JUSTER*: Jurnal Sains dan Terapan*
Vol. 4, No. 1, Januari 2025
p-ISSN: 2809-7661, e-ISSN: 2809-7750

Implementasi *Secure Code* Pada Pengembangan Sistem Keamanan Website Teknik Komputer Universitas Bina Darma Menggunakan Penetration Testing dan OWASP ZAP

Tamsir Ariyadi[1], Andini Putri Salsabila[2] , Yoga Pratama Nugroho[3*]
[1,2,3]Universitas Bina Darma Palembang
Email Corespondent[*]: yogapn02@gmail.com

Abstract

Website security is a very important aspect in protecting data and information from cyber threats. This research aims to implement secure code in developing the security system for the Bina Darma University Computer Engineering website. The methods used include implementing penetration testing and utilizing OWASP ZAP (Zed Attack Proxy) to identify and repair potential vulnerabilities in program code. The research began by conducting security analysis using OWASP ZAP to detect weaknesses such as SQL injection, cross-site scripting (XSS), and other attacks. Based on these findings, secure coding principles were implemented such as input validation, parameterized queries, and data encryption. The research results show that implementing secure code is able to significantly reduce potential vulnerabilities on the websites tested. By integrating penetration testing and OWASP ZAP in the development process, the website security system becomes more reliable in dealing with cyber threats. It is hoped that this study can become a reference in improving the security of web applications in higher education environments.
Keywords*: Secure code, Web security, OWASP ZAP, Penetration testing, System development*

Abstrak

Keamanan website merupakan aspek yang sangat penting dalam melindungi data dan informasi dari ancaman siber. Penelitian ini bertujuan untuk mengimplementasikan secure code pada pengembangan sistem keamanan website Teknik Komputer Universitas Bina Darma. Metode yang digunakan mencakup penerapan penetration testing dan pemanfaatan OWASP ZAP (Zed Attack Proxy) untuk mengidentifikasi serta memperbaiki potensi kerentanan dalam kode program. Penelitian dimulai dengan melakukan analisis keamanan menggunakan OWASP ZAP untuk mendeteksi kelemahan seperti injeksi SQL, cross-site scripting (XSS), dan serangan lainnya. Berdasarkan temuan tersebut, dilakukan penerapan secure coding principles seperti input validation, parameterized queries, dan enkripsi data. Hasil penelitian menunjukkan bahwa penerapan secure code mampu secara signifikan mengurangi potensi kerentanan pada website yang diuji. Dengan mengintegrasikan penetration testing dan OWASP ZAP dalam proses pengembangan, sistem keamanan website menjadi lebih andal dalam menghadapi ancaman siber. Studi ini diharapkan dapat menjadi acuan dalam meningkatkan keamanan aplikasi web di lingkungan pendidikan tinggi.
Kata Kunci: *Keamanan website, OWASP ZAP, Penetration testing, Pengembangan system, Secure code*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong penggunaan website sebagai salah satu media utama dalam menyediakan informasi dan layanan, termasuk di lingkungan pendidikan tinggi. Salah satu media promosi terpopuler saat ini adalah website, yang memiliki jangkauan waktu dan ruang yang tidak terbatas (Yunice Zevanya, 2020). Menurut Tara Rizkayanti & Yunanri, (2023) menjelaskan bahwa website adalah suatu halaman informasi yang disediakan melalui internet sehingga dapat diakses oleh seluruh dunia selagi internet tersebut dapat tersambung. Hal ini sejalan dengan pendapat dari Gregorius Hendita, (2022) yang menjelaskan bahwa website adalah berbagai macam halaman dalam suatu domain yang memuat tentang berbagai informasi agar dapat dibaca dan dilihat oleh sesama pengguna internet melalui mesin pencari.

