Безопасность Web приложений

1 Особенности информационной безопасности Web приложений

1.1

Взаимодействие по сети

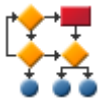
1.1.1 Передача в открытом виде

данных

запросов

1.1.2 Низкий уровень квалификации пользователей в области эксплуатации сетей

1.2



Открытые технологии

1.2.1 HTTP

1.2.2 HTML

1.2.3 JavaScript

1.3

Высокие нагрузки

1.3.1 Большое количество пользователей

1.3.2 Большие объемы данных

1.4

Высокие требования к кроссплатформенности

1.4.1 Поддержка различных браузеров

1.4.2 Поддержка различных версий серверов

2

Top 10 рисков безопасности

2.1 A1 - Injection

2.1.1 Валидация

2.1.2 Разделение поступающих неструктурированных данных и команд

2.1.3 Средства проверки кода

2.2 A3 - Broken Authentication and Session Management

2.2.1 Хэширование и шифрование пароля

2.2.2 Не передавать сессию в качестве параметра URL

2.2.3 Выход по таймауту

2.2.4 Случайный идентификатор сессии для каждой сессии пользователя

2.2.5 Использования протокола с шифрованием при передаче идентификаторов

2.3 A2 - Cross-Site Scripting (XSS)

2.3.1 Валидация вводимых данных

2.3.2 Настройка cookie

2.4 A4 - Insecure Direct Object References

2.4.1 Проверка доступа к запрашиваемым данным и операциям над ними

2.4.2 Избегайте инкрементных (суррогатных целочисленных) идентификаторов

2.5 A6 - Security Misconfiguration

2.5.1 Проверка версий и обновлений используемого ПО

2.5.2 Удалите все ненужное и неиспользуемое ПО

2.5.3 Закройте все неиспользуемые порты

2.5.4 Проверьте блокировку или смену пароля для аккаунта по умолчанию

2.5.5 Проследите, чтобы при возникновении ошибок не выдавалась отладочная информация

2.5.6 Проверьте настройки безопасности используемого фреймворка

2.6 NEW! A6 Sensitive Data Exposure

2.6.1 Шифрование. Использование более сложных алгоритмов, чем простое хеширование (например, хеш с солью)

2.6.2 Избавляйтесь от неиспользуемых важных данных

2.6.3 https

2.7 NEW! A7 Missing Function Level Access Control

2.7.1 Аккуратно пишите код - декомпозируйте функции

2.7.2 По умолчанию всё должно быть запрещено, выполнение функций должно быть разрешено отдельным ролям (пользователям)

2.7.3 Проверка многошаговой транзакции

2.8 A5 - Cross-Site Request Forgery(CSRF)

2.8.1 Используйте сгенерированный случайный токен

2.8.2 Проверка многошаговой транзакции

2.9 NEW! A9 Using Components with Known Vulnerabilities

2.9.1 Подпишитесь на рассылки о новых уязвимостях

2.9.2 Своевременно обновляйте используемое ПО

2.10 A10 - Unvalidated Redirects and Forwards

2.10.1 Валидация параметра, который используется для перехода

2.10.2 Проверяйте право на доступ

2.11 Не вошли в TOP 2013 по сравнению с TOP 2010

2.11.1 A7 - Insecure Cryptographic Storage

Хранение важных данных в зашифрованном виде

Доступ к дешифрованным данным имеют только авторизованные пользователи

Используется криптостойкий алгоритм шифрования

Меняйте ключ шифрования

2.11.2 A8 - Failure to Restrict URL Access

Проверка разрешения доступа к каждой странице

Используйте запрет по умолчанию

В многошаговой транзакции проверяйте связь между шагами

2.11.3 A9 - Insufficient Transport Layer Protection

Шифрования идентификационных данных

Аттрибут "secure" для cookie с важными данными

Валидность сертификата

3

Ресурсы

3.1 OWASP

See link(s): Main_Page

3.1.1 OWASP top 10 for .NET developers

See link(s): OWASP

3.2 Уязвимости и атаки

3.2.1 Вся правда о SSL-сертификатах

See link(s): ssl

3.2.2 Способы идентификации в интернете

See link(s): id

3.2.3 XSS глазами злоумышленника

See link(s): 66057

3.2.4 Злые фишинг картинки

See link(s): 140054

3.2.5 Фотохостинги и privacy ваших фотографий

See link(s): 140003

3.2.6 CSRF

CSRF уязвимости на примере ХабраХабра

See link(s): 134150

Защита ajax-приложения от Cross Site Request атак (CSRF)

See link(s): 144406

Зачем Google добавляет while(1); к своим JSON-ответам? перевод

See link(s): 168461

3.2.7 SQL инъекции

Базовые sql-инъекции в приложениях, использующих язык SQL. Руководство для чайников

See link(s): 157531

3.2.8 Об одной малоизвестной уязвимости в веб сайтах

See link(s): 166855

3.3 Исследование и повышение безопасности

3.3.1 Уязвимы по определению

See link(s): 138779

3.3.2 Ghostery

See link(s): www.ghostery.com

3.3.3 Расширение Collusion для Firefox: визуализация следящих cookies

See link(s): 123823

3.3.4 Browser Security Handbook

See link(s): Main

3.3.5 вопросы безопасности и средства защиты веб-приложений на платформе microsoft

See link(s): 4194.html

3.3.6 Очевидные 3 правила безопасности

See link(s): 143259

3.4 Рекомендации

3.4.1 На пути к созданию безопасного веб-ресурса. Часть 1 — серверное ПО tutorial

See link(s): 168739

3.4.2 На пути к созданию безопасного веб-ресурса. Часть 2 — разработка tutorial

See link(s): 168823

3.4.3 На пути к созданию безопасного (веб)ресурса. Часть 3 — офис, сотрудники

See link(s): 170167

3.4.4 12 навыков создания защищенных веб-приложений

See link(s): 114661

3.5 AJAX

3.5.1 Overcome security threats for Ajax applications

See link(s): index.html

3.5.2 О будущем защищенных Ajax mashup-приложений

See link(s): x-securemashups