УДК 681.31

ІНТЕГРОВАНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ WEB-ДИЗАЙНУ САЙТІВ

Бойко М. О.
Науковий керівник – доц. , к.т.н. Семеренко В.П.

Багато зломів сайтів відбуваються в результаті помилок програмістів, що створють сайт або включають активні компоненти на сайт. Ці помилки можуть використовуватися хакером для отримання доступу до системи або для підвищення своїх привілеїв. Тому необхідно приділяти велику увагу захисту сайту.

Кожен сайт містить вразливості. Їх можна розподілити на три категорії:

– організаційні: основою вразливостей є людський фактор; ці вразливісті вирішується за допомогою певних правил роботи з сайтом або за рахунок спеціального програмного забезпечення.

– проектувальні: уразливість безпосередньо додатка; ці вразливості усуваються шляхом урахування можлих атак при розробці.

– експлуатаційні: атака може бути проведена на рівні сервера або інфраструктури; ці проблеми вирішуються адміністраторами веб-сайтів.

Зараз великої поширеності набуває технологія OAuth 2.0 – протокол взаємодії клієнтського додатку, користувача і сервера, який дозволяє користувачам на сайті проходити авторизацію через соціальні мережі.

Роботу користувача з протоколом OAuth 2.0 можна представити у вигляді послідовності таких кроків:

1. Користувач переадресується на сторінку надання прав клієнтського додатку на зазначені права.

2. Користувач авторизує клієнтський додаток та отримує дозвіл використання тих чи інших особистих даних.

3. Після авторизації клієнтський додаток переадресовує користувача на *redirect_uri*, при цьому відбувається передача параметра *access_token*, який використовується для подальшої взаємодії з сервером.

При роботі з OAuth 2.0 виникає проектувальна вразливість, зловмисник може «прив'язатися» до облікового запису жертви та проходити аутентифікацію на сайті під виглядом жертви.

В даній роботі пропонується вирішення даної вразливості шляхом використання унікальної адреси перенаправлення.