisi server sehingga pengguna akan menerima hasil dari kode yang dituliskan, tetapi tidak akan mengetahui kode apa yang membangunnya. Kelebihan penggunaan PHP adalah kesederhanaan bahasa pemrograman ini untuk pemrogram yang baru mempelajari PHP. Meskipun sederhana, PHP menawarkan banyak fitur canggih untuk pemrogram profesional yang dapat diakses pada daftar panjang fitur-fitur PHP. Hal ini menyebabkan bahasa pemrograman PHP dapat dengan mudah dipelajari oleh pemrogram.

2.3 *Digital Signature*

Digital signature atau tanda tangan digital adalah mekanisme kriptografi yang digunakan untuk mengotentikasi identitas penandatangan dan memastikan integritas dokumen elektronik. Afrianto *et al*. [8] menunjukkan bahwa tanda tangan digital merupakan solusi yang efektif untuk menjaga keaslian dokumen di lingkungan digital, terutama di instansi pemerintahan. Penelitian lain oleh Rakhmawati *et al*. [9] menyoroti penggunaan *Application Programming Interface* (API) dalam mengintegrasikan layanan tanda tangan digital dengan sistem informasi yang ada, yang mempercepat proses penerapan tanpa harus mengembangkan sistem dari awal.

Keunikan metode *digital signature* yang diterapkan dalam penelitian ini terletak pada integrasinya dengan API Balai Sertifikasi Elektronik (BSrE). Metode ini tidak hanya meningkatkan efisiensi penggunaan sistem tetapi juga memastikan bahwa dokumen yang dihasilkan memiliki tingkat keamanan yang tinggi sesuai dengan standar yang ditetapkan oleh pemerintah Indonesia.

2.4 *Secure Coding*

Secure coding adalah praktik penulisan kode perangkat lunak dengan memperhatikan keamanan

sejak tahap awal pengembangan. Menurut Lala *et al*. [3], penggunaan pedoman OWASP sangat penting dalam mengembangkan aplikasi web yang aman. OWASP menyediakan serangkaian daftar periksa yang harus dipenuhi oleh pengembang untuk meminimalkan risiko kerentanan yang umum terjadi, seperti SQL *injection*, *cross-site scripting* (XSS), dan *buffer overflow*. Dalam studi lain, Sołtysik-Piorunkiewicz dan Krysiak [4] mengidentifikasi ancaman keamanan dalam aplikasi web di era Industri 4.0, menekankan bahwa penerapan *secure coding* dapat menjadi mitigasi yang efektif terhadap ancaman-ancaman tersebut.

Pendekatan *secure coding* lainnya termasuk penggunaan alat analisis statis dan dinamis untuk mendeteksi kerentanan sejak dini. Namun, pendekatan ini memerlukan integrasi yang baik dalam proses pengembangan perangkat lunak agar efektif. Metode yang dipilih dalam penelitian ini, yaitu penerapan OWASP *Secure Coding Practices*, dipilih karena keandalannya yang telah terbukti dalam berbagai konteks aplikasi web. Selain itu, OWASP menyediakan panduan yang komprehensif dan mudah diakses oleh pengembang di seluruh dunia.

2.5 Perbandingan Pendekatan *Secure Coding*

Berbagai pendekatan terhadap *secure coding* telah diusulkan dan digunakan dalam pengembangan perangkat lunak. Sebagai contoh, metode penilaian risiko yang menggunakan analisis formal dapat memberikan hasil yang sangat akurat tetapi membutuhkan waktu dan sumber daya yang signifikan. Di sisi lain, pendekatan berbasis *checklist*, seperti OWASP *Secure Coding Practices*, lebih praktis dan dapat dengan mudah diintegrasikan ke dalam alur kerja pengembangan perangkat lunak sehari-hari. Kelebihan dari metode ini adalah fleksibilitas dan kemampuannya untuk diterapkan di berbagai jenis aplikasi tanpa memerlukan modifikasi besar pada proses pengembangan.

Pendekatan OWASP dipilih dalam penelitian ini karena telah diakui secara luas dan dapat diakses oleh berbagai *level* pengembang, dari pemula hingga ahli. Ini memberikan keseimbangan yang baik antara keamanan dan kemudahan implementasi, menjadikannya pilihan yang ideal untuk pengembangan sistem *E-Control* Tugas Akhir yang memerlukan keamanan tinggi tanpa mengorbankan efisiensi.

