Application Security Assurance

For TrakaWEB and Traka Touch

We at Traka take security seriously, and we are well placed to provide our customers with the assurance they are looking for in one of three ways;

- By allowing our software to be subjected to third party security/penetration testing,
- By provide results of penetration testing, subject to company confidentiality considerations
- By demonstrating that our software development methods incorporate application security as a core element.

Traka is constantly subjecting our software to third party independent penetration and security testing and our development team proactively works to incorporate secure testing in our development process to an application security model developed by OWASP, called OWASP10-2017

OWASP 10 Vulnerabilities (2017)

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure deserialization
9. Using components with known vulnerabilities
10. Insufficient logging & monitoring

What is OWASP and the OWASP Top 10?

The Open Web Application Security Project (OWASP) is a non-profit organisation dedicated to providing unbiased, practical information about application security. The OWASP Top 10 Web Application Security Risks was updated in 2017 to provide guidance to developers and security professionals on the most critical vulnerabilities that are commonly found in web applications, which are also easy to exploit. These 10 application risks are dangerous because they may allow attackers to plant malware, steal data, or completely take over computers or web servers..

Traka is a leading player in the asset management space, and has invested significantly in its operational processes to incorporate security as a core element, and is ISO 27001 certified.

Our TrakaWEB and Touch software incorporates many security features including:

- Secure Web Front End (HTTPS)
- Password & PIN data encryption
- Secure communication between components (Transport Layer Security and Message Security)
- Web Front End tested to the Open Web Application Security Project (OWASP) top 10 standards
- API's tested to the Open Web Application Security Project (OWASP) top 10 standards
- Regular in house penetration testing using market leading pen test tools
- Regular customer penetration testing (Facebook, Google, VISA, ExxonMobil etc.)
- Support for customer supplied Web Front End SSL certificates
- Upgrade of Transport Layer Security (TLS1.1 to TLS1.2)
- Full documetation available for setting up HSTS
- Content Security Policy (CSP) implemented
- More secure levels of encryption and hashing
- Signing of the Traka Touch application

traka

ASSA ABLOY

traka

ASSA ABLOY

traka.com