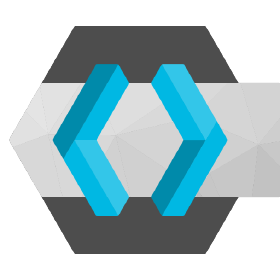
|  |
| --- |
| KeyCloak |
| Billy Hofland  DB03  2023/2024 |



Research Report

Research Report



Table of contents

[Introduction 3](#_Toc153475221)

[Problem description 3](#_Toc153475222)

[Main question: 3](#_Toc153475223)

[Sub-questions: 3](#_Toc153475224)

[Results 5](#_Toc153475225)

[Sub-question 1: 5](#_Toc153475226)

[Sub-question 2: 6](#_Toc153475227)

[Sub-question 3: 6](#_Toc153475228)

[Sub-question 4: 7](#_Toc153475229)

[Resolution 9](#_Toc153475230)

[References 10](#_Toc153475231)

[Version history 11](#_Toc153475232)

# Introduction

## Problem description

Users need to create and remember different credentials for each service associated with TeamVas, my online education platform. Because my application offers different services with multiple accounts this leads to a rather annoying experience and often results in forgotten passwords or the usage of overly simplistic, insecure passwords. Furthermore, without a centralized system, it’s difficult to track user activities and preferences across different services.

## Main question:

Which IAM best aligns with the specific needs, user management, and the demand for a centralized system in an online education platform?

## ­Sub-questions:

1. How does KeyCloak function inside of IAM?
2. Literature study: By looking at the documentation, information about strengths and weaknesses can be found of the most popular IAM systems.
3. How can KeyCloak be integrated with the specific needs and features of an online education platform?
4. Community Research: By searching for various forums and user created posts, The most active community can be found for all the popular IAMs.
5. Observation: By looking at what other people are using and how they are customizing their IAM, and whether this could be a good fit for an online education platform.

1. What are strengths and weaknesses for the 3 most popular IAM Systems?
2. Which OWASP risks are covered by KeyCloak and which do still exist after implementing KeyCloak?
3. Document analysis: By reviewing the official documentation of KeyCloak, I can determine what risks are covered by KeyCloak.
4. SWOT analysis: By conducting a SWOT analysis for KeyCloak, identify the strengths, weakness, opportunities, and threats.

# Results

## Sub-question 1:

**How does KeyCloak function inside of IAM?**

IAM stands for Identity and access management, it is used to control critical information about user access within the organization. Systems used for IAM include but are not limited to single sign-on systems and two-factor authentication. Single Sign-On (SSO) allows users to access multiple applications and services with a single set of credentials. This reduces the number of attack surfaces as there is fewer passwords for potential breach. IAM systems can also be useful for the ability to securely store identity and profile data. (Gittlen, 2021)

KeyCloak is an open-source tool for IAM, it supports Single Sign-On as well as support for different protocols such as OAuth. The system can be distributed in 3 ways including Docker. The importance of KeyCloak is automating the process of authentication in addition to being logged in on several applications and resources of the network. This would be beneficial for an online education platform since it is based on multiple functionalities that require a user to be logged in before using them. (Żyliński, 2021)

The extra security that KeyCloak offers is MFA (multi-factor authentication) also referred to as two-factor authentication, it gives extra security to the sign-in process by requiring the user to provide an additional form of identification. This could something like a PIN or passcode, generated by an external device. MFA is very important in an application since it reduces the security login risks by a lot. (Kinzer, 2021)

## Sub-question 2:

**How can KeyCloak be integrated with the specific needs and features of an online education platform?**

A screenshot of a computer

Description automatically generated

*Source 1: Reddit survey about using identity providers* [*https://www.reddit.com/r/devops/comments/16tmdat/does\_anyone\_here\_use\_keycloak\_as\_their\_main\_idp/*](https://www.reddit.com/r/devops/comments/16tmdat/does_anyone_here_use_keycloak_as_their_main_idp/)

In this reddit survey KeyCloak was voted as most popular IDP, the reactions under this survey provided a good oversight of why KeyCloak can fit the specific needs and features of an online education platform. From looking at the comments I’ve found that KeyCloak has an excellent SLA, this stands for service level agreements and is a promise from the supplier of how much the uptime is for a service. For KeyCloak this is 99,9%+, this is rather useful for an online education platform since downtime could have negative effect on the learning path of a student.