2.6 OWASP *Secure Coding Practices Quick Reference Guide*

OWASP *Secure Coding Practices Quick Reference Guide* mendefinisikan serangkaian praktik pengkodean keamanan perangkat lunak berbasis web [5]. Praktik ini dituliskan dalam format daftar periksa yang dapat diintegrasikan ke dalam siklus hidup pengembangan perangkat lunak. Dengan diterapkannya praktik-praktik ini, kerentanan yang umum terjadi pada perangkat lunak akan berkurang. Pada praktik ini, terdapat 14 daftar periksa. Daftar periksa ini dibedakan berdasarkan kategori pengamanan yang dilakukan pada aplikasi berbasis web. Pada Tabel 1 ditampilkan 14 daftar periksa OWASP *Secure Coding Practices Quick Reference Guide.*

Tabel 1. Daftar Periksa OWASP *Secure Coding Practices Quick Reference Guide*

No.	*Secure Coding Practices Checklist*
1.	*Input Validation*
2.	*Output Encoding*
3.	*Authentication and Password Management*
4.	*Session Management*
5.	*Access Control*
6.	*Cryptographic Practices*
7.	*Error Handling and Logging*
8.	*Data Protection*
9.	*Communication Security*
10.	*System Configuration*
11.	*Database Security*
12.	*File Management*
13.	*Memory Management*
14.	*General Coding Practices*

3. METODE PENELITIAN

Metode penelitian yang akan digunakan pada penelitian ini adalah metode pengembangan *scrum*. *Scrum* merupakan model pengembangan yang mengedepankan kecepatan, sehingga implementasi model *scrum* ini adalah langkah yang tepat untuk pengembangan aplikasi yang cukup kompleks [10]. Hal ini karena pada model ini, proses dapat dilakukan berulang dan memungkinkan menerima perubahan *requirement.* Berikut merupakan beberapa proses pengembangan *scrum:*

1. *Software Planning*

   Perencanaan yang akan dilakukan meliputi definisi lingkup proyek, analisis alat bantu, dan analisis jadwal penelitian.

2. *Requirement Gathering*

   Pada tahap *requirement gathering*, dilakukan pengumpulan kebutuhan bisnis, kebutuhan pengguna, dan kebutuhan sistem. Kebutuhan yang dikumpulkan antara lain pernyataan masalah yang terjadi pada pengelolaan tugas akhir (*problem statement*), pendefinisian visi dari produk (*product vision*), membuat daftar cerita pengguna mengenai hal-hal yang harus dapat dilakukan sistem (*user stories*), mendefinisikan fitur-fitur yang harus dapat dilakukan sistem (*functional requirements*), dan mendefinisikan kebutuhan pelengkap *functional requirements* seperti dokumentasi dan performa program (*non-functional requirements*). Informasi tersebut didapatkan dari wawancara terhadap Ketua Jurusan Kriptografi dan observasi terhadap sistem *e-control* tugas akhir yang telah ada.

3. Product Backlog

Product backlog adalah daftar teratur berisi kebutuhan pengguna yang telah didapatkan dari proses sebelumnya. *Product backlog* ini terdiri atas fitur-fitur yang harus diselesaikan dan diurutkan sesuai dengan nilai, risiko, prioritas, dan kebutuhan. Salah satu item yang akan dicatat pada *backlog* untuk selanjutnya diimplementasikan pada fase *sprint* adalah diagram *Unified Modeling Language* (UML).

4. Sprint

Pada tahap ini dilakukan implementasi dari perencanaan ataupun kebutuhan yang telah disebutkan pada *product backlog.* Pada penelitian ini, fase *sprint* akan dilaksanakan sebanyak tiga kali dengan masing-masing durasinya adalah satu bulan. Terdapat empat peristiwa yang terjadi pada *sprint*, diantaranya:

a. *Sprint Planning*
   Tahap *sprint* dimulai dengan mengadakan *sprint planning* yang berupa pertemuan yang dilakukan oleh tim *scrum* untuk membahas pekerjaan apa saja yang akan dilakukan dalam tahap ini. *Sprint* membahas topik-topik sebagai berikut:
   - Kenapa *sprint* ini penting untuk dilakukan?
   - Apa yang bisa dilakukan pada *sprint* ini?
   - Bagaimana pekerjaan yang telah dipilih akan diselesaikan?

