UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE UNA PLATAFORMA DE EXPERIMENTACIÓN QUE PERMITA EVALUAR EL NIVEL DE SEGURIDAD DE LOS SERVICIOS QUE BRINDA KEYCLOACK CON OAUTH 2.0 PARA DISPOSITIVOS ANDROID Y WEB (ANGULAR).

Trabajo de titulación previo a la obtención del

Título de Ingeniera de Sistemas

AUTORA: MARIA JOSE VIVANCO GONZAGA

TUTORA: LINA PATRICIA ZAPATA MOLINA

Quito - Ecuador

2022

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Maria Jose Vivanco Gonzaga con documento de identificación N°.1716002066: manifiesto que:

Soy la autora y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana puede usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 10 de marzo de 2022

Atentamente,

Maria Jose Vivanco Gonzaga

1716002066

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDADPOLITÉCNICA SALESIANA

Yo, Maria Jose Vivanco Gonzaga con documento de identificación N°.1716002066, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: "Implementación de una plataforma de experimentación que permita evaluar el nivel de seguridad de los servicios que brinda Keycloack con Oauth 2.0 para dispositivos android y web (angular)", el cual ha sido desarrollado para optar por el título de: Ingeniera de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 10 de marzo de 2022

Atentamente,

Maria Jose Vivanco Gonzaga

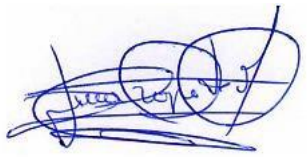
1716002066

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Lina Patricia Zapata Molina con documento de identificación N°0501877278, docente de la Universidad Politécnica Salesiana, declaró que bajo mi tutoría fue desarrollado el trabajo de titulación: IMPLEMENTACIÓN DE UNA PLATAFORMA DE EXPERIMENTACIÓN QUE PERMITA EVALUAR EL NIVEL DE SEGURIDAD DE LOS SERVICIOS QUE BRINDA KEYCLOACK CON OAUTH 2.0 PARA DISPOSITIVOS ANDROID Y WEB (ANGULAR), realizado por Maria Jose Vivanco Gonzaga con documento de identificación N°.1716002066,obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 10 de marzo de 2022

Atentamente,



Ing. Lina Patricia Zapata Molina, PhD

0501877278

IMPLEMENTACIÓN DE UNA PLATAFORMA DE EXPERIMENTACIÓN QUE PERMITA EVALUAR EL NIVEL DE SEGURIDAD DE LOS SERVICIOS QUE BRINDA KEYCLOACK CON OAUTH 2.0 PARA DISPOSITIVOS ANDROID Y WEB (ANGULAR).

IMPLEMENTATION OF AN EXPERIMENTATION PLATFORM THAT ALLOWS TO EVALUATE THE SECURITY LEVEL OF THE SERVICES PROVIDED BY KEYCLOACK WITH OAUTH 2.0 FOR ANDROID AND WEB DEVICES (ANGULAR).

Lina Patricia Zapata[1], Maria Jose Vivanco Gonzaga [2]

Resumen

Las aplicaciones actualmente sufren grandes conflictos en autenticación de inicio de sesión desde diferentes sitios con poca seguridad ya que no se cuenta con una plataforma centralizada que permita gestionar de manera segura los accesos a los sistemas. Actualmente el control de acceso a recursos se realiza en base a roles y permisos otorgados al usuario lo que provoca que la seguridad de aplicaciones Web y Apps sea susceptibles a ataques diarios de malware (software malicioso que es dañino para los sistemas informáticos). De acuerdo con esta problemática se propone la implementación de una plataforma de experimentación que permita evaluar el nivel de seguridad, para esto se diseñara una aplicación Web (Angular) y Apps (Android) utilizando java 8+, spring boot, base de datos postgresql se codificara los niveles de accesos para la autenticación y autorización del acceso al sistema. Posterior a la implementación se realizaran pruebas de seguridad a los empoind webservices, caso de prueba donde si no se dispone de los perfiles o roles de acceso se denegara el inicio de sesión. Keycloak proporciona una plataforma centralizada para el manejo de inicios de sesión único para la protección de datos de accesos desconocidos y no autorizados a través de mecanismos que cuenten con un alto nivel de seguridad al fin de identificar quien realmente está autorizado para acceder a los recursos del sistema.

