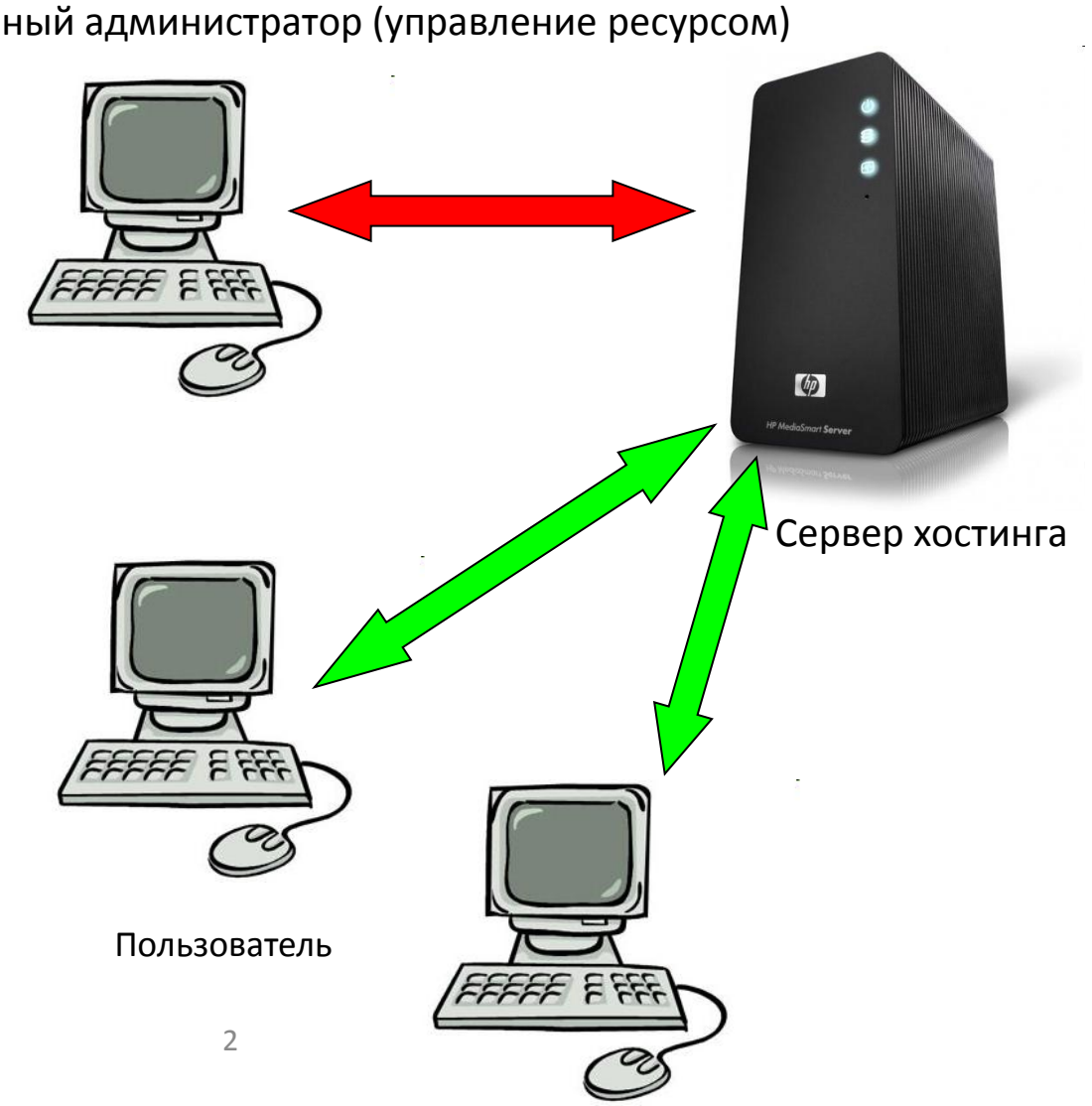
Тестирование на уязвимости WEB-приложений

LVEE-WINTER-2012

Дмитрий Никипелов
ISO/IEC 27001 auditor
Hoster.by

Основные угрозы существованию WEB-ресурсов

- *Угрозы конфиденциальности* – хищение информации
- *Угрозы целостности* – подмена содержимого ресурсов
- *Угрозы доступности* – ограничение доступности или отказ в обслуживании запроса



С чего начать?

- Прежде всего необходимо позаботиться о безопасности платформы (хостинга), т.к. если будут выявлены уязвимости в структуре платформы, говорить о безопасности и тестировании приложений не имеет смысла. В качестве примера можно привести технологию "защищенный хостинг" от Hoster.by, позволяющую получить защищенную базу для размещения приложений.

Способы тестирования на уязвимости

- ***- принцип "белого ящика"*** - тестировщику заранее известно все, включая исходный код . В этом случае проводятся проверки исходного кода на наличие потенциально опасного кодирования (статически - по сигнатурам) и динамически на уровне разработчиков (когда модули подвергаются тестированию на ввод некорректных данных).

- ***-принцип "серого ящика"*** - тестеру предоставляются все полномочия кроме непосредственного доступа к серверу. Проверки происходят на предмет повышения полномочий, выявления ошибок обработки данных, реакцию на некорректные данные. Данный способ позволяет оценить корректность работы ресурса при вводе разных исходных данных, но как и предыдущий метод не позволяет инсценировать атаку на ресурс.

- ***- принцип "черного ящика"*** - тестировщик иммитирует действия потенциального злоумышленника любыми доступными ему способами. При таком способе тестирования проверяется как наличие уязвимостей приложения, так и действия персонала по противодействию атаке и реагированию на инцидент. При проведении подобного тестирования действиям персонала необходимо уделять особое внимание, так как в некоторых случаях способность адекватно реагировать на инцидент имеет решающее значение. Недостатком данного метода является то, что тестер должен иметь весьма высокую квалификацию для достижения эффективных результатов и тестирование занимает достаточно продолжительное время.

Механизм Honey pot