

Security Improvements for a Complex Health Care Application

Tessolve-Case Study



About the Customer

GraphixAsset is a UK-based software company building iPhone and Android apps, designing and building web applications, computer graphics, point-of-sale and motion graphics.

Background

GraphixAsset developed the eMAR (electronic Medical Administration Record) system specifically for a national charity, providing services for people with learning disabilities throughout England. The application maintains MARs (Medical Administration Records) electronically. A web interface provides admin functions whilst end users access the system from their Android smart phone or tablet. GraphixAsset approached Tessolve to perform the security testing.

The Tessolve Technical Solution

Tessolve assureSECURE team tested the eMAR application's defense against an unauthorized attack and identified vulnerabilities that could potentially pose a security threat. Tessolve provided recommendations and guidelines for such threats, which help in protecting the confidentiality and integrity of personal data.

The eMAR web application penetration test was carried out with reference to the OWASP ASVS (Application Security Verification Standard). The Tessolve security experts created a customized security testing checklist for eMAR web application. After running 600+ security test cases, the Tessolve assureSECURE team came up with a list of serious security issues and assisted eMAR developers with fixes.

The eMAR android app penetration testing was performed with the reference to the OWASP Mobile security standard. Tessolve again created a customized checklist and performed in-depth android app security assessment from following three attack vector possibilities.

- Customer-side security assessment
- Server-side security assessment
- Communication level security assessment



Customer Benefits

- Tessolve introduced an efficient methodology for security testing.
- The Tessolve security assessment will improve business continuity.
- The fixes made will minimize Black Hat (malicious) attacks.
- The security assessment will help to protect clients, partners and third party's data.