   Sprint planning dilakukan maksimal dalam waktu 8 jam untuk 1 kali *sprint.*
b. *Daily Scrum*
   Tujuan dari *daily scrum* adalah untuk memeriksa perkembangan terhadap *sprint goal* dan mengadaptasi *sprint backlog* seperlunya. Dalam *daily scrum* pengembang dapat menentukan struktur dan teknik yang diinginkan selama masih sejalan dengan *sprint goal*. *Daily scrum* dilakukan selama 15 menit setiap harinya.
c. *Sprint Review*
   Tujuan dari *sprint review* adalah untuk memeriksa hasil *sprint* dan menentukan langkah penyesuaian selanjutnya. Dalam tahap ini, peneliti akan mempresentasikan hasil sistem *e-control* tugas akhir kepada pihak lokus dan membahas perkembangan menuju sasaran produk.
d. *Sprint Retrospective*
   Tujuan dari *sprint retrospective* adalah untuk merencanakan langkah-langkah untuk meningkatkan kualitas dan efektivitas. Waktu pelaksanaannya maksimal tiga jam dalam satu *sprint*.

Dilakukan peninjauan implementasi *secure coding* berdasarkan OWASP *Secure Coding Practices Quick Reference Guide* ketika seluruh fase *sprint* sudah berakhir. Implementasi *secure coding* akan ditinjau oleh *reviewer* yang berkompeten dalam implementasi *secure coding*. *Reviewer* akan mengecek kesesuaian kode dengan *checklist* OWASP yang telah disediakan. Setelah dilakukan peninjauan *secure coding*, sistem yang telah dibuat berdasarkan *sprint backlog* akan dilakukan pengujian berupa *functional testing*, *user acceptance test*, dan *security testing*. *Security testing* yang dilakukan menggunakan alat OWASP ZAP. Hasil pengujian yang dilakukan dapat menyimpulkan apakah sistem yang dikembangkan telah memenuhi kondisi yang diharapkan oleh lokus dan terbukti dapat mengurangi risiko terjadinya kerentanan pada sistem *e-control* tugas akhir.

5. Delivery

Proses *delivery* atau pengiriman hasil aplikasi ditujukan untuk memastikan bahwa nilai bisnis dapat diakses dan diuji oleh pemangku kepentingan serta memberikan peluang untuk mendapatkan umpan balik yang berharga.

4. HASIL DAN PEMBAHASAN

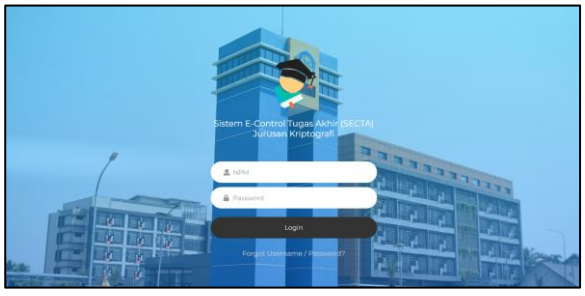
Hasil dari penelitian yang telah dilakukan berdasarkan proses *scrum* menghasilkan penyempurnaan pada beberapa fitur diantaranya, fitur *login*, ganti *password*, input ICP, pengumuman, tugas akhir, dan berkas pelengkap. Penambahan fitur yang dilakukan menghasilkan penerapan tanda tangan digital pada Sistem *E-Control* Tugas Akhir dilakukan melalui integrasi dengan BSrE, sehingga mahasiswa dapat menandatangani *file* secara elektronik dalam sistem.

1. Fitur *Login*

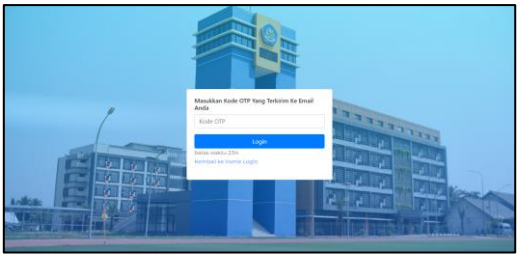
Fitur *login* merupakan halaman pertama yang diakses oleh *user*. Proses *login* ini mencakup *login* menggunakan *username*, *password*, serta kode OTP yang dikirimkan melalui WhatsApp. Pengguna pertama kali akan mengakses halaman login yang ditampilkan pada Gambar 1. Setelah memasukkan kredensial, pengguna harus menginput kode OTP yang ditunjukkan pada Gambar 2.

