НЕПРЕРЫВНАЯ БЕЗОПАСНОСТЬ ДЛЯ НЕПРЕРЫВНОЙ ПОСТАВКИ: ПОРТАЛ «ФАБРИКАНТ» АВТОМАТИЗИРОВАЛ ПРИЕМКУ КОДА С ПОМОЩЬЮ PT APPLICATION INSPECTOR

«Доступность и безопасность площадки "Фабрикант", которую ежедневно посещают тысячи людей, является для нас приоритетом. Злоумышленники постоянно совершенствуют свои методы, поэтому мы искали такие инструменты, которые не только помогут нам оперативно анализировать исходный код приложения, но и обеспечат защиту от атак на время исправления ошибок. Интеграция PT Application Inspector и PT Application Firewall в production-окружение позволила нам минимизировать влияние процессов ИБ на скорость разработки новой функциональности и обеспечить защиту портала от современных киберугроз».

Илья Мальцев, руководитель отдела информационной безопасности торгового портала «Фабрикант»

НЭП — Фабрикант

ПРОФИЛЬ ОРГАНИЗАЦИИ

- **Название:** «Фабрикант»
- **Группа компаний:** «НЭП-Фабрикант»
- **Отрасль:** электронные торги
- **Занимает ведущие позиции:** топ-2 на рынке корпоративных торгов; топ-3 в торгах по банкротству; топ-5 крупнейших ЭТП по 223-ФЗ.
- **Задача:** автоматизированное выявление уязвимостей через внедрение безопасности в процессы непрерывной интеграции и поставки (CI/CD), защита работающих приложений
- **Решение:** анализатор исходного кода PT Application Inspector и межсетевой экран уровня приложений PT Application Firewall
- **Результат:** процесс поиска уязвимостей автоматизирован и встроен в процесс непрерывной интеграции; обеспечена защита работающих приложений через патчинг уязвимостей до их исправления

Электронная торговая площадка «Фабрикант» (fabrikant.ru) входит в группу компаний «НЭП-Фабрикант». Портал «Фабрикант» 12 лет успешно работает в торгово-закупочной отрасли, являясь лидером рынка электронных торговых систем и центром профессиональных компетенций в проведении конкурентных закупочных процедур. Он объединяет более 570 000 компаний из различных отраслей экономики. С его помощью более десяти тысяч поставщиков товаров и услуг находят своих заказчиков и расширяют рынки сбыта. Ежедневно площадку посещают в среднем 55 000 человек.

ЗАДАЧА

Электронные торговые площадки привлекают не только участников торгов, но и киберпреступников. Хранящаяся информация — данные заказчиков и поставщиков, информация о счетах, заявки, протоколы торгов и другие конфиденциальные документы и данные — все это представляет интерес для злоумышленников. Согласно отчету Verizon 2017 Data Breach Investigations Report, атаки на веб-приложения — основная причина всех утечек данных и денег.

Как показали исследования Positive Technologies, проведенные в 2016 году, в 77% случаев сетевой периметр можно преодолеть из-за уязвимостей веб-приложений. В 94% случаев уязвимости позволяли атаковать пользователей приложений, в 20% случаях — получить доступ к базам данных. При успешной атаке злоумышленники могут получить полный контроль над приложением и его исходным кодом, а также доступ к персональным данным и другой конфиденциальной информации.

У «Фабриканта» собственная команда разработчиков, в задачи которой входят улучшение сервиса и добавление новой функциональности. Специалисты по информационной безопасности периодически проводили ручной анализ защищенности веб-приложения. Однако при таком подходе результаты быстро теряли актуальность из-за регулярных обновлений портала. В связи с этим встала необходимость максимально автоматизировать проверку кода и внедрить ее в процесс разработки ПО, а также закрыть риски эксплуатации уязвимостей в работающем приложении, пока разработчики их устраняют.

Решение этих задач требует серьезного подхода к выбору средств защиты. В ходе поиска специалисты «Фабриканта» остановились на комплексном предложении Positive Technologies по защите приложений на базе PT Application Inspector и PT Application Firewall.

ПРЕИМУЩЕСТВО РЕШЕНИЯ

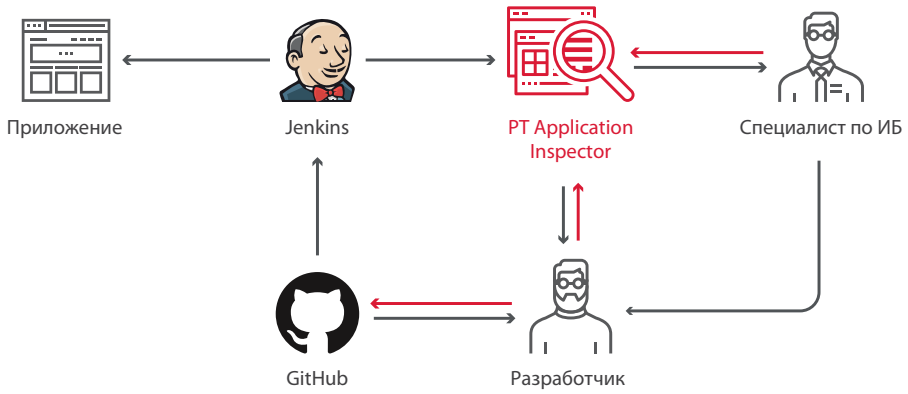
- **Непрерывная безопасность.** Бесшовная интеграция PT Application Inspector и PT Application Firewall для всесторонней защиты в реальном времени.
- **Целенаправленная защита.** Анализ исходного кода при помощи PT Application Inspector, интегрированного с PT Application Firewall для автоматической блокировки атак на найденные уязвимости.
- **Снижение затрат благодаря своевременным исправлениям.** Быстрое и точное обнаружение уязвимостей с рекомендациями по исправлению для разработчиков.
- **Выше эффективность бизнес-процессов.** Гибкий подход, позволяющий экономить время и ресурсы.

РЕШЕНИЕ

Сотрудничество с Positive Technologies началось в 2016 году с пилотного проекта, итогом которого стало внедрение PT Application Inspector и PT Application Firewall.

Анализатор защищенности исходного кода приложений PT Application Inspector сочетает методы статического (SAST), динамического (DAST) и интерактивного (IAST) анализа, что значительно снижает количество ложных срабатываний. Такой подход дает возможность специалистам по безопасности и команде разработки работать только с актуальными угрозами. Для проверки найденных уязвимостей PT Application Inspector формирует тестовые запросы, которые помогают подтвердить возможность эксплуатации этих уязвимостей злоумышленником, а также определить условия выполнения атаки.

Площадка «Фабрикант» построена на базе микросервисной архитектуры, состоящей более чем из 100 независимых друг от друга внутренних сервисов. Учитывая такое большое количество регулярно обновляемых сервисов, для автоматизации процесса тестирования исходного кода PT Application Inspector был внедрен в сам процесс сборки приложений путем объединения с системой непрерывной интеграции.



РЕЗУЛЬТАТЫ

Интеграция PT Application Inspector в процесс разработки и использование анализатора в связке с PT Application Firewall позволили специалистам «Фабриканта» автоматизировать аудит кода, сократить время на верификацию уязвимостей, исправление или патчинг, вырабатывать рекомендации для разработчиков по устранению выявленных уязвимостей. В результате ускорился процесс разработки и развертывания приложений, а также появилась возможность развивать площадку согласно требованиям по информационной безопасности, не нарушая текущих процессов разработки.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays