УДК 004.056

КовальО.П., Резніченко В.А.
Кіровоградський національний технічний університет

Тестування безпеки web-програм

Тестування безпеки - це стратегія тестування, яка використовується для перевірки безпеки системи, а також для аналізу ризиків, пов'язаних із забезпеченням цілісного підходу до захисту програми, атак хакерів, вірусів, несанкціонованого доступу до конфіденційних даних. Дане випробування направлено на діагностику шляхів злому системи, оцінку захищеності веб-додатків або сайту, а також аналіз ризиків, пов'язаних з підходом до захисту від зловмисників, доступу до конфіденційних даних. Базуючись на принципах конфіденційності, доступності та цілісності, тестування безпеки сприяє забезпеченню збереження даних, облікових записів, доступів і підключень користувачів.

Загальна стратегія безпеки грунтується на трьох основних принципах: конфіденційність, цілісність, 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.

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 авторизованим користувачем, ви повинні визначити на скільки важливою є процедура відновлення даних.

Доступність є вимогою 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.

В даний час найбільш поширеними видами вразливості в безпеці програмного забезпечення є такі. XSS (Cross-Site Scripting) - це вид вразливості програмного забезпечення (Web додатків), при якій, на генерованій 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 за шкідливим 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. 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 вразливості, при якому можливо отримати несанкціонований доступ до облікового запису або документам іншого користувача.

Прикладів вразливостей і атак існує величезна кількість. Навіть провівши повний цикл тестування безпеки, не можна бути на 100% впевненим, що система по-справжньому безпечна. 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. *Whittaker, James A. How to Break Web Software: Functional and Security Testing of Web Applications and Web Services / James Whittaker & Mike Andrews – Addison-Wesley Professional, 2006.*
2. *Whittaker, James A. How to Break Software Security / James Whittaker & Hugh Thompson – Addison-Wesley, 2003.*