Dalam Ilham Syaban, dkk (2018) menjelaskan bahwa Sir Timothy John "Tim" Berners-lee adalah penemu website, dan website yang terhubung ke jaringan pertama kali muncul pada tahun 1991. Pada awalnya, Tim membuat situs web untuk memudahkan komunikasi dan update data dengan sesama peneliti di CERN, tempat ia bekerja. Website dapat memuat berbagai jenis media, seperti teks, gambar, suara, dan video, yang memungkinkan setiap orang di seluruh dunia untuk mendapatkan dan mengolah informasi dari berbagai sumber yang tersedia di internet (Ilham Syaban, Norman N, & Anthonius Golug, 2018). Semakin meningkatnya ketergantungan terhadap website juga diiringi dengan meningkatnya ancaman siber, seperti serangan injeksi SQL, cross-site scripting (XXS) dan eksploitasi kerentanan lainnya seperti dapat mencuri data, mengontrol sesi pengguna, menjalankan kode berbahaya, atau digunakan dalam phishing scam. Banyak website telah mengalami kerusakan karena kelemahan ini (Suroto & Asman, 2021).

Untuk menghadapi tantangan tersebut, pengembangan website yang aman menjadi kebutuhan yang tidak dapat diabaikan. Salah satu pendekatan yang dapat diterapkan adalah dengan menerapkan secure code, yaitu praktik pengkodean yang dirancang untuk meminimalkan potensi kerentanan keamanan pada aplikasi web. Selain itu, penggunaan alat seperti OWASP ZAP (Zed Attack Proxy) dalam proses pengujian keamanan dapat membantu pengembang dalam mengidentifikasi dan memperbaiki kelemahan pada sistem.

Menurut Gregorius Hendita (2022) OWASP ZAP adalah aplikasi untuk melakukan pentest untuk menemukan vulnerabilities dalam suatu *web applications* dengan cara mudah. Metodologi penilaian risiko OWASP ZAP adalah cara sederhana untuk menghitung dan mengevaluasi potensi bahaya yang terkait dengan aplikasi. di mana metode ini dapat digunakan untuk menentukan apa yang harus dilakukan terhadap resiko-resiko tersebut. Mengetahui resiko yang akan terjadi akan menghasilkan banyak keuntungan diantaranya, mengurangi resiko yang lebih serius dan menghemat waktu (Naikson Fandier Saragih, dkk 2023).

Menurut Naikson, dkk (2023) dalam jurnal Saragih & Zebua (2023) Penetration testing merupakan tindakan pengujian sistem dengan cara membuat bentuk-bentuk serangan terhadap sistem tersebut sehingga akan diketahui tingkat kerentanannya. Misalnya seperti serangan Cross Site Request Forgery (CSRF) merupakan ancaman aplikasi web yang ditujukan untuk mencuri informasi pengguna aplikasi web. Yang mana Attacker memaksa pengguna web tersebut untuk menjalankan aksi yang tidak di inginkan kepada aplikasi web dimana korban saat ini terautentikasi.

Penelitian ini berfokus pada implementasi secure code dalam pengembangan sistem keamanan website Teknik Komputer Universitas Bina Darma. Dengan memanfaatkan metode penetration testing dan OWASP ZAP, penelitian ini bertujuan untuk mengidentifikasi kerentanan yang ada, mengintegrasikan prinsip-prinsip secure coding, serta meningkatkan kualitas keamanan website. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam memastikan keamanan sistem informasi di lingkungan akademik sekaligus menjadi model untuk pengembangan aplikasi web yang aman di institusi pendidikan lainnya.

METODE

Penelitian ini menggunakan pendekatan eksperimen untuk mengimplementasikan *secure code* dalam pengembangan sistem keamanan website Teknik Komputer Universitas Bina Darma. Langkah-langkah dalam penelitian ini dijelaskan sebagai berikut:

1. Tahap Analisis Kebutuhan

Pada tahap ini, dilakukan identifikasi kebutuhan fungsional dan non-fungsional website, dengan fokus pada aspek keamanan. Analisis mencakup pemetaan terhadap

potensi ancaman dan kerentanan yang relevan dengan sistem.

