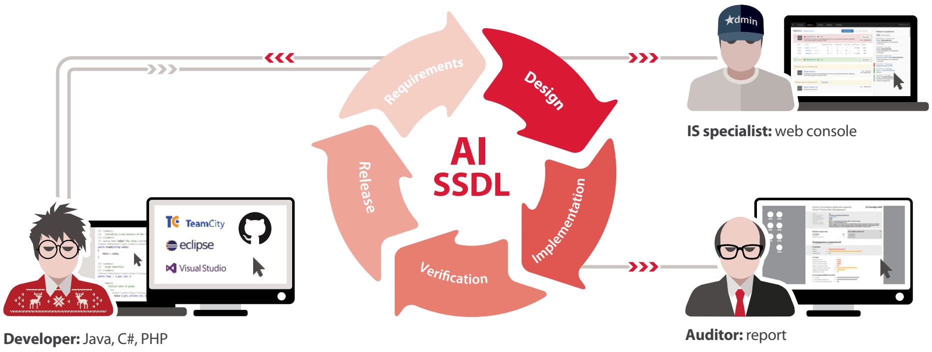
PT APPLICATION INSPECTOR SSDL EDITION™: BUILDING THE PROCESS OF SECURE DEVELOPMENT

Every field of industry—from financial and manufacturing enterprises to telecoms, IT companies, media, and government institutions—is increasingly reliant on applications for automation of daily operations. Official websites, e-commerce and e-banking platforms, workflow and reporting systems, and many other applications besides are designed to engage with customers, reduce the effort involved in routine tasks, and jump start efficiency.

However, increased functionality brings additional application complexity, making it harder to fix critical errors in the software. According to studies by Positive Technologies, all applications contain at least medium-severity vulnerabilities and 70% of them have one or more critical vulnerability. Using the same techniques as hostile hackers, our white-hat experts have demonstrated how these flaws can be exploited to gain access to corporate networks and confidential user data.

The main culprits behind these high levels of software flaws are insufficiently mature information security processes, lack of security awareness, and the absence of convenient tools for developers and IS services. These failings mean security audits happen rarely (if at all), and are typically left until the applications are ready to launch. But patching flaws at this stage is far more expensive than resolving them during the design and development phases.

PT Application Inspector SSDL Edition™ (PT AI SSDL™) is an advanced Application Security Testing solution that addresses the needs of the whole enterprise to resolve these problems. With transparent integration into existing development processes and tools, plus business intelligence features for management reporting and data analytics, PT AI SSDL™ fosters an AppSec-aware culture and supports high quality code testing at all stages of the application lifecycle.



IS specialist: web console

Developer: Java, C#, PHP

Auditor: report

HOW IT WORKS

At the heart of PT AI SSDL™ lies an advanced testing approach that combines the advantages of static (SAST), dynamic (DAST), and interactive code analysis (IAST), and which has proven its efficiency in PT AI Desktop Edition™. The use of multiple testing technologies means application security can remain a priority throughout all development stages—from the very first line of code to application go-live.

The distinguishing feature of PT AI SSDL™ is its flexible integration with corporate IT infrastructure and development and security tools such as Version Control Systems (VCS), Bug Trackers, Integrated Development Environments (IDE) and Continuous Integration (CI)/Build systems. Control panels that are adjustable to a specific process, and graphic interfaces especially designed for separate user roles support the implementation of SSDL processes from the ground up.

Positive Technologies experts are ready to provide methodological and practical assistance if needed.

