Jurnal Infosecure Vol.1 No.2, Oktober 2020
p-ISSN: 2087-1023
MTI-UNLA

KONTROL KEAMANAN APLIKASI R&D MENGGUNAKAN METODE RBAC DENGAN STANDAR OWASP

(Studi Kasus: PT Marin Liza Farmasi)

Mohamad Aziz Adiana

Program Studi Magister, Fakultas Teknik Informatika, Universitas Langlangbuana

azizalmachzumi21@gmail.com

Abstrak— Sistem Research and Development (R&D) sangat penting bagi perusahaan untuk menjaga inovasi dan pengembangan produk yang berkelanjutan. Namun, aplikasi R&D rentan terhadap ancaman keamanan, seperti serangan siber, kebocoran data, dan akses tidak sah. Penelitian ini bertujuan untuk merancang kontrol keamanan menggunakan metode Role-Based Access Control (RBAC) dan standar Open Web Application Security Project (OWASP) guna melindungi aplikasi R&D di PT Marin Liza Farmasi. Metode yang digunakan adalah studi kasus dengan melakukan audit keamanan, analisis risiko, dan evaluasi kontrol akses. Hasil penelitian mengidentifikasi beberapa kelemahan, seperti pemberian hak akses yang berlebihan, kurangnya pemantauan aktivitas, dan kerentanan dalam aplikasi. Implementasi RBAC memastikan bahwa akses terbatas berdasarkan peran pengguna, sementara OWASP membantu mendeteksi serta mengatasi celah keamanan dalam aplikasi. Dengan penerapan kebijakan keamanan yang ketat dan audit berkala, aplikasi R&D di PT Marin Liza Farmasi dapat terlindungi lebih baik.

Kata kunci— Aplikasi R&D, Keamanan Data, RBAC, OWASP, Kontrol Akses.

I. PENDAHULUAN

Database merupakan kunci dalam sistem informasi perusahaan, termasuk sistem Research and Development (R&D) yang berperan penting dalam inovasi dan pengembangan produk. Seiring dengan meningkatnya kompleksitas dan sensitivitas data, database R&D menjadi target utama berbagai ancaman keamanan seperti serangan siber, kebocoran data, dan akses tidak sah. Oleh karena itu, perlindungan data dan kontrol keamanan yang ketat menjadi krusial untuk memastikan integritas, kerahasiaan, dan ketersediaan data. Kontrol keamanan database meliputi beberapa aspek kritis, yaitu kontrol hak akses untuk membatasi akses sesuai peran pengguna, pengaturan parameter keamanan seperti firewall dan enkripsi, serta analisis struktur database dan dokumentasi untuk mengidentifikasi kerentanan. Selain itu, modifikasi aplikasi dilakukan untuk menutup celah keamanan, penerapan aturan keamanan yang konsisten untuk menjaga integritas sistem, serta audit dan pemantauan berkala untuk mengantisipasi potensi ancaman. Penerapan strategi keamanan yang komprehensif melalui metode Role-Based Access Control (RBAC) dan standar Open Web Application Security Project (OWASP) diperlukan untuk mengurangi risiko dan meningkatkan perlindungan data pada database R&D. Ini mencakup penilaian risiko, identifikasi kerentanan, dan implementasi kontrol yang tepat.

II. METODE

Metode Role Based Access Control (RBAC)

Role Based Access Control (RBAC) adalah metode pengaturan akses ke sumber daya komputer atau jaringan berdasarkan peran pengguna dalam organisasi. RBAC membatasi akses berdasarkan tingkat tanggung jawab pengguna, yang dirancang untuk meminimalkan risiko akses tidak sah atau penyalahgunaan data.

Konsep utama RBAC:

- Authorization
  Menentukan apa yang boleh dan tidak boleh dilakukan oleh pengguna.
- Authentication
  Memastikan bahwa identitas pengguna sesuai dengan yang diklaimnya. Analisis SWOT RBAC
- Strengths (Kekuatan)
  Keamanan terstruktur RBAC memungkinkan kontrol granular dengan membatasi akses berdasarkan peran, yang mengurangi risiko akses tidak sah. Efisiensi administratif mempermudah pengelolaan hak akses, terutama dalam organisasi besar yang memiliki banyak pengguna dengan peran berbeda. Scalability sistem mudah diadaptasi untuk perusahaan dengan skala besar atau yang terus berkembang.
- Weaknesses (Kelemahan)
  Kompleksitas dalam konfigurasi implementasi RBAC bisa menjadi rumit dan memerlukan perencanaan yang matang agar peran dan izin selaras dengan kebutuhan bisnis. Rigiditas RBAC terkadang terlalu kaku, tidak memberikan fleksibilitas yang cukup dalam situasi dinamis di mana peran pengguna bisa berubah dengan cepat. Kesalahan administrasi dapat berlaku jika peran dan izin tidak dikelola

dengan benar, ini dapat menyebabkan kesalahan akses yang berbahaya.

