OPTIMASI KEAMANAN *WEB*SERVER TERHADAP SERANGAN *BROKEN ACCESS CONTROL* MENGGUNAKAN FRAMEWORK OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP)

SKRIPSI

Disusun untuk memenuhi sebagian persyaratan

Mencapai derajat sarjana

Disusun Oleh:

Muhammad Dzikri Al Hakim

1800018123

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS AHMAD DAHLAN

2024

*WEB*SERVER SECURITY OPTIMIZATION AGAINST *BROKEN ACCESS CONTROL* ATTACKS USING THE OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP) FRAMEWORK

S1 THESIS

Submitted as one of the requirements for achieving a

Bachelor's degree

Arranged by:

Muhammad Dzikri Al Hakim

1800018123

INFORMATICS STUDY PROGRAM

INDUSTRIAL TECHNOLOGY FACULTY

AHMAD DAHLAN UNIVERSITY

2024

LEMBAR PERSETUJUAN PEMBIMBING

OPTIMASI KEAMANAN WEBSERVER TERHADAP SERANGAN BROKEN ACCESS CONTROL MENGGUNAKAN FRAMEWORK OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP)

Dipersiapkan dan disusun oleh:

Muhammad Dzikri Al Hakim
1800018123

Program Studi S1 Informatika
Fakultas Teknologi Industri
Universitas Ahmad Dahlan

Telah disetujui oleh:

Pembimbing

Prof. Dr. Ir. Imam Riadi M.Kom.
NIPM. 19751216 200103 011 0880702

LEMBAR PENGESAHAN

SKRIPSI

OPTIMASI KEAMANAN WEBSERVER TERHADAP SERANGAN BROKEN ACCESS CONTROL MENGGUNAKAN FRAMEWORK OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP)

Dipersiapkan dan disusun oleh:

Muhammad Dzikri Al Hakim
1800018123

Telah dipertahankan di depan Dewan Penguji
pada tanggal Selasa 15 Oktober 2024
dan dinyatakan telah memenuhi syarat

Susunan Dewan Penguji

Ketua	: Prof. Dr. Ir. Imam Riadi M.Kom.	..... 28/10/24.
Penguji 1	: Taufiq Ismail, S.T., M.Cs.	.....
Penguji 2	: Ir. Nuril Anwar, S.T., M.Kom.	.....

Yogyakarta, 15 Oktober 2024
Dekan Fakultas Teknologi Industri
Universitas Ahmad Dahlan

Prof. Dr. Ir. Siti Jamilatun, M.T.
NIPM : 19660812 199601 011 0784324.

LEMBAR PERNYATAAN KEASLIAN
SURAT PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Muhammad Dzikri Al Hakim

NIM : 1800018123

Prodi : Informatika

Judul TA/Skripsi : OPTIMASI KEAMANAN WEBSERVER TERHADAP SERANGAN BROKEN ACCESS CONTROL MENGGUNAKAN FRAMEWORK OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP)

Dengan ini saya menyatakan bahwa Laporan Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar Ahli Madya/Kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 20 Oktober 2024

Mengetahui,

Dosen Pembimbing

Prof. Dr. Ir. Imam Riadi M.Kom.

NIPM. 19751216 200103 011 0880702

Yang menyatakan,

Muhammad Dzikri Al Hakim

1800018123

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan dibawah ini:

Nama	: Muhammad Dzikri Al Hakim
NIM	: 1800018123
Email	: muhammad1800018123@*web*mail.uad.ac.id
Program Studi	: Informatika
Fakultas	: Teknologi Industri
Judul Tesis	: **OPTIMASI KEAMANAN *WEB*SERVER TERHADAP SERANGAN *BROKEN ACCESS CONTROL* MENGGUNAKAN FRAMEWORK OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP)**

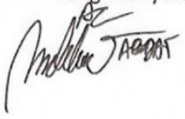
Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah mendapatkan gelar kesarjanaan baik di Universitas Ahmad Dahlan maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian dan implementasi saya sendiri, tanpa bantuan pihak lain kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan di setujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diper*oleh* karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Ahmad Dahlan.

