РІВНІ БЕЗПЕКИ СУЧАНИХ ВЕБ-ЗАСТОСУНКІВ МОВОЮ JAVA SPRING

студ. Д.О. Кузнєцов, Харківський національний університет радіоелектроніки, м. Харків

У сучасному світі не існуї такого користувача, який би не пріоритизував би для себе безпеку в будь-якій сфері попиту. Веб-застосунки теж не є винятком. Навіть звичайна інформаційна сторінка може запросити дані для реєстрації та аутентифікації клієнта задля збору інформації та ведення статистики. Через це, інформаційнє шахрайство та хакерство набуває комерційної вигоди і перехоплення конфіденційних даних стає приорітетом для кожного недоброчесного користувача світової мережі.

Задля цього, протягом останніх 20 років, було створено сотні різноманітних методів безпечної передачі інформації від апаратного кодування до серверного з'єднання. Якщо враховувати всі етапи розробки програмного забезпечення, то можна видлілити такі рівні безпеки [1]:

1) апаратна безпека;
2) міри безпеки на рівні коду та компілятору;
3) безпека в інтернет просторі та браузері;
4) системні або серверні елементи безпеки;
5) моніторінг потенційно-небезпечної активності.

Почнемо з доволі рідкого за вразливостю рівню, але не менш актуального – апаратного. Не секрет, що саме цей рівінь захистити складніше усього, насамперед через те, що сам комп'ютер або сервер, який є уразливим на найнижчому рівні, має тільки двійковий код, який ніяк не може бути захищеним різноманітним софтом. Задля надання безпеки рекомендовано використовувати тільки офіційні модулі комп'ютерної фізичної системи та завантажувати найсучасніше офіційне програмне забезпечення.

Наступним рівнем є код та компілятор. Цей рівень найменш значний, через те, що всі інші рівні запобігають втручанню саме в код програми. Серед сучасних веб-застосунків, основним елементом безпеки є безпека аутентифікації на рівні бібліотек коду, а саме spring security. Ця бібліотека надає додаткові валідації для багаторівневої регістрації конфіденційних даних. Найважливішим аспектом цього рівню є шифрування даних задля передачі між сервісами, що запобігає легкому перехопленню даних через їх неявний вигляд.

Безпека у браузері є найбільш важливим елементом саме для клієнта, через те що самі пошукові системи різні для кожного юзера як і їх налаштування. Серед найактуальніших рекомендацій основним є постійне оновлення браузеру до актуальної версії та сканування локального

комп'ютеру для видалення усіх небезпечних файлів, що можуть автоматично інтегруватися у пошукову систему при встановленні та логувати, або передавати дані на сторонні ресурси, що робить використання усієї інформації вразливим для користувача.

Серверна безпека є найважливішим елементом з усіх завдяки її доступу до всіх елементів головного коду та модулю. Це є "серце" будь-якого веб-застосунку і від нього залежить працездатність усіх модулів. Головним елементом безпеки серверу є різноманітні рівні доступу, які коригуються саме адмінами сервісу. Невід'ємною частиною серверу є унікальні та адаптовані під кожну систему засоби безпеки від різних потенційних атак, такі як антивірусні програми та системи віртуалізації та ізалювання модулів і коду [2].

Останній рівень є похідним від попереднього, бо він важливий лише завдяки системам підтримки серверів та команді підтримки. Основною відповідальністю для спеціалістів є моніторінг активнсті входжень на модулі серверу та запобігання DDos атак. У таких ситуаціях, команди використовують різноманітні засоби безпеки, від відключення маршрутизації на сервер до програм для запобігання підвищення нагрузки на сервер [3].

Усі ці модулі є невід'ємними елементами для кожного веб-застосунку та обов'язковими для стабільної, швидкої і найголовніше безпечної роботи усіх елментів та рівнів програми.

Список літератури: 1. *Singer, P.W., Friedman Allan*. Cybersecurity and Cyberwar: What Everyone Needs to Know. – 2014. – Oxford University Press. **2**. *Soltanian, Mohammad Reza Khalifeh.* Theoretical and Experimental Methods for Defending Against DDoS Attacks. **3.** *Lee, Newton.* Counterterrorism and Cybersecurity: Total Information Awareness. – Springer. – 2015.