• Opportunities (Peluang)

Peningkatan keamanan data dengan meningkatkan perlindungan akses ke data sensitif, RBAC dapat mendukung kepatuhan terhadap regulasi keamanan. Integrasi RBAC dapat diintegrasikan dengan teknologi seperti cloud computing atau IoT untuk memastikan keamanan data pada platform modern. Pengembangan sistem otomasi pada pengelolaan hak akses yang lebih otomatis berdasarkan peran dapat mengurangi kesalahan manusia.

• Threats (Ancaman)

Serangan insider untuk pengguna dengan hak akses yang sah tetapi berniat buruk tetap bisa menjadi ancaman, terutama jika peran-peran tersebut tidak dipantau dengan baik. Kurangnya pemeliharaan pada sistem menyebabkan terjadinya celah keamanan yang dapat merusak pada sistem. Evolusi serangan siber yang terus berkembang dapat menemukan cara untuk mengeksploitasi sistem RBAC yang sudah diimplementasikan.

OWASP

Meningkatkan keamanan perangkat lunak adalah tujuan dari Proyek Keamanan Aplikasi Web Terbuka (OWASP) nirlaba. Pengembang dan spesialis komputer memanfaatkan kerangka OWASP untuk mengamankan situs web. Dengan proyek sumber terbuka dan alat yang dikembangkan OWASP untuk memfasilitasi pengujian sistem, OWASP menawarkan kepada pengembang sebuah platform untuk meningkatkan keamanan sistem. Ide owasp adalah untuk memastikan bahwa pengetahuan atau sumber daya pendidikan apa pun dapat diakses secara bebas dan mudah, sehingga memungkinkan siapa pun meningkatkan keamanan situs web.

OWASP memiliki dokumen-dokumen yaitu:

• OWASP Developer Guide

Panduan Pengembang OWASP adalah dokumen pertama yang perlu dipahami oleh pengembang. Bagi pengembang pemula yang baru mulai membuat situs web dan aplikasi, dokumen ini adalah tempat yang tepat untuk memulai. Perlu diketahui bahwa dokumen ini mengalami revisi pada tahun 2014, dan hasil revisi tersebut menjadi dasar standar keamanan situs web.

• OWASP ASVS

Dokumen berikutnya disebut ASVS, atau Standar Verifikasi Keamanan Aplikasi. Ini adalah standar keamanan global yang dirancang khusus untuk aplikasi online dan dapat dimanfaatkan oleh pemasok, organisasi, dan pelanggan. Menarik untuk dicatat bahwa OWASP mengkategorikan makalahnya di ASVS ke dalam tiga tingkatan: oportunistik, standar, dan lanjutan.

• Security Knowledge Framework

OWASP secara khusus membuat dokumen ketiga untuk memfasilitasi penggunaan ASVS oleh pengembang untuk implementasi aplikasi dan keamanan online.

• Developer Cheat Sheet Series

Dokumen keempat dalam rangkaian contekan pengembang adalah contekan berupa poin-poin yang harus dijawab oleh pengembang.

• OWASP Top 10

OWASP Top 10 berfungsi sebagai referensi bagi pengembang aplikasi web dan tim keamanan untuk mengetahui kerentanan yang mudah dieksploitasi dan perlu segera diperbaiki. Kelemahan ini mempermudah peretas untuk menginfeksi komputer atau situs web dengan malware, mencuri informasi, atau mengambil kendali penuh atas informasi tersebut. Sekelompok spesialis keamanan situs web global biasanya memperbarui 10 Teratas OWASP secara rutin. Untuk melindungi situs web dan data mereka dari peretas, bisnis harus fokus pada sepuluh kerentanan yang tercantum dalam dokumen ini, menurut OWASP.

