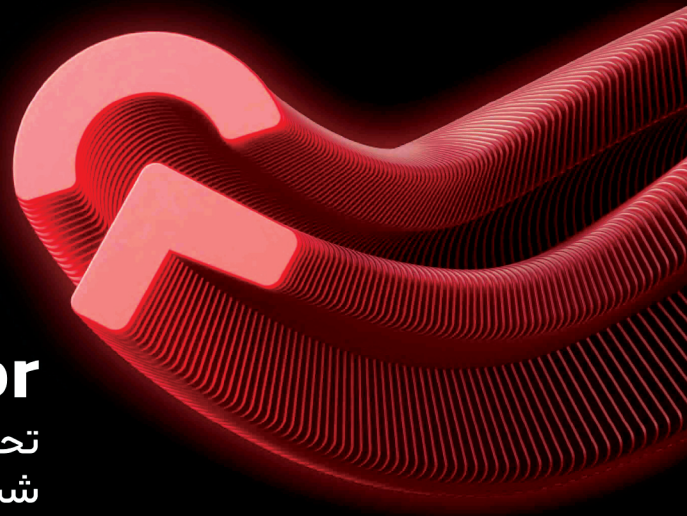


Application Inspector

تحلیل کد منبع.
شناسایی دقیق آسیب پذیری ها.
یکپارچه سازی با فرآیندهای توسعه فعلی.

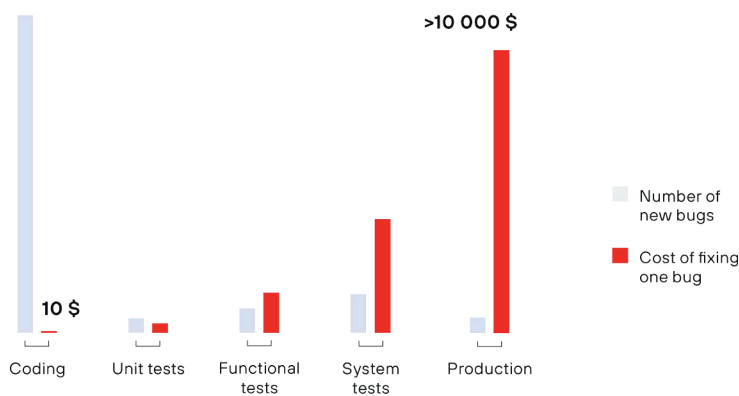


یک ابزار برای شناسایی آسیب پذیری ها
هم در کد منبع و هم در برنامه در حال
اجرا است و با حذف آن ها در مراحل اولیه،
از فرآیند توسعه امن پشتیبانی می کند.

برنامه های وب همچنان یک هدف محبوب برای مهاجمان باقی مانده اند. تحقیقات ما نشان می دهد که از هر
پنج حمله، یکی به منابع وب سازمان ها هدف گیری شده است، که اغلب این حملات به نهادهای دولتی و
مالی، خدمات آنلاین، مراکز علمی و آموزشی، و شرکت های IT انجام می شود.

مهاجمان از آسیب پذیری های موجود بهره برداری می کنند: به طور میانگین، هر برنامه شامل بیش از دو ده
آسیب پذیری است که یک پنجم آن ها حیاتی محسوب می شود. اگر مهاجمان از این آسیب پذیری ها استفاده
کنند، شرکت ممکن است با ریسک های مالی و اعتباری جدی مواجه شود: سرقت داده های مهم، نفوذ به
زیرساخت ها، زمان های توقف، یا حتی خاموشی کامل سیستم های اطلاعاتی.

بیشتر آسیب پذیری ها در کد منبع وجود دارند و بهتر است که در مراحل اولیه توسعه برنامه ها حذف شوند.
این روش بسیار موثرتر از حذف آسیب پذیری ها در مرحله عملیاتی است.



هزینه رفع نقص در مراحل مختلف چرخه عمر برنامه

مزایای PT Application Inspector

ترکیب چهار نوع تحلیل: PT Application Inspector شامل تحلیل آماری (SAST)، پویا (DAST)، تعاملی (IAST)، و تحلیل
اجزای جانبی (SCA) است. این ترکیب بیشترین تعداد آسیب پذیری ها را پوشش می دهد و سیستم فیلترگذاری انعطاف پذیر
امکان اولویت بندی آسیب پذیری ها را بر اساس میزان بحرانی بودن فراهم می کند.

تولید اکسپلویت های آزمایشی: این ابزار اکسپلویت های آزمایشی برای بررسی امکان بهره برداری از آسیب پذیری تولید
می کند. با در نظر گرفتن قواعد گرامری و آزمون فازی در محیط اجرا، هزینه های تیم های توسعه برای تأیید آسیب
پذیری ها را کاهش می دهد.

سیستم لایسنس دهی راحت و شفاف: سیستم لایسنس دهی به گونه ای طراحی شده که امکان مشارکت کل تیم را
در تعداد نامحدودی از پروژه ها فراهم می سازد.



