clearscale

Enhancing Web Application Security for MaiaLearning: A Comprehensive Penetration Testing and Remediation Approach by ClearScale MSP

aws PARTNER Premier Tier Services

maialearning

Industry: Education
Tags: AWS, Security, MSPs

Challenge: MaiaLearning needed to secure its web application against rising cyber threats to protect sensitive student and institutional data.

Solution: ClearScale MSP conducted a month-long comprehensive Web Application Penetration Test to identify and remediate vulnerabilities using AWS services.

Benefits: MaiaLearning mitigated all High and Medium vulnerabilities within its web application.

AWS Services: Amazon CloudWatch, AWS Elastic Beanstalk, AWS ALB, AWS WAF, AWS Lambda, and AWS API Gateway.

Executive Summary

MaiaLearning, a leading provider of career and college readiness solutions, engaged ClearScale MSP to enhance the security of its web application amidst a rising cyber threat landscape. ClearScale ensured MaiaLearning's platform met the highest security standards, effectively reducing the risk of unauthorized access and data breaches.

"ClearScale MSP's thorough penetration testing and expert remediation not only secured our platform against emerging cyber threats but also gave us the confidence that our sensitive data is well-protected, allowing us to focus on guiding students' futures without worrying about security risks."

Barry Coleman, CTO, MaiaLearning

The Challenge

MaiaLearning faced the challenge of ensuring the security of its web application, in an increasingly threatening cyber landscape. With sensitive student and institutional data at stake, any vulnerabilities within the application could result in unauthorized access, data breaches, and significant reputational damage.

Given the importance of its platform in guiding students' future paths, it was critical for MaiaLearning to ensure that its application met the highest security standards to protect against potential threats.

The ClearScale Solution

To address these concerns, MaiaLearning partnered with ClearScale MSP, its AWS Managed Services Provider, to perform comprehensive Web Application Penetration Testing. The testing was conducted over a period of a month within a controlled staging environment, ensuring that live production data remained unaffected.

ClearScale MSP employed a structured methodology, adhering to industry best practices such as the OWASP Testing Guide and the Penetration Testing Execution Standard. The testing process was divided into several stages:

- **Reconnaissance Stage:** ClearScale MSP conducted extensive reconnaissance to identify open ports, subdomains, and other potential entry points that an attacker might exploit. This phase involved scanning for publicly exposed services and gathering intelligence for later stages of testing.
- **Testing Stage:** In the controlled staging environment, ClearScale MSP simulated various attack scenarios to identify vulnerabilities in key areas such as user authentication, session management, and access control. AWS WAF was leveraged as part of the broader web application security strategy, which includes securing APIs hosted on AWS API Gateway, thereby enhancing protection against common web exploits. This phase combined both automated and manual techniques to ensure a comprehensive evaluation of the application's defenses.
- **Findings Analysis:** Vulnerabilities identified during the testing were categorized by severity (Critical, High, Medium, Low) and accompanied by detailed analyses and recommended remediation steps.

Throughout the testing and remediation phases, ClearScale MSP provided ongoing support, ensuring that all identified vulnerabilities were addressed. The solution leveraged key AWS services including Amazon Elastic Beanstalk for deploying and managing applications, AWS ALB for distributing incoming traffic, Amazon CloudWatch for monitoring, AWS WAF for enhanced web application security, AWS API Gateway for managing APIs, and AWS Lambda for automated response to detected vulnerabilities.

Customer Collaboration and Communication

The success of this project was greatly enhanced by the close collaboration between MaiaLearning and ClearScale MSP. From the outset, both teams maintained open lines of communication, which was critical to the effective execution of the project.

- **Pre-Testing Coordination:** ClearScale MSP worked closely with MaiaLearning's IT team to define the testing scope and ensure that all necessary resources were available. This included setting up a controlled staging environment that accurately mirrored the production setup, allowing for realistic and safe testing conditions.
- **Ongoing Updates:** Throughout the testing phase, the Service Delivery Manager ensured that regular updates were provided to MaiaLearning, including preliminary findings. To facilitate real-time communication and ensure swift resolution of any issues, a dedicated Slack channel was established. This channel allowed both teams to collaborate effectively, share updates, and quickly address any critical vulnerabilities.
- **Post-Testing Support:** After the completion of the testing, ClearScale MSP delivered detailed reports and assisted MaiaLearning with the remediation of identified vulnerabilities. This post-testing support ensured that MaiaLearning had the necessary guidance to fully address the issues and bolster their security posture.

The Benefits

As a result of the penetration testing and remediation efforts, MaiaLearning successfully mitigated all identified High and Medium vulnerabilities within its web application. This proactive approach brought several significant benefits:

- Enhanced security posture by strengthening MaiaLearning's defenses, reducing the risk of unauthorized access and data breaches
- Ensured alignment with SOC 2 compliance requirements, further enhancing the trust and confidence of stakeholders in the security and integrity of the platform
- Improved threat detection and response through the integration of AWS services like Amazon CloudWatch and AWS Lambda, which allowed MaiaLearning to detect and respond to security threats in real time
- Reduced risk of data breaches by focusing on user authentication and privilege escalation, greatly diminishing the likelihood of unauthorized access to sensitive student and institutional data
- Increased resilience against cyberattacks by fortifying the application against various forms of cyber threats, ensuring the platform remains reliable and secure
- Compliance with industry standards through adherence to OWASP guidelines and other best practices, ensuring the application meets or exceeds security standards critical for maintaining trust with users and stakeholders
- Peace of mind for stakeholders as a result of successfully resolving vulnerabilities and implementing a solid security framework, ensuring the platform is well-protected against potential threats

About ClearScale

ClearScale is a cloud-native systems integration, strategic consulting, and application development company founded in 2011. The company has successfully delivered more than 1,000 innovative cloud projects for clients ranging from startups to large enterprises across all major industries. ClearScale's cloud experts design, implement, optimize, and manage customized cloud solutions that help customers achieve their business transformation initiatives.