III. HASIL DAN PEMBAHASAN

Identifiakasi celah keamanan ini akan difokuskan pada website R&D di PT Marin Liza Farmasi. Setelah proses identifkasi dilakukan analisis dan pengujian terhadap celah keamanan yang ditemukan untuk menilai tingkat kerentanannya dan potensi dampaknya terhadap sistem. Hasil dari pengujian ini akan menjadi dasar untuk memberikan rekomendasi peningkatan keamanan sistem.

A. Planning

Tahapan perencanan akan mencakup penyusunan strategi terperinci untuk mengidentifikasi celah keamanan pada sistem aplikasi, yang nantinya akan di implementasikan dengan metode RBAC untuk meningkatkan keamanan pada sistem aplikasi dan meminimalisir celah keamanan.

B. Persiapan dan Pengumpulan data

Penelitian menggunakan website http://103.78.36.86:8082/rnd_lucas/auth sebagai objek penelitian targer pengujian celah keamanannya.

Gambar 1. Halaman Utama Website R&D

C. Information Gathering

Pada tahap ini dilakukan pengumpulan informasi dari website target dengan bertujuan untuk mengidentifkasi pontensi kerentanan dan ancaman pada sistem, serta merencanakan serangan yang tepat. Informasi yang dikumpulkan mencakup dari struktur aplikasi, teknologi yang digunakan, serta celah keamanan yang mungkin ada. Tools yang digunakan meliputi OWASP ZAP untuk memindai otomatis terhadap kerentanan umum, SQLMap untuk mengidentifikasi dan mengeksploitasi celah injeksi SQL, dan Burp Suite untuk melakukan analisis mendalam dan manipulasi permintaan HTTP guna menemukan kelemahan pada sistem.

Gambar 2. Halaman Login

Data yang akan di identifikasi terkait aset-aset penting dalam database R&D sebagai berikut:

Gambar 3. database R&D

Terdapat banyak dokumen yang harus dilindungi dari aplikasi R&D, agar data tersebut tidak dapat diretas oleh pihak yang tidak bertanggung jawab dan tidak di rusak datanya. Begitu juga pada aplikasi R&D harus di identifikasi hak akses nya agar tidak ada kesalahan pada human error saat menginput data-data yang penting.

D. Analisis Risiko dan Perancangan Sistem

Perlu dilakukan analisis terhadap database dan aplikasinya untuk mengidentifikasi tingkat risiko keamanan yang ada. Analisis ini bertujuan untuk mengetahui celah keamanan mana saja yang rentan diretas. Dengan demikian, langkah mitigasi dapat diambil untuk memperkuat keamanan sistem secara menyeluruh.

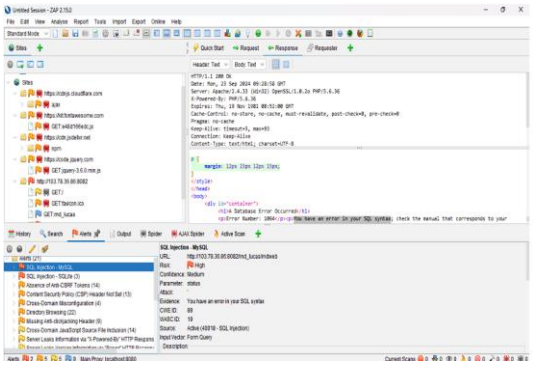
Dari hasil analisis pada Gambar 3 semua tabel di dalam database tersebut berpotensi mengandung data sensitif yang perlu dilindungi, terutama karena berhubungan dengan proses bisnis dan regulasi farmasi. Berikut beberapa tabel yang tampak kritis dan memerlukan perlindungan ekstra:

a. certificate_of_analysis Kemungkinan berisi hasil analisis produk yang sangat penting untuk menjaga standar kualitas dan keamanan produk farmasi.
b. dokumen_ptwo dan dossier_registrasi Tabel ini berpotensi menyimpan dokumen atau data registrasi yang diperlukan untuk kepatuhan regulasi. Informasi ini harus dijaga untuk menghindari penyalahgunaan atau pemalsuan.
c. change_control Biasanya berisi data mengenai perubahan proses atau produk yang harus didokumentasikan secara ketat dalam industri farmasi.
d. masterlist_nie_marin dan masterlist_nie_ptlucasdjaja Bisa berisi data terkait Nomor Izin Edar (NIE) produk yang penting untuk legalitas distribusi produk farmasi.
e. pembuatan_laporan_validasi dan pembuatan_laporan_stabilitas Tabel ini tampaknya berisi laporan validasi dan stabilitas produk yang merupakan bagian penting dari kontrol kualitas.