Abstract

Applications currently suffer great conflicts in login authentication from different sites with little security because there is no centralized platform to securely manage access to systems. Currently, access control to resources is based on roles and permissions granted to the user, which makes the security of Web applications and Apps susceptible to daily malware attacks (malicious software that is harmful to computer systems). According to this problem we propose the implementation of an experimental platform to evaluate the level of security, for this we will design a Web application (Angular) and Apps (Android) using java 8+, spring boot, postgresql database, the access levels will be coded for authentication and

[1] Docente de la Carrera de Ingeniería de Sistemas – Universidad Politécnica Salesiana, Sede Quito – Campus Sur. Autora para correspondencia: lzapata@ups.edu.ec

[2] Estudiante de Ingeniería de Sistemas – Universidad Politécnica Salesiana, Sede Quito – Campus Sur. Autora para correspondencia: mvivanco@est.ups.edu.ec

authorization of access to the system. After the implementation, security tests will be performed to the empoind webservices, test case where if the profiles or access roles are not available, the login will be denied. Keycloak provides a centralized platform for single sign-on management to protect data from unknown and unauthorized access through mechanisms that have a high level of security in order to identify who is actually authorized to access system resources.

1. Introducción

En la actualidad los sistemas informáticos sufren mayor diversidad de conflictos en el proceso de autenticación de usuario para el ingreso al sistema. Según Hacking Ético conocer el ataque es la mejor defensa; en un contexto global, la seguridad se realiza: a nivel de usuario, derechos de acceso (autenticación y control, el usuario sólo debe tener los permisos que le sean concedidos) [1] para así evitar ciberataques por suplantación de identidades al no controlar las sesiones activas e inactivas para salvaguardar los datos y evitar la degradación del sistema por saturación de usuarios y el no aseguramiento de cierre de sesiones después de un determinado tiempo de inactividad.

Al estar el mundo completamente informatizado es de vital importancia proteger los recursos de autorización, según el gobierno de Estados Unidos, se invierten varios billones de dólares para solucionar los incidentes de ciber defensa, los cuales cerca del 40% son de acceso no autorizado. Actualmente el control de acceso a recursos se ejecuta en base a roles y permisos otorgados al usuario, con lo cual no se contaba años atrás. [2] Un mecanismo para dar seguridad al proceso de autentificación es contar con una plataforma centralizada mediante una consola que permita mantener seguro el proceso de inicio de sesión (verificación de contraseñas de autentificación) para iniciar sesiones de trabajo, impidiendo así que puedan quedar abiertas las mismas. La inexistencia de consolas que administren los procesos de inicio de sesión, genera servicios inseguros tanto en aplicaciones web como Android. [3]

Actualmente existen herramientas de desarrollo que permiten gestionar el proceso de autenticación con OpenID Connect es una forma segura, sin embargo, dejan por fuera el uso de una consola la cual permita centralizar de manera segura la autenticación. La herramienta Keyclock es un software de código abierto que nos permite el inicio de sesión único para aplicaciones y servicios modernos, además permite administrar autenticación y acceso a recursos a través de roles, en caso de requerirlos. [4].

La seguridad de los sistemas se basa en identificar primero al usuario (autenticación) para después comprobar si ese usuario tiene acceso al recurso solicitado (autorización).

La autenticación es un proceso que permite determinar la identidad de un usuario del sistema informático (por ejemplo, comparando la contraseña introducida con la contraseña almacenada en la base de datos). La autorización es el proceso de especificar reglas, roles o privilegios de acceso a los recursos del sistema. [3].

El control de acceso basado en roles (de las siglas role based access control), es un paradigma de seguridad basado en la asignación de funciones y autorizaciones. Las funciones y autorizaciones se engloban en los denominados roles de usuario, que determinan el grado de acceso que tienen los usuarios dentro del sistema y las acciones que pueden llevar a cabo dentro del mismo. Keycloak provee un inicio de

sesión único, los usuarios se autentican con Keycloak en lugar de aplicaciones individuales. Esto significa que sus aplicaciones no tienen que lidiar con formularios de inicio de sesión, una vez que han iniciado sesión en Keycloak, los usuarios no tienen que volver a iniciar sesión para acceder a una aplicación diferente. El control de acceso basado en roles tiene como principal objetivo asegurar la confidencialidad, integridad y disponibilidad de la información. [3]

La propuesta del presente se enfoca en construir una plataforma de experimentación que nos permita centralizar la gestión del proceso de autenticaciones de los usuarios a nivel de aplicaciones y servicios, que es una capa adicional al de seguridad en proceso de control de acceso en función del nivel de autenticación de usuarios. La plataforma está conformada por el servidor de autentificación, Keycloack, una aplicación móvil y una aplicación web, diseñadas para gestionar el proceso de autenticación de los usuarios [3], con la plataforma se analizó el nivel de seguridad que brinda el servidor Keyclock al proceso de autentificación. El resultado obtenido, a las pruebas ejecutadas sobre la autentificación realizada a nivel de roles, inicio de sesiones y suplantación de identidad, demuestra que Keyclok es 100% confiable y seguro en el proceso de autentificación.

