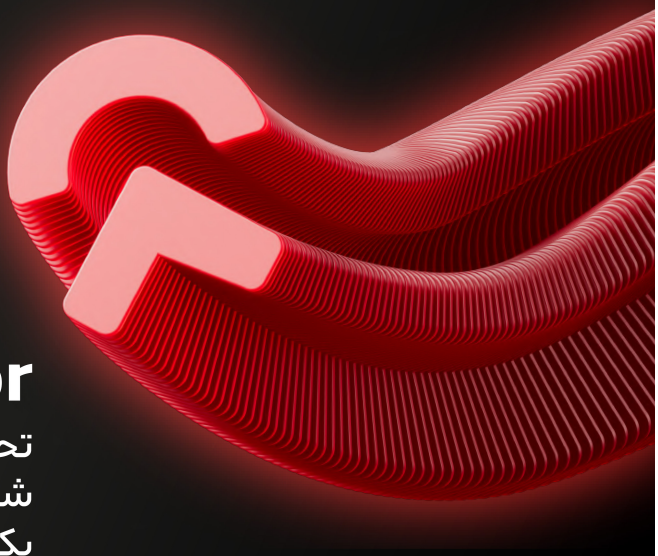
positive technologies



Application Inspector

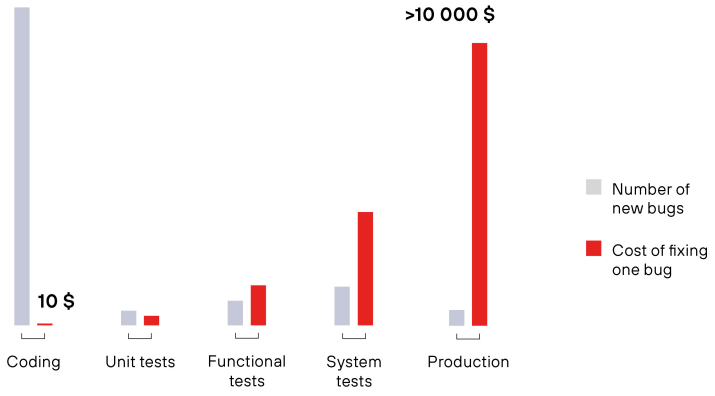
تحلیل کد منبع.
شناسایی دقیق آسیب‌پذیری‌ها.
یکپارچه‌سازی با فرآیندهای توسعه فعلی.

یک ابزار برای شناسایی آسیب‌پذیری‌ها هم در کد منبع و هم در برنامه در حال اجرا است و با حذف آن‌ها در مراحل اولیه، از فرآیند توسعه امن پشتیبانی می‌کند.

برنامه‌های وب همچنان یک هدف محبوب برای مهاجمان باقی مانده‌اند. تحقیقات ما نشان می‌دهد که از هر پنج حمله، یکی به منابع وب سازمان‌ها هدف‌گیری شده است، که اغلب این حملات به نهادهای دولتی و مالی، خدمات آنلاین، مراکز علمی و آموزشی، و شرکت‌های IT انجام می‌شود.

مهاجمان از آسیب‌پذیری‌های موجود بهره‌برداری می‌کنند: به‌طور میانگین، هر برنامه شامل بیش از دو ده آسیب‌پذیری است که یک‌پنجم آن‌ها حیاتی محسوب می‌شود. اگر مهاجمان از این آسیب‌پذیری‌ها استفاده کنند، شرکت ممکن است با ریسک‌های مالی و اعتباری جدی مواجه شود: سرقت داده‌های مهم، نفوذ به زیرساخت‌ها، زمان‌های توقف، یا حتی خاموشی کامل سیستم‌های اطلاعاتی.

بیشتر آسیب‌پذیری‌ها در کد منبع وجود دارند و بهتر است که در مراحل اولیه توسعه برنامه‌ها حذف شوند. این روش بسیار موثرتر از حذف آسیب‌پذیری‌ها 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 آسیب‌پذیری‌ها را پوشش می‌دهد و سیستم فیلترگذاری انعطاف‌پذیر امکان اولویت‌بندی آسیب‌پذیری‌ها را بر اساس میزان بحرانی بودن فراهم می‌کند.

تولید اکسپلویت‌های آزمایشی: این ابزار اکسپلویت‌های آزمایشی برای بررسی امکان بهره‌برداری از آسیب‌پذیری تولید می‌کند. با در نظر گرفتن قواعد گرامری و آزمون فازینگ در محیط اجرا، هزینه‌های تیم‌های توسعه برای تأیید آسیب پذیری‌ها را کاهش می‌دهد.