Selanjutnya akan diterapakan standar kemanan OWASP ZAP dan dilakukan perancang kontrol keamanan akses menggunakan Role-Based Access Control (RBAC). Penerapan ini bertujuan untuk meningkatkan keamanan aplikasi dengan membatasi akses berdasarkan peran, sehingga hanya pengguna yang berwenang dapat mengakses data dan fungsi tertentu. Sebelum penerapan standar keamanan OWASP ZAP dan perancangan kontrol akses dengan RBAC, akan dilakukan pengujian aplikasi untuk mengidentifikasi potensi celah keamanan dan memastikan bahwa seluruh kerentanan dapat terdeteksi. Pengujian ini bertujuan untuk memberikan gambaran lengkap mengenai risiko yang ada, sehingga langkah mitigasi keamanan dapat diimplementasikan dengan tepat. Setelah hasil pengujian didapatkan, standar keamanan akan diterapkan guna memperkuat perlindungan aplikasi dari serangan siber.

E. Vulnerability Assesment

Pada proses Vulnerability Assesment bertujuan untuk mendapatkan sebuah informasi mengenail celah keamanan yang terdapat pada website target. Dalam melakukan pencarian celah keamanan pada website http://103.78.36.86:8082/rnd_lucas/auth menggunakan tools OWASP ZAP dan dilakukan secara manual scanning. Dapat dilihat pada Gambar 4



Gambar 4. Pengujian Menggunakan OWASP ZAP

Dari hasil pengujian pada Gambar 4 pengujian menggunkan Owasp ZAP terdapat beberpa alert yang mengakibatkan terjadi nya celeh kerentanan pada web.

- Absence of Anti -CSRF token dampak yang akan terjadi credensial pengguna akan di dapatkan oleh penyeran serpeti id session cookies dan lain sebagainya.
- Content Security Policy (CSP) Header Not Set dari celah ini dapat mem by pass keamanan dari sisi client mendapatkan informasi yang sensitive atau menyimpan aplikasi berbahaya.
- Cross-Domain JavaScript Source File Inclusion celah nya terdapat file javascript yang tidak dikenal dari domain external dampak nya memungkinkan penyerang menambahkan script agar memanipulasi data yang bisa melukan perubahan fungsionalitas dan pengalihan data.

Berdasarkan dari hasil scanning pada form login bahwa website http://103.78.36.86:8082/rnd_lucas/auth memiliki 12 kerentanan celah keamanan yang berada pada level High dalam hal ini memungkinkan website target masil belum aman, hasil level risiko dapat dilihat pada tabel 1.

Tabel 1. Hasil Scan Celah Keamanan

Celah Keamanan	LK	IM	RS
SQL Injection - MySQL	H	H	High
SQL Injection - SQLite	H	M	Medium
Absence of Anti-CSRF Tokens	H	M	Medium
Content Security Policy (CSP) Header Not Set	H	M	Medium
Cross-Domain Misconfiguration	H	M	Medium
Directory Browsing	H	M	Medium
Missing Anti-clickjacking Header	H	M	Medium
Cross-Domain JavaScript Source File Inclusio	M	M	Low
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	M	M	Low
Server Leaks Version Information via "Server" HTTP Response Header Field	H	M	Low

F. Implementasi RBAC

Pada tahapan ini akan mengimplementasikan metode Role-Based Acces Control (RBAC) pada aplikasi R&D untuk meminalisir celah keamanan pada sistem. RBAC berfungsi untuk membatasi akses pengguna berdasarkan peran dan tanggung jawab masing-masing pengguna, untuk memastikan bahwa hanya pengguna dengan otoritas yang tepat dapat mengakses data atau fitur tertentu. Hal ini untuk mengurangi risiko akses tidak sah dan penyalahgunaan pada sistem. Selain penerapan RBAC yang dilakukan pada sistem aplikasi digunakan juga enkripsi data untuk melindungi data yang sensitif pada sistem. Dengan enkripsi data yang berupa informasi seperti data pribida pengguna atau data penting lainnya akan dikodekan sehingga hanya pihak yang memiliki kuncienkripsi yang dapat membacanya. Hal ini untuk meningkatkan lapisan perlindungan, terutama terhadap potensi pencurian data dan kebocoran data.

Langkah untuk implementasikannya sebagai berikut:

Penerapan pada sistem aplikasi terhadap authentication pada sistem aplikasi untuk mencegah terjadi bug sql injection pada sistem aplikasi.

```
Auth.php
class Auth extends CI_Controller {
    private function _login()
    {
        $username = $this->input->post('username');
        $password = $this->input->post('password');

        $user = $this->db->get_where('user', ['username' => $username])->row_array();

        if ($user) {
            if ($user['is_active'] == 1) {

                if (password_verify($password, $user['password'])) {
                    $data = [
                        'username' => $user['username'],
                        'role_id' => $user['role_id']
                    ];
                    $this->session->set_userdata($data);
                    if($user['role_id'] == 1){
                        redirect('dashboard');
                    }else{
                        redirect('rnd');
                    }
                } else {
                    $this->session->set_flashdata('message', '<div class="alert alert-danger" role="alert">
                    Wrong password!</div>');
                    redirect('auth');
                }
            } else {
                $this->session->set_flashdata('message', '<div class="alert alert-danger" role="alert">
                This username is not yet activated! Contact the Administrator immediately</div>');
                redirect('auth');
            }
```

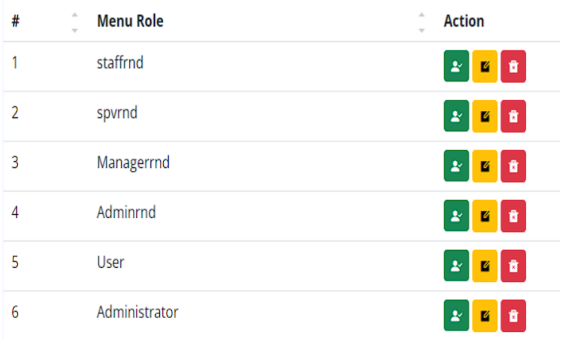
Gambar 5. Script Auth

Pada Gambar 5 script yang digunakan menggunakan Active Record yang merupakan salah satu fitur dari framework sehingga dapat terhindar serang SQL Injection. Dalam query get_where() secara otomatis meng-hendle input yang berpotensi berbahaya, seperti karakter khusus yang digunakan dalam SQL Injection.

	id	nama	username	email	level_akses	password
Edit Copy Delete	1	IT	it	cyberit@gmail.com	Staff RnD	$2y$10$wGFyHoe4ubLY7hv3XZqHk.wiTTVhkUVz7Xr8GlcV7a4...
Edit Copy Delete	2	Administrator	admin	administrator@gmail.com	Super Admin	$2y$10$BwlVM6nFbsuH9JNtn.DVN.qJQB0OQ/hI97kCa57FOfO...
Edit Copy Delete	3	Staff RnD	staff	staffrnd@gmail.com	Staff RnD	$2y$10$VPDBRkSkAlVSbcrVwr135buwU6QiRVlguE64fzsmrGSG.
Edit Copy Delete	4	Alya Fiska Rahnia	Alya	fiskarahniaa@gmail.com	Spv RnD	$2y$10$PeqVQEMIZLn.kHA7VuIqo.2L4OqzMVbVFaNLwlGx9h3...

Gambar 6. Tampilan password yang sudah di enkrip

Pada Gambar 6 password sudah lakukan eknripsi agar meminimalisir akan celah keamanan pada password, kemudian akan diterapkan metode RBAC untuk membatasi setiap akses bagi pengguna dengan level hak akses yang diberikan.