2. Pengumpulan Data Kerentanan

Pengumpulan data dilakukan dengan menggunakan alat OWASP ZAP untuk melakukan pemindaian terhadap website yang sedang diuji. Hasil pemindaian ini akan memberikan informasi mengenai jenis-jenis kerentanan, seperti injeksi SQL, cross-site scripting (XSS), dan kerentanan lainnya.

3. Penetration Testing

Dilakukan simulasi serangan menggunakan OWASP ZAP untuk menguji sejauh mana sistem rentan terhadap ancaman keamanan. Penetration testing dilakukan untuk memastikan bahwa sistem dapat bertahan dari berbagai ancaman yang sering terjadi.

4. Implementasi Secure Code

Berdasarkan hasil analisis kerentanan, dilakukan pengembangan ulang atau perbaikan kode program dengan menerapkan prinsip-prinsip secure coding, seperti:

a. Validasi input untuk mencegah serangan injeksi.
b. Penggunaan parameterized queries untuk melindungi dari SQL injection.
c. Penggunaan enkripsi pada data sensitif.
d. Penerapan mekanisme autentikasi dan otorisasi yang kuat.

5. Pengujian dan Evaluasi

Setelah implementasi secure code, dilakukan pengujian ulang menggunakan OWASP ZAP untuk memastikan bahwa kerentanan yang sebelumnya ditemukan telah diatasi. Hasil pengujian dibandingkan dengan hasil awal untuk mengukur tingkat peningkatan keamanan.

6. Dokumentasi dan Analisis Data

Data yang diperoleh dari proses pengujian sebelum dan sesudah implementasi dianalisis untuk menentukan efektivitas penerapan secure code dalam meningkatkan keamanan sistem. Analisis ini disajikan dalam bentuk grafik dan tabel untuk memudahkan interpretasi.

Metode ini dirancang untuk memastikan bahwa pengembangan sistem tidak hanya memenuhi kebutuhan operasional, tetapi juga mampu memberikan perlindungan yang optimal terhadap ancaman siber.

HASIL DAN PEMBAHASAN

Sangat penting untuk mengembangkan sistem informasi, terutama untuk situs web universitas seperti Universitas Bina Darma. Tujuan penggunaan kode aman adalah untuk mencegah kerentanan yang dapat dimanfaatkan oleh penyerang. Ini melindungi data dan operasi yang dilakukan oleh website. Dalam hal ini, OWASP ZAP (Zed Attack Proxy) dan penetration testing digunakan sebagai alat utama untuk menemukan dan memperbaiki kerentanan pada website Teknik Komputer Universitas Bina Darma.

Testing penetrasi dilakukan untuk menemukan celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Untuk mengevaluasi ketahanan sistem terhadap ancaman, proses ini melibatkan simulasi serangan di dunia nyata. Oleh karena itu, pengembang dapat memahami potensi bahaya keamanan dan mengambil tindakan pencegahan yang tepat. OWASP ZAP juga digunakan sebagai alat bantu untuk tes ini. OWASP ZAP adalah alat yang populer dan berbasis open-source yang digunakan untuk menemukan kerentanan seperti Cross-Site Scripting (XSS), SQL Injection, dan masalah autentikasi.

Hasil pengujian menunjukkan beberapa masalah umum pada tahap awal pengembangan sistem, termasuk input yang tidak divalidasi dengan benar, konfigurasi server yang tidak ideal, dan kesalahan implementasi autentikasi. Dengan menggunakan pedoman OWASP Secure Coding Practices, pengembang dapat mengatasi masalah ini dengan menerapkan prinsip-prinsip keamanan kode seperti sanitasi input, penggunaan pertanyaan parameterized, dan penerapan mekanisme autentikasi yang lebih kuat.

