УДК 004.056
І. Галанський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СИСТЕМА ЗАХИСТУ WEB-ЗАСТОСУНКІВ НА ОСНОВІ ДВОХФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

UDC 004.056
I. Halanskyi

WEB APPLICATION PROTECTION SYSTEM BASED ON TWO-FACTOR AUTHENTICATION

Двофакторна автентифікація (2FA) є важливим елементом сучасних систем безпеки, що забезпечує захист від несанкціонованого доступу за рахунок використання двох незалежних факторів перевірки. Її застосування дозволяє знизити ризик атак типу «людина посередник», фішингу та компрометації облікових даних, що є особливо актуальним для веб-додатків [1].

Під час виконання роботи було проаналізовано існуючі методи автентифікації. Традиційні паролі залишаються поширеним методом, однак їх низький рівень захисту через можливість перехоплення або підбору вимагає пошуку альтернатив. Біометричні методи пропонують високий рівень безпеки, але є дорогими у впровадженні та складними в інтеграції. Одноразові паролі (OTP), зокрема алгоритм TOTP (Time-based One-Time Password), було визначено як оптимальне рішення, яке поєднує високий рівень безпеки, простоту реалізації та доступність [2].

Впровадження системи двофакторної автентифікації включала кілька ключових етапів. Спочатку було визначено архітектуру системи з урахуванням сучасних вимог до безпеки та масштабованості. Для цього було обрано технології PHP як основну мову серверного програмування, MySQL як базу даних, а для надсилання одноразових паролів – бібліотеку PHPMailer.

На етапі реалізації було написано програмний модуль, який відповідає за генерацію одноразових паролів на основі алгоритму TOTP. Алгоритм працює за принципом генерації динамічних кодів, що змінюються з фіксованим часовим інтервалом, забезпечуючи високий рівень захисту за рахунок унікальності кожного пароля. Генеровані паролі надсилаються користувачам через електронну пошту, що є доступним і зручним каналом зв'язку.

Тестування системи показало її ефективність у протидії основним кіберзагрозам. Було перевірено стійкість до атак «людина посередник», перехоплення даних та фішингових атак. Отримані результати підтвердили, що запропоноване рішення відповідає сучасним вимогам до інформаційної безпеки та може бути використане у різних сферах, таких як електронна комерція, банківські системи або корпоративні мережі.

Впровадження двофакторної автентифікації на основі алгоритму TOTP є доступним і ефективним способом підвищення безпеки веб-додатків, що не потребує значних фінансових витрат, але забезпечує високий рівень захисту даних користувачів.

Література

1. Omwoyo R., Kamau J., Mvurya M. A review of Two Factor Authentication Security Challenges in the Cyberspace | International Journal of Advanced Computer Technology. *International Journal of Advanced Computer Technology*. URL: https://ijact.org/index.php/ijact/article/view/112 (дата звернення: 12.11.2024).
2. RFC 6238: TOTP: Time-Based One-Time Password Algorithm / D. M'Raihi et al. *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc6238 (дата звернення: 14.11.2024).