ДВНЗ «ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
Факультет комп'ютерно-інформаційних технологій та автоматизації
Кафедра прикладної математики і інформатики

«До захисту допущено»
Завідувачка кафедри ПМІ

_____ Ольга ДМИТРІЄВА
(підпис) (ім'я та прізвище)

«17» червня 2022 р.

Випускна кваліфікаційна робота
бакалавра

(освітньо-кваліфікаційний рівень)

на тему: «Комплексний захист конфіденційної інформації в учбовому закладі»
зі спецчастиною
«Розробка системи захисту персональних даних учнів закладу»

Виконав: студент 4 курсу, групи КІБ-18
(шифр групи)

Спеціальності (напряму підготовки) 125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Огоновський Є.В. _____
(прізвище та ініціали) (підпис)

Керівник проф. каф. ПМІ, д.т.н., проф. Євген БАШКОВ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент доц. каф. КІ, к.т.н., Юлія ДІКОВА _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Нормоконтроль:

_____ к.т.н., доц. Ірина НАЗАРОВА
(підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

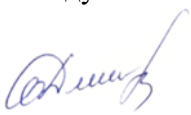
Студент ___ _____
(підпис)

Луцьк – 2022 р.

ДВНЗ «Донецький національний технічний університет»

Факультет комп'ютерно-інформаційних технологій та автоматизації
Кафедра прикладної математики та інформатики
Освітньо-кваліфікаційний рівень (освітній ступінь) _бакалавр
Напрям підготовки (спеціальність) 125 Кібербезпека
(шифр і назва)

ЗАТВЕРДЖУЮ:
Завідувачка кафедри ПМІ



_/Ольга ДМИТРІЄВА

"6".05.2022 року

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Огоновському Євгену Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Комплексний захист конфіденційної інформації в учбовому закладі
Спецчастина: Розробка системи захисту персональних даних учнів закладу_
Керівник роботи Башков Є.О., д.т.н., проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом від "06" травня 2022 року №180
2. Строк подання студентом роботи 15 червня 2022р.
3. Вихідні дані до роботи_результати переддипломної практики; система захисту інформації в навчальних закладах; тестування систем
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно_ розробити):
1) Аналіз проблематики навчальних закладів
2) Огляд засобів захисту персональних даних учнів навчального закладу. Системи автоматизованого тестування;
3) Розробка та дослідження системи захисту персональних даних учныв навчального закладу;

5. Перелік графічного матеріалу
робота містить 27 рисунків, …. слайдів презентації та інший графічний матеріал, у кількості, достатній для демонстрації сутності роботи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 6 травня 2022р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз літератури з предметної області	06.05.2022 – 10.05.2022	
2	Збір інформації і методичних відомостей щодо Захисту додатків	11.05.2022 – 15.05.2022	
3	Розробка структури програмного забезпечення, вибір даних для обробки та експериментів.	16.05.2022 – 22.05.2022_	
4	Тестування системи (модуля)	23.05.2022 – 27. 05.2022	
5	Оформлення пояснювальної записки	28.05.2022 – 08. 06.2022_	
6	Нормоконтроль пояснювальної записки, її перевірка антиплагіатною системою	09.06.2022- 10.06.2022_	
7	Оформлення супутніх матеріалів (розробка графічного матеріалу, написання доповіді, тощо) та рецензування роботи	11.06.2022- 23.06.2022	
8	Захист роботи	24.06.2022	

Студент _ Огоновський Є.В.__
(підпис) (прізвище та ініціали)

Керівник роботи Башков Є.О._____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Огоновський Є. В. Розробка системи захисту персональних даних учнів навчального закладу / Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» за спеціальністю 125 Кібербезпека. – ДВНЗ ДонНТУ, Луцьк, 2022.

Об’єктом дослідження є захист персональних даних учнів навчального закладу.

Предметом дослідження є методи та засоби розробки систем захисту.

Методи досліджень обираються з переліку методів розв’язання задачі класифікації зображень та пошуку найкращого алгоритму для розпізнавання обличчя з гримом (маскуванням) та без нього з метою подальшої ідентифікації.

Науковою новизною одержаних результатів є розробка системи захисту персональних даних учнів навчального закладу.

Метою даної роботи є показати шляхи подолання зазначених труднощів та запропонувати розробку щодо інформаційної безпеки загальноосвітнього навчального закладу.

В ході виконання роботи, було зроблено:

1. Ознайомлення з характеристикою теоретичних основ забезпечення інформаційної безпеки в навчальних закладах.

2. Наведено аналіз підходів до забезпечення інформаційної безпеки в навчальних закладах.

3. Розроблено пропозиції з питань забезпечення інформаційної безпеки в навчальних закладах.

Ключові слова: захист інформації, персональні дані, навчальний заклад.

ABSTRACT

Ogonovsky EV Development of a system for the protection of personal data of students of the educational institution / Graduation thesis for the degree of "bachelor" in the specialty 125 Cybersecurity. - SHEI DonNTU, Lutsk, 2022.

The object of research is the protection of personal data of students of the educational institution.

The subject of research is methods and means of developing protection systems.

Research methods are selected from a list of methods for solving the problem of image classification and finding the best algorithm for face recognition with makeup (masking) and without it for further identification.

The scientific novelty of the obtained results is the development of a system of personal data protection of students of the educational institution.

The purpose of this work is to show ways to overcome these difficulties and to propose the development of information security of the secondary school.

In the course of the work, the following was done:

1. Familiarization with the characteristics of the theoretical foundations of information security in educational institutions.

2. The analysis of approaches to ensuring information security in educational institutions is given.

3. Proposals on information security in educational institutions have been developed.

Key words: information protection, personal data, educational institution.

ЗМІСТ

ВСТУП

Актуальність теми. В нинішній час захист персональних даних набуває все більшої популярності. У зв’язку з цим виникають питання безпеки навчальних закладів та дослідження ризиків розкриття конфіденційних даних або важливих функцій.

Кібератаки на веб-програми відбуваються щодня, і, на жаль, традиційні брандмауери та інші засоби контролю мережевої безпеки не можуть захистити від багатьох векторів атак, які притаманні навчальним закладам. Тестування безпеки начальних закладів критично важливо для захисту програм і організації. Веб-програми, стають найбільшим вектором атак для зловмисників, які прагнуть зламати захист. Доступні користувачам цілодобово і без вихідних, навчальні заклади - найлегша ціль для хакерів, які прагнуть отримати доступ до конфіденційних внутрішніх даних.

Саме тому актуально застосовувати системи автоматизованого тестування навчальних закладів.

Основна мотивація використання систем автоматизованого тестування навчальних закладів полягає в тому, що ручна перевірка коду та традиційні плани тестування забирають багато часу, а нові вразливості постійно вводяться або виявляються.

