Ляшеник В.В., Молотов А.Р.
студенти,
Науковий керівник: **Вовк Р.Б.**
кандидат технічних наук, доцент,
Івано-Франківський національний технічний університет нафти і газу

РОЗРОБКА КОНЦЕПЦІЇ ПРОЕКТУВАННЯ WEB-ОРІЄНТОВАНИХ СИСТЕМ

З розвитком інтернет-технологій і зростанням попиту на web-ресурси виникає проблема у систематизації правил розробки web-систем. Web-системи – це потужні програмні додатки, які складаються з певної кількості прикладних програм, котрі мають систему розмежувань прав та привілеїв і призначені для надання персоналізованого доступу до web-ресурсу великій кількості користувачів.

Основною задачею проектування web-орієнтованих систем є забезпечення безпеки персональної інформації користувачів, коректної роботи з інформацією та зручності у користуванні. Для web-систем безпека відіграє значну роль і коректна робота web-серверів відповідає практично за всі послуги та функціонування мільярдів сайтів в усьому світі внаслідок чого перетворюється на сховище персональних даних користувачів. Для ретельного захисту web-орієнтованих систем потрібні спільні зусилля адміністраторів, програмістів, проектувальників та тестувальників. Також постійної уваги потребують такі аспекти як правильна робота антивірусного програмного забезпечення, операційних систем та контролю за правами доступу.

Основним етапом проектування інтернет-ресурсу є забезпечення максимального рівня безпеки сервера, на якому він знаходиться. Відомо, що основою web-сервера є операційна система, для забезпечення безпеки якої необхідно вчасно встановлювати останні оновлення. Також важливим аспектом безпеки є те, що не варто встановлювати зайві компоненти, оскільки кожен з них може нести в собі потенційну загрозу. Web-орієнтовані системи є досить вразливими через свою відкритість, оскільки за своїм призначенням вони розраховані на обмін інформацією з користувачами. Наприклад, зловмисник може здійснити модифікацію коду, змінити запити до HTTP-сервера або сервера бази даних, або взагалі структуру сторінок сайту, змінивши при цьому первинну функціональність [1]. Іншою важливою вимогою до проектування web-систем є необхідність використання сучасних стандартів і технологій, які повинні відповідати наступним вимогам: простота у супроводі та користуванні, поширеність, кросплатформенність. Зручність користування можна пояснити одним висловом «Logon and Go», тобто все, що потрібно користувачу для коректної роботи з системою це підключення до інтернету, наявність браузера, логін та пароль [2].

Щоб визначити як краще систематизувати процес створення сайту необхідно оцінити основні вразливості web-систем. Тому було розроблено

концепцію згідно якої для забезпечення коректної роботи web-системи необхідно:

1. Підвищувати надійність завдяки впровадженню єдиної системи ведення облікових записів (реєстрація, авторизація, вибірка, обробка).

Проектування будь-яких web-ресурсів повинне бути орієнтоване на відвідувачів, тому інтерфейс має бути простим та зручним. У зв'язку з цим зазвичай використовують спільні облікові записи користувачів, реєстрація та авторизація, яких відбувається лише один раз. Оскільки дані заповнюються тільки в одному екземплярі то пропадає необхідність зберігання відвідувачами великої кількості паролів, зменшується дублювання інформації в базах даних web-системи, полегшується редагування та адміністрування облікових записів. Як приклад, спільні облікові записи реалізовано компаніями Google, Яндекс, Хабрахабр, що забезпечує надзвичайну гнучкість супроводу web-систем та просте користування ресурсом загалом.

2. Створювати програмний код багаторазового використання.

Написання програмного коду на основі уже існуючого (успадкування) оптимізує розробку web-систем, оскільки разом з інкапсуляцією та поліморфізмом успадкування утворює об'єктно-орієнтоване програмування, яке із перезавантаженням та перевизначенням методів в свою чергу дозволяє замінити тисячі рядків коду на декілька методів, тим самим зменшити кількість рядків коду і відповідно помилок в ньому.

3. Налаштовувати коректну перевірку вхідних даних, а саме:

- враховувати особливості методів GET, POST передачі інформації;
- уникати небезпечних прямих посилань на об'єкти;
- уникати віддаленого виконання коду;
- уникати SQL ін'єкцій при роботі з базою даних;
- уникати міжсайтового виконання сценаріїв і підробки запитів;
- опрацьовувати файли, що передаються користувачем;
- використовувати правила заміни посилань.

Надсилання інформації серверній частині web-системи може відбуватись методами GET і POST. Метод GET використовується тоді, коли потрібно передати посилання із наперед вказаними аргументами (обрані категорії, сортування, пошуковий текст). Метод POST слід застосовувати при надсиланні інформації для збереження, обробки тощо. Якщо аргументом GET методу зазначається назва файлу, в подальшому довантажуючись в головну сторінку, то ця назва ретельно перевіряється на доступність та правильність. В протилежному випадку можливий прямий доступ до файлу чи віддалене виконання коду, тобто замість очікуваних значень зловмисник надає користувачу шлях до шкідливого виконуваного файлу.

Серед вхідних даних потрібно фільтрувати спеціальні символи, забезпечуючи безпеку web-системи від міжсайтового виконання сценаріїв, SQL ін'єкцій тощо. Не менш важливою є проблема міжсайтової підміни запитів, для уникнення якої у форму добавляють додаткове поле із унікальним ключем, при відсутності чи некоректності якого запит вважається невірним.

4. Використовувати механізми захисту від переповнення буфера.

