iterasec

Penetration Testing Services for OpenSocial

Client:
OpenSocial

Industry:
Open-Source Community Software

Company Size:
11 to 50 Employees

Services Used:
Penetration Testing, Security Code Review

Client

OpenSocial specializes in building open-source community software for leading organizations such as the European Commission, Greenpeace International, Adidas, and many others. Their platform serves as an internal social network, enhancing collaboration and communication within organizations. OpenSocial provides the core platform and offers support, installation services, and custom development of additional features to tailor the platform to each client's needs.

Background

As OpenSocial expanded its client base to include high-profile organizations, the security of their open-source community platform became a critical priority. The sensitive nature of the data handled by their platform — ranging from internal communications to proprietary information — was in need of a strong security framework. Given the open-source aspect of their platform, they were aware that vulnerabilities could be more easily exploited if not properly managed. OpenSocial sought a thorough security assessment to ensure their platform could withstand potential cyber threats.

The Challenge

OpenSocial approached Iterasec with several specific objectives:

- **Comprehensive Penetration Testing:**
  Conduct a detailed penetration test of their Drupal-based community platform, focusing on both standard vulnerabilities and those specific to Drupal and open-source environments.
- **Iterative Testing and Remediation:**
  Engage in multiple testing cycles to find vulnerabilities, allow OpenSocial to fix them, and then verify the effectiveness of these fixes.
- **Certification of Security:**
  Provide an attestation letter as proof of conducting the penetration tests, fixing the vulnerabilities, and re-testing to ensure all issues were resolved.

The Solution

Iterasec came up with a tailored approach to meet OpenSocial's unique requirements.

Penetration Testing with Drupal Specifics

- **RESTful and SOAP APIs:**
  Assessed both RESTful and SOAP APIs for secure authentication and authorization mechanisms, investigated potential code injection points, and looked for complex business logic flaws.
- **Appliance Web Admin:**
  Investigated administrative functionalities for privilege escalation risks.
- **Reverse Collector:**
  Conducted specialized analysis to identify vulnerabilities in data collection components with the focus on data confidentiality and integrity, as well as on the component s availability.
- **SaaS Infrastructure:**
  Performed a thorough evaluation of the AWS environment, identifying misconfigurations, insecure network setups, and possible attack vectors.

Identification and Reporting of Vulnerabilities

- **Multi Level Vulnerability Detection:**
  Discovered numerous vulnerabilities at various levels, including SQL injection points, cross-site scripting (XSS), access control weaknesses, and configuration issues.
- **Detailed Reporting:**
  Provided comprehensive reports after each testing iteration, outlining the vulnerabilities found, their potential impact, and recommended remediation steps.

Iterative Testing and Collaboration

- **Multiple Testing Cycles:**
  Conducted 2-3 iterations of penetration testing. After each cycle, OpenSocial addressed the identified vulnerabilities.
- **Verification of Fixes:**
  Re-tested the platform to ensure that the fixes were effective and no new vulnerabilities were introduced.
- **Collaborative Approach:**
  Maintained close communication with OpenSocial's development team throughout the process to facilitate quick resolutions and knowledge transfer.

Attestation and Certification

- **Attestation Letter:**
  Upon completion of the final testing cycle, we issued an attestation letter confirming that the platform had undergone thorough penetration testing and that all identified vulnerabilities were resolved.
- **Compliance and Assurance:**
  This certification provided OpenSocial's clients with assurance regarding the security and integrity of the platform.

The Outcome

Our partnership with OpenSocial provided significant benefits:

- **Enhanced Security:**
  The platform's security was substantially improved, reducing the risk of data breaches and cyber-attacks.
- **Client s Confidence:**
  The attestation letter and demonstrable commitment to security enhanced trust among existing and prospective clients.
- **Improved Development Practices:**
  OpenSocial's development team gained valuable insights into secure coding practices, which they integrated into their development lifecycle.
- **Ongoing Security Awareness:**
  The iterative process fostered a culture of continuous security awareness within the organization.

Conclusion

Iterasec penetration testing and code review services enabled OpenSocial to significantly strengthen the security of their open-source community platform. By approaching the testing from a developer's perspective and engaging in multiple remediation cycles, we ensured that the platform could meet the stringent security requirements of high-profile clients. This collaboration allowed OpenSocial to focus on delivering exceptional service and innovation while maintaining the highest standards of security.