У багатьох областях існують нормативні директиви, які потребують використання інструментів систем автоматизованого тестування безпеки. Більше того – і, можливо, найголовніше – окремі особи та групи, які мають намір зламати системи, теж використовують інструменти, і ті, кому доручено захищати ці системи, повинні «йти в ногу» зі своїми супротивниками.

Використання інструментів систем автоматизованого тестування дає безліч переваг, які збільшують швидкість, ефективність та охоплення для тестування програм.

Тести, які вони проводять, відтворюються і добре масштабуються після того, як тестовий приклад розроблений в інструменті, він може бути виконаний для багатьох рядків коду з невеликими додатковими витратами.

Подібного роду інструменти ефективні при виявленні відомих вразливостей, проблем та слабких місць. Їх також можна використовувати в робочому процесі виправлення, особливо під час перевірки, і їх можна використовувати для кореляції та виявлення тенденцій та закономірностей.

Таким чином, застосування систем автоматизованого тестування безпеки навчальних закладів є актуальним задля забезпечення інформаційної безпеки.

На даний час існує досить багато рішень автоматизованого тестування безпеки персональних даних, але дані рішення є недостатньо ефективними та швидкими.

Окрім цього, в нинішній час широкого застосування набуває використання нейронних мереж з метою прогнозування загроз, але сучасні рішення автоматизованого тестування безпеки персональних даних не застосовують даний модуль задля підвищення функціональності.

Саме тому в межах роботи буде розглядатися проектування системи, яка перевершить існуючі аналоги у функціональності та можливості прогнозування.

Метою написання бакалаврської роботи є дослідження та проектування системи автоматизованого тестування безпеки персональних даних у навчальних закладах.

При написанні роботи були поставлені наступні задачі:

1. Виконати огляд літератури з теми дослідження. Дослідити проблеми захисту персональних даних та визначити актуальність автоматизованого тестування;

2. Здійснити огляд засобів захисту навчальних закладів та розглянути системи автоматизованого тестування;

3. Виконати розробку та дослідження системи автоматизованого тестування безпеки навчальних закладів.

Об’єктом дослідження бакалаврської роботи є процес проектування та дослідження системи автоматизованого тестування персональних даних.

Предметом дослідження є система автоматизованого тестування безпеки навчального закладу.

При написанні роботи були використані методи аналізу, порівняння, статистики, проектування.

Наукова новизна отриманих результатів полягає у тому, що вдосконалено існуючі системи автоматизованого тестування безпеки навчальних закладів з застосуванням модуля прогнозування.

1 АНАЛІЗ ПРОБЛЕМАТИКИ НАВЧАЛЬНИХ ЗАКЛАДІВ

1.1 Аналіз статистики атак на навчальні заклади. Класифікація атак та вразливостей

В нинішній час велика увага приділяється інформаційній безпеці персональних даних. Деякі компанії проводять аналіз статистик атак на персональні дані. В межах даного розділу роботи розглянемо таку статистику, а також наведемо основні типи атак на навчальні заклади.

Як зазначається в [1], основні результати цих досліджень, які характеризують рівень безпеки навчальних закладів показують, що:

- у 77% випадків при роботах із зовнішнього тестування на проникнення було виявлено можливість проведення атак для отримання доступу до внутрішніх корпоративних ресурсів через експлуатацію вразливостей навчальних закладів;

- 30% кіберінцидентів пов'язані з атаками на веб-ресурси.

Всі ці дані свідчать про те, що навчальні заклади є однією з основних «мішеней» для зловмисників, тому що велика кількість невиправлених вразливостей та простота їх експлуатації допомагають атакуючим успішно досягати своєї мети — від крадіжки інформації до доступу до внутрішніх ресурсів локальної обчислювальної мережі [1].

Важливо розуміти, що більшість вразливостей можна виявити задовго до атаки, а аналіз вихідного коду веб-сайтів дозволяє виявити у кілька разів більше критично небезпечних вразливостей, ніж тестування систем без дослідження коду.

Основні результати досліджень, які направлені на аналіз захисту персональних даних з точки зору інформаційної безпеки, показують, що [1,2]:

1. Усі персональні дані учнів навчального закладу вразливі За результатами автоматизованого аналізу вихідного коду було встановлено, що всі

школи мають уразливості, причому лише у 6% досліджених систем відсутні вразливості високого ступеня ризику.

2. Користувачі веб-сайтів - основна мета У 85% протестованих веб-застосунків присутні вразливості, які дозволяють проводити атаки на користувачів. Використовуючи дані вразливості, зловмисник може викрадати cookie користувачів, проводити атаки фішинга або заражати їх робочі станції шкідливим програмним забезпеченням.

3. Результати пов'язані з тим, що програми навчальних закладів мають більш складну логіку роботи в порівнянні з інформаційними веб-ресурсами інших організацій, і цей фактор створює передумови для появи більшої кількості вразливостей високого ступеня ризику. Внаслідок експлуатації даних вразливостей зловмисник може спробувати порушити працездатність програми або виконати довільний код на цільовій системі, що може призвести до повного контролю над сервером із веб-сайтом.

4. Усі протестовані школи можуть використовуватись для атак на користувачів. У всіх досліджених державних установ є вразливості, що дозволяють проводити атаки на користувачів. При цьому важливо відзначити, що переважна більшість користувачів таких веб-ресурсів дуже погано обізнані з інформаційною безпекою і легко можуть стати жертвами зловмисників.

5. Відмова в обслуговуванні - найпоширеніша загроза для інтернет-магазинів. У 75% досліджених веб-сайтів, пов'язаних з електронною торгівлею, виявлено вразливості, які потенційно призводять до відмови в обслуговуванні. Реалізація цієї загрози може призвести до значних фінансових втрат для власників [1,2].

Хакерська атака – це комплекс дій, спрямованих на пошук вразливостей у цифрових системах. При цьому слід зазначити, що хакери не завжди займаються шкідливою діяльністю, проте сьогодні термін «хакерство» зазвичай вживається у контексті протиправних дій, а хакерами називають кіберзлочинців, які

прагнуть отримати фінансову вигоду, висловити протест, зібрати певну інформацію [3].

Автоматизований аналіз захищеності, наведений в [1] показав, що всі протестовані веб-сайти містять вразливість різного ступеня ризику. При класифікації вразливостей за рівнем ризику було встановлено, що більшість їх (65%) належить до середнього рівня небезпеки.

Розподіл вразливостей за рівнем ризику наведений на рис. 1.1.

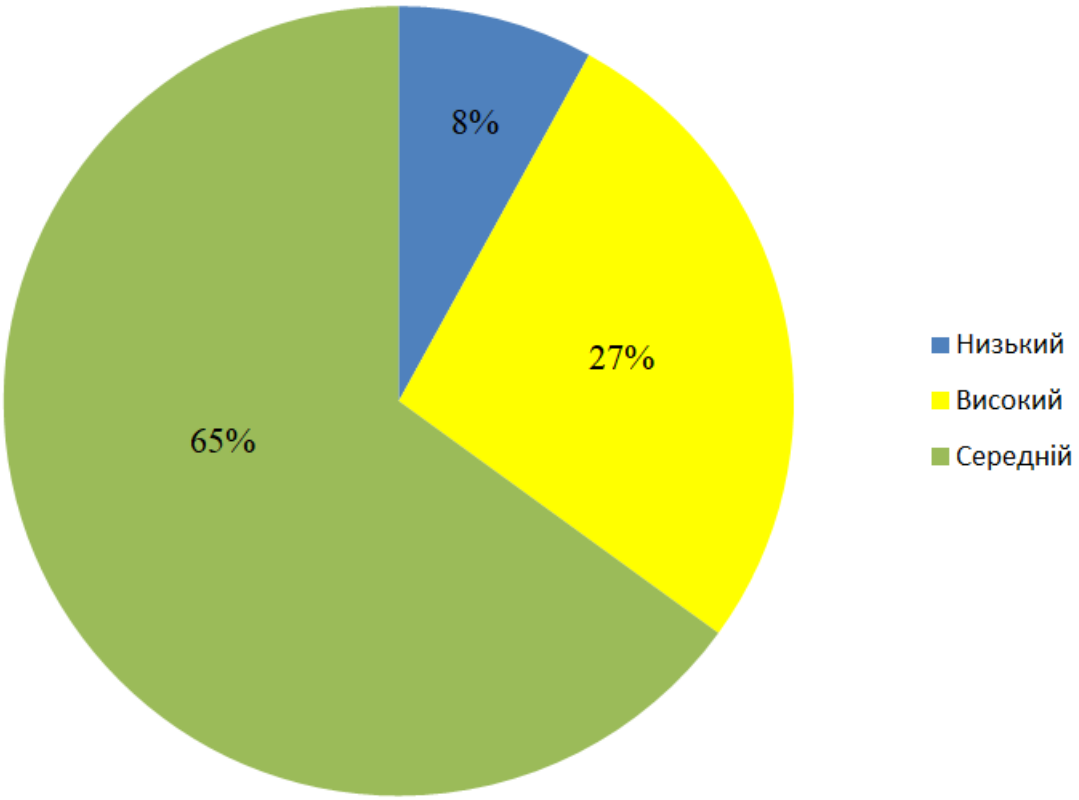


Рис. 1.1 — Розподіл вразливостей за рівнем ризику

Джерело: авторська розробка

При оцінці систем за максимальним рівнем ризику виявлених вразливостей було встановлено, що лише у 6% досліджених веб-сайтів відсутні вразливості високого рівня ризику. Слід враховувати, що досліджувані сайти є типовими CMS-платформами і містять велику кількість коду, написаного їх власниками. Але при цьому не слід забувати, що успішна експлуатація навіть

однієї критично небезпечної вразливості на практиці може призвести до повної компрометації програми або навіть сервера (рис. 1.2).

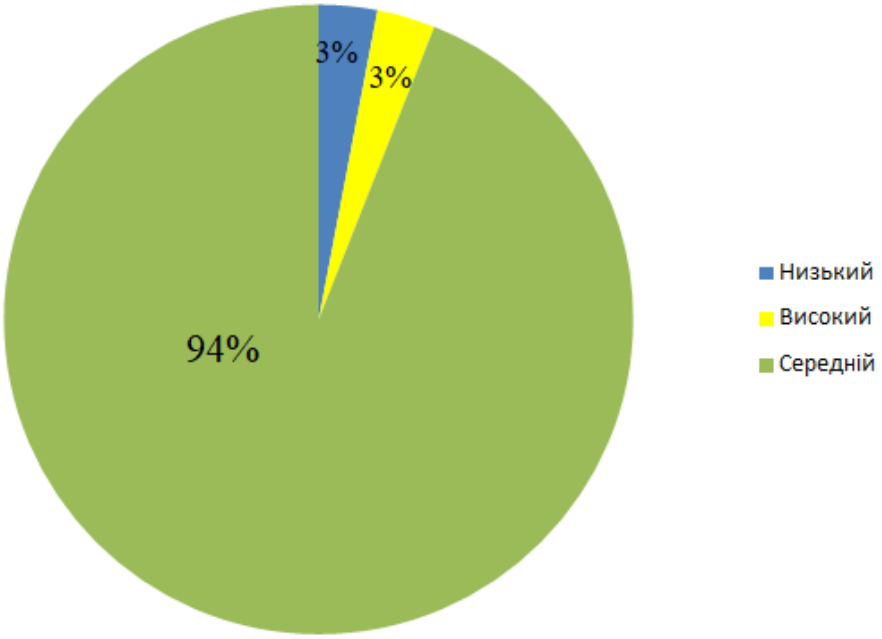


Рис. 1.2 — Розподіл систем за максимальним рівнем ризику виявлених вразливостей

Джерело: авторська розробка

Найпоширеніша вразливість, що виявилася при автоматизованому аналізі вихідного коду сайтів та наведена в аналізі [1] — «Міжсайтове виконання сценаріїв», за допомогою якої зловмисник може проводити фішингові атаки на клієнтів веб-сайтів або заражати їхні робочі станції шкідливим програмним забезпеченням. Ця вразливість також лідирує і в аналогічному рейтингу, що базується на результатах ручного тестування веб-сайтів.

Друга за поширеністю вразливість — «Розщеплення HTTP відповіді», при успішній експлуатації якої зловмисник може проводити атаки на клієнтів веб-програми, засновані на відправці браузеру подвійної HTTP відповіді, що атакується, вміст заголовків і полів якого частково контролюється порушником.

На третьому місці - вразливість високого рівня ризику "Читання довільних файлів", за допомогою якої зловмисник може отримати несанкціонований доступ до вмісту довільного файлу на сервері. Таким чином, порушник може

отримати вихідний код веб-сайту, облікові дані та іншу інформацію, що обробляється в системі.

З десяти найпоширеніших вразливостей п'ять мають високий рівень ризику, і їх експлуатація може призвести до серйозних наслідків. Наприклад, у деяких випадках внаслідок експлуатації вразливості «Створення довільного файлу» зловмисник може виконати довільний код на цільовій системі та надалі повністю скомпрометувати сервер, що атакується [1].

Класифікацією вразливостей веб-сайтів також займається Консорціум з безпеки веб-сайтів WASC (Web Application Security Consortium).

Консорціумом WASC розроблено спеціальний документ, в якому описано класифікацію вразливостей веб-сайтів – WASC Threat Classification [4].