Найбільш небезпечною вразливістю у будь-якій системі є переповнення буфера, оскільки присутня можливість виконання інструкцій процесора з привілеями вразливого потоку. Оброблення інформації у програмах відбувається організацією буферів певного розміру, які розміщуються в стеку, де зберігаються також адреса повернення функції, значення регістрів та інше. Стек – це частина адресного простору програми, в якому присутній і сам програмний код у вигляді інструкцій процесора. При переповненні дані, що не вмістились в буфер, записуються за його межами, тому зловмисник може підмінити адресу повернення та виконати набір команд попередньо згенерувавши їх на вхід web-системи.

В сучасних операційних системах реалізовано функцію запобігання виконання даних (DEP) із області пам’яті, поміченої як «не для виконання». До цього ж програмістами web-сайтів прийнято використовувати засоби з вбудованим захистом від переповнення накопичувача: мови програмування, окремі їх функції. Слід зазначити, що розміщення даних у статичній чи динамічній пам’яті не позбавляє від переповнення буферу, а лише забороняє підміну адреси повернення функції [3].

5. Налаштовувати алгоритми роботи з паролями.

Не рекомендовано зберігати паролі користувачів у відкритому вигляді, а необхідно їх перетворювати у хеш-код за допомогою алгоритмів MD5, SHA1 чи SHA-2 і випадкового модифікатора. В цьому випадку відновити пароль буде неможливо, тому здійснюють генерацію нової хеш-суми і алгоритм авторизації на сайті передбачає порівнювання кодів з бази даних та вхідного паролю.

6. Зменшувати вимоги до апаратних ресурсів шляхом оптимізації програмного коду та мінімізації дублювання інформації у базі даних.

Одним із головних методів оптимізації програмного коду web-ресурсу є кешування – процес зберігання часто використовуваних значень в швидкісній пам’яті під певним ключем. Воно водночас дозволяє зменшити використання оперативної пам’яті, запам’ятовуючого пристрою, процесорного часу та мережі. Критерій ефективності визначається відношенням кількості запитів, для яких знайшлась відповідь у кеші, до загального числа запитів. Вважається неефективною реалізація кешування якщо результат становить менше 50-60%. Проблему інвалідації вирішують поміркованим оновленням кешу відмітивши поточні дані застарілими. В іншому випадку може з’явитись ситуація одночасного оновлення однакової інформації декількома процесами, що вимагає зайвих ресурсів [4].

7. Організовувати захист від DDOS атак.

8. Розміщувати компоненти на єдиному домені.

9. Виконувати перевірку на права доступу до елементів web-системи.

10. Враховувати появу неочікуваних помилок при роботі web-програм.

11. Налаштовувати коректний вивід інформації [2; 5].

Отже, в результаті даного дослідження було проаналізовано основні вразливості інтернет-ресурсів і враховуючи кількість помилок при їх розробці була розроблена концепція проектування web-орієнтованих систем. Вона містить аспекти на які необхідно звертати увагу розробникам при створенні

web-додатків, а саме на захист персональних даних користувачів, оптимізацію програмного коду для зменшення вимог до апаратних ресурсів, налаштування конфігурації серверів і т.п.

Список використаних джерел:

1. Sophos Plc. Забезпечення безпеки веб-сайтів [Електронний ресурс] / Sophos Plc, SophosLabs. – 2007. – Режим доступу до ресурсу: https://yandex.ru/support/webmaster/protecting-sites/basics.xml

2. Бойко Н.І. Моделювання Web-орієнтованих систем та напрямки розвитку Web-ресурсів / Н.І. Бойко – Вісник Національного університету «Львівська політехніка». – 2012. – № 743 : Інформаційні системи та мережі. – С. 16–25.

3. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – Київ: Видавнича група BHV, 2009. – 608 с. – ISBN 966-552-167-5.

4. Масштабирование бекенда [Електронний ресурс] // Журнал «Хакер». – 2012. – Режим доступу до ресурсу: https://xakep.ru/2012/11/30/backend-zoom/

5. Докукін Є. Безпека веб-додатків та веб-систем [Електронний ресурс] / Є. Докукін. – 2015. – Режим доступу до ресурсу: http://websecurity.com.ua/

Молявка О.С.

аспірант,

Науковий керівник: **Пугачевський Г.Ф.**

доктор технічних наук, професор,

Київський національний торговельно-економічний університет

ВПЛИВ ФІЗИКО-МЕХАНІЧНИХ ВЛАСТИВОСТЕЙ НА ФОРМУВАННЯ ЯКОСТІ ПАНЧІШНО-ШКАРПЕТКОВИХ ВИРОБІВ ВІДОМЧОГО ПРИЗНАЧЕННЯ

На сучасному етапі розвитку трикотажної промисловості актуальним є оптимізація асортименту та поліпшення якості випущеної продукції при більш ефективному використанні вітчизняних сировинних ресурсів.

Метою роботи є проведення ряду досліджень для розширення асортименту та покращення міцності панчішно-шкарпеткових виробів (далі ПШВ). Для створення нових артикулів шкарпеток з підвищеними експлуатаційними характеристиками за рахунок використання нової сировини.

На сьогодні велика кількість робіт присвячена дослідженню якості та розробці ПШВ [1-4]. Їх дослідження в основному спрямовані на розробку нових технологій в’язання та надання бактерицидних властивостей методом просочення бактерицидними розчинами.

На нашу думку є необхідність у розробці та дослідженні панчішно-шкарпеткових виробів відомчого призначення виготовлених з натуральної національної сировини, без використання нових фінансово затратних технологій.