2. Ganti *Password*

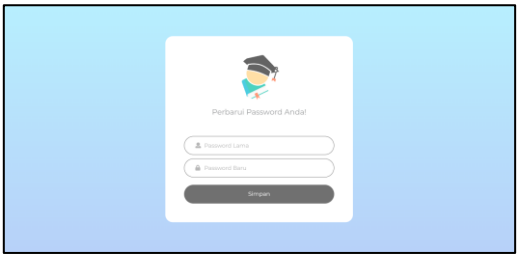
Halaman ganti *password* dapat dilihat pada Gambar 3. Dalam fitur ini, pengguna harus menginputkan *password* lama sebagai autentikasi akun pengguna dan menginputkan *password* baru. Jika *password* lama benar, maka *password* baru akan dicek. *Password* baru wajib terdiri atas minimal 8 karakter yang terdiri atas minimal satu karakter huruf besar, satu karakter huruf kecil, satu karakter angka, dan satu karakter spesial.



Gambar 1. Halaman Login



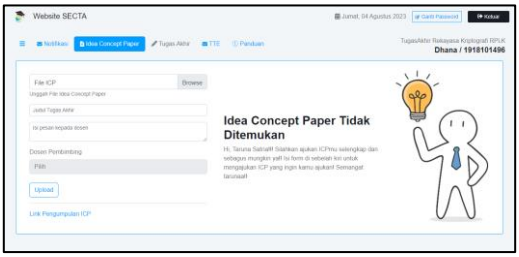
Gambar 2. Halaman Input Kode OTP



Gambar 3. Halaman Ganti *Password*

3. Input ICP

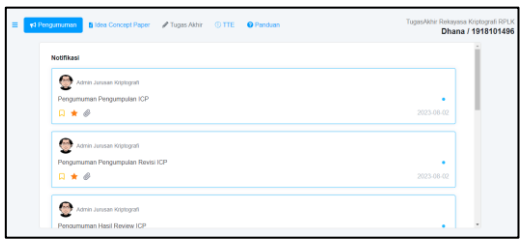
Pada fitur input ICP, mahasiswa dapat mengajukan ICP dengan memasukkan judul ICP, melampirkan *file* pengajuan ICP, dan memilih dosen pembimbing yang akan diajukan seperti pada Gambar 4.



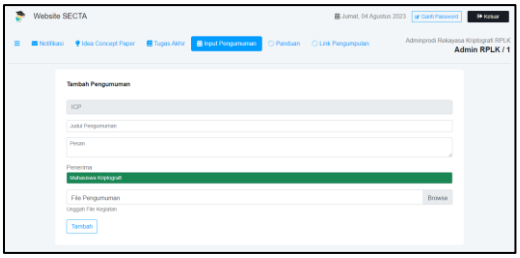
Gambar 4. Halaman Pengajuan ICP

4. Pengumuman

Halaman pengumuman berisi informasi seputar tugas akhir yang dapat diakses oleh mahasiswa yang dapat dilihat pada Gambar 5. Pengumuman akan dikirimkan kepada mahasiswa sesuai dengan jurusannya. Untuk melakukan input pengumuman, admin prodi harus memasukkan kegiatan apa yang akan dibahas, isi pesan, dan *file* lampiran yang ingin dikirimkan. Hal ini dapat dilihat pada Gambar 6.



