Kaspersky Application Security Assessment

kaspersky

Независимо от того, разрабатываете ли вы корпоративные приложения своими силами или приобретаете их у сторонних разработчиков, вы наверняка знаете, что одна-единственная ошибка в коде может привести к возникновению уязвимости, в результате которой вы подвергнетесь атакам, наносящим значительный финансовый или репутационный ущерб.

Новые уязвимости могут возникать и в процессе жизненного цикла приложения, в результате обновления программного обеспечения или небезопасной конфигурации компонентов, а также в результате применения новых методов атак.

Сервисы «Лаборатории Касперского» по оценке безопасности приложений позволяют выявить уязвимости в приложениях любого типа - от крупных облачных решений, ERP-систем, онлайн-банкинга и других специфических бизнес-приложений до встроенных и мобильных приложений на различных платформах (iOS, Android и других).

Преимущества сервиса

Сервис Kaspersky Application Security Assessment помогает владельцам и разработчикам приложений:

- Избежать финансовых, операционных и репутационных потерь благодаря проактивному обнаружению и устранению уязвимостей, используемых в атаках на приложения
- Сократить расходы на устранение уязвимостей, обнаружив их в приложениях, находящихся на стадии разработки и тестирования, до того, как они попадут в пользовательскую среду, где их устранение может привести к значительным сбоям и затратам.
- Поддержка жизненного цикла разработки безопасного программного обеспечения (S-SDLC), направленного на создание и поддержку безопасных приложений.

Сочетая практические знания и опыт с лучшими мировыми практиками, наши эксперты обнаруживают недостатки в системах безопасности, которые могут подвергнуть вашу организацию таким угрозам, как:

Утечка конфиденциальной информации

Проникновение и изменение данных и систем

Инициирование атак типа «отказ в обслуживании»

Совершение мошеннических действий

Следуя нашим рекомендациям, можно устранить выявленные в приложениях уязвимости и предотвратить подобные атаки.

Состав сервиса

Проверяемые приложения могут включать официальные веб-сайты и бизнес-приложения, стандартные или облачные, в том числе встроенные и мобильные.

Сервис предоставляется в соответствии с вашими потребностями и спецификой приложения и могут включать в себя:

- тестирование «черного ящика» – эмуляция внешнего злоумышленника
- тестирование методом «серого ящика» – эмуляция легитимных пользователей с различными профилями и анализ бизнес-логики приложения
- тестирование «белого ящика» – анализ с полным доступом к приложению, включая исходные коды; этот подход является наиболее эффективным с точки зрения выявления количества уязвимостей.
- Если для защиты приложений используются системы Web Application Firewall (WAF), они могут быть переведены в режим мониторинга или активированы и реагировать на атаки (в этом случае работа ведется в два этапа: с отключенной защитой и в активном режиме для проверки выявленных находок).

Подход "Лаборатории Касперского" к анализу безопасности приложений

Анализ защищенности приложений проводится экспертами "Лаборатории Касперского" как вручную, так и с использованием автоматизированных инструментов, с полным соблюдением конфиденциальности, целостности и доступности ваших систем и в строгом соответствии с международными стандартами и лучшими практиками, такими как:

- Классификация угроз Консорциума по безопасности веб-приложений (WASC)
- Руководство по тестированию веб-безопасности OWASP
- Руководство по тестированию мобильной безопасности OWASP
- Другие стандарты, в зависимости от сферы деятельности и местоположения вашей организации.

Члены команды проекта – опытные профессионалы, обладающие глубокими и актуальными практическими знаниями в данной области, включая различные платформы, языки программирования, фреймворки, уязвимости и методы атак. Они выступают на ведущих международных конференциях и оказывают консультационные услуги по вопросам безопасности крупнейшим поставщикам приложений и облачных сервисов, включая Oracle, Google, Apple, Facebook и PayPal.

Варианты оказания сервиса

В зависимости от типа услуг по оценке безопасности, специфики систем и ваших требований к условиям работы, сервис может предоставляться удаленно.

Результаты

Уязвимости, которые могут быть выявлены с помощью Kaspersky Application Security Assessment, включают:

- Недостатки в аутентификации и авторизации, включая многофакторную аутентификацию
- Инъекции кода (SQL Injection, OS Commanding и т.д.)
- Логические уязвимости, приводящие к мошенничеству
- - Уязвимости на стороне клиента (межсайтовый скриптинг, подделка межсайтовых запросов и т. д.)
- Использование слабой криптографии
- Уязвимости в клиент-серверных коммуникациях
- Небезопасное хранение или передача данных, например, отсутствие маскировки PAN в платежных системах
- Недостатки конфигурации, в том числе приводящие к сеансовым атакам
- Раскрытие чувствительной информации
- Другие уязвимости веб-приложений, приводящие к угрозам, перечисленным в WASC Threat Classification v2.0 и OWASP Top Ten.

Результаты предоставляются в виде итогового отчета, включающего подробную техническую информацию о процессах оценки, результатах, выявленных уязвимостях и рекомендациях по их устранению, а также резюме с описанием последствий для руководства. При необходимости могут быть подготовлены видеоролики и презентации для вашей технической команды или высшего руководства.

Новости о киберугрозах: www.securelist.ru
Новости IT-безопасности: business.kaspersky.ru
Кибербезопасность для малого и среднего бизнеса: kaspersky.ru/business
Кибербезопасность для крупных предприятий: kaspersky.ru/enterprise

www.kaspersky.ru

#kaspersky
#активируйбудущее