2. Configuración de la plataforma de experimentación

2.1 Arquitectura de la plataforma

La figura 1 muestra los elementos requeridos en la plataforma de experimentación creada.

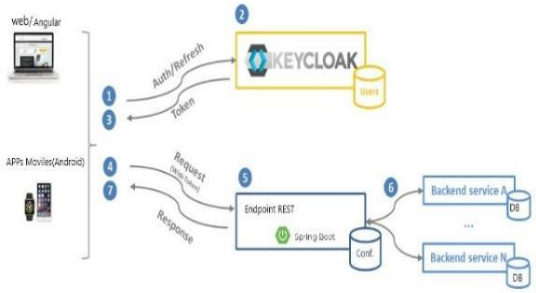


Figura 1. Arquitectura de implementación.

2.2 Elementos de la arquitectura

Los elementos considerados en la arquitectura son:

- **Servidor Keycloak:** Es una solución open source (o código abierto) de autenticación y autorización centralizada entres sus principales características se tiene: Consola de administración para la gestión centralizada de usuarios, roles / usuarios, clientes (aplicaciones); Sincronización de usuarios desde LDAP y Active Directory servers o RDBMS; Social Login, habilita la gestión de login Google, GitHub, Facebook, Twitter y otras soluciones de redes sociales. [3].

- **Spring Boot:** Es un Framework de desarrollo open source (o código abierto) basado en java permite el desarrollo de microservicios ayuda a optimizar los tiempos de desarrollo en la creación y despliegue de aplicaciones informáticas en general, permitiendo a los desarrolladores enfocarse en la lógica del negocio de la aplicación. Se presenta en forma empaquetada, en un JAR, con todas las dependencias para poder ejecutarse sin necesidad de instalar un servidor web, y funciona como una aplicación standalone. [5]

- **Base de datos Postgresql:** Es un sistema de base de datos relacional de alta disponibilidad, capaz de funcionar de manera estable en el servidor,

es consistente y tolerante a fallos. [4] Esto es debido a su capacidad de establecer un entorno de Alta disponibilidad que permite a los clientes puedan realizar consultas de solo lectura mientras que los servidores están en modo de recuperación o espera. Esto permite la ejecución de tareas de mantenimiento o recuperación sin bloquear completamente el sistema.

- **Aplicación Web (Angular):** Para facilitar las pruebas de experimentación de la plataforma implementada, se desarrolló una aplicación web que permite el ingreso de las contraseñas de usuarios y su posterior verificación en las bases de datos de usuarios creada en el Postgresql. Esta aplicación es utilizada por los usuarios en general que mediante la respectivas GUI`s los usuarios realizan el registro de sus datos y el proceso de ingreso de credenciales.Fue desarrollada la parte web en Angular 10 con node. Js16.

- **Aplicación Android:** Es otra aplicación creada para facilitar las pruebas de experimentación de la plataforma implementada, que permite el ingreso de las contraseñas de usuarios y su posterior verificación en la base de datos de usuarios creada en el Postgresql, de igual manera que la aplicación web. [6]

- **Empoint Rest (Api Rest):** Es un mecanismo digital utilizado en las aplicaciones para conectar diferentes instancias del tráfico de información, las computadoras de las empresas u organizaciones, los portátiles o celulares podrían considerarse como Endpoint. [6]

2.3 Configuración de la plataforma

2.3.1. Instalación y configuración de Keycloack.

La instalación del Servidor Keycloak debe ser en modo independiente. Una vez levantado el servidor, se procede a la configuración, para ello se debe crear un usuario de administrador para que dirija a la consola de administración, iniciamos sesión con el usuario Administrador. [2]

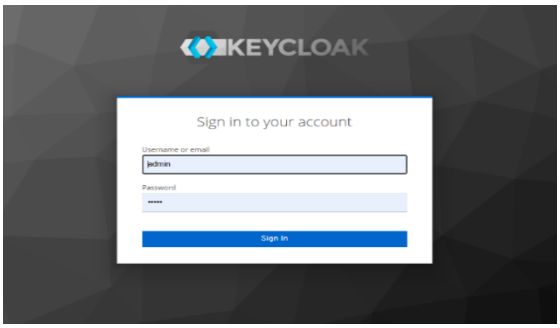


Figura 2. Configuración usuario administración.