Gambar 7. Role Akses

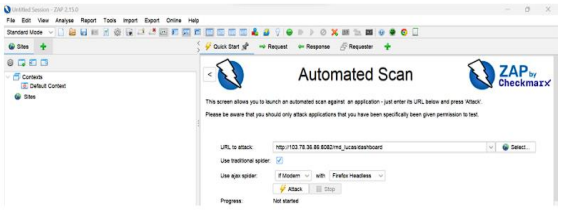
Pada Gambar 7 masing pengguna memiliki hak akses masing-masing diantara lain sebagai berikut:

Tabel 2. Role Akses

Role Akses	Akses Menu	Keterangan
Staff RND	Dashboard, Monitoring, Roadmap.	Pada role akses Staff RND hanya menginput data, lihat data, edit data, tidak bisa menghapus data. Menu yang boleh
		diakses hanya menu Monitoring yang di dalam menu tersebut bisa akses data identitas produk, pembuatan dossier registrasi, dan menu roadmap.
Spv RND	Dashboard, Monitoring, Roadmap, Master NIE	Role akses Spv RND bisa input data, lihat data, hapus data, dan bisa memantau kegiatan yang dilakukan oleh staff maupun user biasa untuk mengolah data.
Manager RND	Dashboard, Monitoring, Roadmap, Master NIE.	Manager RND bisa melakukan pemantau kegiatan yang dilakukan oleh Staff dan Spv RND. Dan jika ada tidak kesesuaian pada pengeloha data yang sudah dilakukan maka bisa di reject datanya dan dikembalikan lagi untuk diperbaiki.
Admin RND	Dashboard, Monitoring, Roadmap, User Setting	Admin RND bisa melakukan input data, edit data, lihat data, dan hapus data. Admin RND bisa melakukan approved pada pengguna baru yang akan mengakses menu pada aplikasi.
User	Dashboard, Monitoring	Hanya di berikan akses untuk input data pada monitoring tidak bisa hapus data.
Administrator	All Menu	Dapat mengakses apapun pada sistem aplikasi dan memantau setiap aktifitas pada sistem.

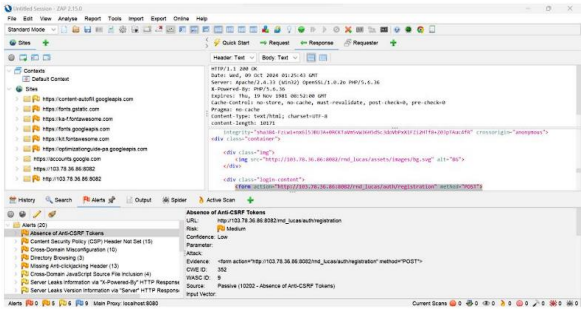
G. Pengujian

Pada tahapan ini pengujian sistem aplikasi yang sudah di terapan metode RoleBased Access Controller (RBAC). Tahap pengujian sebagai berikut: Langkah pertama menggunakan OWASP ZAP untuk scanning celah kerentanan pada sistem aplikasi.



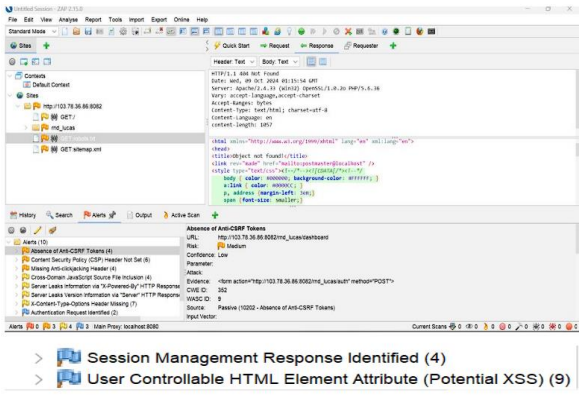
Gambar 8. Automated Scan OWASP ZAP

Masukan URL
http://103.78.36.86:8082/rnd_lucas/dashboard
untuk scanning



Gambar 9. Hasil Scanning Pertama

Pada Gambar 9 memberikan informasi dari hasil scanning yang pertama menunjukan bahwa kerentanan di level medium tidak di level high. Sebelum melanjutkan scanning ke tahap kedua maka akan diperbaiki dulu script dari sistem nya untuk meminimalisir celah kemanannya.



Gambar 10. Hasil Scanning Tahap Kedua

Dari hasil tahap kedua scanning kerentanan dari sistem aplikasi maka sudah berkurang celah kemanan nya.

