LEGALINTELLIGENCE

Security Statement

by Comsec

Introduction

The partnership between legal Intelligence and Comsec originated several years ago. Since information security is a continuous development, Comsec performs regular security assessments to ensure that Legal Intelligence applies the latest security standards. As part of the multi-year collaboration, Comsec performed an application security assessment on the responsive website of Legal Intelligence (incorporating the Single Sign On facility). The test focused mainly at the application level since Sentia, the hosting company of Legal Intelligence, has ISO27001 procedures and automated test in place to guarantee information security at the infrastructural level. This security statement contains information about Comsec, the scope, the type of tests and the security statement. Appendix A elaborates more deeply into the general methodology.

About Comsec

As a leading Information security service provider, Comsec has been working for more than 25 years with leading organizations across the private and public sectors to overcome security challenges effectively. Comsec has developed sound methodologies for security testing on online applications. To accomplish security, Comsec applies state-of-the-art internal tools and guidelines using a dedicated team of application security specialists.

The applied security assessment methodology (see appendix A) is designed to enable thorough assessment and concrete risk evaluation. In a structured process, Comsec consultants combine techniques and tools used by hackers and security researches into an analyzed process that includes interviews, design reviews and security code reviews. This process enables detecting vulnerabilities and identifying possible attack scenarios for any technology or architecture. In order to complete the risk evaluation process, the results of the vulnerability assessment process are considered in light of the business impact.

Scope

Legal Intelligence requested Comsec, as a leading information security advisory group, to assess the security aspects of the responsive website, including the Single Sign On facility. To maintain a high level of security at code level, Legal Intelligence also asked Comsec to host a code review sessions with key developers and review the control assess policy at the headquarters of Legal Intelligence.

Type of Tests

Under the scope of the evaluation, the following elements were addressed in the security assessment:

- Business Validation Checks
  These checks are important in order to prevent unauthorized actions. For example, sending specially crafted requests to the application in order to perform unauthorized operations.
- Data Access Layer Protection & Data Validation
  Exploiting issues in the implementation of the web application's connectivity with its data sources. Example for vulnerabilities that could enable this attack vector is SQL Injection.

- Session Management
  Exploiting issues in the implementation of the session including:
  - Initialization of the session and generation of the session identifier
  - Representation and storage of session object on the server side
  - Representation and storage of session on the client side
  - Content (and encryption) of session identifiers
  - Session termination and timeout
- Authentication Mechanisms
  Exploiting issues in the authentication mechanism of the application, including issues such as:
  - Inability of the application to restrict anonymous access to sensitive resources

  - Missing protection of credentials
  - Unsafe implementation of the login and logout procedures
  - Insufficient Password policy and lockout mechanism
  - Exposing Error Messages in authentication pages

  This will be performed in order to obtain unauthorized access to various types of information and functions.

- Authorization Mechanism
  Exploiting issues in the authorization system in order to access restricted functions, information or interfaces. Examples for vulnerabilities that could enable this attack vector are insecure direct object reference vulnerabilities, failure to restrict URL access, missing authorization check.
- Memory Corruption and DoS

  Exploiting issues in the core components of the system or its framework, in order to derive the system to an unstable state and potentially crash it. In some cases this could also enable memory corruption in the application, and allow remote code execution.
- Combined Attacks and Attack Scenarios
  In real life scenarios, an attacker will combine various attack vectors together to a complex attack scenario.
- Protection against frequently detected vulnerabilities
  Such as injection, cross-site scripting, insecure direct object references, cross-site request forgery, security misconfiguration, insecure cryptographic storage, failure to restrict URL access, insufficient transport layer protection and invalidated redirects & forwards

Security Statement/Conclusion

Comsec hereby confirms to have collaborated with Legal Intelligence on testing and improving the security level of the online services offered by Legal Intelligence. In 2015, various tests were conducted following the general methodology as described in appendix A and the defined scope. To maintain security at code level, a code review was conducted with key developers.

Comsec states that the www.legalintelligence.com and the Single Sign On facility meets the latest security standards and that security is well addressed at code level.

Appendix A: Methodology for Application Security Testing

The Comsec methodology for application security assessments is designed to enable compressive and thorough assessment and concrete risk evaluation. In a structured process, Comsec consultant combines techniques and tools used by hackers and security researches into an analytical process including interviews, design reviews and security code reviews. The process enables detecting vulnerabilities and identifies possible attack scenarios efficiently from any given technology or architecture. The results of the vulnerability assessment process are considered in light of the business impact.

