Секція 2

БЕЗПЕКА API ІНТЕРФЕЙСУ

Єлюхін Р. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г. А.

Актуальність. API працюють як backend частина багатьох сучасних веб-додатків, утому числі додатків у банківській сфері, сфері інтернет-платежів та у медичній сфері. Тому дуже важливо захистити конфіденційні дані, які вони передають завдяки API інтерфейсу.

API-системи стрімко розвиваються, так каталог API, сервісу ProgrammableWeb, у період з 2016 року по 2018 рік виріс на 35% в цілому, і на 98% у фінансовій сфері [1]. Все більше компаній роблять сої API публічно відкритими, ріст трафіку клієнтських запитів до API виріс на 168% у порівнянні з минулим 2021 роком [2]. Але з зі зростанням кількості API викликів зростає і інтерес зловмисників до цього вектору атаки, так зловмисний трафік виріс на 117% за аналогічний період, і наразі становить 2,1% від загальної кількості трафіку API запитів [2].

З сучасних загроз можна відмітити вразливості в Tesla Backup Gateway APIs(які відповідають за електросистему господарства з сонячними панелями), через які у публічному доступі опинилися дані про споживання та виробництво енергії (ім'я, країна та штат, назва комунальної компанії тощо). Також можна відмітити атаку на API сайту findadoctor.com, через яку зловмисники отримали особисті дані 1,41 млн американських лікарів [3].

Метою даної роботи є підвищення ефективності методів боротьби з загрозами API інтерфейсу.

Основні положення. Серед найбільш актуальних вразливостей API можна виділити [4]:

− некоректна автентифікація користувачів - механізми автентифікації часто функціонують некоректно, дозволяючи зловмисникам компрометувати дані автентифікації або експлуатувати недосконалості в реалізації механізму з метою тимчасового чи постійного присвоєння облікового запису користувача;

− відсутність обмежень на кількість запитів та споживання ресурсів - це може вплинути на продуктивність API, що призводить до відмови в обслуговуванні (DoS);

− масове перепризначення параметрів - присвоєння даних, що надійшли від користувача, наприклад у форматі JSON, моделі даних без належної фільтрації параметрів на базі білого списку зазвичай призводить до масового перепризначення параметрів. Зловмисник може змінити властивості об'єктів, до яких не повинен мати доступ.

Для вирішення цих проблем ми можемо використовувати наступні рекомендації [5]: автентифікація та авторизацію варто використовувати на основі токенів, а не прямих логінів/паролів; варто використовувати https протокол з шифруванням TLS, замість htttp протоколу; використовувати обмеження швидкості та регулювання кількості запитів від одного користувача за одиницю часу.

Висновки. API інтерфейс дуже швидко розвивається за останні роки, тому він все частіше стає ціллю атак зловмисників. Для запобігання вразливостей інтерфейсу варто їх визначити та знати, також треба враховувати і додатково до них вхідних вразливостей форматів даних, таких найбільш розповсюджених форматів передачі даних в API як JSON та XML. Тож для боротьби з вразливостями API інтерфейсу варто використовувати ряд рекомендацій, таких як додатково встановлювати на веб-сервер автоматичні системи захисту з фільтрами запитів, а також розвивати захист на рівні архітектури і функціонуванні системи в цілому.

Список літератури

1. Financial APIs continue to see big growth. ProgrammableWeb. URL – www.programmableweb.com/news/financial-apis-continue-to-see-big-growth/research/2020/08/26 (дата звернення: 09.11.2022);
2. API Security Trends. *Salt*. URL – salt.security/api-security-trends (дата звернення: 09.11.2022);
3. Data at Risk: API Vulnerabilities. *10Guards*. URL – https://10guards.com/en/articles/data-at-risk-api-vulnerabilities/ (дата звернення: 09.11.2022);
4. OWASP API Security Project. *OWASP*. URL – https://owasp.org/www-project-api-security (дата звернення: 10.11.2022);
5. API Security: The Complete Guide to Threats, Methods & Tools. *Bright*. URL – brightsec.com/blog/api-security/#rest-api-vs-soap-security (дата звернення: 10.11.2022).

Відомості про авторів

Єлюхін Роман Валерійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 068-756-69-94, r.yeliukhin@student.csn.khai.edu
Землянко Георгій Андрійович, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, g.zemlynko@csn.khai.edu