iterasec

Web App Penetration Test for Edutech Startup

Self Leaders

Client:
SelfLeaders

Industry:
Education & Business Administration

Company Size:
11-50 Employees

Services Used:
Penetration Testing, Application Security Training, Security Remediation Support

Client

SelfLeaders is a Swedish company specializing in personal development and corporate culture transformation. Since its inception in 2009, SelfLeaders has been empowering individuals and organizations through a variety of educational modules and tools focused on self-leadership. Catering to businesses of all sizes, NGOs, and public sector organizations, they deliver training events and workshops that foster personal growth and professional development. With a dedicated team of 11-50 employees based in Stockholm, SelfLeaders has established itself as a pivotal player in the education and business administration sectors.

Background

As SelfLeaders expanded its reach, the company developed a specialized corporate training and education platform used by numerous large companies and enterprises. Recognizing the platform's critical role in delivering their services, SelfLeaders understood the importance of ensuring its security. Protecting sensitive client data and maintaining the integrity of their platform were paramount, especially given the high-profile nature of their clientele.

The Challenge

SelfLeaders approached Iterasec with the goal of evaluating the current state of security of their corporate training and education platform. The key objectives were:

- **Security Assessment:**
  Perform a thorough penetration test to identify any severe vulnerabilities that could be exploited by malicious actors.
- **Data Protection:**
  Ensure the safeguarding of sensitive data to maintain client trust and comply with regulatory requirements.
- **Operational Continuity:**
  Prevent potential disruptions such as denial-of-service attacks that could impact the delivery of their services.

The Solution

Iterasec deployed a specialized team to address SelfLeaders' needs, consisting of a Senior Penetration Tester, a Security Engineer, and a Delivery Manager. The approach included:

Comprehensive Penetration Testing

- **Vulnerability Identification:**
  Systematically probing the application to uncover security weaknesses, including both common and obscure vulnerabilities.
- **Exploitation Attempts:**
  Simulating attack scenarios to understand how vulnerabilities could be leveraged in real-world situations.
- **Risk Analysis:**
  Assessing the potential impact of each identified vulnerability on the confidentiality, integrity, and availability of the platform.

Detailed Reporting and Recommendations

- **Findings Summary:**
  An executive overview highlighting the critical and high-severity vulnerabilities discovered.
- **Technical Details:**
  In-depth explanations of each vulnerability, including how they were found and the potential risks associated.
- **Remediation Guidance:**
  Clear, actionable recommendations for addressing each security issue.

Collaborative Remediation Support

- **Fix Security Issues:**
  Assist in patching vulnerabilities to ensure they were effectively resolved.
- **Validate Fixes:**
  Perform follow-up testing to confirm that the applied fixes addressed the vulnerabilities without introducing new issues.
- **Knowledge Sharing:**
  Provide insights and best practices to prevent similar vulnerabilities in future developments.

Complimentary Security Training

- **Secure Coding Practices:**
  Techniques to write code that is resilient against common security threats.
- **Threat Modeling:**
  Understanding potential attack vectors and how to anticipate them during the development process.
- **Ongoing Security Maintenance:**
  Strategies for integrating security considerations into regular workflows.

The Outcome

The collaboration between Iterasec and SelfLeaders yielded significant benefits:

- **Enhanced Security Posture**
  The penetration test identified:
  - 1 Critical-Severity Vulnerability: A compromise of the company's SMTP server, which could have allowed attackers to intercept or manipulate email communications.
  - 2 High-Severity Vulnerabilities: Multiple instances of broken access control, enabling unauthorized access to sensitive data.
  - Additional Vulnerabilities: Including denial-of-service (DoS) risks and several GraphQL-related security issues.
- **Improved Platform Integrity**
  The timely patching of all identified issues led to the release of a more secure version of the platform. This not only protected existing clients but also enhanced the platform's appeal to prospective customers concerned about security.
- **Strengthened Client Trust**
  By demonstrating a commitment to security, SelfLeaders reinforced trust with their clients. This commitment is particularly crucial when dealing with personal development and corporate culture, areas where confidentiality and integrity are vital.
- **Empowered Development Team**
  Through hands-on support and training, the development team gained valuable security expertise. This empowerment enables them to proactively address security considerations in future projects, fostering a culture of security awareness within the organization.

Conclusion

The partnership between Iterasec and SelfLeaders highlights the importance of proactive cybersecurity measures in today's digital landscape. Our tailored approach identified and mitigated critical vulnerabilities and contributed to the long-term security posture of SelfLeaders through knowledge transfer and ongoing support. SelfLeaders continues to provide exceptional services to their clients, confident in the robustness of their technology and the trustworthiness of their operations.