Лабораторная работа № 3 «Тестирование безопасности и производительности»
(2 часа)

Цель работы: Изучение принципов стратегии и программного обеспечения по тестировании безопасности и производительности.

1 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Основные цели тестирования безопасности:

1. Обеспечение безопасности онлайн-транзакций
2. Защита конфиденциальной информации от несанкционированного доступа
3. Минимизация риска утраты, искажения или хищения данных
4. Увеличение сопротивления DoS-атакам

Для достижения целей безопасности наши специалисты выполняют аудит потенциальных угроз с учетом специфики программного обеспечения и используют оптимальные методы тестирования безопасности.

Результаты тестирования безопасности

Мы стремимся обеспечить ясность результатов и процессов тестирования для наших клиентов. Вы получите:

1. Полный перечень угроз безопасности и уязвимостей тестируемого ПО
2. Подробный отчет о проведенных тестах

Аудит защищенности бизнес приложений.

Анализ бизнес-приложений позволит получить независимую профессиональную оценку защищенности критичных информационных активов и подробные рекомендации по повышению их безопасности.

Критичная для бизнеса информация, интересная злоумышленникам, обычно хранится и обрабатывается в таких информационных системах, как различные веб-приложения, СУБД, ERP. Это сложные корпоративные приложения, аудит которых должен проводиться отдельно, так как необходимо учитывать специфику каждого приложения и использовать соответствующие модели нарушителя.

Когда следует проводить аудит приложений?

- Для уже используемых критичных приложений – с выбранной периодичностью либо при внесении изменений;
- Перед запуском в эксплуатацию нового бизнес-приложения;
- При добавлении надстроек к существующим приложениям;
- В случае инцидента ИБ, связанного с функционированием приложения, и при подозрении на некорректную работу приложения с точки зрения ИБ.

Рассмотрим типы приложений требующих проведения аудита безопасности.

SAP-системы – обеспечение защищенности корпоративных систем управления ресурсами предприятия (ERP-систем) является одной из важнейших задач служб информационной безопасности современных компаний.

СУБД Oracle – анализ защищенности корпоративных сетей все чаще показывает, что в целом уровень безопасности заметно возрос, однако ряду проблем до сих пор не уделяется должного внимания. Одна из них – это защищенность корпоративных систем управления базами данных (СУБД).

Системы ДБО – система дистанционного банковского обслуживания является ключевым ресурсом банка, безопасности которого следует уделять особое внимание.

Мобильные приложения – использование мобильных телефонов стало повсеместным и повседневным. ПО, которое раньше было доступно только на компьютере, сейчас доступно и на телефоне.

Интеграционные шины (Enterprise Service Bus, ESB) позволяют реализовать обмен данными как между внутренними системами, такими как ERP или АБС, так и между компаниями-партнерами.

Встроенные системы (Embedded) – компьютерные системы, предназначенные для выполнения определенных специфичных задач.

Исходный код – в настоящие время большинство атак происходит на уровне приложений. Поэтому безопасность программного обеспечения имеет наивысший приоритет. В особенности это относится к заказной разработке.

Веб-приложения – веб-приложения больше других подвержены угрозам безопасности, так как по определению доступны из сети Интернет.

2 ЗАДАНИЕ

1. Изучить теоретические сведения
2. Подготовить отчет, который должен содержать цель, задание, краткие теоретические сведения, выводы по работе.

3 ТРЕБОВАНИЕ К ОТЧЕТУ

В отчете должны быть отображены следующие пункты:

1. Задание.
2. Краткие теоретические сведения по тестированию безопасности и производительности. Подготовить реферат о современных подходах, методах и инструментах по проведению тестирования.
3. Выводы.

4 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите основные цели тестирования безопасности программного обеспечения.
2. Типы приложений требующих проведения аудита безопасности.
3. Перечислите основные виды уязвимости в безопасности программного обеспечения.
4. Перечислите основные этапы тестирования производительности.
5. Перечислите дополнительные виды тестирования производительности.