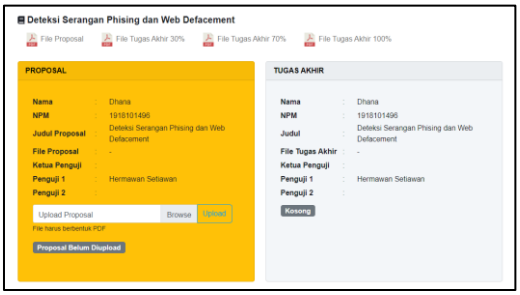
Gambar 5. Halaman Pengumuman



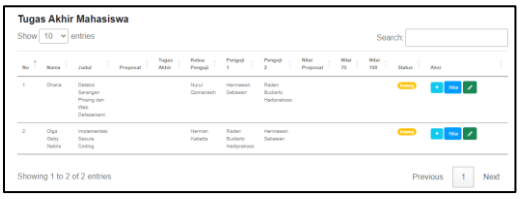
Gambar 6. Halaman Input Pengumuman

5. Tugas Akhir

Menu tugas akhir merupakan menu utama yang ada pada sistem ini. Di dalamnya, mahasiswa dapat mengumpulkan berkas proposal dan tugas akhirnya. Seperti yang ditampilkan pada Gambar 7, pada halaman ini juga ditampilkan dokumen-dokumen yang telah dikumpulkan oleh mahasiswa. Sebelum mahasiswa mengunggah proposal, admin prodi harus menentukan dosen penguji masing-masing mahasiswa pada halaman tugas akhir admin yang ditampilkan pada Gambar 8.



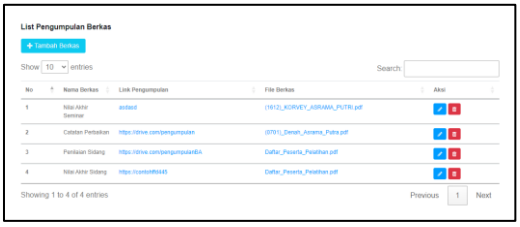
Gambar 7. Halaman Tugas Akhir



Gambar 8. Halaman Tugas Akhir Admin

6. Berkas Pelengkap

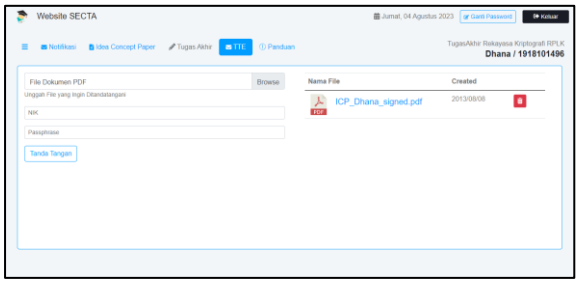
Fitur berkas pelengkap merupakan fitur pada sisi admin prodi yang digunakan untuk mengunggah *file-file* pelengkap sidang serta link pengumpulannya. Sehingga, mahasiswa dapat mengunduh *file* tersebut dan mengunggah *file* yang sudah diberikan identitas pada *link* yang disediakan. Fitur ini dapat dilihat pada Gambar 9.



Gambar 9. Halaman *Link* Pengumpulan Berkas

7. Tanda Tangan Elektronik Dokumen

Sistem *E-Control* Tugas Akhir berintegrasi dengan BSrE dalam menggunakan layanan tanda tangan digital. Mahasiswa dapat menandatangani *file* secara elektronik di dalam sistem ini tanpa perlu membuka sistem yang lain. Fitur ini terdapat pada menu "TTE".



Gambar 10. Halaman Tanda Tangan Elektronik

Seperti yang ditampilkan pada Gambar 10, mahasiswa dapat memilih *file* berekstensi PDF yang ingin diberikan tanda tangan, kemudian mengisi NIK dan *passphrase* yang sudah didaftarkan untuk layanan *E-Sig*n BSrE, kemudian ketika klik "Tanda Tangan" maka akan menambahkan di *list history file* yang telah ditandatangani oleh pengguna.

Hasil dari *User Acceptance Test* yang ditampilkan pada Tabel 2 menunjukkan bahwa 25 dari 26 pengguna setuju bahwa penambahan dan penyesuaian fitur pada Sistem *E-Control* Tugas Akhir sudah berjalan baik, mudah digunakan, dan sesuai dengan kebutuhan pengguna. Namun, terdapat 1 pengguna yang tidak setuju terhadap penambahan fitur ini. Analisis lebih lanjut mengungkapkan bahwa pengguna tersebut merasa bahwa fitur tanda tangan elektronik terlalu rumit dan memerlukan langkah tambahan yang dianggap tidak perlu. Pengguna ini juga menyebutkan bahwa akan lebih nyaman menggunakan metode tanda tangan manual karena sudah terbiasa dengan prosedur tersebut.