Yogyakarta, 20 Oktober 2024

Yang Menyatakan



Muhammad Dzikri Al Hakim

1800018123

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama	: Muhammad Dzikri Al Hakim
NIM	: 1800018123
Email	: muhammad1800018123@*web*mail.uad.ac.id
Program Studi	: Informatika
Fakultas	: Teknologi Industri

Dengan ini saya menyerahkan hak *sepenuhnya* kepada Perpustakaan Universitas Ahmad Dahlan untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut

Saya **(mengijinkan/~~tidak mengijinkan~~)*** karya tersebut diunggah ke dalam Repository Perpustakaan Universitas Ahmad Dahlan.

Demikian pernyataan ini saya buat dengan sebenarnya.

Yogyakarta, 20 Oktober 2024

Muhammmad Dzikri Al Hakim

Mengetahui,

Pembimbing

Prof. Dr. Ir. Imam Riadi M.Kom.

NIPM. 19751216 200103 011 0880702

KATA PENGANTAR

Alhamdulillah puji syukur kehadirat Allah SWT atas berkat rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Optimasi Keamanan *Web*server Terhadap Serangan *Broken access control* Menggunakan Framework Open Worldwide Application Security Project (OWASP)" dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memper*oleh* gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan. Sholawat dan salam dilimpahkan kepada Nabi Muhammad SAW berkat rahmat dan karunianya telah membawa kita ke dunia yang penuh teknologi seperti saat ini. Adapun skripsi ini sebagai syarat untuk mendapatkan gelar Sarjana Komputer dan tentunya peneliti mendapatkan ilmu yang bermanfaat. Doa dan rasa terima kasih kepada semua pihak yang telah membantu dalam menyelesaikan skripsi. Penulis mengucapkan terima kasih sebesar-besarnya kepada:

1. Prof.Dr. Muchlas, M.T., Rektor Universitas Ahmad Dahlan
2. Prof. Dr. Ir. Siti Jamilatun, M.T. Dekan Fakultas Teknologi Industri Universitas Ahmad Dahlan
3. Dr. Murinto, S.Si, M.Kom. selaku Kepala Program Studi Informatika Universitas Ahmad Dahlan
4. Prof. Dr. Ir. Imam Riadi M.Kom., yang telah memberikan bimbingan, arahan, dan masukan yang sangat berarti dalam penyelesaian skripsi ini.
5. Seluruh dosen dan tenaga pendidik Program studi Informatika Universitas Ahmad Dahlan Yogyakarta yang telah memberikan ilmu yang bermanfaat serta membantu proses *admini*strasi selama saya kuliah.
6. Kedua orang tua penulis terutama almh. Ibu penulis dan keluarga yang selalu memberikan doa, dukungan, dan semangat dalam setiap langkah yang penulis tempuh.
7. Sahabat, rekan-rekan seperjuangan, yang selalu menjadi sumber inspirasi, motivasi, dan dukungan dalam proses perkuliahan dan penyusunan skripsi ini.
8. Orang tua dari sahabat dan rekan-rekan seperjuangan yang terkadang menyebut nama penulis didalam do'a.

Semoga segala bantuan yang telah diberikan semua pihak akan menjadi amal dan dapat balasan yang setimpal dari Allah SWT dan tugas akhir ini akan menjadi informasi yang bermanfaat bagi pembaca atau pihak yang membutuhkan. Terimakasih.

Yogyakarta, 20 Juli 2024

Muhammad Dzikri Al Hakim

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

OPTIMASI KEAMANAN *WEB*SERVER TERHADAP SERANGAN *BROKEN ACCESS CONTROL* MENGGUNAKAN FRAMEWORK OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP)

Muhammad Dzikri Al Hakim

1800018123

ABSTRAK

Penelitian ini bertujuan untuk menganalisis keamanan pada sistem manajemen Perhutani berbasis *Website*, dengan fokus pada kerentanan *Broken access control*. Kerentanan ini dapat memungkinkan pengguna yang tidak berwenang untuk mengakses data sensitif atau fitur yang seharusnya dilindungi. Untuk mende*teks*i dan menganalisis kerentanan tersebut, digunakan alat pengujian OWASP ZAP yang dikenal efektif dalam menemukan kelemahan keamanan pada aplikasi berbasis *web*. Sistem manajemen Perhutani berbasis *web* ini digunakan untuk berbagai aktivitas *admin*istratif, seperti pengajuan surat izin, riwayat pelatihan, dan dokumen lainnya yang terkait dengan operasi perusahaan.

