Лабораторная работа № 6

Ролевое управление доступом. Разработка защищённых приложений

Цель работы

Познакомиться с концепцией ролевого управления доступом и способами защиты программного обеспечения от существующих угроз. Научиться разрабатывать приложения, которые используют ролевое управление доступом для разграничения полномочий пользователей. Получить навыки защиты разработанной программы от несанкционированного копирования и других угроз, которым может подвергаться программное обеспечение.

Указание к работе

Используя лекции и дополнительную литературу [1, 2, 3], изучить угрозы, которым подвергается приложение в реальном мире, и способы защиты от возможных атак на приложения. Изучить концепцию ролевого управления доступом.

Реализовать программы, выполняющие указанные в задании действия.

Задание

I. Реализовать приложение с графическим интерфейсом, удовлетворяющее следующим требованиям.
   1. Приложение проводит аутентификацию пользователя.
   2. Каждый пользователь программы должен относиться к какой-нибудь группе пользователей (роли), членам которой доступны *различные* функциональные возможности программы.
   3. Программа должна принимать от пользователя некоторые данные и, возможно, после некоторой обработки, отображать их. При этом должна осуществляться защита от возможных атак на приложение. При разработке защиты нужно предположить, что приложение работает с базой данных, в которой сохраняет введённые пользователем данные.

II. Реализовать приложение-инсталлятор, позволяющее установить на компьютер пользователя приложение, реализованное в предыдущем пункте задания. Требования к приложению:
   1. Приложение-инсталлятор совместно с устанавливаемым приложением должно обеспечивать защиту программного продукта от несанкционированного тиражирования.
   2. Приложение-инсталлятор должно иметь защиту от возможных атак на него.

III. Протестировать правильность работы разработанных приложений.

Дополнительные критерии оценивания качества работы

1. Количество элементов защиты:
   1 – в программе успешно реализовано не менее 5 элементов защиты;
   0 – в программе успешно реализовано не менее 2 элементов защиты;
   л.р. не принимается – иначе.

Контрольные вопросы

1. Ролевое управление доступом.
2. Атака «переполнение буфера».
3. Атака «SQL-инъекции».
4. Атака, эксплуатирующая ошибки канонизации.

5. Атака «XSS» (межсайтовое кодирование).
6. Принцип минимизации привилегий.
7. DoS-атака (отказ в обслуживании).

Список литературы

1. Нортроп, Т. Разработка защищённых приложений на Visual Basic .NET и Visual C# .NET : учебный курс Microsoft / Т. Нортроп. – М. : Издательство "Русская редакция", 2007. – 688 с.
2. Скляров, Д.В. Искусство защиты и взлома информации / Д.В. Скляров. – СПб. : БХВ-Петербург, 2004. – 288 с.
3. Ховард, М. Защищённый код : пер. с англ. / М. Ховард, Д. Лебланк. – 2-е изд., испр. – М. : Издательско-торговый дом "Русская редакция", 2004. – 704 с.