Supported languages:

Java, PHP, C#, Visual Basic .NET, JavaScript, TypeScript, Python, Kotlin, Go, C/C++, Objective-C, Swift, SQL (T-SQL, PL/SQL, MySQL)

Deployment:

Linux + Docker containers + SSO (SAML, OpenID Connect, LDAP)

CI/CD integration:

Jenkins, TeamCity, GitLab CI (CLI), Azure

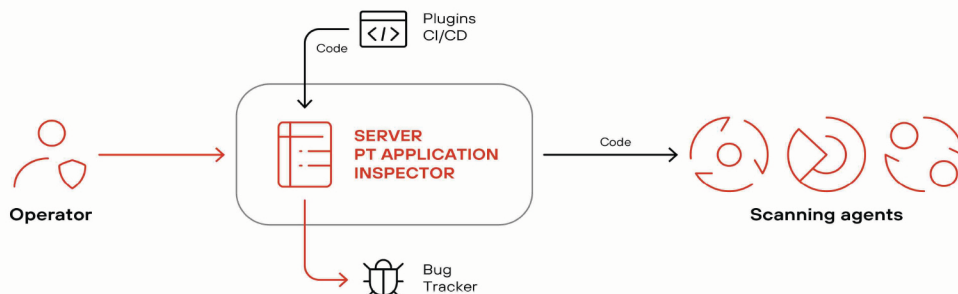
IDE integration:

JetBrains, Visual Studio Code

Bug tracker integration:

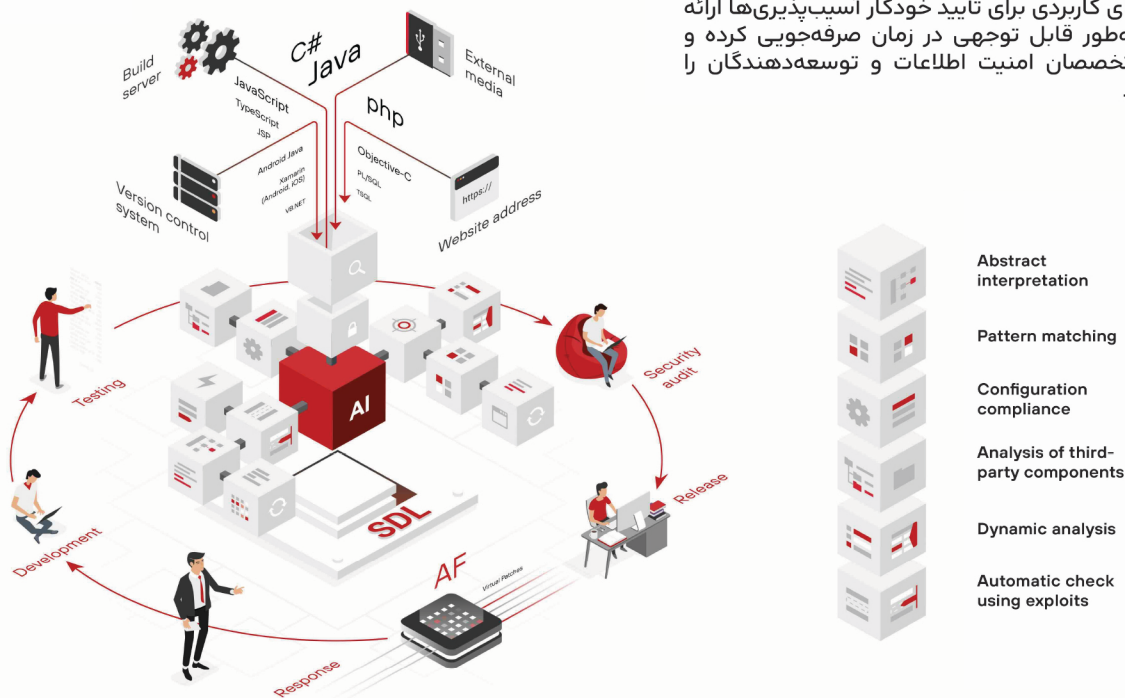
API: REST API (Swagger)

PT Application Inspector به طور موثر در فرآیندهای توسعه یکپارچه می شود. این ابزار از یکپارچگی با Jenkins، TeamCity، GitLab CI و **Azure پشتیبانی می کند و دارای مدل کنترل دسترسی مبتنی بر نقش و پلاگین های آماده برای اتصال به سیستم های ساخت و تحویل برنامه، باگ ترکرها، و محیط های توسعه (IDE) است.



طرح یکپارچه سازی PT Application Inspector در فرآیند توسعه موجود

How it works



Info@parspouya.com
Info@ptsecurity.info

ویرا ارتباط پارس پویا
آدرس: تهران، خیابان شریعتی، دوراهی قلهک
کوچه مرشدی، پلاک ۲، واحد ۲
تلفن: ۰۲۱-۷۵۳۹۷۰ داخلی ۲۰۰ و ۲۰۰۰