Dibahas juga bahwa penerapan kode aman secara teratur selama siklus hidup

pengembangan perangkat lunak (SDLC) sangat penting untuk mengurangi ancaman keamanan. Selain itu, tim pengembang dapat memastikan bahwa kerentanan baru tidak ada pada setiap iterasi sistem dengan menggunakan ZAP OWASP berulang. Selain itu, pendekatan ini meningkatkan kesadaran pengembang dan stakeholder akan pentingnya menjaga keamanan aplikasi web.

Secara keseluruhan, penggunaan penetration testing dan OWASP ZAP untuk menerapkan kode aman meningkatkan keamanan situs web Teknik Komputer Universitas Bina Darma. Metode ini dapat digunakan untuk membangun sistem yang lebih kuat dan aman dari serangan siber, yang dapat membantu operasi organisasi secara lebih aman dan terpercaya.

Tabel 1. Keamanan website

No	Jenis kerentanan	Deskripsi	Resiko	Solusi scure code
1	SQL Injection	Input user tidak divalidasi dengan baik	Tinggi	Menggunakan parameterized queries
2	Cross-Site Scripting (XSS)	Data user dieksekusi langsung di browser	Tinggi	Melakukan escaping pada output
3	CSRF	Serangan yang mengeksploitasi sesi aktif user	Sedang	Implementasi token CSRF
4	Open Redirect	Pengalihan URL tidak aman	Rendah	Validasi dan sanitasi input URL

Tabel ini menjelaskan berbagai jenis kerentanan yang sering ditemukan saat membuat aplikasi web, terutama pada situs web Teknik Komputer Universitas Bina Darma. Setiap kerentanan digambarkan dengan deskripsi, tingkat risiko yang dihasilkan, dan solusi untuk mengatasi kerentanan dengan menerapkan kode aman.

Sebagai contoh, SQL Injection adalah kerentanan dengan risiko tinggi yang dapat dicegah dengan menggunakan pertanyaan parameterized. Kerentanan seperti Cross-Site Scripting (XSS) dan Cross-Site Request Forgery (CSRF) juga dapat dicegah dengan menerapkan teknik pengamanan seperti escaping output dan token CSRF. Tabel di atas juga dapat membantu tim pengembang memahami tindakan mitigasi yang diperlukan untuk memastikan keamanan website secara menyeluruh.

KESIMPULAN

Studi ini menunjukkan bahwa menggunakan penetration testing dan OWASP ZAP untuk menerapkan kode aman meningkatkan keamanan situs web Teknik Komputer Universitas Bina Darma. Penggunaan ZAP OWASP membuat website lebih aman dan andal karena mengidentifikasi dan memperbaiki kerentanan keamanan seperti SQL Injection, Cross-Site Scripting (XSS), dan CSRF melalui validasi input, parameterized queries, dan token CSRF.

DAFTAR PUSTAKA

Kusuma, G. H. A. (2022, Agustus). *Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik*, *16*(Jurnal Teknologi Informasi), 178-184.

Rizkayanti, T., & W, Y. (2023, Desember). *Analisis Keamanan Website Sistem Informasi Administrasi Kependudukan Menggunakan Metode Vulnerability Assessment*, *1*(Jurnal Teknologi Informatika Dan Komputer), 1-9.

Surentu, Y. Z., Warouw, D. M. D., & Rembang, M. (2020). *Pentingnya Website Sebagai Media Informasi Destinasi Wisata Di Dinas Kebudayaan Dan Pariwisata Kabupaten Minahasa*, *2*.

Suroto, & Asman. (2021, April). *Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (Xss) Dan Metode Pencegahannya*, *11*.

Syaban, I., Syaban, I., Mewengkang, N. N., & Golug, N. (2018, Juni). *Peranan Penggunaan Website Sebagai Media Informasi Dinas Pariwisata Kabupaten Halmahera Utara*.