УДК 004.657
А. Романець, Г. Козбур
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

БЕЗПЕКА СОЦМЕРЕЖІ ПІД ЧАС АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА

UDC 004.657
A. Romanets, G. Kozbur

SOCIAL NETWORK SECURITY DURING USER AUTHENTICATION

Авторизація та реєстрація є невід'ємною частиною для роботи будь-якої соцмережі. Проте на етапі авторизації або реєстрації вебсайт є дуже вразливим, оскільки недбросовісні користувачі можуть зашкодити базі даних методом надсилання певних запитів. Тому потрібно запровадити валідацію даних та перевіряти усі дані, що надсилаються на сервер з боку клієнта. Система має бути захищена від перебору паролів зловмисниками для доступу до акаунта. Особливу увагу потрібно приділити безпеці соцмережі, від цього може залежати стабільна робота усього вебсайту.

Потрібно реалізувати функцію валідації даних як на сервері, так і на клієнті, яка буде приймати як параметри самі дані та тип валідації (включаючи регулярні вирази). Викликати таку функцію можна за кілька рядків коду. Будь-які дані, що потрапляють на сервер із клієнта, повинні бути очищені, оскільки це може вплинути на життєздатність всієї соцмережі та безпеки даних користувачів. При реєстрації через e-mail проводиться перевірка на наявність пошти в базі даних. Якщо користувач з таким e-mail вже зареєстрований, відбувається перевірка на прив'язані сервіси. До того, як користувач не підтвердив свій e-mail, його обліковий запис є тимчасовим. Це дозволяє керувати правами доступу (наприклад, таким користувачам можна обмежити набір дозволених дій), автоматично очищати базу від неактивованих облікових записів. У базі даних тимчасовий обліковий запис можна відрізняти від звичайного простою булевою позначкою або зберігати в окремій таблиці. Для реалізації підтвердження e-mail можна використати вже готові рішення. Листи можуть надсилатися з багатьох сторінок продукту, тому потрібно створити єдину функцію для цього. Враховуючи, що на сервері реалізовано очищення БД від неактивних акаунтів, потрібно встановити термін дії підтверджуючого посилання, який буде меншим, ніж період активності тимчасових акаунтів. Це виключить помилки, коли користувач намагається підтвердити пошту, а його тимчасовий обліковий запис вже видалено. Дуже важливо, щоб посилання на зміну пароля не було «вічним». Тому під час перевірки посилання на сервері, безпосередньо, перевіряється його термін дії. Однак для убезпечення від зловмисників не слід показувати повідомлення про «застаріле» посилання, вказавши просто на загальну помилку «неправильне посилання». Іноді це може створити незручність для користувачів, проте підвищить рівень безпеки. Також не можна дозволяти користувачам кілька разів скидати пароль за одним посиланням. Тому після першого переходу з листа посилання потрібно деактивувати. Для захисту від перебору паролів потрібно реалізувати функцію перевірки ір-адреси користувача та обмежити кількість спроб вводу паролю.

Література

1. Adrian W. West. Practical PHP and MySQL Website Databases: A Simplified Approach. Apress, 2018. P. 61–74.
2. Awa Melvine. Complete user registration system using PHP and MySQL database. URL: https: //cutt.ly/B1HKUA2.
3. Ruslan. Створюємо реєстрацію на сайті з допомогою PHP і MySQL. URL: https://cutt.ly/ q1HJHUN.