NAME: RANTI AMUDA
ROLE: Cloud Security Engineer

TASK: Securing Web Application Deployment in AWS

As a Cloud Security intern, I successfully designed and implemented a secure web application in AWS, adhering to industry best practices. This experience highlights my ability to deploy cloud-based applications with a focus on security, including HTTPS enforcement, SSL/TLS certificate management, and Web Application Firewall (WAF) configuration. The outcome ensures a resilient, secure, and high-performing web presence in the cloud.

Project Scope & Key Responsibilities

1. Secure Deployment of a Static Website

Hosted a static website using Amazon S3 with restricted public access to minimize attack surfaces.

Integrated Amazon CloudFront as a Content Delivery Network (CDN) for enhanced performance and DDoS mitigation.

Configured Amazon Route 53 for domain name management and DNS security.

2. Implementing HTTPS with SSL/TLS Encryption

Provisioned an SSL/TLS certificate using AWS Certificate Manager (ACM) to secure communications.

Configured CloudFront to enforce HTTPS, ensuring all connections are encrypted.

Automated SSL/TLS certificate renewal to maintain continuous encryption.

3. Enhancing Security with AWS Web Application Firewall (WAF)

Deployed AWS WAF to monitor and filter incoming traffic based on security rules.

Applied AWS Managed Rules to protect against common threats such as SQL Injection, Cross-Site Scripting (XSS), and HTTP Floods.

Configured custom rules to block unauthorized geographic locations and suspicious IP addresses.

4. Access Control & Continuous Monitoring

Enforced strict IAM policies to implement the Principle of Least Privilege (PoLP).

Enabled AWS CloudTrail and AWS Config for auditing security configurations and tracking changes.

Set up Amazon GuardDuty for real-time threat detection and anomaly monitoring.

Business Impact & Key Outcomes

- Successfully deployed a secure and scalable web application in AWS.
- Enforced HTTPS with SSL/TLS to protect user data and ensure compliance.
- Implemented AWS WAF to proactively mitigate web-based attacks.
- Established robust access controls and continuous monitoring to maintain security integrity.
- Improved resilience against DDoS attacks and unauthorized access.

- Step-by-step documentation with architecture diagrams and screenshots.
- AWS configurations, IAM policies, and security rule definitions.
- Security audit logs from AWS CloudTrail, AWS WAF, and GuardDuty.

This experience serves as a strong validation of my expertise in securing cloud-based web applications and my ability to implement industry-leading security measures in AWS environments.