Міністерство освіти і науки України

Запорізький національний технічний університет

Кафедра програмних засобів

РЕФЕРАТ

з дисципліни «Якість програмного забезпечення та тестування» на тему:

«МЕТОДИ ТЕСТУВАННЯ ПРАЦЕЗДАТНОСТІ»

Виконав:

студент гр. КНТ-415 Д. О. Тарасенко

Прийняв:

к.т.н., професор Г. В. Табунщик

2018

ЗМІСТ

[МЕТОДИ ТЕСТУВАННЯ БЕЗПЕКИ 3](#_Toc527306869)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 6](#_Toc527306875)

# МЕТОДИ ТЕСТУВАННЯ безпеки

Тестування безпеки - комплекс досліджень програмного продукту, спрямований на тестування, виявлення та виправлення дефектів, пов'язаних з безпекою призначених для користувача даних, а саме:

Цілісність. Обмеження кола користувачів, що мають доступ до даних, визначення ступеня шкоди, завданої при втраті тих чи інших даних.

Доступність. Являє собою вимоги про те, що ресурси повинні бути доступні авторизованому користувачеві, внутрішньому об'єкту або пристрою. Як правило, чим більш критичний ресурс тим вище рівень доступності повинен бути.

Конфіденційність. Приховування певних ресурсів або інформації. Під конфіденційністю можна розуміти обмеження доступу до ресурсу деякої категорії користувачів, або іншими словами, за яких умов користувач авторизований отримати доступ до цього ресурсу.

В ході тестування, найчастіше тестувальник грає роль зломщика, і починає маніпулювати різними чином додатком:

• Спроби дізнатися пароль за допомогою зовнішніх засобів.

• Атака системи за допомогою спеціальних утиліт, які аналізують захисту.

• Подавлення, приголомшення системи (в надії, що вона відмовиться обслуговувати інших клієнтів).

• Цілеспрямоване введення помилок в надії проникнути в систему в ході відновлення.

• Перегляд несекретних даних в надії знайти ключ для входу в систему.

Можна виділити кілька основних видів уразливості:

* XSS (Cross-SiteScripting) - це вид уразливості програмного забезпечення (Web додатків), при якій, на генерованої сервером сторінці, виконуються шкідливі скрипти, з метою атаки клієнта;
* XSRF / CSRF (RequestForgery) - це вид уразливості, що дозволяє використовувати недоліки HTTP протоколу. Зловмисники працюють за такою схемою: посилання на шкідливий сайт встановлюється на сторінці, що користується довірою у користувача, при переході по шкідливої ​​посиланням виконується скрипт, який зберігає особисті дані користувача (паролі, платіжні дані і т.д.), або відправляє СПАМ повідомлення від особи користувача , або змінює доступ до облікового запису користувача, для отримання повного контролю над нею;
* Codeinjections (SQL, PHP, ASP і т.д.) - це вид уразливості, при якому стає можливо здійснити запуск виконуваного коду з метою отримання доступу до системних ресурсів, несанкціонованого доступу до даних або виведення системи з ладу;
* Server-SideIncludes (SSI) Injection - це вид уразливості, що використовує вставку серверних команд в HTML код або запуск їх безпосередньо з сервера;
* AuthorizationBypass - це вид уразливості, при якому можливо отримати несанкціонований доступ до облікового запису або документам іншого користувача.

# Зазвичай визначити необхідний вид тесту безпеки можна за кількома критеріями:

# 1) мети тестування;

# 2) дані про систему, які можна надати аудиторам;

# 3) точка входу в систему (актуально тільки для тестування локальних мереж).

# Виходячи з цілей, тестування безпеки ділиться на два види: тестування на проникнення (англ. Penetration Testing) і оцінка захищеності (англ. Vulnerability Assessment).

Наступний критерій вибору виду тесту безпеки - надаються аудиторам дані про систему. Залежно від того, якою інформацією володіють тестувальники перед початком тестів, можливі три варіанти:

* тестування методом чорного ящика - тестувальники не отримують ніяких відомостей про систему, навіть облікових записів; на вході вони мають тільки перелік IP-адрес або посилання на сайт;
* тестування методом сірого ящика - тестувальникам надаються валідниє облікові записи і обмежена інформація про систему;
* тестування методом білого ящика - тестувальникам надається повна інформація про систему: облікові записи, карти мереж, технологічні специфікації, вихідний код веб-додатків.

Останній критерій - точка входу в систему. Цей критерій враховується тільки при проведенні тестування на проникнення на рівні локальної мережі. Тут може бути два варіанти:

* зовнішній тест на проникнення - тестам піддаються тільки зовнішні IP-адреси компанії, доступні з мережі Інтернет;
* внутрішній тест на проникнення - тест проводиться всередині корпоративної мережі; тестувальникам надається виділене робоче місце в компанії або доступ у внутрішню мережу по VPN.

Як правило, внутрішній тест на проникнення проводиться тільки при наявності відповідних вимог в галузевих стандартах або якщо необхідно перевірити рівень захищеності від так званих інсайдерських атак, тобто здійснюваних співробітниками самої компанії.

Отже, розглянуті основні критерії вибору виду тестування безпеки. Комбінування цих критеріїв допоможе більш точно висловити потреби при складанні запиту з тестування. Якщо важливо протестувати систему ретельно, можна вибрати комбінацію оцінки захищеності і тестування на проникнення методом білого ящика. Якщо ж є жорсткі обмеження за часом або фінансів, то найбільш раціональним рішенням буде тестування на проникнення методом чорного ящика.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вибір виду тестування безпеки ПО [Електронний ресурс]. – Режим доступу: <http://software-testing.ru/library/testing/security/1986-security-testing>
2. Інженерія якості програмного забезпечення:навчальний посібник / Г.В Табунщик, Р.К. Кудерметов, Т.І. Брагіна. – Запоріжжя: ЗНТУ, 2013. – 180 с.
3. Тестування безпеки ПО [Електронний ресурс]. – Режим доступу: https://qalight.com.ua/baza-znaniy/testirovanie-bezopasnosti/