УДК 004.415.5
С. Вишковський
(Тернопільський національний технічний університет імені Івана Пулюя)

ІНФОРМАЦІЙНИХ ВЕБ-САЙТІВ ТА МЕТОДІВ ЇХ УСУНЕННЯ ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ

За останнє десятиліття Web-сайти (Web-додатки) пройшли шлях від статичних сторінок до динамічних інтерактивних порталів з широкою функціональністю і складними системами управління інформацією. Сьогодні Web-додатки не тільки є гідними конкурентами багатьом прикладним програмам для настільних ПК, а й продовжують розширювати межі використання завдяки перевагам величезних хмарних сервісів. Практично кожне офісне прикладне програмне забезпечення має аналог, який працює через Web-браузер. Користувачі можуть з легкістю створювати, редагувати і поширювати інформацію через Web-браузери незалежно від матеріального становища і пристроїв, що використовуються, позбуваючись від кайданів офісу і настільних ПК.

Додатки використовують SQL-запити для того, щоб отримувати, додавати, змінювати або видаляти дані, наприклад при редагуванні користувачем своїх особистих даних або заповненні анкети на сайті. При недостатній перевірці даних від користувача, зловмисник може впровадити в форму Web-інтерфейсу додатку спеціальний код, що містить шматок SQL-запиту. Такий вид атаки – SQL-ін'єкція. Це найнебезпечніша вразливість, що дозволяє зловмисникові отримати доступ до бази даних і можливість читати / змінювати / видаляти інформацію, яка для нього не призначена. Крім ін’єкцій баз даних, загроза типу «ін'єкція» існує для будь-якого іншого середовища, яке отримує дані ззовні. Ще один поширений випадок – це ін’єкція командного інтерпретатора операційної системи, так звані «OS injections».

Міжсайтовий скриптинг – ще одна помилка валідації, яка дозволяє передати JavaScript код на виконання в браузер користувача. Атаки такого роду часто також називають HTML-ін’єкціями, адже механізм їх впровадження дуже схожий з SQL-ін’єкціями, але на відміну від останніх, впроваджуваний код виконується в браузері користувача.

Безпека Web-додатків вимагає наявності безпечної конфігурації всіх компонентів інфраструктури: компонентів програми (таких як фреймворки – frameworks), веб-сервера, сервера баз даних і самої платформи. Налаштування компонентів сервера за замовчуванням найчастіше небезпечні і відкривають можливості до атак.

В доповіді буде висвітлено основні підходи до виявлення вразливостей веб-додатків на прикладі інформаційного сайту «Travel Anywhere».