Letter Of Assurance

Prepared for: Livepro

Prepared by: Adrian Wood, Technical Director,
And
Griffin Francis, Application Security Specialist
on the 22/07/2016.

Contact:
WHITEHACK
info@whitehack.com.au
1300 85 54 87
www.whitehack.com.au

Livepro Web Application Assessment

WHITEHACK conducted a web application vulnerability assessment and penetration test against the web application environment provided by Livepro between September and November 2017. Testing was conducted in an effort to evaluate the application's security posture with regard to the items listed in OWASP and included unauthenticated and authenticated testing.

- *OWASP provide a list of application security requirements or tests that can be used by architects, developers, testers, security professionals and even consumers to define what a secure application is.*

The assessment was undertaken by Adrian Wood who is a highly experienced web application security auditor, endorsed under numerous certification programs and assurance standards and Griffin Francis, an application security specialist with international recognition and experience.

WHITEHACK have reviewed the Livepro Web Application and prepared a Report of Findings which records the applicability and compliance with specific OWASP controls. Once discovered vulnerabilities were remediated, WHITEHACK retested the application in order to issue this letter of assurance.

WHITEHACK'S assessors finding is that the applicable OWASP controls relating to the broad consensus of application security controls are implemented and are operating effectively.

Livepro should advise WHITEHACK of any significant future changes to the services, which might influence the effectiveness of the implemented OWASP controls. Livepro should remain informed of future releases of the OWASP manual, which may include changes which may affect the status of this document.

Regards,

Adrian Wood
Technical Director, WHITEHACK Pty Ltd, & WHITEHACK LLC.

Livepro OWASP Top 10 – Quick Results Table

OWASP Top 10 represents a broad consensus about what the most critical web application security laws are. Adopting awareness of the OWASP Top 10 is one of the most effective steps towards improving the software development process within an organization.

OWASP Top 10	Effective	Partially Effective	Not Effective	Statement of Control Effectiveness
A1 – Injection	✓			Livepro correctly keep untrusted data separate from commands and queries through various methods.
A2–Broken Authentication and Session Management	✓			Livepro use a strong set of authentication and session management controls.
A3 – Cross Site Scripting	✓			Livepro separate untrusted data from active browser content.
A4 – Insecure Direct Object References	✓			Livepro prevent insecure direct object references and protect each user accessible object.
A5 – Security Misconfiguration	✓			Livepro use a repeatable hardening process through the configuration of all devices, and follows appropriate system hardening standards based on industry consensus, validated by an independent third party.
A6 - Sensitive Data Exposure	✓			Livepro uses safe cryptography to protect from various insider and external user attacks. We recommend *bcrypt* hashing for passwords.
A7 – Missing Function Level Access Control	✓			Livepro has a consistent and easy to analyze authorization module.
A8 – Cross-Site Request Forgery	✓			Livepro include an unpredictable token in each HTTP request via WAF.
A9 – Using Known Vulnerable Components	✓			Livepro monitor the security of third party components and patch where necessary.
A10 – Invalidated Redirects and Forwards	✓			Livepro is appropriately avoiding redirects and forwards to avoid phishes attempting to garner users trust.

Executive Summary

This initial analysis of the web-application showed that it is generally sound against most common attack methods used by malicious threat actors on web applications. However, the application in some areas was not correctly sanitizing bad input in real time which caused some Cross Site Scripting and Injection vulnerabilities after authentication, but these were quickly patched and a process to prevent relapses put in place, including a WAF deployment.

The speed in which these issues were patched and released to production shows that a great level of competency and also that a high level of development controls is present.

Our retesting of the application found no relapses or problems with the implementation of fixes.

Questions?

Contact:
WHITEHACK
info@whitehack.com.au
1300 85 54 87
www.whitehack.com.au