OWASP REPORT

“Cinema_Now”

Andreea Șindrilaru
Fontys University of Applied Sciences
S3-CB-01

Table of Contents

	Likelihood	Impact	Risk	Actions	Planned
A01:2021-Broken Access Control	Likely	Severe	High	Implement access control to minimize CORS usage.	N/A
A02:2021-Cryptographic Failures	Low	Low	Low	Using UUIDs.	fixed
A03:2021-Injection	Likely	Moderate	Low	JPA provides input sanitization	N/A
A04:2021-Insecure Design	Low	Moderate	Low	Write unit and integration tests to validate all critical flows.	Unit tests, Integration tests
A05:2021-Security Misconfiguration	Very likely	Severe	High	Sending security directives to clients	Possibly switching to OAuth2
A06:2021-Vulnerable and Outdated Components	Very unlikely	Moderate	Low	Remove unused dependencies, continuously inventory versions of application	fixed
A07:2021-Identification and Authentication Failures	Likely	Moderate	Moderate	Multi-factor authentication	N/A
A08:2021-Software and Data Integrity Failures	Likely	Moderate	Moderate	Ensure that CI/CD pipeline has proper segregation, configuration, and access control to ensure integrity of the code.	N/A

A09:2021-Security Logging and Monitoring Failures	*Very likely*	*Severe*	*High*	*Penetration testing and scans by dynamic application security testing tools.*	*N/A*
A10:2021-Server-Side Request Forgery	*Very likely*	*Severe*	*High*	*In the application layer, all client-supplied data should be sanitized and validated. The URL schema, port and destination should be enforced.*	*N/A*