Ngybhoo9

## Sub-question 3:

## Sub-question 4:

**What is OWASP?**

OWASP is an international organization that focuses on web application security. The OWASP top 10 are the most critical risks involved in web development. These are updated in real time and include but are not limited to Injection, broken authentication, and sensitive data exposure. OWASP also provides recourses, tools, and best practices to assist in mitigating these risks. This includes guidelines for secure coding and official documentation further explanations.

**What are the top 3 OWASP risks (2023) that KeyCloak covers?**

The far most popular OWASP risk is broken object level authorization, this occurs to APIs who do not verify whether clients should have access to the data they are requesting. KeyCloak combats broken object level authorization by having role-based access control, this assigns roles to users and grants permission to these users.

The second most popular OWASP risk is broken authentication, this risk results in attackers gaining access to compromised passwords, keys, or session tokens. KeyCloak prevents this using multi-factor authentication as well as including protocols such as OpenID Connect and SAML 2.0, which allow for securely authenticated users and services.

The third most popular OWASP risk is broken object property level authorization, this differs from the most popular risk because this OWASP goes deeper, specifically to the properties of an object. An attacker attempts to find breaches inside of the properties of an object, changing information about a user for example or try to find undocumented API endpoints that relate to an object’s properties. KeyCloak makes sure API endpoints are secured and can only be reached by authorized users.

**SWOT analysis**

**Strengths:**

KeyCloak provides features for access management, including Single Sign-On and Multi factor authentication. More however it can provide a customizable user interface, which could be applied to an online education platform.

**Weaknesses:**

KeyCloak’s deployment and setup process can be difficult, especially if you do not wish to use Docker. KeyCloak can be resource-intensive, requiring significant server resources for optimal performance. This might be challenging with limited IT infrastructure.

**Opportunities:**

Because of increasing awareness around data security and privacy, IAM solutions like KeyCloak are on the rise. This trend presents an opportunity for KeyCloak to expand its user base.

**Threats:**

The fast pace of technological development in the cybersecurity and IAM fields means that KeyCloak needs to continually evolve to stay relevant. Another huge thread would be vulnerabilities within KeyCloak. Any significant security breach could damage KeyCloak’s reputation and user trust.

|  |  |  |
| --- | --- | --- |
| KeyCloak | Positive | Negative |
| Intern | KeyCloak provides features for access management. | KeyCloak’s deployment and setup process can be difficult. |
| Extern | IAM solutions like KeyCloak are on the rise. | The fast development in IAM systems requires KeyCloak to stay updated |

# Resolution

# References

Gittlen, S. (2021, August). *What is identy and access management*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

Kinzer, K. (2021, Septembre 14). *The intersection of IAM and MFA*. Retrieved from Jumpcloud: https://jumpcloud.com/blog/the-intersection-of-identity-and-access-management-iam-and-multi-factor-authentication-mfa

Matias, M. (2022, 07 14). *Avoid XSS Attacks in Vue*. Retrieved from dev-academy: https://dev-academy.com/vue-xss/

Srivastava, V. (2023, 04 01 ). *How to Secure Your Angular App*. Retrieved from Telerik: https://www.telerik.com/blogs/how-to-secure-your-angular-app#:~:text=Angular%20uses%20several%20security%20features,be%20loaded%20into%20a%20webpage.

Thinkster. (2023, 10 26). *Realworld*. Retrieved from Github: https://github.com/gothinkster/realworld

Vindula, O. (2023, 06 6). *Mitigating XSS attackos in React applications*. Retrieved from medium: https://medium.com/@omalwijegunawardana/mitigating-xss-attacks-in-react-applications-194c46472379

Żyliński, B. (2021, Octobre 11). *What Keycloak Is and What It Does*. Retrieved from DZone: https://dzone.com/articles/what-is-keycloak-and-when-it-may-help-you

# Version history

|  |  |
| --- | --- |
| **When?** | **What?** |
| 30/11/2023 | Initial setup of Main/Sub questions, problem description |
| 5/12/2023 | Sub question 1 finished, research on OWASP |
| 13/12/2023 | Start on sub question 4, Keycloak and OWASP |