УДК 004.492.2

ТРИРІВНЕВА МОДЕЛЬ ОЦІНКИ ЗАХИЩЕНОСТІ ВЕБ-ЗАСТОСУНКІВ

І. Б. Шевчук[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В даній роботі представлена модель оцінки веб-застосунків, яка складається з трьох основних рівнів: оцінка вразливостей веб-застосунку, оцінка отримана на основі тестів на проникнення та оцінка відповідності даного веб-застосунку до вимог. А також розглянено опис кожного з етапів та обґрунтування їх важливості.

Ключові слова: веб-застосунки, модель оцінки, тестування на проникнення, вразливості, сканери

Вступ

Веб-застосунки в сучасному світі знайшли своє місце практично у всіх областях діяльності. Це спеціальні програмні забезпечення, які використовуються для найрізноманітніших цілей.

Проте, не зважаючи на важливу роль, є і зворотна сторона: їх компрометація може призвести до катастрофічних наслідків. Для звичайного користувача це може обернутись крадіжкою особистих даних. Щодо компаній – то це може призвести до того, що вона втратить репутацію, позбудеться важливих клієнтів, зазнає фінансових втрат. Саме тому, безпека веб-застосунку не менш важлива, ніж реалізація його основних функцій.

Постановка задачі полягає в створенні оптимальної моделі оцінки захищеності веб-застосунків, яка допомагає оцінити рівень захищеності з різних сторін та отримати найбільш детальну картину щодо даного веб-застосунку.

1. Безпека веб-застосунків

Для того щоб максимально забезпечити безпеку – необхідно знати рівень захищеності веб-застосунку, а для цього потрібно використовувати відповідні способи її отримання.

Безпека веб-застосунку – це властивість даної програми функціонувати без прояву різних негативних наслідків для конкретної комп'ютерної системи.

Рівень безпеки веб-застосунку – це показник, який характеризує ймовірність того, що при певних умовах використання веб-застосунку буде отримано потрібний результат.

В роботах [1, 2] було показано, які існують можливі способи для перевірки захищеності веб-застосунку. До найпоширеніших відносять такі:

1) Виявлення вразливостей за допомогою сканерів безпеки.
2) Тести на проникнення.
3) Статичне та динамічне тестування.
4) Тестування системи за допомогою стандартного набору тестів (функціональне тестування; перевірка сумісності; тестування продуктивності; тестування безпеки).
5) Аналіз веб-застосунку вручну. Моделювання загроз.

2. Результати досліждення

В залежності від того, яка мета переслідується, використовується один із тих способів для перевірки захищеності, що були наведені раніше. Проте, зважаючи на загрози, що можливі для даної системи, зазвичай формується певний перелік перевірок.

По – суті, можна по – різному комбінувати перераховані підходи до аналізу захищеності, доповнюючи процес дослідження такими можливостями, які необхідні для конкретного веб-застосунку. Оскільки ціллю даної роботи було створення оптимальної моделі, то в результаті аналізу можливих комбінацій даних способів було створено трирівневу модель оцінки захищеності веб-застосунків.

На рис. 1 зображено модель оцінки захищеності веб-застосунків. Основними її етапами є:

1) Відповідність веб-застосунку до вимог.
2) Виявлення вразливостей за допомогою сканерів безпеки.
3) Тестування на проникнення.

Кожен із цих компонентів є невід'ємною частиною, оскільки захищеність веб-застосунку розглядається з різних сторін, що в кінцевому результаті дає можливість побачити цілісну картину щодо нього. Розглянемо детальніше кожну складову моделі.

Перший рівень моделі надає можливість переконатись, що застосунок розроблений відповідно до «Стандарту оцінювання відповідності безпеки застосунків» [3] та відповідає усім вимогам. Насамперед при оцінці захищеності веб-застосунку потрібно визначити тип даних, що оброблюється даним веб-застосунком, тип індустрії, що він охоплює та лише тоді, перевіряти його на виконання спеціально

[a] irochkash5@gmail.com

підібраним вимогам. Результатом – є звіт, в якому описується статус кожної вимоги до оцінювання відповідності. Зважаючи на нього, можна визначити в якому стані знаходиться веб-застосунок згідно зі Стандартом, оцінити рівень його захищеності та скласти подальші рекомендації щодо покращення безпеки.

На другому етапі здійснюється перевірка системи за допомогою сканерів безпеки. Даний рівень оцінки є не менш важливий, оскільки в результаті досліджень за період останніх років було зроблено висновок, що на 4 % зросла кількість вразливостей високого та середнього рівнів в порівнянні з минулими роками. Використання автоматизованого аналізатора дозволяє виявити в 3 рази більше вразливостей, ніж ручні методи аналізу. Основною задачею на даному рівні є виявлення вразливостей та оцінка ступеню вразливості системи (дана процедура здійснюється на основі стандарту `OWASP` [4] , що визначає найбільш критичні вразливості системи).