Згідно з документом WASC Threat Classification, уразливості веб-сайтів діляться за наступними етапами життєвого циклу програмного забезпечення:

- етап проектування - охоплює вразливості, які можуть виникнути внаслідок помилок у проектуванні веб-сайту;

- етап реалізації - охоплює вразливості, які можуть виникнути через помилки при реалізації компонентів веб-сайту, наприклад – написання програмного коду

- етап розгортання - охоплює вразливості, які можуть виникнути під час налаштування веб-сайту до роботи, наприклад, - неправильна конфігурація веб-сервера;

Помилки, які можуть бути допущені на різних етапах життєвого циклу програмного забезпечення, описані у списку CWE (Common weakness enumeration), сформованого корпорацією MITRE. Згідно з даними веб-сайту корпорації MITRE, CWE є базовим стандартом при ідентифікації слабких місць у програмному забезпеченні та запобігання їх появі [5].

Кожному недоліку до списку надано власний ідентифікатор (ID), список містить близько тисячі CWE ID. При описі вразливості бази даних вразливостей може бути вказано CWE ID для додаткової інформації.

Остання редакція документа розглядає такі типи атак на веб-сайти [6]:

- вставка інструкцій (Injection) - відбувається вставка SQL - інструкцій, що передаються на обробку веб-сайту, яка після їх отримання може почати виконувати довільні команди;

- некоректна аутентифікація (Broken Authentication) - функції аутентифікації можуть бути реалізовані таким чином, що дозволяють оминати паролі або отримувати ідентифікатори користувачів;

- витік критичних даних (Sensitive Data Exposure) - недостатня захищеність персональних даних;

- атаки на засоби аналізу XML-введення (XML Eternal Entities) – зловмисники можуть завантажувати XML-файли на сервер або включати шкідливий код у документ XML;

- неправильний контроль доступу (Broken Access Control) - контроль доступу реалізовано таким чином, що авторизовані користувачі можуть мати у системі такі повноваження, які повинні мати;

- небезпечна конфігурація оточення (Security Misconfiguration) – відсутність оновлень та неправильна конфігурація окремих компонентів веб – сайтів може нести додаткову загрозу безпеці;

- міжсайтове виконання сценаріїв (XSS) - зловмисник отримує можливість виконувати сценарії у браузері жертви, перехоплювати сценарії користувача, перенаправляти користувачів на інші веб-сайти;

- незахищений процес десеріалізації (Insecure Deserialization) – зловмисник може порушувати логіку роботи веб-програми, підробляючи об'єкти програми, що призводить до віддаленого виконання коду зловмисника;

- використання компонентів з відомими вразливостями (Using Components with Known Vulnerabilities) - програмне забезпечення, у якого термін підтримки вже вичерпано, або яке є не оновленим, що може залучити більше зловмисників до його злому;

- недостатній моніторинг та ведення журналів подій (Insufficient Logging and Monitoring) - погано організований механізм ведення журналів подій та моніторингу може призвести до того, що зловмисники можуть неодноразово робити атаки на веб-сайти, залишаючись непоміченими.

Згідно з дослідженнями компанії Vercode, яка займається тестуванням захищеності програмного забезпечення, при проведенні тестування на проникнення в 74% програм знаходиться як мінімум одна вразливість зі списку OWASP Top – 10 [7].

Подаємо нижче опис кожної з вразливостей.

1) Вставлення інструкцій. Прикладом вставлення інструкцій може бути вставка SQL - інструкцій.

Атака типу "вставка SQL - інструкцій" може бути реалізована через некоректну обробку вхідних даних, що використовуються в SQL - запитах.

Далі виконано аналіз прикладу здійснення атаки типу вставки SQL - інструкцій.

Якщо існує серверне програмне забезпечення, яке отримує вхідний параметр id, використовує його для створення SQL-запиту, то PHP - скрипт обробки запиту може мати такий вигляд:

$Id = $_REQUEST['id'];

$ Res = mysqli_query ("SELECT * FROM news WHERE id_news =". $ Id);

Якщо на сервер буде передано параметр id, що дорівнює 5 (http://example.org/script.php?id=5), то виконається наступний SQL-запит:

SELECT * FROM news WHERE id_news = 5

Але якщо зловмисник передасть id рядок -1 OR 1 = 1 (http://example.org/script.php?id=-1+OR+1=1), виконається запит:

SELECT * FROM news WHERE id_news = -1 OR 1 = 1

Отже, зміна вхідних параметрів шляхом додавання до них конструкцій мови SQL викликає зміну в логіці виконання SQL-запиту (у прикладі вище

замість запису із заданим ідентифікатором будуть обрані всі наявні в базі запису).

На рис. 1.3 зображено інтерфейс тестового веб-сайту, що дозволяє користувачам виводити списки транзакцій, здійснених за певний період [7].

Введення наступного значення дозволяє виконати команду, яка повертає вміст бази даних, включаючи імена та паролі користувачів: union select userid, null, username + " + password, null from users--.

Рис. 1.3 — Інтерфейс тестової веб-програми

Джерело [7]

Згідно з рис. 1.3, перша частина значення, введеного в поле дати. Ці дані обробляються веб-сайтом. За датою слідує оператор union, що означає початок SQL - команди. Методом спроб та помилок зловмисник може обчислити назву

таблиці, що містить дані про облікові записи користувачів (вона називається users), та кількість полів у ній.

Після цього зловмисник використовує цю інформацію для складання SQL - команди select, що повертає дані з таблиці користувачів. Отримана інформація, що містить імена та паролі облікових записів користувачів, відображається на веб-сторінці у формі для виведення списку транзакцій [7].

2) Некоректна автентифікація. Згідно з дослідженнями, зловмисники можуть мати доступ до сотень мільйонів допустимих комбінацій імені користувача та паролю для заповнення форм у веб-сайтах, адміністративних списках облікових записів, інструментах перебору значень за словником [7].

Зловмисникам достатньо отримати доступ лише до кількох облікових записів або лише одного облікового запису адміністратора, щоб зламати систему, вкрасти гроші, використовувати методи шахрайства, викрасти конфіденційну інформацію та ін.

Атаки на засоби аутентифікації можливі, якщо веб-сайт має такі слабкі місця [7]:

- місця для заповнення облікових даних, коли зловмисник має список допустимих імен користувачів та паролів;

- відсутній захист від реалізації атак методом перебору;

- дозволено прості або відомі паролі, такі як "password" або "admin/admin";

- використовуються неефективні процеси відновлення облікових даних та забутих паролів, які не можуть бути безпечними;

- відсутня багатофакторна автентифікація;

- надання ідентифікаторів сеансу в URL-адресі.

