УДК 004.492.2

Шатц К.О., магістрант, Лимаренко Ю.О., доцент, науковий керівник,

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ WEB-ЗАСТОСУНКІВ З ВИКОРИСТАННЯМ БІБЛІОТЕКИ GOOGLE MAPS API

Запорізька державна інженерна академія, кафедра ПЗАС

Сучасний інтегрований світ побудований на мільярдах веб-серверів, що підтримують роботу інформаційних систем, а також забезпечують виконання різних функцій починаючи від торгових операцій і закінчуючи підтримкою електронного уряду. Всі ці системи містять не тільки персональні дані, а і фінансову інформацію, яка вимагає захисту. Останні роки ознаменувалися збільшенням кількості атак, які націлені на web-сервери. Злочинність у цій сфері стала більш організованою і перейшла від дій студентів хакерів, до цілком осмислених дій з масового збору паролів і крадіжки фінансової інформації. Проте спеціалізованих засобів захисту веб-додатків досить мало, здебільшого це завдання покладають на розробників. Це і використання різних фреймворків, засобів санації, очищення даних, нормалізації і багато чого іншого.

Для побудови універсального засобу для захисту веб-додатків різної складності було обрано мову PHP, тому що більшість сайтів розроблено саме на цій мові. Згідно з дослідженням компанії Positive Technologies найбільш поширеними атаками у порядку убивання є: впровадження операторів SQL, виконання команд ОС, вихід за межі призначеної директорії (Path Traversal), міжсайтове виконання сценаріїв, відмова в обслуговуванні, підключення локальних файлів, впровадження зовнішніх сутностей XML, завантаження довільних файлів, підробка міжсайтових запитів. [1]

Створений програмний комплекс дозволяє виконувати комплексний аналіз веб-додатку на можливі загрози та допомогти уникнути іх. Отримані результати можуть використовуватися кінцевим споживачем для досягнення наступних цілей:

- захист свого бізнесу та інформації від зловмисників;
- збільшення контролю над сайтом;
- спостереження за кількістю і якістю атак;
- керування доступу до додатку користувачів;
- перегляд карти загроз;

Методика досліджень включає в себе побудову системи аналізу, збереження даних та обробки цих даних. Обробка буде виконуватися за допомогою засобів мови програмування PHP, а створення та візуалізація буде виконуватися за допомогою таких засобів, як HTML5 - мова розмітки гіпертекстових документів, CSS3 - спеціальна мова, що використовується для опису зовнішнього вигляду сторінок, написаних мовами розмітки даних та JavaScript - це невибаглива до ресурсів мова програмування з функціями першого класу, код якої інтерпретується або компілюється під час виконання. За збереження даних буде відповідати MySQL, що добре працює з мовою PHP.

Розроблений програмний комплекс складається з таких частин:

- **Захист від Mass Requests**

Масові запити багаторазово поповнюють веб-сайт, щоб зробити великий обсяг трафіку та перевантаження сайту. Треба бути обережним, при використанні даного виду захисту, бо він може заблокувати частину трафику веб-сайту.

- **Захист від SQL Injection**

За фактом, SQL запит являє собою програму. Повноцінну програму - з операторами, змінними і строковими літералами. Проблема ж полягає в тому, що ми цю програму збираємо динамічно, на ходу. На відміну від наших PHP скриптів, які написані раз і назавжди, і не змінюються на основі даних, що надходять, SQL запит кожен раз динамічно формується заново. І, як наслідок, невірно відформатовані дані

можуть зіпсувати запит, або навіть поміняти його, підставивши непередбачувані нами оператори. [2]

- **Захист від користувачів, які користуються Proxy та Tor**

Це досить простий модуль, який відповідає за виявлення користувачів, які користуються Proxy та Tor.

- **Модуль інтерфейсу користувача**

Цей модуль відповідає за налашутвання рівня захисту сайта, за відображення атак. Користувач зможе обрати, від яких атак йому потрібен захист.

- **Генератор паролів для захисту від Brute force та атак з перебором по словнику.**

Висновки:

1. Після дослідження предметної області та детального аналізу поставленої проблеми було встановлено актуальність розробки системи пошуку та усунення вразливостей на веб-ресурсі.
2. Шляхом аналізу різних видів атак та проведення теоретичних і практичних досліджень було сформовано набір методів для дослідження, проведено їх порівняння та аналіз, а також було визначено стек технологій та інструментів розробки, визначено їх відносну продуктивність, ступінь інтеграції та зручність використання.

Література

1. Атаки на Веб-приложения. Веб-ресурс, Режим доступу до ресурсу: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Applications-Attacks-rus.pdf
2. Защита от SQL-инъекций в PHP и MySQL, Веб-ресурс, Режим доступу до ресурсу: https://habr.com/post/148701/
3. Kaspersky Lab. The evolution of phishing attacks: 2011 - 2013. Режим доступу до ресурсу: http://media.kaspersky.com/pdf/Kaspersky_Lab_KSN_report_The_Evolution_of_Phishing_Attacks_2011