Application Security Assessment Test Process

The general methodology of the application security test will rely on several key activities:

1. Gathering information about the application by reviewing technical documents (design documents, functional descriptions, reports of previous tests performed, development documentation and others), interviews with developers and programmers, interactions with application owner and such.
2. Initial analysis of the application structure, interfaces, data flow, sensitive modules, infrastructure, business logic and concept.
3. Review of specific parts of the application in more details, based on a Top-Down analysis of sensitive and vulnerable application modules
4. Performing automated tests and various reviews to seek for bugs and security vulnerabilities using specialized Application Security Scanners and testing tools.
5. Review of specific parts in the application at the code level, based on a Top-Down analysis of sensitive and vulnerable application modules, such as authentication mechanisms, authorization mechanisms and more.
6. Performing manual examinations to search for bugs and security vulnerabilities according to specific attack scenarios, and performing tests in light of known application vulnerabilities. As scanning and automatic tools are unable to provide real business logic breaches, the Comsec team will constantly analyze the business impacts of the detected findings, whether discovered by an automated tool, hands-on code review or manual security tests.
7. Analysis of the gathered data and the results of the various checks. The analysis includes categorizing the detected vulnerabilities and prioritizing them according to the business and technical context of the application. Comsec methodology includes a systematic Security Risk Analysis & Evaluation process.
8. Report formulation; Documentation of the findings, the risk that result from them and initial recommendations for their mitigation. In addition, when needed, Comsec will provide supplementary technical information, including screenshots, URLs and more.

Application Security Assessment Test Methods

The following table presents a list of test and methods the will be included in the security assessment:

Test	Validation method
Input Validation Tests: Testing for Reflected XSS; Testing for presistance XSS; Testing for DOM based XSS testing for Flash based XSS;	Hand on Manual Test; Automated Scanning; Code review;
Password Policy: Password length, life time and complexity; implementation of forgot password interface; implementation of password reminder functions; implementation of password modification functions;	Hand on manual test; interviews; code Review;
Session Management: Testing for Session Fixation; Testing of storage of session on client and server side; Testing for content (and encryption) of session identifiers; Session termination and timeout; Testing of security of session cookies;	Hand on manual test; interviews; code Review;
Implementation of Secure Transport Layer Security	Hand on manual test; Automated Scanning;
Implantation of Cryptography: Key Management; storage cryptography materials; implementation of custom ciphers;	Hand on manual test; Code Review;
Authorization and Authentication: SSO Implementation; implementation authorization and authentication checks; Secure storage of credentials; Login Error Messages; Testing for path traversal; Testing for Privilege Escalation; Testing of the implementation of the authentication pages; Testing for authentication and authorization protocols (i.e. openID, OAuth, SAML) on all platforms.	Hand on manual test; Code Review; Automated Scanning;
Auditing Mechanism And Policies	Interviews; Hand on manual test;
Security of source code repositories: Access Restriction, authentication and authorization;	Interviews; Hand on manual test;
Implementation client-side defensive measures: CSRF protection tokens; ClickJacking protection; Frame Spoofing protections	Hand on manual test; Code Review;
Validation of business logic: General validation checks; Testing for Race Conditions;	Hand on manual test; Code Review;
Security of Internal Processes: Access Restriction, authentication and authorization;	Hand on manual test; Code Review; Automated Scanning; Interviews

Test	Validation method
Information Leakage: error messages; response headers; redundant code; remarked out HTML code;	Hand on manual test; Code Review; Automated Scanning;
Security Configuration: Inspection of configuration files of the application; review of the server configuration; review SSL settings; Testing for HTTP methods;	Hand on manual test; Automated Scanning; Interviews;
Injection Attacks: SQL Injection; LDAP Injection; XML Injection; Code Injection; HTTP Header injection;	Hand on manual test; Code Review; Automated Scanning;
Testing of File Upload Mechanism	Hand on manual test; Code Review; Automated Scanning;
Testing for Anti-Script and Anti Flood Mechanisms	Hand on manual test; Automated Scanning; Code Review;
Testing for or Mobile device Browser Cache	Hand on manual test; Automated Scanning;
Testing for Redundant Function: Testing for redundant code, backup, and old files;	Hand on manual test; Automated Scanning;
Testing For Public Access To Administrative Interfaces	Hand on manual test; Automated Scanning; Code Review;
Testing for Mobile app SSL certificate validation process	Hand on manual test; Code Review;
Testing for Mobile app integration in hybrid mobile-web environment	Hand on manual test; Code Review;
Testing implementation of Services API: Testing of interfaces such as XML-RPC, SOAP, REST and JSON.	Hand on manual test; Automated Scanning; Code Review;

These tests will also review protection against the OWASP[1] Top Ten vulnerabilities:

A1 Injection	A6 Sensitive Data Exposure
A2 Broken Authentication and Session Management	A7 Missing Function Level Access Control
A3 Cross-Site Scripting (XSS)	A8 Cross-Site Request Forgery (CSRF)
A4 Insecure Direct Object References	A9 Using Components with Known Vulnerabilities
A5 Security Misconfiguration	A10 Unvalidated Redirects and Forwards

[1] https://www.owasp.org/index.php/Main_Page