УДК 004.056.5:004.7

магистр А.И. Романов
ГВУЗ «Национальный горный университет»

ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ ВЕБ – ПРИЛОЖЕНИЙ. ОСНОВНЫЕ МЕТОДЫ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ

В данной работе рассматривается определение тестирования безопасности веб – приложений, сферы применения данного вида тестирования. Особое внимание уделяется методам тестирования безопасности, а также сложностям при проведении подобных мероприятий.

Тестирование безопасности требуется для приложений самых различных сфер применения. Это могут быть обычные веб – приложения; приложения с важной коммерческой или персональной информацией, подлежащей защите; различные платежные системы, где риск потери информации может оцениваться в значительные суммы; приложения с повышенными требованиями к целостности; а также популярные и широко используемые сейчас социальные сети.

Тестирование безопасности как вид нефункционального тестирования

Тестирование безопасности – это один из видов нефункционального тестирования. При таком виде тестирования основной акцент ставится на т.н. «негативное» тестирование – изучается и анализируется поведение ПО в разных стрессовых ситуациях, особое внимание уделяется ошибкам, которые выдает приложение. В некоторых случаях изучение ошибок помогает обнаружить уязвимости, «слабые» места в ПО.

В общем случае, тестирование – это процесс проверки заявленных к продукту требований и реально реализованной функциональности, который осуществляется путем наблюдение за его работой в искусственно созданных ситуациях, на ограниченном наборе тестов, выбранных определенным образом. [3] Поэтому тестирование безопасности, как и любой другой вид тестирования, проводится на основе поставленных требований. Как дополнение к требованиям составляется матрица рисков безопасности. Именно на основе этих документов осуществляется процесс тестирования.

Измерить качество тестирования безопасности довольно сложно. Ведь возможен тот факт, что во время выполнения тестов было найдено и устранено огромное количество уязвимостей. Но одна лишь ненайденная уязвимость может стать для приложения решающей.

При тестировании безопасности важно помнить, что уязвимости – это такие же дефекты в ПО, как и обычные функциональные ошибки. Но в случае уязвимостей, ущерб от их обнаружения и эксплуатации может быть намного выше.

Методы тестирования безопасности

1. Основным методом тестирования безопасности является т.н. code review – просмотр исходного кода приложения. [1] Как правило, просмотр выполняется квалифицированным разработчиком. Тестировщик же, в свою очередь, может использовать утилиты для статического и динамического анализа: RATS, cppcheck и др. Данный метод позволяет обнаружить уязвимости в коде еще на этапе реализации проекта.

2. Fuzz – тестирование – это еще один метод тестирования безопасности. Суть данного метода тестирования состоит в том, что на вход приложения подаются заведомо неверные, непредусмотренные или случайные данные. Таким образом, мы изучаем поведение приложения при использовании самых различных входных данных. При применении фаззинга – тестирования можно обнаружить ошибки обработки входных данных, утечки памяти, неверные коды ошибок. Существует ряд программных средств для проведения фаззинг тестирования – Skyfish, SPIKE Proxy, OWASP WSFuzzer (Soap).

3. Тестирование на проникновение (penetration testing). Данный метод позволяет проводить тестирование, взаимодействуя с приложением исключительно с пользовательской стороны. Тестировщик может использовать как автоматические сканнеры безопасности, такие как skipfish или wapiti, так и анализаторы сети. Немаловажным аспектом при тестировании на проникновении является ручное (исследовательское)

тестирование – ведь программные средства не всегда могут обнаружить все уязвимости в безопасности.

Сложности в тестировании безопасности веб – приложений

К основным сложностям тестирования безопасности можно отнести:

1. Кроссбраузерность приложений. Пользователи могут использовать различные виды браузеров, таких как Mozilla Firefox, Opera, Google Chrome, Safari, Internet Explorer, а также их разные версии (в некоторых случаях очень устаревшие).

2. Использование разных ОС. На веб – приложение не должна никоим образом влиять операционная система, используемая пользователем.

3. Неточная или некорректная формулировка требований относительно безопасности в техническом задании продукта.

Перечень литературы:

1. Очир Абушинов. «Особенности тестирования безопасности ПО». SQA Days 2010.

2. http://searchsoftwarequality.techtarget.com/answer/Web-application-security-testing-basics

3. http://www.protesting.ru/testing/types/security.html