Химач Д.С., учень
Шатківський В.М., вчитель
Відокремленого підрозділу "Науковий ліцей"
Державного університету "Житомирська політехніка"

АНАЛІЗ НАЙПОШИРЕНІШИХ ВРАЗЛИВОСТЕЙ ВЕБСАЙТІВ

У сучасному цифровому світі вебсайти стали невід'ємною частиною нашого життя, але разом із їх поширенням зростають ризики, пов'язані з вразливостями, які можуть бути використані зловмисниками. Організація OWASP щорічно формує рейтинг найкритичніших проблем безпеки вебсайтів, його можна знайти в OWASP Top Ten. Серед них особливу увагу привертають ін'єкції такі як SQL Injection та XSS, і така вразливість як Broken Access Control, які можуть мати руйнівні наслідки для безпеки вебсайтів. [1]

Ін'єкції залишаються однією з найсерйозніших загроз, оскільки вони дозволяють зловмисникам впроваджувати шкідливий код у запити, що виконуються системою. SQL Injection є класичним прикладом такої атаки, за якої небезпечний SQL-код може бути виконаний, якщо дані, введені користувачем, передаються у запити до бази даних без належної перевірки. Наслідки можуть включати витік або видалення даних, а також отримання несанкціонованого доступу до адміністративних функцій. Для захисту від SQL-ін'єкцій рекомендується використовувати підготовлені запити та суворо обмежувати права доступу до бази даних. Інший поширений тип ін'єкцій — XSS, який спрямований на впровадження шкідливого коду, зазвичай JavaScript, що буде виконуватися в браузері користувача. XSS може бути використаний для крадіжки cookie, перенаправлення користувачів на фішингові сайти або виконання шкідливих дій.

XSS має три основні види, які визначаються способом впровадження та виконання шкідливого коду:

Stored XSS є найнебезпечнішим, оскільки шкідливий код зберігається на сервері і виконується щоразу, коли користувач відкриває заражену сторінку. Наприклад, якщо зловмисник вставить небезпечний JavaScript у форму коментарів, цей код автоматично виконуватиметься для всіх користувачів, які переглядають коментарі.

Reflected XSS виникає, коли шкідливий код потрапляє у відповідь сервера через введені користувачем дані, наприклад, через URL або форму пошуку. Такий код виконується лише тоді, коли користувач переходить за спеціально сформованим посиланням.

DOM-based XSS є специфічною формою атаки, яка працює на рівні клієнтського коду в браузері і використовує недоліки JavaScript для маніпулювання DOM без участі сервера.

Broken Access Control — ще одна критична вразливість, яка дозволяє зловмисникам отримати доступ до ресурсів або функцій, які мали б бути для них недоступними. Наприклад, зловмисник може вручну змінити URL, щоб отримати доступ до конфіденційної інформації чи виконати адміністративні дії. Часто ці помилки виникають через відсутність серверних перевірок прав доступу. [2]

Отже, безпека веб-додатків є критично важливим аспектом у сучасному цифровому середовищі, де загрози постійно еволюціонують. Вразливості, такі як (SQL Injection, XSS та Broken Access Control, які виділені у рейтингу OWASP Top Ten, демонструють, наскільки серйозними можуть бути наслідки недостатнього захисту систем. Розуміння механізмів цих атак, їх типів і способів експлуатації дає змогу розробникам більш усвідомлено підходити до створення безпечного коду.

Список використаних джерел

1. OWASP Top Ten | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-top-ten/ (date of access: 02.12.2024).
2. A01 Broken Access Control - OWASP Top 10:2021. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/Top10/A01_2021-Broken_Access_Control/ (date of access: 02.12.2024).