Penetration Testing and Vulnerability Scanning

Application security is crucial to keep customer data security. That is why E-days conducts annual third-party penetration testing and weekly vulnerability scans to make sure the e-days code is secured against the latest threats.

Vulnerability Scanning

E-days uses Detectify Deep Scan to perform weekly vulnerability scans n pre-live code to prevent weakness being release into the production environment.

Detectify runs automated security tests on the e-days web application to test over 1500 vulnerabilities, including the OWASP Top 10 and CORS vulnerabilities.

Penetration Testing

Third-party penetration testing to carried out annually by Sec-1 Ltd. Sec-1 are a CREST member. CREST provides standards-based accreditations to companies providing penetration testing services.

Penetration Test Report

You can download the executive summary of the latest penetration test below.

Executive Summary Report – March 2019

Penetration Test Remediation

The following vulnerabilities were discovered in our annual penetration test, performed in March 2019

High Impact

none

Medium Impact

1. Strict Transport Security not enabled: A code fix has now been put in place to enforce HTTPS.
2. Insecure SSL/TLS Ciphers Supported: E-days now only allows TLS 1.2, this can be checked using https://www.ssllabs.com/ssltest/
3. Insecure SSL Certificate Detected: This was a false positive affecting only connections via the RDP port, which is not open to external connection
4. SSH Weak Encryption Algorithms Supported: The identified component supporting weak encryption algorithms has now been removed.
5. Outdated jQuery library detected – The jQuery library is currently in the process of being upgraded. It should be noted that client side scripts within e-days have no access to unauthenticated data stores and individual vulnerabilities in the library as detailed at http://bit.ly/2Hk7M3E have been mitigated in e-days on a case by case basis. We believe the use of the old library does not present any risk to the security of the application or data.