Metode yang digunakan dalam penelitian ini melibatkan dua pendekatan utama, yaitu pemindaian otomatis dan pengujian manual. Pemindaian otomatis dilakukan untuk mende*teks*i kerentanan umum yang sering terjadi di aplikasi *web*, seperti kelemahan pada konfigurasi *Cross-Origin Resource Sharing* (CORS), absennya token Anti-CSRF, serta penggunaan pustaka *JavaScript* yang rentan. Pengujian manual dilakukan untuk mengeksplorasi lebih jauh potensi kerentanan *Broken access control* dengan mencoba mengakses halaman atau data yang seharusnya hanya bisa diakses oleh pengguna berwenang. Selain itu, pengujian manual juga digunakan untuk memverifikasi apakah kerentanan yang terde*teks*i pada pemindaian otomatis benar-benar dapat dieksploitasi.

Hasil penelitian menunjukkan bahwa sistem manajemen Perhutani memiliki beberapa kerentanan serius yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Temuan ini menekankan pentingnya penerapan mekanisme kontrol akses yang lebih ketat dan implementasi langkah-langkah mitigasi, seperti pembaruan pustaka yang rentan dan perbaikan konfigurasi keamanan. Penelitian ini memberikan kontribusi dalam memberikan rekomendasi perbaikan untuk meningkatkan keamanan situs *web* dan melindungi data sensitif dari potensi serangan. Rekomendasi perbaikan mencakup implementasi token Anti-CSRF, peningkatan pengaturan CORS, serta pembaruan pustaka yang digunakan untuk memperkuat keamanan aplikasi.

Kata Kunci : Kerentanan, Keamanan, Mitigasi, OWASP ZAP, Website

*WEB*SERVER SECURITY OPTIMIZATION AGAINST *BROKEN ACCESS CONTROL* ATTACKS USING THE OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP) FRAMEWORK

Muhammad Dzikri Al Hakim

1800018123

ABSTRACT

This study aims to analyze the security of the Perhutani *web*-based management system, focusing on the *Vulnerability* of *Broken access control*. This *Vulnerability* allows unauthorized *user*s to access sensitive data or features that should be protected. The OWASP ZAP *testing* tool, known for its effectiveness in identifying security weaknesses in *web* applications, was used to detect and analyze these vulnerabilities. The Perhutani *web*-based management system is used for various *admin*istrative activities, such as submitting leave requests, training records, and other documents related to company operations.

The methods used in this research involve two main approaches: *Automated Scanning* and manual *testing*. *Automated Scanning* was conducted to detect common vulnerabilities often found in *web* applications, such as weaknesses in *Cross-Origin Resource Sharing* (CORS) configurations, the *Absence of Anti-CSRF Tokens*, and the use of vulnerable *JavaScript* libraries. Manual *testing* was conducted to further explore potential *Broken access control* vulnerabilities by attempting to access pages or data that should only be accessible by authorized *user*s. Additionally, manual *testing* was used to verify whether the vulnerabilities detected in the *Automated Scanning* could actually be exploited.

The results of the study show that the Perhutani management system has several serious vulnerabilities that could be exploited by malicious actors. These findings highlight the importance of implementing stricter access control mechanisms and taking mitigation steps, such as updating vulnerable libraries and improving security configurations. This research contributes by providing recommendations to enhance *Website* security and protect sensitive data from potential attacks. The recommended improvements include implementing Anti-CSRF tokens, strengthening CORS settings, and updating libraries used to bolster the application's security.

Keywords: *Mitigation, OWASP ZAP, Security, Vulnerability, Website*.