Or Bitan

Business Card

Shenkar - Cloud Computing

Lecturer - Amit Dunsky

Table of Contents

1. Introduction

The system is a business card website designed to present my professional profile and capabilities. Key features include personal information, a photo gallery, a resume (CV), a QR code linking to my GitHub profile, social media links, and a contact form. This system is hosted on AWS using a serverless architecture, primarily leveraging AWS Amplify and AWS Lambda, The system sends email via AWS SES and sends system logs to AWS CloudWatch.

AWS services: Amplify, API GatWay, Lambda, CloudWatch ,SES ,IEM.

- **Purpose**

  The purpose of this system is to:
  - **Showcase:** Display my professional information and achievements in a structured and appealing manner.
  - **Connectivity:** Facilitate connections with potential employers and collaborators through direct contact links and a form.
  - **Security:** Ensure that all user interactions and data transmissions are secure, protecting both the user's and my personal information.
- **Scope**

  The scope of this system includes the development, deployment, and maintenance of a business card website that serves as an online representation of my professional profile. It aims to provide a platform for potential employers and colleagues to learn about my skills, view my resume, connect with me on social media, and contact me directly through a secure form.

2. Security

To ensure the security of the system and mitigate potential attack vectors and attack surfaces, the following measures are implemented:

- **Cross-Site Scripting (XSS) Protection**
  - **Input Sanitization**: All user inputs are sanitized by replacing potentially dangerous characters with -invalid-, preventing the execution of malicious scripts.
- **Serverless Architecture**
  - **AWS Lambda**: Utilizes AWS Lambda, eliminating traditional servers and thus reducing the attack surface.
  - **Managed Services**: AWS handles updates and patches, improving overall security.
- **HTTPS**
  - **Encryption**: All communications are encrypted using HTTPS, ensuring data integrity and security during transmission.

- **Monitoring**
  - **AWS CloudWatch:** monitoring the system behavior with CloudWatch to find suspicious actions.
- **Email Security**
  - **Challenge**: Ensuring that emails sent through the contact form are secure and not susceptible to spoofing or phishing.
  - **Solution**: Using AWS SES to send emails, which includes features such as DKIM, SPF, and DMARC to authenticate emails and improve deliverability.

3. Challenges and solutions

Injection Attacks:

- **Challenge:** Preventing unauthorized data injection.
- **Solution:** Implementing strict input validation and sanitization.

Cross-Site Scripting (XSS):

- **Challenge**: Preventing the execution of malicious scripts.
- **Solution**: Replacing dangerous characters with -invalid- and using Content Security Policy (CSP) headers.

4. Attack Vector and Surfaces

- **Attack Vectors:**

  The primary vulnerabilities in this system stem from the content of the emails, and we mitigate these vulnerabilities by:

  - **Injection Attacks**:
    Definition: Techniques that inject malicious data into a program to manipulate its execution.
    Mitigation: Implement strict input validation and sanitization to ensure only expected data is processed.

  - **Cross-Site Scripting (XSS)**:
    Definition: A type of attack where malicious scripts are injected into trusted websites.
    Mitigation: Replace dangerous characters with -invalid-, use Content Security Policy (CSP) headers, and sanitize user inputs.

- **Attack Surfaces:**

  The attack surface primarily relates to the components and processes involved in sending and receiving these emails securely :

  - **AWS SES Configuration**:
    Description: The configuration settings within AWS SES that determine how emails are sent, including sender policies, recipient policies, and content filtering rules.
    Mitigation:Properly configure SES to enforce security protocols such as DKIM, SPF, and DMARC to authenticate emails and prevent spoofing or phishing attempts.

  - **Email Content Handling:**
    Description: How the system handles and processes the content of emails, including message formatting, attachments, and embedded links.
    Mitigation:Implement content filtering and validation mechanisms to sanitize incoming email content and prevent malicious payloads or scripts from executing.

By understanding and addressing these attack vectors and surfaces, we can minimize the risk of security breaches and ensure the integrity and reliability of the business card website.