Прикладом атаки на засоби автентифікації може бути випадок, коли зловмисник знає секретний ідентифікатор сеансу і може представитися веб-серверу автентифікованим користувачем та скомпрометувати обліковий запис.

На рис. 1.4 зображено приклад тестового веб-сайту, де показаний результат виконання скрипту для отримання ідентифікатора сеансу [7].

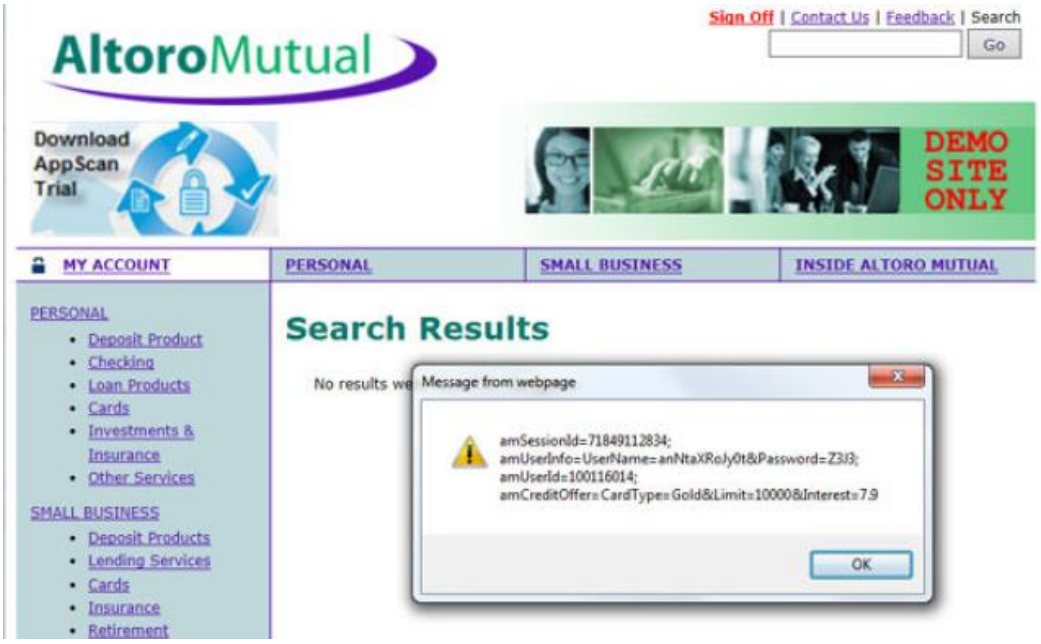


Рис. 1.4 — Приклад роботи тестового скрипту

Джерело [7]

3) Витік критичних даних. Згідно з дослідженнями, протягом останніх кількох років викрадення критичних даних було поширеною атакою. Головним недоліком при цьому залишається відсутність шифрування конфіденційних даних або коли використовуються нестійкі до злому криптографічні алгоритми, засоби генерації ключів та управління [7].

Для визначення можливості витоку критичних даних треба визначити, які дані потребують захисту в кожному конкретному випадку при їх передачі та зберіганні. Такими даними можуть бути паролі, номери кредитних карток, медичні записи, особиста інформація та ділова документація або конфіденційна інформація. Для всіх цих типів даних необхідно перевірити [7]:

- чи є дані, що передаються у вигляді відкритого тексту (це стосується таких протоколів, як HTTP, SMTP та FTP);

- чи використовуються старі чи нестійкі до злому криптографічні алгоритми у системі чи коді;

- як реалізований механізм розподілу та управління криптографічними ключами;

- чи використовується поштовим клієнтом недійсний сертифікат, отриманий від сервера.

Одним із сценаріїв витоків важливих даних може бути процес шифрування програмою номерів кредитних карток у базі даних за допомогою автоматичного шифрування бази даних. Однак ці дані автоматично розшифровуються під час завантаження, дозволяючи застосовувати вставки SQL - інструкцій для отримання номерів кредитних карток у вигляді відкритого тексту.

Іншим сценарієм витоку критичних даних може бути веб-сайт, де не використовується протокол захисту транспортного рівня TLS (Transport Layer Security) для всіх сторінок або використовуються нестійкі до злому криптографічні алгоритми шифрування [7].

Зловмисник може здійснити моніторинг мережного трафіку (наприклад, у незахищеній бездротовій мережі), знизити рівень зв'язків з HTTPS до рівня HTTP, перехопити запити та викрасти дані з cookie користувача. Нападник відтворює цей файл cookie і перехоплює сеанс користувача, отримуючи доступ або змінюючи особисті дані.

Крім того, таким чином може змінюватись одержувач грошового переказу. Також до витоку критичних даних може спричиняти використання простих алгоритмів обчислення хеша пароля.

У такому разі всі хеші можуть бути обчислені за допомогою райдужних таблиць попередніх хешів за допомогою графічних процесорів [7].

4) Атаки на засоби аналізу XML – введення XML (eXtensible Markup Language) – це стандарт для обміну структурованими даними у текстовому форматі.

XML-файлу може мати такий вигляд [7]:

version = "1.0" encoding = "UTF-8"?>

<Order>

<Product>1234</product>

<Count>1</ count>

<Orderer>

<Contact> Jan P. Monsch</contact>

<Account>789</account>

</Orderer>

</Order>

Можливі цілі при здійсненні атаки:

- Мережевий сервіс;

- генератор XML;

- XML-аналізатор;

- Код програми.

Нижче наведені можливі приклади організації атак засобами аналізу XML - введення.

На рис. 1.5 наведено приклад визначення типу даних, який називається foo, з елементом bar, з яким пов'язане слово "World" [7].

Рис. 1.5 — Приклад передачі даних XML-елементів до аналізатора

Джерело[7]

Згідно з дослідженнями, XML - об'єкти можуть використовуватися зловмисниками для атак "Відмова в обслуговуванні" шляхом вставки об'єктів з елементами, всередині яких знаходяться інші елементи тощо. На рис. 1.6 представлений приклад запиту до XML – аналізатора та результат обробки запиту.

Request

```
POST http://example.com/xml HTTP/1.1

<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar "World ">
  <!ENTITY t1 "&bar;&bar;">
  <!ENTITY t2 "&t1;&t1;&t1;&t1;">
  <!ENTITY t3 "&t2;&t2;&t2;&t2;&t2;">
]>
<foo>
  Hello &t3;
</foo>
```

Response

```
HTTP/1.0 200 OK

Hello World World World World World World Wor
ld World World World World World World World
World World World World World World World Wor
ld World World World World World World World
World World World World World World World Wor
ld World World World
```

Рис. 1.6 — Приклад передачі до XML - аналізатору об'єкта з вкладеними елементами та результат обробки запиту

Джерело[7]

Надсилаючи необхідні запити до XML-аналізатора, зловмисник, який володіє інформацією про структуру веб-сайту, може дізнатися інформацію про програмне забезпечення, яке використовується [7].

