Research report  
Keycloak

**­­­­­­­­­­­**

**Afbeelding met schermopname, Graphics, Lettertype, logo

Automatisch gegenereerde beschrijving**

Student name: Rowan van der Weel.

Student number: 4924576

Class: DB-04

Teacher: Tim Kurvers

Version: 1.0

Date: 21-09-2023

Table of contents

[**Introduction** 3](#_Toc150523526)

[Problem description 3](#_Toc150523527)

[Main question 3](#_Toc150523528)

[Sub questions 3](#_Toc150523529)

[**Results** 4](#_Toc150523530)

[Sub question 1 4](#_Toc150523531)

[Sub question 2 4](#_Toc150523532)

[Sub question 3 4](#_Toc150523533)

[Sub question 4 4](#_Toc150523534)

[**Resolution** 5](#_Toc150523535)

[Conclusion 5](#_Toc150523536)

[Recommendation 5](#_Toc150523537)

[**References** 6](#_Toc150523538)

[**Version History** 7](#_Toc150523539)

# **Introduction**

## Problem description

In today's digital world, keeping online information secure is crucial. Businesses and organizations need effective tools to manage who can access their apps and data, ensuring only the right people get in while keeping everything safe. This challenge calls for Identity and Access Management (IAM) solutions.

Keycloak, an open-source IAM tool, steps in to help solve these challenges. The problem we are tackling is how to manage user identities, control who can access what, and make sure everything stays secure in modern apps. Without a good IAM system, there is a risk of security issues, not meeting compliance standards, and a lack of control over who gets to use what.

The main purpose of this research report is to understand its features and how well it can manage identity and access management. My goal is to implement in my personal project: “GamifyWork” and to determine for which project(s) it could be suitable.

## Main question

How can Keycloak be integrated into 'GamifyWork' for efficient identity and access management?

## Sub questions

1. What is IAM and how does Keycloak play a part in it?
   1. **Literature study:** Searching for academic papers, articles, and blog posts that discuss about Keycloak and other IAM’s.
   2. **Expert interview:** Conduct interviews with an expert in the field of Identity and   
      Access Management (IAM) and Keycloak.
2. How does Keycloak address specific OWASP security risks?
   1. **Document analysis:** Reviewing the official documentation for Keycloak. Look for sections or documents that explicitly outline the security measures.
   2. **SWOT analysis:** Conduct a SWOT analysis for Keycloak. Identify the Strengths, Weaknesses, Opportunities, and Threats associated with the IAM tool.
3. How easily can Keycloak integrate with the specific features of GamifyWork.
   1. **Community research:** Engage with online communities, forums, and social media groups dedicated to each of these frameworks. Observe discussions, queries, and the level of activity within these communities. Take note of the number of members, frequency of posts, and responsiveness to inquiries.
   2. **Observation:** Observe and analyse real-world applications or projects built using Keycloak. Pay attention to how developers have customized it to meet specific requirements.
4. To what extent does Keycloak allow for customization of the user interface, and how can this be delivered to align with the branding of "GamifyWork"?
   1. **Prototyping:** Develop a demonstration prototype displaying the potential customization capabilities of Keycloak's user interface in alignment with the branding of "GamifyWork."
   2. **Usability testing:** Gather feedback on the prototype through usability testing sessions with stakeholders and potential users.

# **Results**

## Sub question 1

**What are identity access management systems?**Identity and access management (IAM) is a system that helps businesses manage digital identities. It allows IT managers to control user access to essential information. IAM includes tools like single sign-on and two-factor authentication for secure access. Additionally, it ensures that only necessary and relevant data is shared, promoting data security (Rosencrance & Gittlen, 2021).

IAM offers diverse key benefits.

1. Enhanced Data Security: IAM strengthens cybersecurity by efficiently managing privileged access. It provides robust control over user access, reducing the risk of data breaches, identity theft, and unauthorized access to sensitive corporate information across various devices.
2. Facilitates Compliance: Integrating IAM into business operations aids in meeting regulatory requirements, including authentication methods, user access reviews, and resource location access.
3. Minimizes Human Errors: IAM tools automate access management, eliminating manual errors associated with privilege settings. This not only frees up the IT team from tedious tasks but also reduces the chances of human error, streamlining operations and cutting costs.
4. Ensures Data Confidentiality: IAM tools provide a secure way to grant access, maintaining confidentiality by restricting access to specific individuals or groups while safeguarding sensitive information.
5. Streamlines IT Workloads: IAM enables simultaneous updates of access privileges across the organization, reducing the number of IT tickets for password resets. This streamlines IT workflows and enhances efficiency. (Why Is Identity and Access Management Important?, sd)



**What is Keycloak?**

Keycloak, an open source "Identity and Access Management" tool under Apache License 2.0, serves as the upstream project for Red Hat SSO. Supporting multiple platforms based on chosen protocols, it was released in September 2014 and is actively developed by the Red Hat team, welcoming contributions. (Żyliński, 2021).

Additional feature highlights of Keycloak are:

* Single sign-on (SSO) support
* User federation (i.e., support for external identity providers)
* Support for popular protocols like OAuth2 and OpenID Connect
* Multifactor authentication (MFA)
* Fine-grained access control (Hmza, 2023).

## Sub question 2

**OWASP**

The Open Web Application Security Project (OWASP) is a non-profit organization founded in 2001, with the goal of helping website owners and security experts protect web applications from cyber-attacks. OWASP has 32,000 volunteers around the world who perform security assessments and research (OWASP, sd).

I will research the [top 10](https://owasp.org/API-Security/editions/2023/en/0x11-t10/) security risks for Keycloak.

[**Broken Object Level Authorization**](https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/)

In Keycloak, handling Object Level Access Control (OLAC) involves setting up authorization policies and permissions based on object identifiers. Keycloak provides a flexible and customizable approach to implement object-level authorization checks. [Here's](https://www.youtube.com/watch?v=kBBf9k8RtrE) a general guide on how Keycloak manages Object Level Access Control.

[**Broken Authentication**](https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authentication/)

Keycloak addresses Broken Authentication risks through diverse measurements. It supports secure authentication protocols like OAuth 2.0 and OpenID Connect. Multi-Factor Authentication adds an extra layer of security. Brute force protection is built-in, temporarily locking user accounts after multiple failed login attempts. Keycloak's session management controls session duration and idle timeouts to prevent unauthorized access. Administrators can enforce strong password policies, including length, complexity, and expiration. User self-service features enable password resets and profile updates. Identity federation integrates with external providers for enhanced security. (Server Administration Guide, 2022)

**Documentation**

According to the official [documentation](https://access.redhat.com/documentation/en-us/red_hat_build_of_keycloak/22.0/html/server_administration_guide/mitigating_security_threats#doc-wrapper) of Keycloak, these are the points:

## Sub question 3

## Sub question 4

# **Resolution**

## Conclusion

## Recommendation

# **References**

# **Version History**

|  |  |
| --- | --- |
| **When?** | **What?** |
| 10/11/2023 | First start, initialized it. |
| 30/11/2023 | Main- and sub questions with the specific methods. |