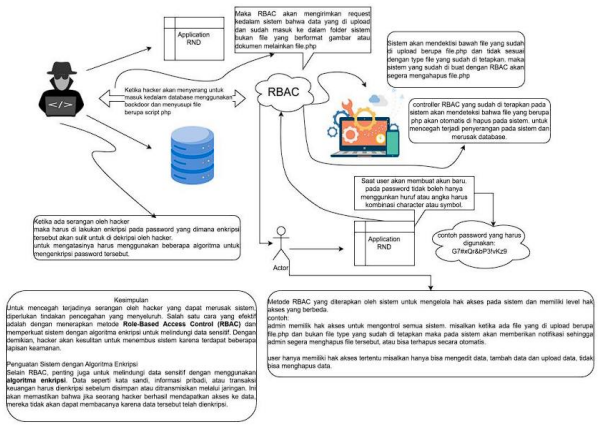
Tabel 3. Hasil Scanning Pertama

Celah Keamanan	LK	IM	RS
Absence of Anti-CSRF Tokens	M	L	Low
Content Security Policy (CSP) Header Not Set	M	L	Low
Cross-Domain Misconfiguration	M	L	Low
Directory Browsing	M	L	Low
Missing Anti-clickjacking Header	M	L	Low
Cross-Domain JavaScript Source File Inclusio	M	L	Low
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	M	L	Low
Server Leaks Version Information via "Server" HTTP Response Header Field	M	L	Low
Strict-Transport-Security Header Not Set	L	L	Low
X-Content-Type-Options Header Missing	L	L	Low

Tabel 4. Hasil Scanning Kedua

Celah Keamanan	LK	IM	RS
Absence of Anti-CSRF Tokens	M	L	Low
Content Security Policy (CSP) Header Not Set	M	L	Low
Cross-Domain Misconfiguration	M	L	Low
Directory Browsing	M	L	Low
Missing Anti-clickjacking Header	M	L	Low
Cross-Domain JavaScript Source File Inclusio	M	L	Low
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	M	L	Low
Server Leaks Version Information via "Server" HTTP Response Header Field	M	L	Low
Strict-Transport-Security Header Not Set	L	L	Low
X-Content-Type-Options Header Missing	L	L	Low
Authentication Request Identified	L	L	Low
User Controllable HTML Elemen Attribute (Potensial XXS)	L	L	Low

Pada tabel 3, dan tabel 4 bahwa hasil dari scanning aplikasi tidak kerentan nya rendah hal ini sudah di implementasikan dengan metode RBAC bisa membantu untuk meminimalisir tingkat kerentan pada sistem. Jika di bandingkan dari hasil gambar IV.5, dan tabel IV.2 dari hasil scanning aplikasi nya yang tadinya banyak celah kemanan dan berada pada tingkat level high setelah menggunakan metode RBAC tingkat kerenantan nya bisa berkurang dan berada di level medium dan level low.



Gambar 11. Skema Implementasi Dan Pengujian

Dari hasil implementasi dan pengujian pada sistem aplikasi RND menggunakan metode RBAC dapat disimpulkan bahwa metode RBAC dapat membantu untuk meningkatkan keamanan sistem aplikasi. RBAC memungkinkan penganturan akses berdasarkan peran dan tanggung jawab pengguna, sehingga hanya pengguna dengan otoritas tertentu yang dapat mengakses data yang sensitif. Hal ini untuk mencegah akses tidak sah, menjaga integritas data, serta mengurangi risiko kebocoran data informasi.

H. Evaluasi

Dari hasil yang sudah diuji dengan menggunakan tools OWASP ZAP pada aplikasi R&D terdapat banyak celah keamanan yang terbuka sehingga peretas bisa memanfaatkan dari celah keamanan untuk bisa mengakses server, mengambil data, dan merusak data. Setelah dilakukan pengujian maka diimplementasikan dengan metode RBAC guna untuk meminimalisir celah keamanan pada sistem aplikasi. Hal yang dilakukan nya adalah sebagai berikut:

1. Perbaikan pada script.
2. Pemberian kontrol hak akses yang di dasari oleh metode RBAC.
3. Menambahkan validasi pada sistem aplikasi.
4. Menggunakan enkripsi pada data yang sensistif.

Langkah selanjutnya diuji kembali setelah semua diimplementasikan, maka tahapan metode RBAC pada sistem yang sudah diterapkan mampu meminimalisir celah keamanan. Sehingga metode RBAC berguna untuk sistem aplikasi R&D dengan kontrol keamanan yang diberikan. Hal yang akan dilakukan untuk selanjutnya harus guna untuk meningkatkan kemanan lebih lanjut maka harus dilakukan pengecekan dan pengujian terhadap aplikasi, serta jika ada kelemahan pada aplikasi maka segara harus ditindak lanjuti untuk diperbaiki agar celah keamanan nya bisa tertutup. Setidaknya dianjurkan untuk pengujian dan perbaikan aplikasi harus dilakukan minimal seminggu sekali agar aplikasi terhindar dari kerentanan dan serangan cyber.

