Міністерство освіти і науки України

Запорізький національний технічний університет

кафедра програмних засобів

РЕФЕРАТ

з дисципліни: «Якість програмного забезпечення»

на тему: «Тестування працездатності»

Виконав:

студент групи КНТ-415 К. А. Калоян

Перевірила: Г. В. Табунщик

Запоріжжя

2018

# ЗМІСТ

[ЗМІСТ 2](#_Toc527623030)

[1. Тестування безпеки або Security and Access Control Testing 3](#_Toc527623031)

[1.1 Принципи безпеки програмного забезпечення 3](#_Toc527623032)

[1.2 Види вразливостей 3](#_Toc527623033)

[1.3 Висновок 4](#_Toc527623034)

[2. СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 5](#_Toc527623035)

# Тестування безпеки або Security and Access Control Testing

Тестування безпеки - це стратегія тестування, яка використовується для перевірки безпеки системи, а також для аналізу ризиків, пов'язаних із забезпеченням цілісного підходу до захисту додатки, атак хакерів, вірусів, несанкціонованого доступу до конфіденційних даних.

## Принципи безпеки програмного забезпечення

Загальна стратегія безпеки грунтується на трьох основних принципах:

1. конфіденційність
2. цілісність
3. доступність

**Конфіденційність** - це 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.

**Цілісність**. Існує два основних критерії при визначенні поняття цілісності:

Довіра. Очікується, що ресурс буде змінений тільки відповідним способом певною групою користувачів.

Пошкодження і відновлення. У разі коли дані пошкоджуються або неправильно змінюються авторизованим або не авторизованим користувачем, ви повинні визначити на скільки важливою є процедура відновлення даних.

**Доступність** є 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.

## Види вразливостей

В даний час найбільш поширеними видами вразливості в безпеці програмного забезпечення є:

* XSS (Cross-Site Scripting) - це вид уразливості програмного забезпечення (Web додатків), при якій, на генерованої сервером сторінці, виконуються шкідливі скрипти, з метою атаки клієнта;
* XSRF / CSRF (Request Forgery) - це вид вразливості, що дозволяє використовувати недоліки HTTP протоколу, при цьому зловмисники працюють за такою схемою: посилання на шкідливий сайт встановлюється на сторінці, що користується довірою у користувача, при переході по шкідливому ​​посиланню 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;
* Code injections (SQL, PHP, ASP і т.д.) - це вид вразливості, 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-Side Includes (SSI) Injection - це вид вразливості, що використовує вставку серверних команд в HTML код або запуск їх безпосередньо з сервера;
* Authorization Bypass - це вид уразливості, при якому можливо отримати несанкціонований доступ до облікового запису або документам іншого користувача

## Висновок

Прикладів вразливостей і атак існує величезна кількість. Навіть провівши повний цикл тестування безпеки, не можна бути на 100% впевненим, що система по-справжньому захищена. Але можна бути впевненим в тому, що відсоток несанкціонованих проникнень, крадіжок інформації і втрат даних буде в рази менше, ніж у тих хто не проводив тестування безпеки.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тестирование безопасности или Security and Access Control Testing [Електронний ресурс]. – Режим доступу: http://www.protesting.ru/testing/types/security.html
2. Інженерія якості програмного забезпечення:навчальний посібник / Г.В Табунщик, Р.К. Кудерметов, Т.І. Брагіна. – Запоріжжя: ЗНТУ, 2013. – 180 с.