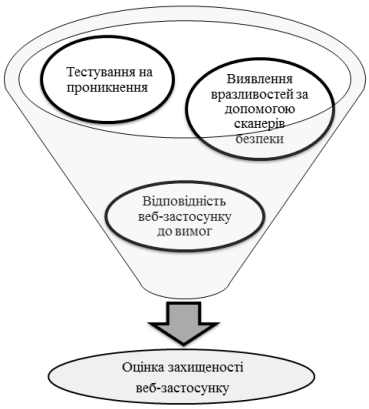

Рис. 1. Трирівнева модель оцінки захищеності веб-застосунків

Заключним етапом, що є тісно пов'язаним з попередніми двома є тестування на проникнення. В свою чергу, за допомогою нього частково здійснюється перевірка відповідності до вимог. Виконуючи тестування на проникнення на даному етапі, вже не береться до уваги стандарт і методологія `OWASP`, проте можуть бути задіяні інші, такі як `OSSTMM`, `NIST`. Та все ж головним способом проведення даного тестування є використання сучасних методів та інструментів, які використовують саме зловмисники. Даний етап є досить важливим, оскільки тест на проникнення – часткове моделювання дій зловмисника по проникненню в інформаційну систему. Проведені роботи дозволяють виявити уразливості і, якщо це можливо, здійснити ще одне проникнення, реалізувавши знайдені вразливості та ті, що були знайдені сканерами безпеки. Отже, на даному етапі можливо оцінити рівень захищеності веб-застосунку зі сторони зловмисника.

3. Застосування моделі оцінки захищеності

У зв'язку із договором було протестовано сайт `http://dictionary.krajina-znan.com.ua/`, сайт обрано з дозволу власника.

На першому етапі було визначено, що сайт містить відкриту інформацію, тому необхідно щоб даний веб-застосунок відповідав вимогам першого рівня. Було перевірено на відповідність вимог таких категорій: обробка шкідливих даних, контроль доступу, управління сеансами. В результаті перевірки було виявлено, що даний веб-застосунок не має достатнього рівня захищеності, оскільки не відповідає стовідсотково усім необхідним вимогам.

Другий рівень перевірки було здійснено за допомогою таких сканерів безпеки як `IronWasp`, `Skipfish`, `WPscan`, оскільки вони мають різні підходи сканування, для того, щоб можна було краще оцінити ситуацію та прийняти рішення щодо усунення виявлених недоліків. В результаті сканування було сформовано 3 звіти та виявлено такі типи вразливостей як `XSS`, `SQL-injection`, `same-origin method execution`, `Arbitrary File Upload`, `Timing Side Channel Attack`, `Publish Post & Mark as Sticky Permission Issue`, `SSRF`, `CSRF` та інші, з яких 8 вразливостей критичного рівня, 5 середнього та 1 низького. Даний результат свідчить про те, що ступінь захищеності даного веб-застосунку – низький.

При проведенні тестування на проникнення, спочатку було здійснено спробу реалізувати вразливості, що було знайдено на попередньому кроці та лише після цього здійснено проникнення за допомогою нових технологій. В результаті було виявлено нові вразливості та перевірено, що вразливості, які були знайдено сканерами мають місце в даному веб-застосунку.

Проаналізувавши отримані результати було оцінено рівень захищеності даного веб-застосунку та складено перелік проблем безпеки, що притаманні для досліджуваного об'єкту.

Висновки

Отже, за допомогою трирівневої моделі оцінки захищеності було встановлено, що сайт `http://dictionary.krajina-znan.com.ua/` – має низький рівень безпеки.

Зважаючи на те, що в даній моделі присутні різні підходи щодо визначення захищеності – було отримано розширений результат, в якому відображено проблеми безпеки з різних аспектів.

Перелік використаних джерел

1. Козлов Д. Д./Петухов А. А. Методы обнаружения уязвимостей в web-приложениях — 2006. — 12 с.
2. Рябов А. Обзор бесплатных сканеров защищенности веб-сайтов — 2012.
3. OWASP. Стандарт оцінювання відповідності безпеки додатків 3.0 OWASP — 2015. — 73 с.
4. OWASP. Десять найбільш критичних ризиків для безпеки веб-додатків — 2013. — 22 с.
5. Penetration Test Guidance Special Interest Group PCI Security Standards Council. PCI Data Security Standard (PCI DSS) — 2015. — 43 с.