Приклад можливих інструкцій у XML – файлі та результат роботи XML – аналізатора наведено на рис. 1.7.

Request

```
POST http://example.com/xml HTTP/1.1

<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar SYSTEM
  "file:///etc/lsb-release">
]>
<foo>
  &bar;
</foo>
```

Response

```
HTTP/1.0 200 OK

DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04 LTS"
```

Рис. 1.7 — Приклад передачі XML - аналізатору об'єкта з інструкціями визначення операційної системи

Джерело[7]

5) Неправильний контроль доступу. Призначення контролю доступу – забезпечити виконання вимог політики безпеки таким чином, щоб користувачі системи не змогли виконувати у системі дії, що виходять за межі повноважень користувачів. Прикладом контролю доступу може бути обмеження доступу до ресурсів неавторизованих користувачів [7].

Однак, як відомо, обмеження доступу до ресурсів може стосуватися не тільки файлів та баз даних, а також:

- програм;
- спеціальних функцій сайтів;
- спеціальних полів даних;
- пам'яті;
- приватних чи захищених змінних
- носіїв інформації;
- засобів передачі інформації.

Недоліки в засобах контролю доступу зазвичай призводять до несанкціонованого розкриття інформації, модифікації або знищення всіх даних або виконання бізнес-функцій за межами користувача. Загальні уразливості засобів контролю доступу включають:

- обхід перевірок контролю доступу шляхом зміни URL-адреси, внутрішнього стану програми, HTML-сторінки або просто використання спеціального інструменту атаки на програмний інтерфейс;

- можливість за допомогою первинного ключа змінювати всі записи інших користувачів, що дозволяє переглядати та редагувати чужі облікові записи;

- підвищення привілеїв (повноваження користувача у системі без проходження етапів авторизації, або повноваження адміністратора після входу до системи як користувача;

- маніпулювання метаданими, такими як повторне використання або заміна токенів керування доступом або файлів cookie, за допомогою яких можна підвищувати привілеї в системі.

6) Небезпечна зміна оточення. Згідно з даними досліджень організації OWASP, можливість неправильної конфігурації оточення, тобто середовища функціонування веб-сайту, може статися на будь-якому рівні компонентів програми, включаючи мережеві сервіси, платформу, веб-сервер, сервер сайтів, базу даних та ін.

Автоматизовані сканери вразливості можуть виявляти неправильні конфігурації, використовувати облікові записи або стандартні конфігурації.

Доступність автоматизованих засобів пошуку вразливостей допомагає зловмисникам здійснити несанкціонований доступ до деяких системних даних або функціональних можливостей. Іноді такі недоліки призводять до повного розкриття структури системи та викрадення конфіденційних даних.

Додаткову загрозу несе наявність програмного забезпечення, яке не оновлюється [7].

7) Міжсайтове виконання сценаріїв. Атаки на веб-системи, в яких уразливість полягає в тому, що виконується вставка коду зловмисника в сторінку веб-програми, яка буде виконана на комп'ютері користувача при відкритті ним цієї сторінки і відбувається взаємодія цього коду з веб-сервером зловмисника.

Даний тип атаки відомий як XSS – атаки.

8) Незахищена десеріалізація. Процес серіалізації використовується для передачі об'єктів по мережі та збереження їх у файлах. Для цього об'єкт заповнюється потрібними даними, потім викликається код серилізації, і результатом є XML - документ або документ іншого формату.

Результат серіалізації передається стороною, що приймає, по електронній пошті або HTTP. Одержувач створює об'єкт того самого типу, який був до серіалізації, тим самим проводячи процес десеріалізації.

9) Використання компонентів із відомою вразливістю. У структурі веб-програми використовується багато компонентів, виробники яких можуть відрізнятися. По-перше, при використанні різних компонентів при побудові веб-сайти слід враховувати, що при створенні компонентів на кожному з можливих

етапів виробником можуть бути допущені помилки, які можуть призводити до виникнення вразливостей цих компонентів. Компонентами веб-сайтів можуть бути реалізації різних сервісів, сторонні бібліотеки, системи керування контентом, реалізації веб-серверів, операційні системи тощо [7].

По-друге, якщо вразливість компонента існує, її можна знайти виробником компонента, користувачем чи зловмисником. Завдання виробника полягає у виправленні вразливості. Але виправлення вразливості може зайняти деякий час, який можуть використовувати зловмисники для атак на користувачів програм, які містять компоненти з уразливістю.

10) Недостатній моніторинг та ведення журналів подій. Як відомо, використання зловмисниками можливої недостатньої реалізації процесу моніторингу та ведення журналів подій є основою майже всіх основних інцидентів. Однією зі стратегій визначення того, чи достатній рівень моніторингу реалізований - це перевіряти журнали реєстрації подій після проведення тестування на проникнення.

До недоліків безпеки програми належать невстановлені або некоректно налаштовані значення різних властивостей та директив. Наприклад, у деяких сайтах не було встановлено властивості requireSSL, що відповідає за встановлення прапора secure для HTTP заголовка Set-Cookie, який визначає необхідність передачі cookie тільки за захищеним з'єднанням (HTTPS). Недоліки такого роду відповідно до класифікації вразливостей OWASP6 відносяться до категорії A5 - Security Misconfiguration.

Розподіл виявлених вразливостей відповідно до класифікації OWASP Top 10 наведено на рис. 1.8. Усі вразливості, які не входять до списку 10 найнебезпечніших, були поміщені до категорії "Інші" [1].

