УДК 004.946

Гнатишин М. – ст. гр. СН-41
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ РИЗИКІВ БЕЗПЕКИ ТЕХНОЛОГІЙ ВЕБ-РОЗРОБКИ

Науковий керівник: к.т.н., доцент Фриз М. Є.

Hnatyshyn M. A.
Ternopil Ivan Puluj National Technical University

RESEARCH OF WEB DEVELOPMENT TECHNOLOGY SECURITY RISKS

Supervisor: PhD, Assoc. Prof. M. Fryz

Ключові слова: веб-безпека, загроза, захист.
Keywords: web security, threat, protection.

Веб-безпека дуже важлива в наш час. Веб-сайти завжди схильні до загроз чи ризиків безпеці. «Недостатня захищеність веб-сайту може призвести до викрадення важливих даних клієнта. Прикладом цього можуть бути дані кредитної картки або реєстраційні дані клієнта. Це може стати причиною розповсюдження конфіденційних даних користувачів сайту та знищення власного бізнесу» [4]. Загроза безпеці визначається як ризик, який потенційно може завдати шкоди комп'ютерним системам і організаціям. Атаки на безпеку в основному спрямовані на викрадення, зміну або знищення частини особистої та конфіденційної інформації, викрадення місця на жорсткому диску та незаконний доступ до паролів.

Для запобігання проблем, що виникають через ненадійність сайтів, варто впроваджувати тестування. «Тестування веб-безпеки має на меті виявити вразливі місця у веб-додатках та їх конфігурації. Основною метою є прикладний рівень. Перевірка безпеки веб-додатку часто передбачає надсилання різних типів вхідних даних, щоб спровокувати помилки та змусити систему поводитись несподіваним чином. Ці так звані «негативні тести» перевіряють, чи робить система щось, для чого вона не призначена» [3].

Загрози веб-безпеці постійно з'являються та розвиваються, але можна виділити найбільш популярні атаки, а саме: SQL ін'єкція, XSS (міжсайтовий сценарій), віддалене виконання команд та обхід шляху. Результатами виконання таких атак можуть стати несанкційний доступ до обмеженого вмісту, зламані облікові записи користувачів, установка шкідливого коду та багато іншого.

Міжсайтові сценарії (XSS) – «це тип ін'єкцій, під час яких шкідливі сценарії впроваджуються на безпечні та надійні веб-сайти. XSS-атаки відбуваються, коли зловмисник використовує веб-програму для надсилання шкідливого коду, як правило, у формі сценарію сторони браузера, іншому кінцевому користувачеві. Недоліки, які дозволяють цим атакам бути успішними, досить широко поширені та виникають у будь-якому місці, де веб-додаток використовує вхідні дані від користувача в межах вихідних даних, які він генерує, без їх перевірки чи кодування. Міжсайтові сценарії (XSS) атаки відбуваються, коли дані надходять у веб-програму через ненадійне джерело, найчастіше через веб-запит, чи дані включаються в динамічний вміст, який надсилається веб-користувачу без перевірки на шкідливий вміст» [2].

«Недоліки SQL ін'єкції є результатом класичної відмови фільтрувати ненадійні дані. Помилки ін'єкцій можуть виникнути, при умові, якщо невідфільтровані дані передаються на SQL сервер (ін'єкція SQL), у браузер (через міжсайтовий сценарій), на сервер LDAP (ін'єкція LDAP) або будь-де ще. Проблема полягає в тому, що зловмисник може вводити команди для викрадення браузерів клієнтів, що призводить до втрати даних» [1]. Все, що програма отримує з ненадійного джерела, має бути відфільтровано, бажано відповідно до білого списку.

Отже, для того, щоби запобігти небезпеки успішного злому сайту, потрібно дотримуватися певних правил. Найпростішим, але дуже важливим рішенням є встановлення надійного паролю. «Пароль забезпечує першу лінію захисту від несанкціонованого доступу до пристрою та особистої інформації. Доцільно дотримуватися вимог до паролів, наприклад, створити такий, що складатиметься мінімум з восьми символів, включаючи великі літери, малі літери, спеціальні символи та цифри» [4]. Також важливо передбачити перевірку даних, що запобігатиме потраплянню неправильно створених даних в інформаційну систему. Перевірку даних слід виконувати як на стороні сервера, так і на стороні клієнта. Розробнику необхідно бути дуже обережним, створюючи повідомлення про помилки, які генеруються для надання інформації користувачам під час доступу користувачів до веб-сайту. У повідомленні не може міститися інформація, що зможе бути використана зловмисниками, наприклад для спроби входу – якщо користувачу не вдається ввійти, повідомлення про помилку не повинно повідомляти користувачеві, яке поле є неправильним: ім'я користувача чи пароль. «Важливою порадою також є регулярне оновлення програмного забезпечення, оскільки хакери можуть знати про вразливі місця в певному програмному забезпеченні» [4]. Такі, на перший погляд, прості поради можуть вберегти сайт від злому, чи ускладнять роботу хакерів.

Список використаних джерел

1. 10 Common Web Security Vulnerabilities [Ел. ресурс]. − Режим доступу: https://www.toptal.com/security/10-most-common-web-security-vulnerabilities
2. Cross Site Scripting (XSS) [Ел. ресурс]. − Режим доступу: https://owasp.org/www-community/attacks/xss/
3. Web Application Security [Ел. ресурс]. − Режим доступу: https://www.synopsys.com/glossary/what-is-web-application-security.html
4. Web Security Considerations [Ел. ресурс]. − Режим доступу: https://www.geeksforgeeks.org/web-security-considerations/