A continuación, se describe la configuración de los siguientes servicios en el servidor Keycloack:

- **Reino**: se debe configurar el Reino maestro para administrar el usuario, rol y cliente utilizado por nuestro servicio REST de Spring Boot que posteriormente se lo va utilizar, ver gráfico 3.

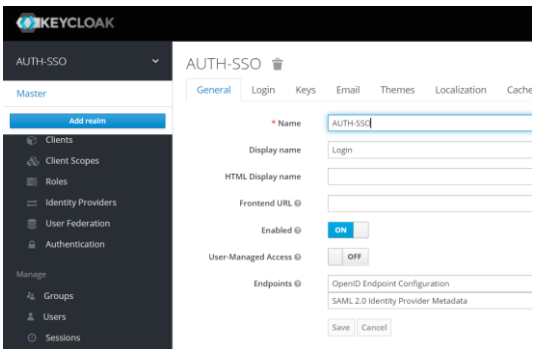


Figura 3. Creación de reino AUTH-SSO

Si es necesario se pueden crear más reinos, ver figura 4, de lo contrario se procede a crear un rol para poder

categorizar al usuario en una aplicación y poner determinadas funciones.

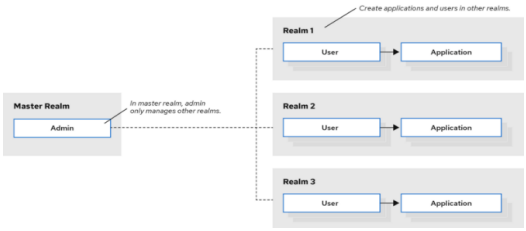


Figura 4. Estructura de creación de reino

- **Roles:** En el panel de configuración de Roles seleccionar la opción Add Role y se desplegara la pantalla para añadir el nuevo rol se procede a crear dos roles, uno como administrador y otro como usuario ver Figura 5.

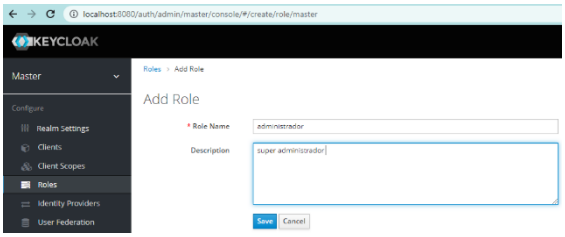


Figura 5. Configuración de roles

- **Creación de clientes.** En el panel de configuración de Keycloack seleccionar la opción Clients, pulsamos el botón Create y se desplegara la pantalla de Add Cliente se, se procede con la creación de dos usuarios uno para la aplicación Web Angular y otro para Apps Android ver Figura 6.

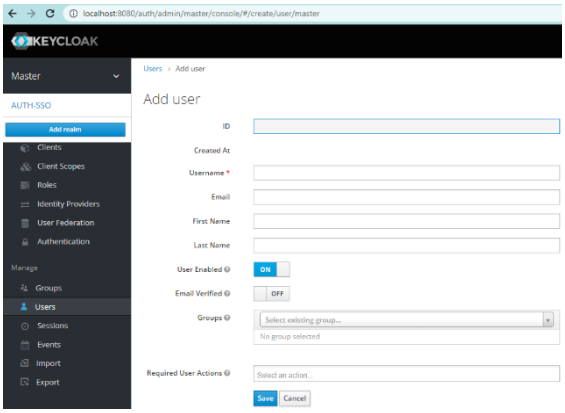


Figura 6. Creación de clientes

- **El token**:

Los clientes de OAuth2 (como las aplicaciones frontales) pueden obtener tokens de acceso del servidor utilizando el punto final de tokens y utilizar estos mismos tokens para acceder a los recursos protegidos por un servidor de recursos (como los servicios back-end). Del mismo modo, los Servicios de Autorización de Keycloak proporcionan extensiones a OAuth2 para permitir que los tokens de acceso sean emitidos en base al procesamiento de todas las políticas asociadas con el/los recurso(s) o el/los ámbitos(s) solicitados. [8]

Los servidores de recursos pueden imponer el acceso a sus recursos protegidos basándose en los permisos concedidos por el servidor y mantenidos por un token de acceso.

