FLUKE®

OneQA Security Document

OneQA Security Document

Table of Contents

OneQA Security Document

1. Purpose and Benefits

The purpose of this document is to provide a clear and comprehensive overview of the security measures and practices implemented in OneQA. It serves as a guide to understanding the strategies and techniques used to ensure the application's and its data's security. By detailing these measures, the document helps in raising security awareness among stakeholders, demonstrating compliance with industry standards, managing risks effectively, building trust and transparency, and preparing for security incidents. It also supports continuous improvement and operational efficiency by serving as a vital reference for security teams, developers, and stakeholders.

2. Security Features in OneQA

2.1 Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) in OneQA ensures that access to data is managed efficiently through different roles such as Author, User, and Admin. Each role has specific permissions tailored to their functions: Authors can create and modify content, Users can view and interact with the content, and Admins have full control over the system, including managing other users' access. This structured approach ensures that users only have access to the data necessary for their roles, following the principle of least privilege. RBAC enhances security by limiting exposure to sensitive data and maintaining strict control over who can perform specific actions within the application.

2.2 Data Encryption

Our application, hosted on the AWS cloud, employs robust data encryption measures to protect information both in transit and at rest. This ensures that all sensitive data is encrypted using industry-standard protocols, safeguarding it from unauthorized access and breaches. By leveraging AWS’s advanced encryption capabilities, we maintain the highest levels of data security and integrity, giving our users peace of mind.

2.3 Secure User Authentication

We employ a robust password-based authentication system with a stringent password policy to ensure the security of user accounts. The registration process involves generating a one-time token sent to the registered email address, enhancing the verification process. Users must create passwords that meet strict complexity requirements, including a minimum length and a mix of character types. Password reset procedures are also secured through email, ensuring that only authorized users can change their credentials. This combination of strong password policies and secure email verification helps protect against unauthorized access and potential breaches.

2.4 Audit Logging

In the OneQA application, we leverage Amazon CloudWatch Logs to track all API calls. This allows us to maintain comprehensive and detailed logs of user activities and system interactions. By utilizing CloudWatch, we ensure that every API call is recorded and monitored, providing a robust mechanism for auditing and security analysis. This helps in identifying potential security incidents, troubleshooting issues, and ensuring compliance with regulatory requirements. The logging data is securely stored and can be easily accessed for real-time monitoring and historical analysis, enhancing the overall security and operational efficiency of the application.

3. Regular Security Updates

We prioritize the security of our application by implementing regular security updates. We utilize tools like Veracode, Sonar scanner and SBOM for continuous scanning of application vulnerabilities. Any identified issues are promptly addressed within a 60-day window. Additionally, our rigorous penetration testing helps identify potential security risks before they become problems. Regular server patch updates are also performed to ensure that our infrastructure remains secure and up to date, providing a robust defence against emerging threats.

4. Penetration Testing

We regularly conduct thorough penetration testing to identify and address potential se curity weaknesses within our application. This proactive approach involves simulating c yberattacks to uncover vulnerabilities before malicious actors can exploit them. The in sights gained from these tests allow us to strengthen our defenses and ensure the resil ience of our security measures. By continually assessing and improving our security po sture, we mitigate risks and safeguard our application against emerging threats. Regula r penetration testing is a critical component of our commitment to maintaining robust security standards and protecting user data.

5. Incident Response Plan

We have a well-defined Incident Response Plan to address security incidents promptly and effectively. Users can reach out to our customer support via [oneqasupport@flukebiomedical.com] for assistance. Our internal response plan is designed to swiftly identify, assess, and mitigate security incidents, ensuring minimal impact on our systems and users. By having a structured and efficient incident response strategy, we enhance our ability to protect against and recover from security threats, maintaining the integrity and availability of our application.

6. Secure Coding Practices

Our secure coding practices are essential in maintaining the integrity and security of our applications. These practices involve adhering to established guidelines and

standards that prevent vulnerabilities and ensure robust code quality. We prioritize input validation to avoid common vulnerabilities such as SQL injection and cross-site scripting. Output encoding is utilized to protect against attacks by ensuring that user-generated content is displayed safely. Strong authentication and password management policies are enforced to secure user accounts. Regular code reviews, security testing, and automated tools like Sonar scanner, Veracode help in identifying and fixing security issues promptly.

By following these practices, we ensure that our code remains secure and resilient against potential threats.

7. Threat Modeling

At OneQA, we practice threat modelling to enhance the security of our product. Threat modelling involves identifying, analysing, and mitigating potential security threats to the application early in the development lifecycle. By systematically evaluating possible attack vectors, we can anticipate and address vulnerabilities before they become issues.

Benefits:

Proactive Security: Identifying threats early allows us to implement security measures before potential exploits can be realized, making the product more robust.

Cost-Efficiency: Addressing security issues during the design phase is far more cost-effective than fixing them post-deployment.

Improved Design: Helps in creating a more secure architecture by understanding and mitigating risks upfront.

Enhanced Compliance: Ensures that our product meets industry security standards and regulatory requirements, which is critical for user trust and legal compliance.

Comprehensive Coverage: Ensures all possible threats are considered, leading to a well-rounded security strategy.

Through threat modelling, OneQA can maintain a high-security standard, reducing risks and ensuring the safety of user data and application integrity.

8. Code Signing in OneQA

OneQA ensures the integrity and authenticity of its executable files through the practic e of code signing. Code signing involves digitally signing the executable files to verify th eir source and confirm that they have not been tampered with. This process provides a ssurance to users that the software is legitimate and has not been altered by malicious actors. By implementing code signing, OneQA enhances the security of its software dis tribution, protecting against threats such as malware injection and unauthorized modif

ications. This commitment to code integrity reinforces user trust and upholds the high est security standards.

9. Training and Awareness

   Our team is regularly provided with comprehensive training on security best practices and protocols. This training ensures that all members are aware of the latest security threats and how to mitigate them. By fostering a culture of security awareness, we empower our team to identify and respond to potential risks effectively. Regular workshops, updates on emerging threats, and practical training sessions help in maintaining a high level of security awareness across the organization, contributing to the overall security posture of our application.

10. Server Location

    All the infrastructure for OneQA is hosted in the AWS Frankfurt region. This choice of location ensures high availability, reliability, and compliance with European data protection regulations. By leveraging AWS's robust security measures and infrastructure, we provide a secure and efficient environment for our application, ensuring optimal performance and data protection.