

Лабораторная работа № 11-12

Тестирование безопасности

Цель: получение навыков тестирования безопасности информационной системы.

Теоретические вопросы

Тестирование восстановления.

Тестирование безопасности.

Технологии тестирования безопасности.

Тестирование безопасности – оценка уязвимости программного обеспечения к различным атакам.

Компьютерные системы очень часто являются мишенью незаконного проникновения. Под проникновением понимается широкий диапазон действий: попытки хакеров проникнуть в систему из спортивного интереса, месть рассерженных служащих, взлом мошенниками для незаконной наживы. Тестирование безопасности проверяет фактическую реакцию защитных механизмов, встроенных в систему, на проникновение. В ходе тестирования безопасности испытатель играет роль взломщика. Ему разрешено все:

- попытки узнать пароль с помощью внешних средств;
- атака системы с помощью специальных утилит, анализирующих защиты;
- подавление, ошеломление системы (в надежде, что она откажется обслуживать других клиентов);
- целенаправленное введение ошибок в надежде проникнуть в систему в ходе восстановления;
- просмотр несекретных данных в надежде найти ключ для входа в систему.

При неограниченном времени и ресурсах хорошее тестирование безопасности взломает любую систему. Задача проектировщика системы – сделать цену проникновения более высокой, чем цена получаемой в результате информации.

Задание № 1. Изучите и опишите одно из средств выявления уязвимостей:

Таблица 1. Обзор средств выявления уязвимостей, работающих на уровне кода

Наименование средства	Назначение	Поддерживаемые языки программирования	Примечание
Иностранные средства выявления уязвимостей			
Its4	Статически просматривает исходный код для обнаружения потенциальных уязвимостей защиты	C/c++	Отмечает вызовы потенциально опасных функций, таких, как strcpy/memcpy, и выполняет поверхностный семантический анализ, пытаясь оценить, насколько опасен такой код, а также дает советы по его улучшению
Rats(rough auditing tool for security)	Просматривает исходный текст, находя потенциально опасные обращения к функциям	C/c++, php, perl, python	Использует сочетание проверок надежности защиты от семантических проверок в its4 до глубокого семантического анализа в поисках дефектов, способных привести к переполнению буфера, полученных из mops
Flawfinder	Просматривает исходный текст, находя потенциально опасные обращения к функциям	C/c++	Выполняет поиск функций, которые чаще всего используются некорректно, присваивает им коэффициенты риска (опираясь на такую информацию, как передаваемые параметры) и составляет список потенциально уязвимых мест, упорядочивая их по степени риска
Flexelint (pc-lint)	Производит семантический анализ исходного кода, анализ потоков данных и управления	C/c++	В конце работы выдаются сообщения нескольких основных типов: – возможен нулевой указатель – проблемы с выделением памяти (например, нет free() после malloc()) – проблемный поток управления (например, недостижимый код); – возможно переполнение буфера, арифметическое переполнение;

Наименование средства	Назначение	Поддерживаемые языки программирования	Примечание
			– предупреждения о плохом и потенциально опасном стиле кода
Parasoft c++ test	Формирование тестов анализа уязвимостей на уровне метода, класса, файла и проекта	C++	Генерирует тестовый код, вызывая для его подготовки компилятор visual c++
Coverity	Используется для выявления и исправления дефектов безопасности и качества в приложениях критического назначения	C/c++, java	Способен с минимальной положительной погрешностью обрабатывать десятки миллионов строк кода, обеспечивая 100-процентное покрытие трассы
Klocwork k7	Предназначен для автоматизированного статического анализа кода, выявления и предотвращения дефектов программного обеспечения и проблем безопасности	C/c++, java	Выявляет коренные причины недостатков качества и безопасности программного обеспечения
Codesurfer	Может применяться для поиска ошибок в исходном коде, для улучшения понимания исходного кода	C/c++	Позволяет проводить анализ указателей, использовать и определять переменные, зависимости данных, строить графы вызовов
Fxcop	Способен обнаружить более 200 недочетов (или ошибок) в следующих областях: – архитектура библиотеки; – правила именования; – производительность; – безопасность	C/c++	Откомпилированный код проверяется с помощью механизмов рефлексии, парсинга msil и анализа графа вызовов
Qaudit	Быстрый анализ исходных файлов на наличие переполнения буфера, ошибок форматной строки, запросов исполняемых вызовов, переменных среды, и функций, имеющих проблемы защиты	C/c++	Написать на интерпретируемом языке perl, прост в использовании
Российские средства выявления уязвимостей			
Ак-вс	Автоматизированный анализ исходных текстов, с целью выявления потенциально опасных сигнатур	C/c++, java, pascal, c#, php, assembler	Позволяет проводить статический анализ исходных текстов, динамический анализ, имеет базы сигнатур для каждого из поддерживаемых языков программирования
Аист-с	Автоматизированный анализ исходных текстов	C/c++	Позволяет проводить статический анализ исходных текстов
Ксайт	Автоматизированный анализ исходных текстов	C/c++	Позволяет проводить статический анализ исходных текстов
Уса	Предназначено для выявления потенциально опасных сигнатур	C/c++, pascal, perl, plm	Имеет базы сигнатур для каждого из поддерживаемых языков программирования

Наименование средства	Назначение	Поддерживаемые языки программирования	Примечание
Viva64	Помогает отслеживать в исходном коде потенциально опасные фрагменты, связанные с переходом от 32-битных систем к 64-битным	C/c++	Помогает писать корректный и оптимизированный код для 64-битных систем

Задание № 2. Разработать приложение (мини базу данных), состоящее из следующих элементов:

1. Поле 1, поле 2 сгруппированы в отдельную область (*groupBox*)
2. Элемент список (*listBox*), в который записываются данные с введенных полей
3. Кнопки *Добавить*, *Удалить*, *Найти*
4. Поле для вывода количества элементов списка (*label*)

Вариант	Поле 1	Поле 2
1	Имя	Телефон
2	Марка автомобиля	Модель авто
3	Название браузера	Версия
4	Город	Численность населения
5	Страна	Город
6	Язык программирования	Тип данных
7	Информационная система	Вид тестирования
8	Модель телефона	Операционная система
9	Тип сайта	Среда разработки
10	Вид компьютерной графики	Тип файла

Пример интерфейса представлен на рисунке:

Задание № 3. Добавить в программу форму авторизации по имени и паролю.

Задание № 4. Оформить отчет.