WHITEHACK

Letter Of Assurance

Prepared for: *Livepro*

Prepared by: Adrian Wood, Technical Director,
28.5.2019

Contact:
WHITEHACK
info@whitehack.com.au
www.whitehack.com.au

Livepro Security Assessment

WHITEHACK conducted a web application vulnerability assessment and penetration test against the web application environment provided by *Livepro* between February and April 2019. Testing was conducted in an effort to evaluate the application's security posture with regard to both application and infrastructure vulnerabilities and included unauthenticated and authenticated testing. Given *Livepro's* primary role is as a cloud based SaaS provider, OWASP was the primary point of reference documentation.

- *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.

WHITEHACK have reviewed the *Livepro's* environment 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 of their remediation and our confidence in *Livepro* at this point in time.

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 or other 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

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 – Sensitive Data Exposure	✔			Livepro uses safe cryptography to protect from various insider and external user attacks. Note: we recommend *bcrypt* hashing for passwords.
A4-XML External Entities	✔			Livepro protects against exploitation of vulnerable XML content by restricting the upload of XML, and by not allowing hostile content in an XML document, resulting in exploitation of vulnerable code, dependencies or integrations.
A5 – Broken Access Control	✔			Livepro do not allow access to objects or references that are beyond a users permission set.
A6 -Security Misconfiguration	✔			Livepro are preparing 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.
A7 – Cross Site Scripting (XXS)	✔			Livepro has a consistent and easy to analyze authorization module.
A8 – Insecure Deserialization	✔			Livepro include an unpredictable token in each HTTP request via WAF.
A9 – Using Known Vulnerable Components	✔			Livepro have a process to monitor the security of third party components and dependencies and patch where necessary.
A10 – Insufficient Logging and Monitoring	✔			Livepro use centralize monitoring across their platform.

Executive Summary

This analysis of *Livepro* showed that it is generally sound against most common attack methods used by malicious threat actors on applications and their supporting infrastructure. However, the application in some areas was not adequately protecting certain data constraints, but these were quickly patched and a process to prevent relapses put in place.

Improvements to consistency of data validation across the environment have been put in place - across the rapidly growing environment.

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 as per the original report's recommendations.

Questions?

Contact:
WHITEHACK
info@whitehack.com.au
www.whitehack.com.au