Security Assessment Report — DesignMate Web Application

Prepared by: Ali Yasser

Date: October 2025

Project: Final AWS Web Application

Architecture: Frontend (S3) → Backend (Lambda) → Database (RDS) → Authentication (Cognito) → Monitoring (CloudWatch) → Infrastructure (CloudFormation)

1. Objective

The purpose of this security assessment is to evaluate the confidentiality, integrity, and availability of the DesignMate Web Application, ensuring that AWS best security practices are applied across all used services.

2. Scope

The assessment covers all active components in the project: VPC, RDS (MySQL), AWS Lambda, Amazon S3, Amazon Cognito, IAM Roles, and CloudWatch.

3. Architecture Security Overview

Component	Security Measures Applied	Risk Level	Comments
VPC	Private & Public subnets created via CloudFormation. NAT gateway used for private subnet outbound internet access. Security groups restrict access by port.	Low	Network isolation implemented correctly.
RDS MySQL	Deployed in private subnet (not publicly accessible). Only Lambda can connect via internal VPC.	Low	Sensitive data isolated from public internet.
Lambda Functions	Environment variables store DB credentials (using AWS Secrets Manager recommended). IAM role with least privilege access to RDS.	Medium	Improve by using AWS Secrets Manager instead of plain env vars.

S3 (Frontend)	Public access blocked except static hosting. Bucket policies reviewed.	Low	Static content only, no sensitive data stored.
Cognito (Auth)	MFA available. Strong password policy enforced.	Low	Enables secure user authentication.
IAM Roles	Separate roles for Lambda, RDS, and EC2. Least privilege principle mostly followed.	Medium	Should audit policies for unused permissions.
CloudFormation Templates	Automates deployment with consistent security configuration.	Low	Prevents human misconfiguration.

4. Security Risks Identified

1. Lambda Environment Variables – store DB credentials in plaintext. Mitigation: Use AWS Secrets Manager.

2. IAM Roles – Lambda execution role might have broad permissions. Mitigation: Restrict to specific actions/resources.

3. No HTTPS on S3 frontend. Mitigation: Add CloudFront + SSL.

4. RDS Backup & Encryption. Mitigation: Enable encryption and auto-backups.

5. Overall Security Rating

Network & Infrastructure: Strong
Authentication & Access Control: Strong
Data Protection: Strong
Monitoring & Logging: Moderate
IAM Permissions: Moderate
Overall: Secure with minor improvements.

6. Conclusion

The DesignMate Web Application demonstrates strong AWS security foundations using VPC segmentation, Cognito authentication, and CloudFormation-managed infrastructure. Minor refinements are recommended for production-grade compliance, including secrets management, HTTPS, and alerting.

URL:

http://designmate-frontend-aliyasser-dev.s3-website.eu-north-1.amazonaws.com