OWASP Security Report

Security risks	Likelihood	Impact	Risk	Actions possible	Planned
A01:2021 – Broken Access Control	High	Severe	High	None, fixed	Yes
A02:2021 – Cryptographic Failures	Likely	Severe	Moderate	None, cannot use HTTPS	No
A03:2021 – Injection	Likely	Severe	High	None, prevented	Yes
A04:2021 – Insecure Design	Likely	High	Moderate	None, actions taken already	Yes
A05:2021 – Security Misconfiguration	Not Likely	Moderate	Moderate	Remove console logging of errors	Yes
A06:2021 – Vulnerable and Outdated Components	Not Likely	Low	Low	None	No
A07:2021 – Identification and Authentication Failures	High	High	Moderate	Do not accept weak passwords	No, risk accepted
A08:2021 – Software and Data Integrity Failures	Likely	High	Moderate	None	No, risk accepted
A09:2021 – Security Logging and Monitoring Failures	Likely	Moderate	Low	Log events like authentication, failed authentication, etc.	No, risk accepted
A10:2021 – Server-Side Request Forgery (SSRF)	Not Likely	Severe	Low	None, no user-supplied URL's are being used	No