BUSINESS BENEFITS

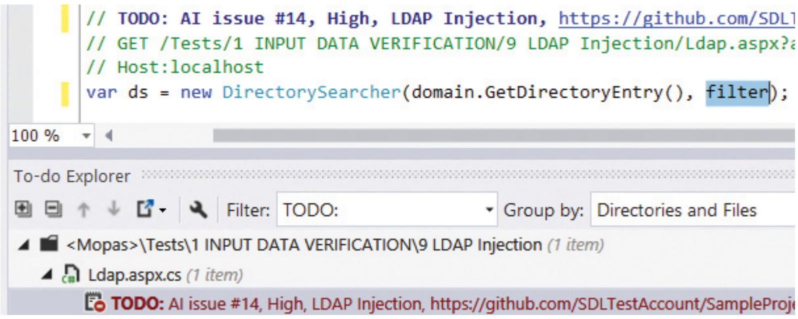
- **Enhance software quality levels.** The secure software development lifecycle (SSDL) supports the creation of high quality and sustainable applications. PT AI SSDL™ helps organizations to implement SSDL in both workflows and corporate culture.
- **Reduce development costs.** Automated vulnerability detection and elimination saves human resources, time, and most importantly reduces costs.
- **Mitigate risk and damage.** Detecting and eliminating vulnerabilities at every stage of development dramatically reduces the amount of errors and the costs of patching. This lowers risk and improves usability which, in turn, encourages user loyalty.
- **Drive operational efficiency.** PT AI SSDL™ helps developers to develop more secure software without being security experts, reducing the need for narrow profile specialists and encouraging teamwork with smooth business processes.
- **Manage compliance with regulatory requirements.** Many standards bodies now require app developers to detect and fix vulnerabilities before they can achieve certification. PT AI SSDL™ manages compliance with the requirements of PA DSS, PCI DSS and many other leading standards.

INFORMTION SECURITY BENEFITS

- **Wide coverage and in-depth analysis.** PT AI SSDL™ has an embedded database of software vulnerabilities and third-party libraries. Configuration verification capabilities also ensure web server settings are safe.
- **Automated vulnerability assessment.** PT AI SSDL™ automatically generates "exploits"—the most secure test queries that demonstrate exactly how hackers could use each vulnerability to attack an application. These requests help in confirming vulnerabilities, creating tasks to fix the code and following them up.
- **Continuous protection.** Many large-scale companies employ PT Application Inspector™ alongside PT Application Firewall™. Exploits generated by PT AI™ allow the firewall to create virtual patches and quickly protect applications while vulnerabilities are being fixed.
- **Simplified code acceptance.** PT AI SSDL™ is suitable for rapid analysis of third party or modified code. This drastically reduces application security testing expenses, as there is no need for manual operations.

DEVELOPMENT BENEFITS

The best interface is no interface. Developers interact with PT AI SSDL™ via fine-tuned development tools and the source code itself. Seamless integration with version control systems allows developers to transfer finished code for further analysis and view the results without leaving their familiar IDE and bug tracking systems. This enables continuous integration and delivery. Developers don't have to learn or access additional consoles or become distracted by outside systems. All detected problems and remediation recommendations can be found as an annotation to the source code.



```
// TODO: AI issue #14, High, LDAP Injection, https://github.com/SDLT
// GET /Tests/1 INPUT DATA VERIFICATION/9 LDAP Injection/Ldap.aspx?a
// Host:localhost
var ds = new DirectorySearcher(domain.GetDirectoryEntry(), filter);
```

To-do Explorer

Filter: TODO:

Group by: Directories and Files

- <Mopas>\Tests\1 INPUT DATA VERIFICATION\9 LDAP Injection *(1 item)*
  - Ldap.aspx.cs *(1 item)*
    - **TODO:** AI issue #14, High, LDAP Injection, https://github.com/SDLTestAccount/SampleProje

Microsoft Visual Studio IDE and code annotation with a detected vulnerability

PT AI SSDL™: A SOLUTION FOR THE ENTIRE TEAM

- **Role-based access control (RBAC).** Each group of users (developers, security managers, auditors, and administrators) is granted a suitable level of access to data and interacts with PT AI SSDL™ via an interface that is relevant to their particular role.
- **Analytics and business intelligence.** Using PT AI SSDL™, analysts can perform both qualitative and quantitative code security assessments, discover trends, check theories, and perform benchmarking between several projects. For their part, security managers and auditors are able to measure the KPIs of the development process and control team efficiency.
- **Flexible reporting and notifications.** Every team member receives notifications and reports that are tailored to their role. This functionality is powered by the PT AI SSDL™ query builder that retrieves data based on a query, a schedule, or as a response to a certain event. Reports are displayed in the control panel or sent by email.
- **Manufacturer independence.** PT AI SSDL™ adapts to the unique requirements of each organization or project without any need to submit frequent feature or change requests to the vendor. New releases of PT AI SSDL™ will retain custom changes and ensure backward compatibility.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com