OWASP REPORT

"Playvera"

Ivan Ovcharov
Fontys University of Applied Sciences
S3-CB-01

Table of Contents

Ivan Ovcharov
Fontys University of Applied Sciences
S3-CB-01

	Likelyhood	*Impact*	*Risk*	*Actions*	*Planned*
A01:2021-Broken Access Control	*High*	*Severe*	*High*	*Denying force browses and functionality by default*	*N/A*
A02:2021-Cryptographic Failures	*Low*	*Low*	*Low*	*Making sure that the algorithms used are up to date*	*N/A, Fixed*
A03:2021-Injection	*Not Likely*	*Moderate*	*Very Low*	*Whitelist server-side input, safe API's and using ORMS*	*N/A, Fixed*
A04:2021-Insecure Design	*Low*	*Moderate*	*Low*	*Unit/integration testing, separating layers between their importance.*	*Fixing unit testing*

Ivan Ovcharov
Fontys University of Applied Sciences
S3-CB-01

A05:2021-Security Misconfiguration	*High*	*Severe*	*Low*	*Security headers, avoiding the use of localstorage for storing JWT's*	*Possibly switching to Autho*
A06:2021-Vulnerable and Outdated Components	*Low*	*Moderate*	*Low*	*Removing unused dependencies, components and files. Obtaining tools from official sources.*	*N/A*
A07:2021-Identification and Authentication Failures	*Likely*	*Moderate*	*Moderate*	*Multi-factor authentication, weak password check, session creator.*	*N/A*
A08:2021-Software and Data Integrity Failures	*Low*	*Severe*	*Moderate*	*Ensuing libraries and dependencies are from trusted repositories. Ci/cD has proper*	*N/A*

				segregation.	
A09:2021-Security Logging and Monitoring Failures		*Severe*	*Moderate*	*Making sure that suspicious or malicious accounts are held for enough time to be fixed. All login and access control can be logged*	*N/A*
A10:2021-Server-Side Request Forgery	*High*	*Severe*	*Moderate*	*Data sanitization, disabling HTTP redirections, no raw responses to clients.*	*N/A*