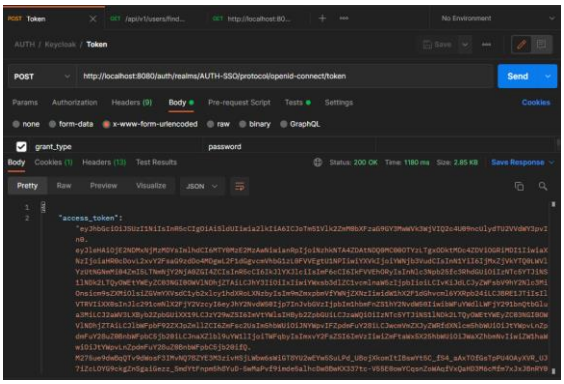


Figura 7. Configuración del token

2.3.2 Aplicación Spring Boot

Permite la comunicación entre el servidor Keycloak y las aplicaciones informáticas tanto web como Android, para ello se debe disponer de los siguientes servicios: [6]

- Una aplicación Spring Boot.

- El módulo web Spring Boot Starter.
- Dependencias de Spring Inicializado.

Estos servicios permiten que, a través de la Postman, se envíen las peticiones, de autentificación, que realiza la aplicación web o Android al Keycloak.

2.3.3 Boot para iniciar la aplicación

Para la inicialización del Boot, se requiere la ejecución de los siguientes pasos:

- Tener restricciones de seguridad para la aplicación.
- Activación del adaptar Keycloak para permitir o denegar las solicitudes de acceso a los recursos de acuerdo con la configuración.

Las restricciones a nivel de servicios que provee el Keycloak, permiten que cada solicitud a URL sea autorizada si el usuario es válido en función del rol de spring-user, previamente configurado.

Se activa el nivel de registro DEBUG que brinda Keycloak a fin de visualizar con mayor detalle en la consola todo el proceso de autenticación de usuarios.

2.3.4 Base de datos PostgreSQL

Todos los datos de usuarios y sus credenciales son registrados en la base de datos Postgres y esta base de datos [8] interactúa con Keycloak, para lo cual es necesario ejecutar los siguientes pasos: crear un usuario administrador en PostgreSQL con el privilegio de user ADMIN.

- Iniciar sesión, con un usuario deon privilegios administrador, en PostgreSQL.
- En Postgresql se otorga privilegios al usuario administrador.
- Se inicia al servicio Keycloak.

En la figura 8 se observa la activación de los servicios de Keycloak.

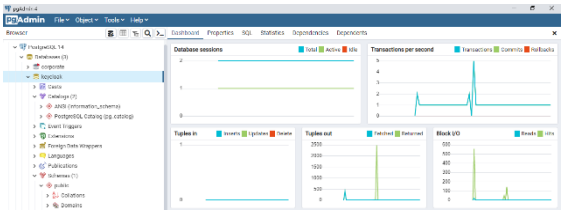


Figura 8. Base de Datos PostgreSQL

3. Pruebas y análisis de resultados

Las pruebas a realizadas en esta sección buscan probar la confiabilidad y robustez de Keycloak, en el proceso de autenticación y autorización de usuarios mediante creación de roles, suplantación de identidades y cierre de sesiones activas.

#	PRUEBA	DETALLE
1	Roles	Validar la autenticación de usuarios con roles no autorizados
2	Roles	Revisar la autenticación de usuarios con roles autorizados
3	Suplantación de identidad	Comprobar la autorización de acceso mediante usuario y clave correcta
4	Suplantación de identidad	Verificar la autenticación de usuarios con cuentas desactivadas e inexistentes.
5	Sesiones	Comprobar el cierre de todas las activas.
6	Sesiones	Controlar el cierre de sesiones después de un tiempo de inactividad.

Tabla 1. Tabla de resumen de pruebas ejecutadas

3.1 Herramientas requeridas:

3.3.1 Servidor Keycloack.

Permite iniciar sesión con el usuario Administrador para poder asignar los roles, visualizar los loguemos de usuarios con las diferentes aplicaciones tanto web como móvil, revisar las sesiones inactivas.

3.3.2 Postman.

Se utiliza el REST API, a través de esta herramienta se solicita un token de autenticación y autorización a nombre del

usuario administrador maestro validando los parámetros: Client_id, username, password.

3.3.3 Aplicación Web (Angular) y móvil.

Aplicaciones desarrolladas, en forma separada, para el proceso de registro de autentificación de usuarios. En este proceso se determina las credenciales de inicio de sesión requeridas para realizar las diferentes pruebas dentro de la aplicación web y de la plataforma de pruebas en general en el desarrollo de la app móvil.

A continuación, se describen los escenarios de pruebas de tres casos considerados en el proceso de autentificación y la evaluación de los resultados obtenidos en cada caso.