سیستم لایسنس‌دهی راحت و شفاف: سیستم لایسنس‌دهی به‌گونه‌ای طراحی شده که امکان مشارکت کل تیم را در تعداد نامحدودی از پروژه‌ها فراهم می‌سازد.

نسخه آزمایشی رایگان

آسیب‌پذیری‌های موجود در کد خود را بررسی کنید – پروژه آزمایشی رایگان PT Application Inspector را سفارش دهید.

PT Application Inspector به‌طور موثر در فرآیندهای توسعه یکپارچه می‌شود. این ابزار از یکپارچگی با GitLab CI، TeamCity، Jenkins، و Azure** پشتیبانی می‌کند و دارای مدل کنترل دسترسی مبتنی بر نقش و پلاگین‌های آماده برای اتصال به سیستم‌های ساخت و تحویل برنامه، باگ ترکرها، و محیط‌های توسعه (IDE) است.

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

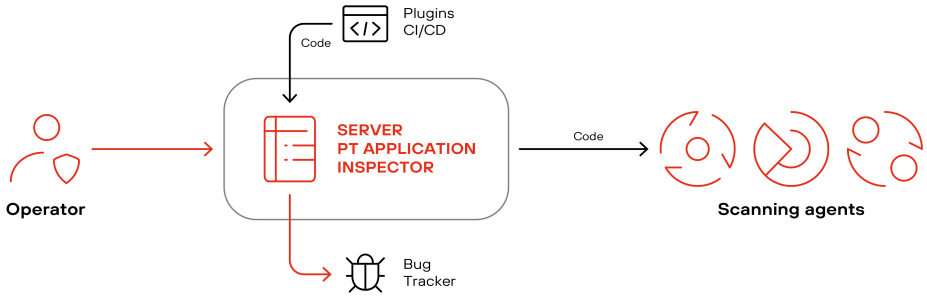
Deployment: Linux + Docker containers + SSO (SAML, OpenID Connect, LDAP)

CI/CD integration: Jenkins, TeamCity, GitLab CI (CLI), Azure

IDE integration: JetBrains, Visual Studio Code

Bug tracker integration: Jira

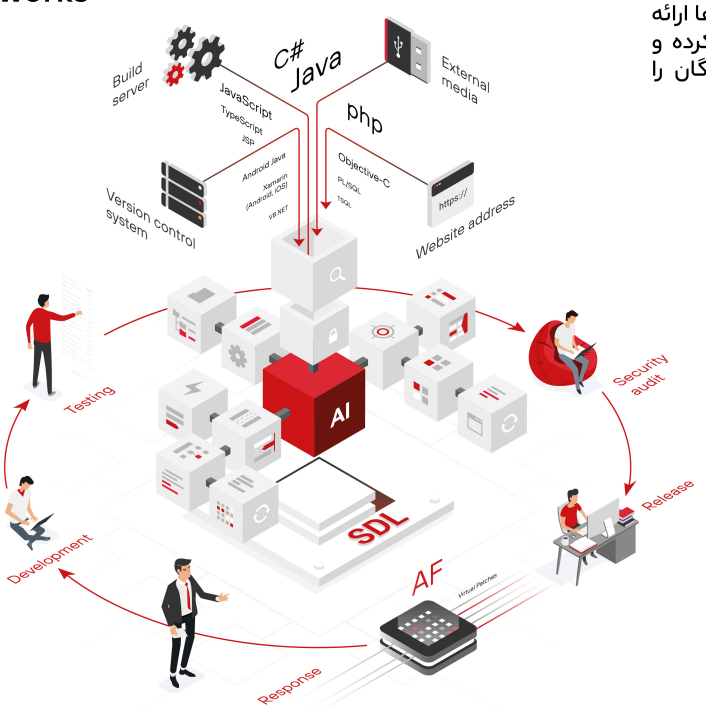
API: REST API (Swagger)

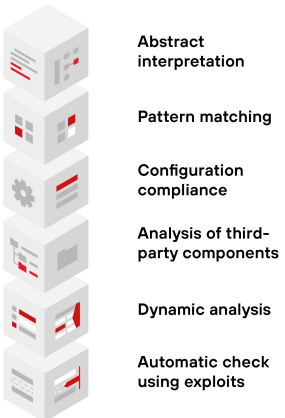


طرح یکپارچه‌سازی PT Application Inspector در فرآیند توسعه موجود

How it works

PT Application Inspector تنها تحلیلگر کد منبع در بازار روسیه است که ابزارهای کاربردی برای تأیید خودکار آسیب‌پذیری‌ها ارائه می‌دهد، که به‌طور قابل توجهی در زمان صرفه‌جویی کرده و تعامل بین متخصصان امنیت اطلاعات و توسعه‌دهندگان را تسهیل می‌کند.





