АНАЛІЗ ІНФОРМАЦІЙНИХ РИЗИКІВ МЕДИЧНИХ ВЕБ-СЕРВІСІВ

Сидоренко З.М.[1], Трубіцин О.О.[2], Крамчанінов М.О.[2]
[1]«Харківський національний університет радіоелектроніки», м. Харків
[2]«Харківський ліцей № 14 Харківської міської ради», м. Харків

На сьогоднішній день проблема безпеки медичних веб-додатків продовжує залишатися однією з найбільш актуальних. Це обумовлено розвитком функціоналу та зростанням кількості медичних додатків, а також кількості користувачів. Завдяки використанню медичних веб-сервісів лікувальні заклади можуть надавати різноманітні консультативні послуги пацієнтам. В деяких випадках вести віддалений моніторинг стану хворого. Саме тому управління інформаційними ризиками кібер-безпеки веб-додатків стоїть на шляху подальшого розвитку телемедицини.

Метою доповіді є аналіз сучасних ризиків інформаційної безпеки медичних веб-сервісів. Проведений авторами аналіз проблемної області дозволив виділити наступні, найбільш поширені, сучасні загрози порушення інформаційної безпеки веб-додатків, що можуть привести до втрати конфіденційності медичних даних:

1. Вразливість SQL Injection (SQLi). Ця вразливість становить загрозу для даних, розміщених на сайтах, що працюють під управлінням реляційних баз даних, таких як MySQL, PostgreSQL, sqlite. У багатьох випадках зловмисник може змінювати або видаляти ці дані, викликаючи постійні зміни у вмісті або поведінці програми. Успішна атака SQL-ін'єкції може призвести до несанкціонованого доступу до конфіденційних даних, таких як паролі, дані кредитних карток або особиста інформація користувачів.

2. XSS Injection (Cross Site Scripting). Цей тип уразливості дозволяє впроваджувати довільний шкідливий код на стороні клієнта або сервера, який часто називають RCE (Remote Code Execution).

3. IDOR (Insecure Direct Object References). Ця вразливість дозволяє отримати несанкціонований доступ до веб-сторінок та файлів у разі помилок налаштувань доступу до них на боці сервера.

4. Також слід зазначити, що значна кількість медичних веб-сервісів побудована на базі систем керування вмістом, таких як: WordPress, Joomla, Drupal. Тож, використання застарілих версій цих систем та плагінів може надати зловмиснику контроль за адміністративною панеллю.

В якості прикладу можна навести старий плагін для WordPress – Bricks версії якого, починаючи від 1.9.6 та старіші схильні до вразливості CVE-2024-25600, яка дозволяє віддалено отримати доступ до адміністративної панелі.

Проведений аналіз дозволяє зробити висновки, що серед значних загроз інформаційної безпеки додатків продовжують і досі залишатися вже досить добре відомі вразливості. Тож одним з головних факторів безпеки є регулярне підвищення компетенції розробників та адміністраторів веб-додатків. Участь програмах навчання, проведення професійних тематичних семінарів, обмін опитом та регулярне підвищення кваліфікацій фахівців за напрямком «кібер-безпека».