ОСНОВНІ ЗАГРОЗИ ВЕБ ЗАСТОСУНКІВ

Куценко Д.О., Федорченко В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Метою доповіді аналіз основних загроз в веб застосунках.

Веб застосунки використовуються для різних потреб суспільства, поступово збільшується використання нових технологій розробки та створення більш масштабних технічних рішень: інтернет магазинів, e-comerce платформ, тощо.

Технічний розвиток веб застосунків у свою чергу зумовлює виникнення нових загроз інформаційної безпеки, саме тому необхідно постійно вдосконалювати методики та алгоритми захисту веб застосунків з метою подальшого виявлення та протидії загрозам.

Серед основних видів загроз особливо необхідно приділити увагу наступним типам загроз на веб застосунки, а саме: міжсайтовий скриптинг, SQL ін'єкції, відмова в обслуговуванні, обхід каталогів, та впровадження команд [1]. Найбільш поширеними серед них у наш час є міжсайтовий скрипінг, SQL ін'єкція, та відмова в обслуговуванні.

Міжсайтовий скрипінг дозволяє зловмисникові впроваджувати шкідливий код через веб-сайт в браузери інших користувачів. SQL-ін'єкції дозволяють зловмисникам виконувати довільний код SQL в базі даних, дозволяючи отримувати, змінювати або видаляти дані незалежно від дозволів користувача. Відмова в обслуговуванні зазвичай досягається за рахунок наповнення цільового сайту підробленими запитами, так що доступ до сайту порушується для законних користувачів [2].

Обхід каталогів зумовлює отримання доступу до частин файлової системи веб-сервера, зловмисником.

Також існує загроза включення файлу, де користувач може вказати файл для відображення або виконання в даних, переданих на сервер. Атаки з впровадженням команд дозволяють зловмиснику виконувати довільні системні команди в операційній системі сервера.

Для протидії загрозам необхідно дотримуватися основних заходів інформаційної безпеки та користуватися інструментами та алгоритмами виявлення загроз. Загалом, регулярна зміна паролів, відмова від використання застарілих протоколів, налаштування і використання HTTPS/HSTS допоможе захистити інформацію в веб застосунках від основних загроз.

Список літератури

1. List of Attacks / Open Web Application Security Project. URL: https://owasp.org/www-community/attacks/.

2. Top 10 Web Application Security Risks / Open Web Application Security Project. URL: https://owasp.org/ www-project-top-ten