- Abstract interpretation
- Pattern matching
- Configuration compliance
- Analysis of third-party components
- Dynamic analysis
- Automatic check using exploits

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com

Positive Technologies یک ارائه‌دهنده پیشرو جهانی در راهکارهای امنیت اطلاعات است. بیش از ۳٬۳۰۰ سازمان در سراسر جهان از فناوری‌ها و خدمات توسعه‌یافته توسط شرکت ما استفاده می‌کنند. در طول ۲۰ سال گذشته، مأموریت ما مقابله با اقدامات هکرها قبل از وارد آمدن آسیب غیرقابل‌قبول به کسب‌وکارها یا صنایع مختلف بوده است.

Positive Technologies اولین و تنها شرکت امنیت سایبری در روسیه است که در بورس مسکو (MOEX: POSI) عمومی شده است. ما را در شبکه‌های اجتماعی (Habr، Twitter) و بخش اخبار در ptsecurity.com دنبال کنید.

آیا شرکت شما تحت حمله قرار گرفته است؟

شبکه و محیط خارجی خود را بررسی کنید.برای درخواست آزمایشی رایگان PT ، با ما تماس بگیرید.

pt@magsaco.ir

درباره Positive Technologies

Positive Technologies یکی از ارائه‌دهندگان برتر راهکارهای ارزیابی آسیب‌پذیری، مدیریت تطبیق و تحلیل تهدیدات به بیش از ۳,۰۰۰ مشتری در سطح جهانی است. راهکارهای ما به‌طور یکپارچه در سراسر کسب‌وکار شما کار می‌کنند: حفاظت از برنامه‌ها در حال توسعه، ارزیابی آسیب‌پذیری‌های شبکه و برنامه‌ها، اطمینان از تطبیق با الزامات قانونی و مسدودسازی حملات در زمان واقعی. تعهد ما به مشتریان و پژوهش‌ها به Positive Technologies شهرتی به عنوان یکی از معتبرترین مراجع در امنیت SCADA، بانکداری، مخابرات، برنامه‌های وب و ERP داده است و در گزارش IDC به عنوان سریع ترین شرکت در حال رشد در مدیریت امنیت و آسیب‌پذیری در سال ۲۰۱۲ شناخته شده است. برای اطلاعات بیشتر درباره Positive Technologies، به سایت ptsecurity.com مراجعه کنید.

منبع: پیش‌بینی جهانی مدیریت امنیت و آسیب‌پذیری IDC 2013–2017 و سهم فروشندگان در سال ۲۰۱۲، سند شماره 242465، آگوست ۲۰۱۳. بر اساس رشد درآمد سالانه در سال ۲۰۱۲ برای فروشندگانی با درآمد بیش از ۲۰ میلیون دلار.

MAGSA magsaco.ir شرکت مگسا (مهندسی گسترش سامانه امن) یکی از شرکت های با سابقه و فعال در حوزه امنیت فضای تولید و تبادل اطلاعات است که در سال ۱۳۸۲ شکل گرفت و در سال ۱۳۸۴ تاسیس شد. حوزه های اصلی فعالیت این شرکت با دو رویکرد اصلی است.

رویکرد فنی امنیت که شامل امنیت نرم افزار، امنیت شبکه، امنیت اطلاعات و امنیت زیرساختهای صنعتی است. رویکرد مدیریت امنیت که شامل طراحی طرحهای جامع امنیت شبکه، طرح جامع امنیت سایبر، ارزیابی سطح بلوغ امنیت سایبری و پیاده سازی سیستم مدیریت امنیت اطلاعات است. طی دو دهه گذشته، خدمات گوناگونی در هر دو حوزه توسط شرکت به سازمانها، نهادها، شرکت ها و سایر مشتریان شرکت ارائه شده است.

درحال حاضر مگسا به عنوان شرکت توزیع کننده محصولات PT در ایران فعالیت میکند

شرکت Positive Technologies

Positive Technologies پیشرو در صنعت امنیت سایبری و ارائه‌دهنده جهانی راهکارهای امنیت اطلاعات است.

ماموریت ما: حفاظت از کسب‌وکارها و صنایع مختلف در برابر حملات سایبری و آسیب‌های غیرقابل‌تحمل.

بیش از ۳,۳۰۰ سازمان در سراسر جهان از فناوری‌ها و خدمات توسعه‌یافته توسط شرکت ما استفاده می‌کنند.

ptsecurity.com