Damn Vulnerable AWS API

Design Document

Team Number

sdmay24-11

Client

RSM - Jon Schnell

Adviser

Julie Rursch

Team Members/Roles

Ashler Benda - Client Interaction

Garret Arp - Team Website Lead

Karthik Kasarabada - Client Interaction

Andrew Bowen - Scrum Master

Ahmed Nasereddin - Identity & Access Management

Ayo Ogunsola - Identity & Access Management

Ethan Douglass - Testing Lead

Email

sdmay24-11@iastate.edu

Website

sdmay24-11.sd.ece.iastate.edu/

Revised: 09/06/2023 v1.0

Executive Summary

Development Standards & Practices Used

GitLab

Agile Sprint Development Cycle

AWS Security Testing Standards

AWS/Cloud Network Architecture

OWASP Top Ten

Summary of Requirements

Deliberately incorporates common AWS-specific vulnerabilities. These vulnerabilities should include misconfigured permissions, security group issues, identity and access management flaws, and more.

Create a diverse set of AWS scenarios that reflect real-world use cases, including AWS Lambda functions, S3 buckets, EC2 instances, and IAM roles. Each scenario should have associated vulnerabilities that mimic those found in actual AWS environments.

Provide comprehensive documentation that outlines the vulnerabilities, attack vectors, and potential exploitation techniques present in the Damn Vulnerable AWS API. Include a step-by-step walkthrough of common AWS security risks.

Implement an incident response component that enables users to analyze logs, identify security incidents, and assess the impact of potential breaches within the Damn Vulnerable AWS API. This component should offer insights into AWS-specific log analysis techniques.

Realistically mimic AWS services and vulnerabilities, ensuring an authentic learning experience.

Implement safeguards to prevent unintended damage to actual AWS resources and ensure that the environment is safe for experimentation.

Provide clear and detailed documentation to guide users through the vulnerabilities and potential attacks.

Utilize AWS services such as Lambda, S3, EC2, IAM, and CloudWatch to create the API environment.

Develop custom code and configurations to introduce vulnerabilities into the AWS API.

Implement logging and monitoring to capture user interactions and security incidents within the environment.

Applicable Courses from Iowa State University Curriculum

List all Iowa State University courses whose contents were applicable to your project.

CPRE 230

CPRE 231

CYBE 234

CYBE 430/530

COMS 309

CPRE 489

ENGL 314

New Skills/Knowledge acquired that was not taught in courses

List all new skills/knowledge that your team acquired which was not part of your Iowa State curriculum in order to complete this project.

- Design of CloudFormation Templates
- Knowledge of AWS Resources
- Knowledge of AWS Services - S3, EC2, IAM, CloudWatch
- Professional documentation & communication with Clients
- Pentesting
- Role Based Access Controls

Table of Contents

1 Team 5

1.1 Team Members 5

1.2 Required Skill Sets for Your Project 5

(if feasible – tie them to the requirements) 5

1.3 Skill Sets covered by the Team 5

(for each skill, state which team member(s) cover it) 5

1.4 Project Management Style Adopted by the team 5

1.5 Initial Project Management Roles 5

2 Introduction 5

2.1 Problem Statement 5

2.2 Requirements & Constraints 5

2.3 Engineering Standards 5

2.4 Intended Users and Uses 6

3 Project Plan 6

3.1 Project Management/Tracking Procedures 6

3.2 Task Decomposition 6

3.3 Project Proposed Milestones, Metrics, and Evaluation Criteria 6

3.4 Project Timeline/Schedule 6

3.5 Risks And Risk Management/Mitigation 7

3.6 Personnel Effort Requirements 7

3.7 Other Resource Requirements 7

4 Design 8

4.1 Design Context 8

4.1.1 Broader Context 8

4.1.2 User Needs 8

4.1.3 Prior Work/Solutions 8

4.1.4 Technical Complexity 9

4.2 Design Exploration 9

4.2.1 Design Decisions 9

4.2.2 Ideation 9
4.2.3 Decision-Making and Trade-Off 9
4.3 Proposed Design 9
4.3.1 Design Visual and Description 10
4.3.2 Functionality 10
4.3.3 Areas of Concern and Development 10
4.4 Technology Considerations 10
4.5 Design Analysis 10
4.6 Design Plan 10
5 Testing 11
5.1 Unit Testing 11
5.2 Interface Testing 11
5.3 Integration Testing 11
5.4 System Testing 11
5.5 Regression Testing 11
5.6 Acceptance Testing 11
5.7 Security Testing (if applicable) 11
5.8 Results 11
6 Implementation 12
7 Professionalism 12
7.1 Areas of Responsibility 12
7.2 Project Specific Professional Responsibility Areas 12
7.3 Most Applicable Professional Responsibility Area 12
8 Closing Material 12
8.1 Discussion 12
8.2 Conclusion 12
8.3 References 13
8.4 Appendices 13
8.4.1 Team Contract 13

List of figures/tables/symbols/definitions (This should be the similar to the project plan)

1 Team

1.1 Team Members

Student Members:

1) _Ashler Benda_____ 2) _Ahmed Nasereddin_____

3) _Garrett Arp_____ 4) _Ethan Douglass_____

5) _Andrew Bowen_____ 6) _Karthik Kasarabada_____

7) _Ayo Ogunsola_____

1.2 Required Skill Sets for Your Project

(if feasible – tie them to the requirements)

- Basic programming
- Knowledge of AWS Resources
- Pentesting
- Technical Writing/Documentation
- Digital Forensics
- Incident Response
- Role Based Access Controls
- AWS Safeguards

1.3 Skill Sets covered by the Team

Ashler Benda - Pentesting, Active Directory Testing, Relay Attacks, Basic Programming, Web App Design, Technical Documentation

Ahmed Nasereddin - Active Directory, IAM, Basic Programming (Java, C,Python, C#), Technical Writing

Ayo Ogunsola - Active Directory, Pentesting, Basic AWS, Basic Programming (Java, C, Python, C#), Technical Documentation, IAM

Karthik Kasarabada - Pentesting AD, Intermediate AWS (ECS, IAM), Basic Programming (Python, C, Java), Technical Writing

Andrew Bowen - Pentesting, Kerberos, Active Directory, Basic Web Frontend, Basic Programming (C, Java, Python), Technical Writing

Ethan Douglass - Basic Programming (SQL, C#, Python, Java), Active Directory, Technical Writing

Garrett Arp - Technical Writing, Basic Programming (SQL, C#, Python, Java), Intermediate Microsoft Azure, Intermediate Terraform and Ansible Infrastructure Engineering, Basic Web Frontend

1.4 Project Management Style Adopted by the team

Weekly agile style team meetings

1.5 Initial Project Management Roles

Team Organization (Scrum Master): Andrew Bowen

Client Interaction: Ashler B, Karthik K.

Review Testing Lead: Ethan Douglass

Team Website: Garrett Arp

Identity & Access Management: Ahmed Nasereddin, Ayo Ogunsola