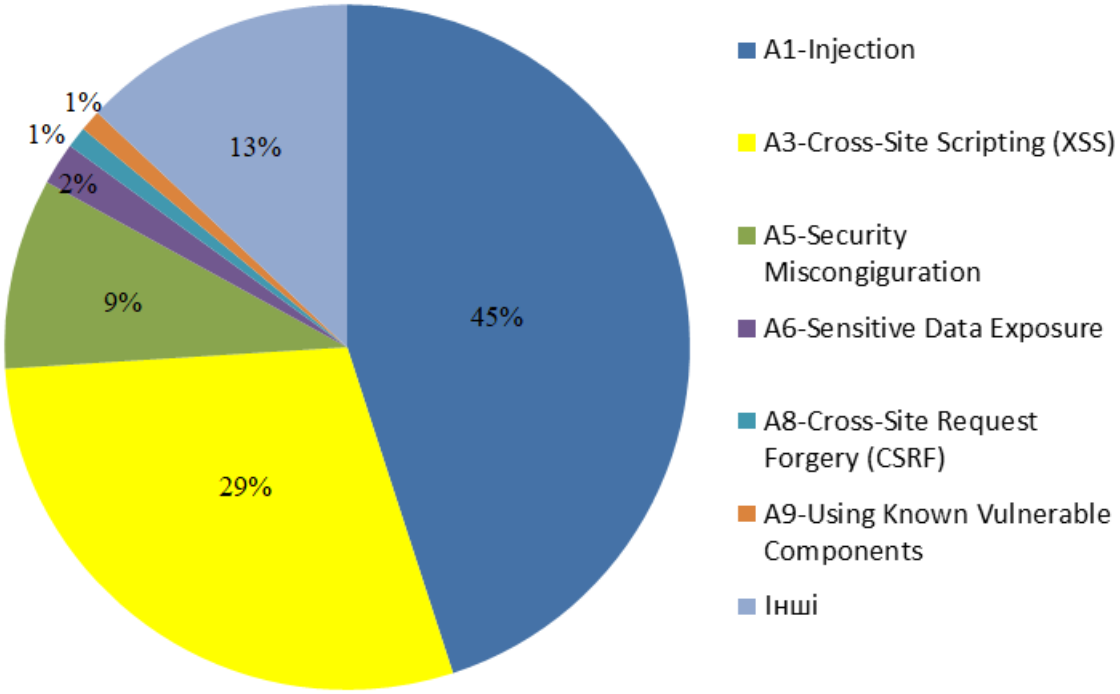


Рис. 1.8 — Розподіл виявлених вразливостей відповідно до класифікації OWASP Top 10

Джерело [1]

Проте в 2021 році, зважаючи на світову ситуацію, в огляді OWASP Top 10 відбулися певні зміни. Дані зміни наведені на рис. 1.9.

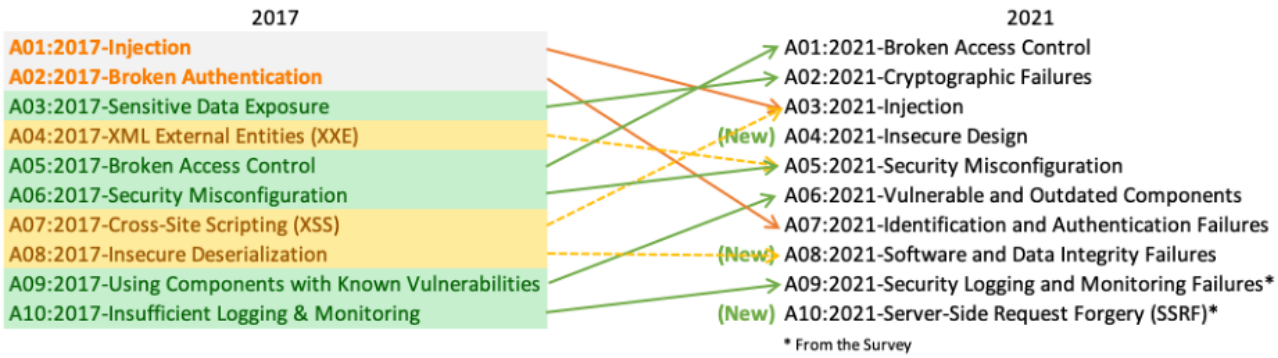


Рис. 1.9 — Зміни в огляді вразливостей веб-сайтів OWASP Top 10

Джерело [1]

У 80% досліджених програм фінансових організацій виявлено вразливість "Міжсайтове виконання сценаріїв", і майже в половині — вразливість "Розщеплення HTTP-відповіді". Саме через ці вразливості в 87% програм можливе проведення атак на користувачів веб-сайтів. Загроза відмови в обслуговуванні пов'язана з можливістю успішної експлуатації вразливостей високого ступеня ризику "Впровадження зовнішніх сутностей XML" та "Зміна довільних файлів".

Крім того, за допомогою вразливості "Зміна довільних файлів" зловмисник може спробувати виконати довільний код на цільовій системі, що дасть йому повний контроль над сервером із веб-сайтом.

1.2 Проблеми захисту персональних даних

У міру розвитку технології для захисту персональних даних слід дотримуватися і надійних заходів безпеки. Загрози безпеки веб-застосунків реальні і відбуваються по всьому світу. Стандартних заходів вже недостатньо для захисту від загроз, що розвиваються.

З розвитком технологій постійно з'являються нові вектори атак. Зараз як ніколи потрібні комплексні інструменти безпеки. Раніше захист кінцевих точок пристроїв та мережна безпека були остаточними заходами захисту. Потім були мобільні та хмарні технології, що значно знизили ефективність мережної безпеки і суттєво зруйнували підхід захисту, орієнтований на горизонт, на який так часто покладалися.

Нині еволюціонує зовсім новий підхід до доступу до систем бек-офісу, відкриваючи нові можливості для бізнесу - як законні, так і незаконні. В даний час організації все більше покладаються на інтерфейси прикладного програмування (API) для стимулювання інновацій, швидкість розробки та надання нових можливостей монетизації.

Але, згідно з OWASP Топ-10: "За своєю природою API-інтерфейси розкривають логіку програми та конфіденційні дані, такі як особиста інформація (PII), і через це API-інтерфейси все частіше стають мішенню для зловмисників". Перенесення важливих компонентів на клієнтську сторону сайтів (тобто за межами захисту традиційної мережевої безпеки) створює нову масивну поверхню атаки, збільшуючи ризик атак, таких як зламування форми, підробка об'єктної моделі документа (DOM), зловживання сеансом, накладання атаки та зловживання API [9].

На жаль, багато організацій, як і раніше, вважають, що брандмауер веб-застосунків (WAF) - це все, що потрібно для захисту веб-сайтів від загроз безпеки. Насправді,WAF - це лише частина рішення. Традиційні методи безпеки, такі як WAF, не можуть зупинити сьогоднішні атаки на веб-застосунки, які в багатьох випадках виходять з браузера поза сферою дії мережної безпеки. На той час, коли вони спрацьовують – якщо взагалі будь-коли – у зловмисника вже немає конфіденційної інформації, і все, що можна зробити, – це зосередити зусилля на боротьбі зі шкодою.

Оскільки зловмисники продовжують виявляти нові вектори атак, організації повинні відповідати тим самим, щоб забезпечити належний та повний захист критично важливих активів та даних.

Приблизно 95% веб-сайтів працюють на JavaScript та HTML5 - мовах, які можна легко перехопити, переглянути та зламати. Це залишає веб-застосунки та API-інтерфейси вразливими для атак на стороні клієнта, особливо якщо вони покладаються тільки на традиційні інструменти захисту периметра, такі як WAF. За даними Symantec, понад 4800 веб-сайтів щомісяця зазнають злому. Атаки з метою крадіжки даних на стороні клієнта - це лише один із векторів загроз, з якими стикаються веб-сайти, тому важливим є багаторівневий підхід до безпеки [10].

