УДК 004.418
Б. Тригубець
(Тернопільський національний технічний університет імені Івана Пулюя)

РОЗРОБКА CMS ТА МЕТОДІВ ЗАХИСТУ WEB-САЙТІВ НА ЇЇ ОСНОВІ

UDC 004.418
B. Tryhubets
(Ternopil Ivan Puluj National Technical University, Ukraine)

DEVELOPMENT OF CMS AND WEB SITE SECURITY METHODS

Основну частину сучасного інформаційного простору та мережі інтернет вцілому складають web-сайти, саме на них генерується інформаційний контент та зберігаються дані про користувачів. Якщо доступ до даних, які зберігаються на web-ресурсах, та доступ до інструментів для їх генерації, отримують зловмисники, вони можуть бути використані в корисливих цілях та завдати великих фінансових та репутаційних збитків компанії, яка потрапила під атаку.

В цій магістерській роботі було проаналізовано основні загрози безпечному функціонуванню web-сайтів, розглянуто правила, яких потрібно дотримуватись при їх розробці, та при розробці інструментів, за допомогою яких web-сайт буде адмініструватися. Захист web-сайту можна умовно поділити на захист сервера, на якому він знаходиться, та захист програмної частини, яку використовує як рядовий користувач, так і адміністратор.

Було розглянуто приклади основних груп атак на серверну частину та запропоновано методи захисту від них:

DDoS-атакам в реаліях сьогоднішніх маштабів можна успішно протистояти лише за допомогою використання спеціалізованих сервісів, таких як Cloudflare. Висока пропускна здатність сервісу та детальний аналіз усіх джерел трафіку, який надходить на сайт, на основі використання власних алгоритмів допомагає вистояти навіть при потужних DDoS-атаках;

Уникнути несанкціонованого доступу через FTP/SSH можливо використовуючи SSH-ключі, доступ через нестандартні порти в налаштуваннях серверу, налаштувючи обмеження кількості невдалих спроб авторизації та блокуванню доступу до певних директорій, у яких зберігаються важливі файли системи, або ж дозволити доступ до них тільки з певного IP;

Запобігти атаці «людина посередині» та витоку придатних для читання данних можна використовуючи для HTTP-з'єднання SSL-сертифікат, та нової версії протоколу HTTP/3;

Розглянуто основні груп атак на програмну частину та методи захисту від них:

Вразливості неправильної обробки вхідних даних відкривають можливісті для SQL-ін’єкцій та XSS-атак. Використання популярних функцій для екранування вхідного коду, перевірка усіх вхідних даних через форми та GET-запити, а також правильна робота з доступом до файлів Cookies допомагає ліквідувати ці вразливості.

Недостатня аутентифікація та авторизація на web-сайті призводить до виконання критичних дій від імені адміністратора, та доступу рядових користувачів до важливих функцій у адмін-панелі. Використовуючи двохфакторну аутентифікацію з використанням додатку Google Authenticator з тимчасовим паролем, цю вразливість можна нейтралізувати, а розмежування прав доступу між користувачами допоможе уникнути проблеми людського фактору. Власна розробка допоможе уникнути використання стандартизованих методів атак, які доступні для інших популярних CMS.

Використовуючи розроблену CMS, у яку інтегровані вищенаведені методи захисту, можна суттєво зменшити загрозу несанкціонованого доступу до інформації, яка знаходиться на сайті, та забезпечити його стабільну роботу.