Ketidaksetujuan dari pengguna ini menyoroti pentingnya memberikan pelatihan atau tutorial yang lebih mendalam tentang cara menggunakan fitur baru, serta mempertimbangkan alternatif yang lebih sederhana untuk pengguna yang mungkin merasa kurang nyaman dengan teknologi baru. Meskipun demikian, mayoritas pengguna merasa bahwa fitur baru ini secara signifikan meningkatkan efisiensi, terutama dalam hal keamanan dan kemudahan akses dokumen.

Kemudian dilakukan pengujian terhadap fungsi-fungsi yang terdapat pada sistem untuk memastikan *functional requirement* yang dibuat pada tahap *requirement gathering* terpenuhi secara keseluruhan. Pengujian ini dilakukan terhadap 34 *test* case yang diturunkan dari 22 *use case.* Hasil *functional testing* menunjukkan bahwa keseluruhan fungsi telah berjalan dengan baik. Hasil pengujian ini dapat dilihat pada Tabel 3.

Tabel 2. Hasil Kuesioner *User Acceptance Test*

Kode Pertanyaan	Jawaban Ya	Jawaban Tidak
P1	26	0
P2	26	0
P3	26	0
P4	26	0
P5	26	0
P6	26	0
P7	25	1
P8	26	0
Jumlah	207	1
Rata-rata (%)	99,5%	0,48%

Tabel 3. Hasil *Functional Testing*

Use Case ID	*Test Case ID*	*Actual Result*
UC.1	FT_001	Sesuai
	FT_002	Sesuai
UC.2	FT_003	Sesuai
UC.3	FT_004	Sesuai
	FT_005	Sesuai
UC.4	FT_006	Sesuai
UC.5	FT_007	Sesuai
UC.6	FT_008	Sesuai
	FT_009	Sesuai
UC.7	FT_010	Sesuai
UC.8	FT_011	Sesuai
UC.9	FT_012	Sesuai
	FT_013	Sesuai
UC.10	FT_014	Sesuai
UC.11	FT_015	Sesuai
UC.12	FT_016	Sesuai
	FT_019	Sesuai
UC.13	FT_020	Sesuai
	FT_021	Sesuai
UC.14	FT_022	Sesuai
	FT_023	Sesuai
UC.15	FT_024	Sesuai
UC.16	FT_025	Sesuai
	FT_026	Sesuai
UC.17	FT_027	Sesuai
	FT_028	Sesuai
UC.18	FT_029	Sesuai
UC.19	FT_030	Sesuai
UC.20	FT_031	Sesuai
UC.21	FT_032	Sesuai
	FT_033	Sesuai
UC.22	FT_034	Sesuai

Pengukuran tingkat keamanan sistem E-Control Tugas Akhir dilakukan dengan *scanning* menggunakan *tool* OWASP ZAP serta peninjauan keamanan secara manual berdasarkan OWASP *checklist.* Tabel 4 menunjukkan hasil perbandingan kerentanan yang muncul pada pengujian dengan melakukan *scanning* OWASP ZAP.

Pada penelitian tahun 2022 oleh Cahyanto terdapat 27 kerentanan yang terjadi, sedangkan pada penelitian ini terdapat total 14 kerentanan yang terdeteksi. Penerapan keamanan yang dilakukan terbukti dapat mengurangi kerentanan sebesar 48,15%. Hal ini menunjukkan bahwa penerapan keamanan yang dilakukan dapat mengurangi kerentanan yang terjadi jika dibandingkan dengan penelitian sebelumnya di tahun 2022.

Tabel 4. Perbandingan Hasil *Scan* dengan Kerentanan yang Sama

Kerentanan	Hasil *Scan* 2023	Hasil *Scan* 2022
Content Security Policy (CSP) Header Not Set	2	5
Missing Anti-clickjacking Header	1	2
Server Leaks Version Information via "Server" HTTP Response Header Field	4	4
X-Content-Type-Options Header Missing	3	9

Selain itu, pengukuran keamanan juga dilihat dari hasil peninjauan *secure coding* berdasarkan daftar periksa OWASP *Secure Coding Practices Checklist*. Peninjauan dilakukan oleh seorang *expert* yang menguasai bidang *secure coding.* Hasil dari peninjauan dapat dilihat pada Tabel 5.