3.2 Escenario 1:

Autenticación de usuarios: esta directiva se comprueba que el servidor Keycloak valide que el proceso de autentificación de los usuarios, a través de la aplicación web o Android, de forma exitosa en función del rol asignado, para ello es necesario cumplir los prerrequisitos citados en la tabla 2.

Modulo a Probar: Autenticación de usuarios con roles autorizados y no autorizados.	**Plataforma**: Keycloack Postman
	ID Caso: CS001
Pre Requisitos: 1. Iniciar sesión en Keycloack con un usuario administrador. 2. Tener los usuarios registrados previamente en los diferentes dispositivos.	

Tabla 2. Tabla autenticación de usuarios.

Para la prueba se consideraron 30 intentos de autentificación con usuarios con diferentes roles. En los casos donde el rol no correspondía el Keycloak no permitió el acceso, mientras que en los casos de roles válidos la autentificación fue exitosa. En las figuras 9 y 10 se observa el proceso de autentificación de un usuario cuyo rol no corresponde, solo tiene un rol de USER y no se les autoriza el acceso a los recursos.

Figura 9. Autenticación usuario rol

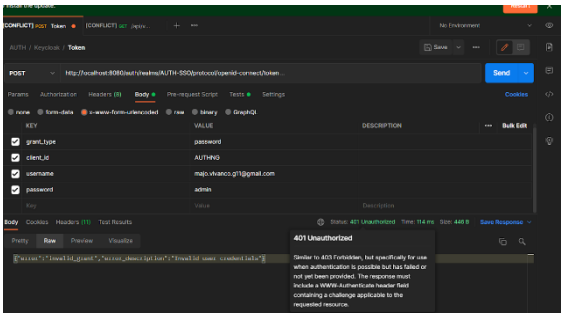


Figura 10. Token de servicio de servicio de acceso denegado.

Se validó la confiabilidad y seguridad mediante la utilización de roles en la autenticación de cada uno de los usuarios previamente registrados.

3.2 Escenario 2:

Suplantación de identidades: En función de autenticación con usuarios y claves incorrectas o cuentas desactivadas e inexistente a través de la aplicación web o Android se comprobará que el servidor Keycloak valide que no exista suplantación de identidades a medida que los usuarios no autorizados puedan acceder a la

aplicaciones o recursos del sistema, para ellos es necesario cumplir con los prerrequisitos citados en la tabla 3.

Modulo a Probar: Suplantación de identidades	**Plataforma**: Keycloack Postman
	ID Caso: CS010
Pre Requisitos: 1. Iniciar sesión en Keycloack con un usuario administrador. 2. Asignar roles, perfiles accesos a un determinado grupo de usuarios.	

Tabla 3. Tabla pre requisitos suplantación de identidades.

Para la prueba se consideraron 40 intentos entre ellos 10 con autenticaciones de usuarios no registrado, 10 con cuentas inactivas, en el caso de los usuarios no registrados. Keycloack no permitió el inicio de sesión, denegando el servicio de autenticación y permitiendo vulnerar el acceso al sistema con usuarios no autorizados, mientras que en los inicios de sesión con usuarios registrados y cuentas activas se consideraron 20 intentos donde la autenticación fue exitosa, permitiendo la autenticación de los usuarios en las diferentes plataformas tanto web como Android. En las figuras 11y 12 se muestra el proceso de denegación de acceso de autenticación.

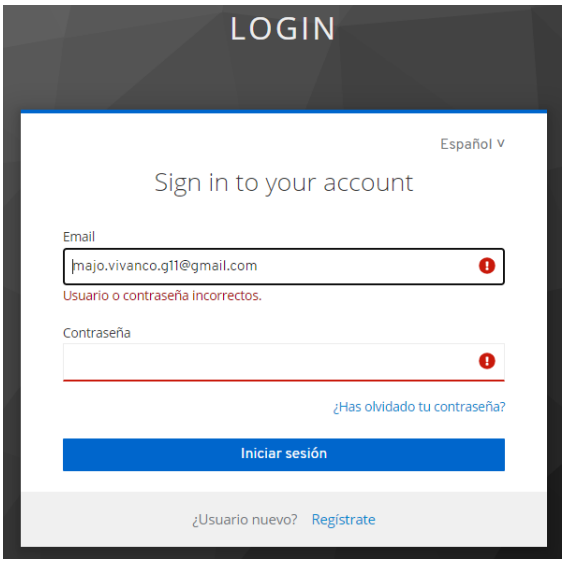


Figura 11. Denegación servicio de autenticación.