5. The Approach

To create a secure and reliable business card website, we adopted a serverless architecture using AWS services. The following steps outline our approach:

Design and Architecture

- **Serverless Framework**: We chose AWS Amplify and AWS Lambda for a scalable and maintainable architecture, eliminating the need for traditional servers and reducing operational overhead.
- **Component-Based Design**: The website is designed with reusable components for personal information, photos, resume, QR code, social media links, and the contact form.

Development and Integration

- **Frontend Development**: Utilizing modern web technologies to build a responsive and user-friendly interface.

- **Backend Development**: Implementing AWS Lambda functions to handle form submissions and email notifications using aws SES.

Security Measures

- **Input Sanitization**: Ensuring all user inputs are sanitized to prevent XSS and other injection attacks.
- **HTTPS**: Enforcing HTTPS for secure data transmission.
- **Authentication**: Implementing AWS Amplify's built-in authentication mechanisms (coming soon).
- **CORS**: Configuring CORS to restrict access to trusted origins.
- **Email Security**: Using AWS SES to securely send emails from the contact form.

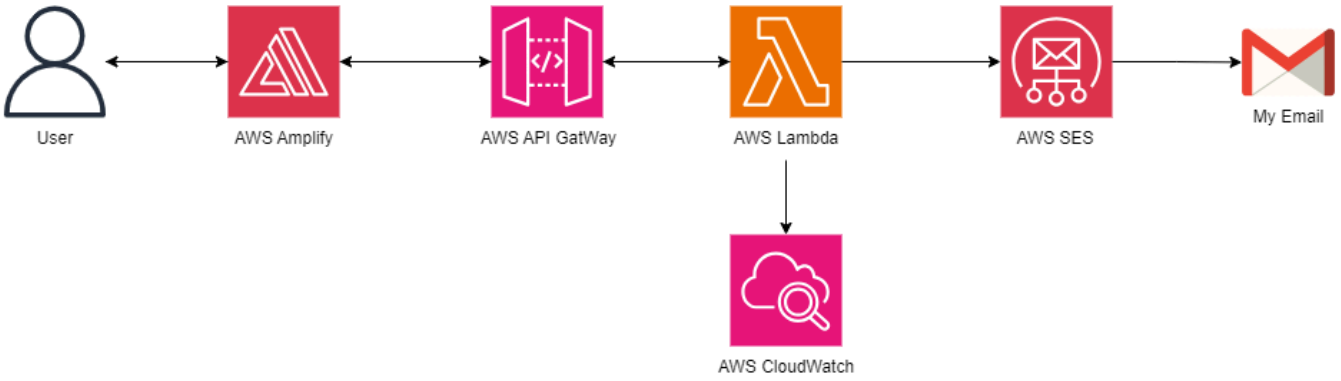
Deployment

- **Continuous Deployment**: Using AWS Amplify for seamless deployment and updates.

6. Flow

1. **User Interaction**: Users visit the website provided by AWS Amplify and interact with various components (viewing personal info, photos, resume, etc.).
2. **Form Submission**: Users fill out the contact form to send messages.
3. **Data Processing**: AWS Lambda processes the form data and sends it to the specified email using AWS SES.
4. **Response**: The system provides feedback to the user about the successful submission of their message.

7. Diagram



8. Implementation Plan

Phase 1: Setup

- **Setup AWS Services**: Configure AWS Amplify, Lambda, SES, and other necessary services like AWS CloudWatch, AWS IEM.

Phase 2: Development

- **Frontend Development**: Build the website with personal information, photos, resume, QR code, social media links, and contact form.
- **Backend Development**: Implement AWS Lambda functions to handle form submissions and send emails via AWS SES.

Phase 3: Integration

- **Connect Frontend and Backend**: Ensure the frontend properly communicates with the backend services.
- **Deploy Application**: Deploy the application using AWS Amplify.

9. Conclusion

The business card website is a comprehensive system designed to present my professional profile securely. Leveraging AWS serverless architecture and implementing robust security measures ensures a reliable and secure user experience. The implementation plan and approach will guide the successful deployment and maintenance of the system.

Video link:
https://drive.google.com/file/d/1EmxXCyRpC_xsNsQuUS8gMFWX2YEwKvyb/view?usp=sharing