Tabel 5. Hasil Peninjauan *Secure Coding* berdasarkan Daftar Periksa OWASP *Secure Coding Practices Checklist*

No.	Jenis Daftar Periksa	Diterapkan	
		Ya	Tidak
1.	*Input Validation*	15	1
2.	*Output Encoding*	6	0
3.	*Authentication and Password Management*	20	14
4.	*Session Management*	11	8
5.	*Access Control*	10	14
6.	*Cryptographic Practices*	3	3
7.	*Error Handling and Logging*	8	16
8.	*Data Protection*	10	2
9.	*Communication Security*	1	7
10.	*System Configuration*	6	10
11.	*Database Security*	9	4
12.	*File Management*	7	7
13.	*Memory Management*	6	3
14.	*General Coding Practices*	8	4

Total terdapat 120 poin keamanan yang telah diterapkan dari keseluruhan poin sebanyak 213. Jika dibandingkan dengan penelitian sebelumnya, yaitu hanya menerapkan 51 poin keamanan. Penelitian sebelumnya hanya menerapkan 4 daftar periksa Keamanan yang kemudian ditingkatkan pada penelitian ini dengan menerapkan keseluruhan daftar periksa. Terdapat 9 daftar periksa yang baru diterapkan yaitu *output encoding, session management, access control, cryptographic practices, error handling and logging, communication security, system configuration, memory management,* dan *general coding practices*. Hal ini menunjukkan bahwa keamanan sistem telah banyak ditambahkan dan diperkuat.

5. KESIMPULAN

Penerapan tanda tangan elektronik BSrE dan perbaikan Sistem *E-Control* Tugas Akhir telah sesuai dengan proses bisnis tugas akhir mahasiswa yang ditunjukkan dengan hasil *User Acceptance Test* dengan 99,95% respon menilai bahwa penambahan dan penyesuaian fitur pada Sistem *E-Control* Tugas Akhir sudah berjalan baik, mudah digunakan, dan sesuai dengan kebutuhan pengguna. Selain itu, penerapan *secure coding* pada Sistem *E-Control* Tugas Akhir berdasarkan OWASP *Secure Coding Practices Quick Reference Guide* terbukti efektif dalam mengurangi risiko kerentanan pada sistem sebesar 48,15%, yang dibuktikan dengan berkurangnya item kerentanan pada hasil pengujian keamanan.

REFERENSI

[1] S. Ghory dan H. Ghafory, "The Impact of Modern Technology in the Teaching and Learning Process," *International Journal of Innovative Research and Scientific Studies,* pp. 168-173, 2021.

[2] A. Akbar dan N. Nia, "Tantangan dan Solusi dalam Perkembangan Teknologi Pendidikan di Indonesia," dalam *Prosiding Seminar Nasional Pendidikan Program Pascasarjana Universitas PGRI Palembang*, Palembang, 2019.

[3] S. K. Lala, A. Kumar dan Subbulakshmi, "Secure Web development using OWASP Guidelines," dalam *International Conference on Intelligent Computing and Control Systems*, San Francisco, 2021.

[4] A. Sołtysik-Piorunkiewicz dan M. Krysiak, "The Cyber Threats Analysis for Web Applications Security in Industry 4.0," *Studies in Computational Intelligence,* vol. 887, 2020.

[5] "OWASP Secure Coding Practices Quick Reference Guide," 2010. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf.

[6] STSN, "Keputusan Ketua Sekolah Tinggi Sandi Negara No.001 Tahun 2011 Tentang Pedoman Tugas Akhir," 2019.

[7] PHP, "What is PHP?," The PHP Group, [Online]. Available: https://www.php.net/manual/en/intro-whatis.php. [Diakses 20 Desember 2022].

[8] I. Afrianto, A. Heryandi, A. Finandhita dan S. Atin, "Prototype of E-Document Application Based on Digital Signatures to Support Digital Document Authentication," *Materials Science and Engineering,* p. 879, 2020.

[9] N. A. Rakhmawati, S. H. Suryawan, M. A. Furqon dan D. Hermansyah, "INDONESIA'S PUBLIC APPLICATION PROGRAMMING INTERFACE (API)," *Jurnal Penelitian Pos dan Informatika,* vol. 9, no. 2, pp. 85-96, 2019.

[10] K. Schwaber dan J. Sutherland, "The Scrum Guide," 2020.