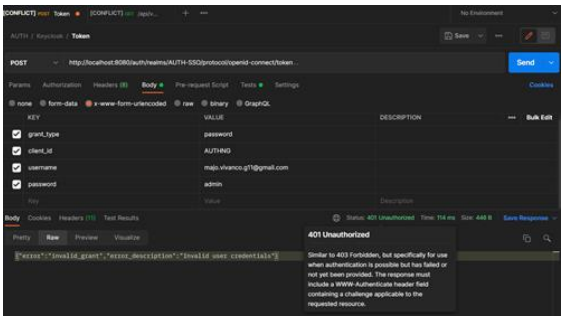


Figura 12. Token de denegación servicio de autenticación.

La seguridad que presenta Keycloack con la generación del token de autenticación es confiable y no se evidencian vulnerabilidades de usuarios no autorizados.

3.3 Escenario 3:

Desconexión de sesiones: En función de mitigar un Ciberataque se comprobará que el servidor de keycloack utiliza un mecanismo de cierre de sesiones activas e inactivas de usuarios con accesos a la aplicación web o Android mediante un Logout all (desconexión de sesiones), de forma exitosa para ello es necesario cumplir los prerrequisitos citados en la tabla 4.

Modulo a Probar: Desconexión de sesiones activas e inactivas.	**Plataforma**: Keycloack, Postman
	ID Caso: CS020
Pre Requisitos: 1. Iniciar sesión en Keycloack con un usuario administrador. 2. Iniciar varias sesiones en el entorno web y Android.	

Tabla 4. Tabla pre requisitos desconexión de sesiones.

Para la prueba se consideraron 30 sesiones para las aplicaciones Web y Apps. Keycloack maneja autenticación centralizada e inicio de sesión único, delegación de autenticación (Google, Facebook, etc.), autogestión de usuarios (recovery de password, desbloqueo de

cuentas). Para la integración front-end AngularJS Keycloack proporciona un adaptador javascript que permite la comunicación entre el front-end y el servidor Keycloack, este adaptador comprueba si el usuario está autenticado y tiene autorización a los recursos del sistema.

En las figuras 13 y 14 se muestra el proceso de configuración y desconexión de las sesiones activas e inactivas.

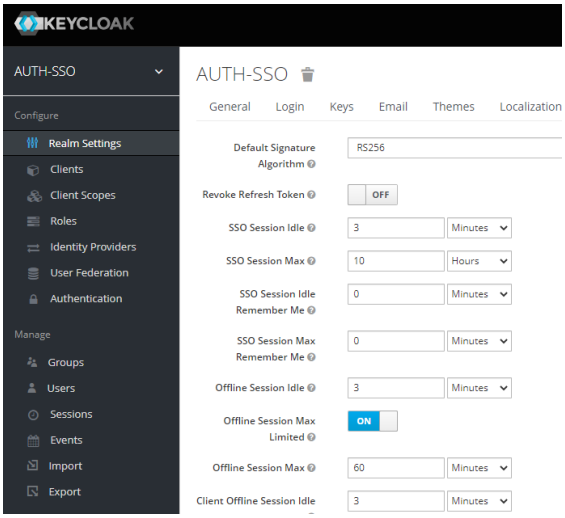


Figura 13. Configuración desconexión de sesiones

Figura 14. Cierre de sesiones activas e inactivas

Mediante la desconexión de sesiones activas e inactivas en Keycloack es eficiente y confiable con lo cual podemos salvaguardar nuestros datos de Ciberataque o degradaciones del sistema por saturación de usuarios activos.

4. Evaluación y Análisis de resultados

La autenticación de usuarios la aplicación utiliza la emisión de Tokens lo que permite inyectar y configurar restricciones de seguridad en las aplicaciones.

Para la autenticación de usuarios se utilizó el método ID de cliente y secreto, descrito en la especificación OAuth2. El cliente tiene un secreto, que debe ser conocido tanto por el adaptador (aplicación) como por el servidor Keycloak. [3]

El método HttpServletRequest.logout(), ejecuta una llamada contra el servidor de Keycloack y se emite un token de actualización de cierre de sesiones.

Por estas razones se recomienda utilizar los métodos de autenticación de usuarios y cierre de sesiones para proteger los recursos de las aplicaciones de modo que siempre se mantenga una interacción con el servidor Keycloak actualizando y generando nuevos tokens.

