Security Compliance Document

OpenVidStreamer

by Radoslav Radev

Advanced Software Engineering Semester 6

23/04/2024

ver. 1

Introduction

- **Purpose**: This document outlines the security measures and compliance status of OpenVidStreamer regarding the OWASP Top 10 security risks and CIA requirements.
- **Scope**: Covers all aspects of the platform, from frontend interactions to backend processes and data handling.

Compliance and Prevention of OWASP Top 10

We will look into OWASP top 10 vulnerabilities and how vulnerable OpenVidStramer is, what kind of mitigations are in place.

- **Injection**
  - *Entity Framework for ORM*: Utilizes parameterized queries, inherently protecting against SQL Injection attacks.
- **Broken Authentication**
  - *Token-Based Authentication*: Ensures secure handling of user sessions and authentication processes.
- **Sensitive Data Exposure**
  - *Use of TLS*: Secures data in transit, preventing interception by unauthorized parties. - NOT IMPLEMENTED
    - This is not implemented due to proeject`s budget, and the cost of purchasing an SSL certificate
  - *Data Handling Practices*: No sensitive data (e.g., financial information) is stored on the system; all payment processing is managed via Stripe.
- **Security Misconfiguration**
  - Regular updates and security patches are applied to ensure that the system is not vulnerable to attacks due to misconfiguration.
- **Cross-Site Scripting (XSS)**:

    - React's rendering engine inherently protects against XSS by escaping strings automatically.

- **Insecure Deserialization**:
    - Not applicable as our system does not involve deserialization of data from untrusted sources.

- **Using Components with Known Vulnerabilities**:
    - Continuous monitoring and updating of all components to ensure there are no known vulnerabilities, Quodana is integrated into the CI pipeline and will notify if vulnerable packages are used

- **Insufficient Logging and Monitoring**:
    - Comprehensive logging and monitoring systems are in place to detect and respond to potential security threats promptly.

CIA Analysis

Availability

The availability of the system components and data processed is crucial for a video streaming service like OpenVidStreamer, which aims to handle significant user traffic and provide continuous service.

- **Frontend (User Interface)**: Essential (3)
    - The UI must be always available to ensure users can access and interact with the platform anytime.
- **Backend Services (APIs, Microservices)**: Required (2)
    - Backend services must be highly available to manage user requests, video streaming, and data transactions without interruptions, but can tolerate brief, planned downtimes if needed.
- **Database Systems**: Essential (3)
    - High availability is necessary to ensure all user data and video metadata are consistently accessible for operations.
- **Payment Processing (via Stripe)**: Important (1)
    - We can tolerate brief downtime since the payment of the subscription occurs only once per month for user, and the user will be notified and have 1week to pay his subscription before his platform access is disabled.

Integrity

The integrity of data in a video streaming platform ensures that data is accurate, consistent, and reliable.

- **User Data (Email Addresses)**: High (2)
    - User emails must be accurately recorded and maintained to ensure communications and account management are correctly handled.
- **Video Content and Metadata**: High (2)
    - Integrity of video content and associated metadata is critical to ensure that the content delivered to the user matches what was uploaded by content creators.
- **Transaction Data**: Absolute (3)
    - Integrity for all transaction data processed through Stripe must be absolute to prevent fraud and ensure accurate billing and subscription management.

Confidentiality

Confidentiality protects sensitive information from unauthorized access or disclosure.

- **User Data (Email Addresses)**: Confidential (2)

    - User emails are considered sensitive and should be protected to prevent unauthorized access and potential privacy violations.
- **Video Content and Metadata**: Company Confidential (1)
    - While video content is intended for public consumption, unpublished or private videos require protection until they are officially released or remain private based on user settings.
- **Transaction Data**: Confidential (2)
    - Financial transactions, even though handled by Stripe, need a high degree of confidentiality regarding the platform's handling of any transaction records or logs.

Privacy

Privacy considerations specifically focus on personally identifiable information (PII).

- **User Data (Email Addresses)**: PII (p)
    - Email addresses are classified as personally identifiable information and must be protected accordingly to prevent misuse or unauthorized sharing.

Data Security

- **User Data Handling**
    - *Minimal Data Retention*: The platform stores only the minimal amount of data required for operation, specifically user emails. No other personally identifiable information or sensitive data is held.
- **Third-Party Integration**
    - *Stripe for Payment Processing*: https://stripe.com/docs/security/stripe

Security Practices and Protocols

- **Regular Audits**: Security audits will be conducted to ensure ongoing compliance and identify potential vulnerabilities.
- **Development and Maintenance Practices**: The Agile development methodology is employed, allowing for iterative and continuous improvement of security practices and rapid response to potential threats.

Security Risk	Mitigation	Implemented
Injection	Utilizes parameterized queries via Entity Framework for ORM	Yes
Broken Authentication	Token-Based Authentication	Yes
Sensitive Data Exposure	Use of TLS	No
	Data Handling Practices (using Stripe)	Yes
Security Misconfiguration	Regular updates and security patches	Yes
Cross-Site Scripting (XSS)	React's rendering engine escapes strings automatically	Yes
Insecure Deserialization	Not applicable	N/A
Using Components with Known Vulnerabilities	Continuous monitoring and updating via Quodana integrated into CI pipeline	Yes

Insufficient Logging and Monitoring	Comprehensive logging and monitoring systems	Yes

Application Should Implement	**Implemented**
Ensure the frontend user interface is highly available.	Yes
Maintain high availability of backend services.	Yes
Ensure high availability of database systems.	Yes
Maintain reliability in payment processing through Stripe with user notifications for downtime.	Yes
Accurately record and maintain user email addresses.	Yes
Ensure the integrity of video content and metadata.	Yes
Maintain absolute integrity of transaction data processed through Stripe.	Yes
Protect user email addresses from unauthorized access.	Yes

Safeguard unpublished or private video content.	Yes
Ensure confidentiality in handling transaction records or logs from Stripe.	Yes

Conclusion

This document confirms the proactive measures taken by the OpenVidStreamer platform to ensure robust security and compliance with international standards. Our commitment to maintaining high security and compliance standards protects both our users and their data.

Glossary

- **OWASP**: Open Web Application Security Project
- **CIA**: Confidentiality, Integrity, and Availability
- **PCI DSS**: Payment Card Industry Data Security Standard
- **ORM**: Object-Relational Mapping

References

- OWASP Top 10 - https://owasp.org/www-project-top-ten/
- Stripe Security - https://stripe.com/docs/security/stripe