Лабораторная работа №2

Анализ защищённости программных систем

Часть 2.
Оценка защищённости сторонних программных систем

Теоретические основы

Одной из задач анализа программных систем является оценка их защищённости. При оценке таких систем необходимо руководствоваться комплексным подходом. В качестве такого подхода может выступать методика оценки защищённости сторонних систем.

Методика должна включать анализ защищённости различных аспектов программных систем:

– анализ физических устройств хранения и обработки данных;

– анализ операционной системы и программного окружения;

– анализ исходного кода сторонней системы на предмет потенциальных уязвимостей;

– анализ компонентов сторонней системы, в том числе используемых СУБД, используемых библиотек, веб-серверов, используемых протоколов и т. д.;

– анализ взаимодействия между компонентами системы;

– анализ организационных мер пользования системой;

– анализ пользования системой на предмет не ожидаемых результатов, в следствие которых может быть нарушена целостность, доступность и конфиденциальность и т. д.

При анализе программных систем, необходимо учитывать возможные атаки на каждый компонент или группу компонентов системы. Наиболее популярные атаки указаны в теоретических основах лабораторной работы №2.1.

Существует большое количество программных продуктов для анализа безопасности веб-приложений [5][6], среди которых немало программ с открытым исходным кодом. С помощью ряда программных продуктов возможно

– осуществить сканирование веб-приложений по принципу «чёрного ящика»,

– осуществить поиск всех доступных веб-ресурсов (веб-страниц, изображений, CSS файлов и т. д.) по указанному адресу,

– проанализировать приложение на уязвимость с помощью различных видов инъекций (SQL, скриптовых, HTTP и т. д.),

– проанализировать приложение на уязвимость XSS атакам и т. д.

Инструментальные и вспомогательные средства

1. Виртуальная машина с установленной ОС (Windows, Linux).
2. Вариант выполненной лабораторной работы №2.1.

Задание для самостоятельной работы

1. Разработать методику оценки защищённости систем.
2. Выполнить анализ предоставленного приложения с позиций
   - политики безопасности операционной системы,
   - политики безопасности компонентов приложения и их взаимодействия между собой,
   - сетевой политики безопасности,
   - безопасности конфиденциальности данных.
3. Предложить комплекс мер по усовершенствованию приложения.
4. Предложить рекомендации по безопасному использованию приложения.
5. Оформить отчёт о проделанной работе.

Отчётность

Результат выполненной работы должен быть представлен в виде
- разработанной методики оценки защищённости,
- анализа защищённости предоставленной системы,
- предложенного комплекса мер усовершенствования системы,
- предложенные рекомендации по безопасному использованию системы,
- отчёт о проделанной работе.

Отчёт должен быть оформлен в соответствии с документом http://www.bsuir.by/m/12_100229_1_80040.pdf.

Отчёт должен содержать следующую информацию.
1. Постановка задачи.
2. Краткое описание предоставленной системы.
3. Разработанная методика оценки защищённости системы.

4. Анализ защищённости предоставленной системы по разработанной методике.

5. Предложенный комплекс мер по усовершенствованию защищённости предоставленной системы.

6. Предложенные рекомендации по безопасному использованию предоставленной системы.

7. Вывод. В выводе должны быть представлена семантическая и прагматическая составляющие проделанной работы.

Список рекомендуемых источников

1. Ховард, М. Защищённый код // М. Ховард, Д. Лебланк — М.: Русская редакция, 2004. — 704 с.
2. Ховард, М. 24 смертных греха компьютерной безопасности. Библиотека программиста // М. Ховард, Д. Лебланк, Дж. Вьега — СПБ.: Питер, 2010. — 400 с.
3. Панасенко, С. П. Алгоритмы шифрования. Специальный справочник / С. П. Панасенко. – СПб.: БХВ-Петербург, 2009. - 576 с.
4. Официальный сайт CWE: Common Weakness Enumeration [Электронный ресурс]. – Электронные данные. – Режим доступа: http://cwe.mitre.org/ Дата доступа: 20.08.2014.
5. Vulnerability Scanning Tools [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools. Дата доступа: 20.08.2014.
6. Web application security scanner list [Электронный ресурс]. – Электронные данные. – Режим доступа: http://projects.webappsec.org/w/page/13246988/Web%20Application%20Security%20Scanner%20List Дата доступа: 20.08.2014.