El la figura 15 se muestra las diferentes pruebas realizadas para: Autenticación de usuarios con roles autorizados y no autorizados, suplantación de identidades y desconexión de sesiones, evidenciando pruebas satisfactorias en los escenarios analizados, donde se realizó la suma de todos los datos (1) referente a intentos fallidos y no fallidos en cada uno del proceso de autentificación considerados:

$$\sum_{1}^{n} = 1\, x_i \qquad (1)$$

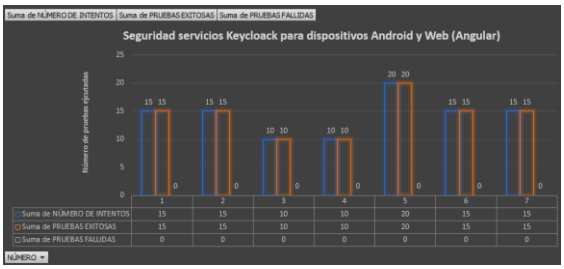


Figura 15. Evaluación pruebas Keycloak

La seguridad es un aspecto importante para las aplicaciones Web y Apps Keycloak es uno de los servidores IDAM (Identity and Access Management) de código abierto más prometedores en vista que se puede implementar y adaptar fácilmente ya que permite resolver el inicio de sesión único

para aplicaciones web y servicios web basados en REST. El objetivo principal de keycloakes hacer que la seguridad se lo suficientemente simple proporcionando funciones de seguridad listas para usar y se puede personalizar fácilmente según las necesidades de las distintas organizaciones.

Para la autenticación de usuarios con roles autorizados y no autorizados Keycloack no permitió los accesos a usuarios sin la asignación de un rol especifico.

Keycloack no admitió el acceso al sistema a usuarios desconocidos ya que el control de autenticación y autorización de inicios de sesión se realiza a través de tokens protegiendo los datos mediante mecanismos robustos y así evita la suplantación de identidades, identificando con mayor seguridad que usuarios están autorizados para acceder a los recursos de la aplicación.

Para la desconexión de sesiones activas e inactivas, Keicloack en todos los casos de pruebas bloquea los inicios de sesión salvaguardando los datos de Ciberataque o degradaciones del sistema por saturación de usuarios activos.

5. Conclusiones

Luego de haber efectuado los diferentes escenarios de pruebas el nivel de seguridad de los servicios de Keycloack referente a autenticación de usuarios con roles autorizados y no autorizados; suplantación de identidades; desconexión de sesiones activas e inactivas; para dispositivos Android y Web (Angular) los tokens se generan apropiadamente en el sentido de tiempo de respuesta y autenticación hacia los recursos del sistema.

Es de transcendental importancia proteger los recursos de autorización y acceso a datos para poder determinar dicha seguridad se levantó una plataforma de experimentación con Keycloack y se desarrolló un apis (REST) que utiliza el servidor de autenticaciones Keycloak, a fin de integrar con tecnologías externas como es apps móviles y web para ratificar lo expuesto se demuestra en base a pruebas la confiabilidad y robustez que brinda la herramienta al no permitir el acceso a la aplicación a usuarios no autorizados.

La implementación de este tipo de herramientas que permite la administración de autenticación de acceso a recursos a través de roles, token permite al usuario final tener una mayor confianza al acceder a los datos de las diferentes aplicaciones.

6. Referencias

[1] ACISSI, «Seguridad Informática,» de *Hacking Ético Conocer el ataque para una mejor defensa*, Barcelona, ENI, 2015, pp. 27-30.

[2] M. Goldsmith, «Cybersecurity Incident & Important Consumer Information,» 217. [En línea]. Available: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

[3] Keycloak, «Documentation Guides Keycloak,» 2021. [En línea]. Available: https://www.keycloak.org/documentation.

[4] D. P. D. Paiva, «Reauthentication modules for Keycloak authentication server,» nº 2, p. 6, 2021.

[5] M. Stamp, Information Security Principles and Practice, Texas: Wiley, 2022.

[6] ANDROID STUDIO, «Guía de Usuario Android Studio,» Android Developers, 19 06 2020. [En línea]. Available: https://developer.android.com/studio/debug?hl=es. [Último acceso: 12 01 2022].

[7] Spring Boot, «Learn Spring,» Spring, 15 03 2020. [En línea]. Available: https://spring.io/projects/spring-boot. [Último acceso: 20 01 2022].

[8] K. documentation, «Authorization Services Guide,» [En línea]. Available: https://www.keycloak.org/docs/latest/authorization_services/.

[9] postgresql, «Documentation postgresql,» [En línea]. Available: https://www.postgresql.org/docs/.