IV. SIMPULAN

Berdasrkan hasil penelitian yang telah diuraikan pada bab sebelumnya, dapat disimpulkan bahwa:

1. Berdasarkan kerentanan yang ditemukan, maka penelitian ini menghasilkan dokumen berisi rekomendasi yang spesifik berdasarkan hasil analisis, dengan kontrol keamanan menggunakan mteode Role-Based Access Control (RBAC) mampu meminimalisir celah keamanan pada sistem.
2. Berdasarkan dari hasil implementasi menggunakan metode Role-Based Access Control (RBAC) berhasil menutup celah keamanan pada script aplikasi R&D. Role-Based Access Control (RBAC) bisa membatasi akses sesuai peran dan tanggung jawab pengguna, sehingga meminimalisir kerentanan yang disebabkan oleh hak akses berlebihan atau akses tidak sah. OWASP ZAP membantu mengidentifikasi celah keamanan seacara komprehensif. Hasil temuan OWASP ZAP kemudian ditindak lanjuti dengan penerapan kontrol keamanan menggunakan RBAC untuk menutup celah tersebut dan memperkuat perlindungan aplikasi.

REFERENSI

[1] Siregar, Firman Hamonangan et al. 2017. Analisis Metode Role-Based Access Control Pada Sistem Pengamanan Basis Data Dengan Konsep CIA. 1–7. Di akses 8 Agustus 2017 (http://journal.stth medan.ac.id/mahasiswa/index.php/doc_ download/373-v1254- lxiii analisis-metode role-based-access-control-pada-sistem pengamanan-basis-data-dengan-konsep cia).

[2] Strembeck, M. 2004. Conflict Cheking of Separation of Duty Constraints in RBAC Implementation Experiences. Hal. 1–6 in In Proc. of the Conference on Software Engineering.

[3] Asrianda. 2016. Kontrol Akses dan Keamanan Data bagi Penduduk Miskin. Hal. 51–55 in Proceeding Seminar Nasional Ilmu Komputer (SEMINASIK), vol. 1. Bireun, Aceh: Fakultas Ilmu Komputer Universitas Almuslim, 11 - 18 November 2016. Di akses 9 Juli 2017 (http://www.academia.edu/34671943/KONTROL_AKSES_DAN_KEAMANAN_DATA_BAGI_PENDUDUK_MISKI N).

[4] Chen, Fang dan Ravi S. Sandhu. 1996. Constraints for role-based access control. Proceedings of the first ACM Workshop on Role-based access control - RBAC ’95 (7):14–es. Di akses 18 Juli 2017 (http://dl.acm.org/citation.cfm?id=27015 2.270177).

[5] Abzug et al. (2003). System Security Engineering Capability Maturity Model (SSE- CMM) Model Description Document Version 3.0. Pennsylvania. Carnegie Mellon University.

[6] ndreu A. “Professional pen testing for Web applications.” John Wiley and Sons, pp. 9-10, 2006.

[7] Singh H., Surender J. and Pankaj K. V. "Penetration Testing: Analyzing the Security of the Network by Hacker’s Mind." Volume V IJLTEMAS, pp 56 – 60, 2016.

[8] Wang X., Luhua W, Gengyu W, Dongmei Z, and Yixian Y. "Hidden web crawling for SQL injection detection."3 rdIEEE. International Conference on, Broadband Network and Multimedia Technology (IC-BNMT), pp. 14-18, 2010.

[9] B. Bin Halib, E. Budiman, and H. J. Setyadi, “Teknik Hacking Web Server Dengan Sqlmap Di Kali Linux,” J. Rekayasa Teknol. Inf., vol. 1, no. 1, pp. 67–72, Jun. 2017, doi: 10.30872/JURTI.V1I1.642.

[10] Goel, J. N., and Mehtre B. M. "Vulnerability assessment and penetration testing as a cyber defence technology." 57 Procedia Computer Science, pp.710-715, 2015.