Як видно з недавніх зламів веб-сайтів на British Airways та Ticketmaster, навіть якби WAF був на місці та правильно налаштований, він не зміг би

запобігти цим порушенням на стороні браузера / клієнта. Як тільки експлойти були виявлені, сотні тисяч клієнтських записів вже були витягнуті.

Таким чином, безпека – ключова особливість розробки захисту персональних даних. Щоб залишатися конкурентоспроможними на ринку, компанії повинні пропонувати нові рішення безпеки, щоб протистояти хакерам та надавати своїм клієнтам надійні та безпечні програми.

Проте більшість безпеки персональних даних залежить від обізнаності розробників про кіберзагрози та запланованого моніторингу дій програми.

1.3 Ієрархія захисту персональних даних

Зростання кількості та якості загроз інформаційної безпеки в комп'ютерних системах не завжди призводить до адекватної реакції у вигляді надійної системи та безпечних інформаційних технологій. У більшості комерційних і державних організацій, не кажучи вже про звичайних користувачів, як засоби захисту використовуються лише антивірусні програми та розмежування прав доступу користувачів за паролями.

Існує кілька засобів забезпечення інформаційної безпеки.

Антивірусне програмне забезпечення є важливою частиною надійної програми безпеки. При правильному налаштуванні ризик зараження шкідливим програмним забезпеченням значно знижується (хоча і не завжди - згадайте про вірус Melissa).

Але жодна антивірусна програма не може захистити організацію від зловмисника, який використовує для входу легітимну програму, або від законного користувача, який намагається отримати несанкціонований доступ до файлів.

Будь-яка комп'ютерна система в організації обмежує доступ до файлів, ідентифікуючи користувача, який входить у систему. Коли система налаштована правильно, при встановленні необхідних дозволів для легальних користувачів, є

обмеження на використання файлів, до яких вони не мають доступу. Однак система контролю доступу не забезпечить захист, якщо зловмисник через уразливості отримує доступ до файлів як адміністратор. Така атака буде вважатися судовим позовом адміністратора.

Перший - найпростіший і обов'язковий. Тут головний інструмент захисту – firewall. Firewall має лімітувати використання сервісів, що надаються користувачам. Також firewall повинен стежити за всіма з'єднаннями як з одного, так і з іншого боку. Не варто застосовувати програми незрозумілого походження, треба віддавати перевагу ліцензійному ПЗ.

Другий рівень безпеки передбачає конфігурацію операційної системи, під керуванням якої працює веб-сайт. Кожна операційна система дозволяє створювати контрольні аркуші безпеки (security checklist). Ці установки повинні бути узгоджені з операційними системами вендорів. Важливо також, щоб новий сайт вчасно вносився в security cheklist, а не відключав його.

Третій рівень орієнтовано вже на мережу. Необхідно оснастити датчиками атаки мережного обладнання та програмного забезпечення провайдера, що забезпечує хостинг. Головне, щоб сигнал, що надійшов про небезпеку, був правильно оброблений і нейтралізований.

Четвертий рівень безпеки – встановлення програмного забезпечення на рівні хостингу. Це значно складніше завдання. По-перше, тут можна зіткнутися із запереченнями самої хостинг-компанії. А по-друге, таке програмне забезпечення набагато складніше простих датчиків. З цієї причини і рівень безпеки вищий.

Рівень 5 має два підрівні - A та B. Рівень 5A - це встановлення спеціального програмного забезпечення, що виконує роль прошарку між операційною системою веб-сервера та всіма сайтами. Такий буфер дозволяє запобігти атакі хакерів на вразливі програми, які беруть під контроль всю операційну систему під час виконання. Це не найдешевший варіант, тому що, як і на попередньому

рівні, необхідно забезпечити підтримку програмного забезпечення, яким оперують веб-сервери.

Рівень 5В є установкою орієнтованих на конкретні програми firewall або проксі-серверів. Вони орієнтовані на HTTP-протокол і дозволяють запобігти атакам, перш ніж потенційні зловмисники зможуть дістатися до запуску сайтів, встановлених на веб-сервері. Однак, проксі-сервер – це суттєве обмеження у роботі.

Шостий рівень – своєрідна вершина безпеки. Тут допускається використання лише довірчих операційних систем та працюючих під їх керуванням сайтів. Іншими словами, всі функціонуючі сайти та операційні системи повинні бути максимально адаптовані, або розроблені спеціально для специфічних потреб компанії. Це найдорожчий, але й найефективніший спосіб захисту. До того ж вимагає спеціальної підготовки від адміністратора мережі, а часто й від користувачів, що також тягне за собою додаткові витрати.

1.4 Висновки до першого розділу

Результати дослідження показують, що аналіз вихідного коду веб-застосунків дозволяє знайти велику кількість вразливостей різного ступеня ризику і в процесі розробки систем захисту персональних даних значно підвищити захищеність кінцевого продукту. У цьому незалежно від стадії розробки доцільно застосовувати автоматизовані засоби, оскільки швидкість роботи аналізатора перевищує можливості ручного аналізу.

Інформація є одним із об'єктів цивільного права, у тому числі права власності, володіння, користування. До захищеної інформації належать відомості, що є об’єктом власності та підлягають захисту відповідно до вимог нормативно-правових документів або вимог, висунутих власником інформації.

2 ОГЛЯД ЗАСОБІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ УЧНІВ НАВЧАЛЬНОГО ЗАКЛАДУ. СИСТЕМИ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ

2.1 Методи пошуку вразливостей. Перспективні методи захисту

Як вже зазначалося у першому розділі, сьогодні веб-додатки стають найпопулярнішим інструментом, що пропонує користувачам набір різних послуг. Однак попередні дослідження показали, що багато веб-додатків можуть піддаватися різноманітним вразливостям.

Наступний невичерпний список функцій слід переглядати під час тестування безпеки веб-додатків. Неправильна реалізація кожного з них може призвести до уразливостей [11]:

- Конфігурація програми та сервера. Можливі дефекти пов'язані зі змінами шифрування / криптографії, конфігураціями веб-сервера тощо;

- Перевірка введення та обробка помилок. SQL-ін'єкції, міжсайтові сценарії (XSS) та інші поширені вразливості ін'єкцій є результатом поганої обробки введення та виведення;

- Аутентифікація та управління сеансами. Уразливості, які можуть призвести до видачі себе за іншу особу. Також слід враховувати повноваження та захист;

- Авторизація. Тестування здатності програми захищатися від вертикального та горизонтального підвищення привілеїв.

- Бізнес-логіка. Важлива для більшості програм, які забезпечують бізнес-функції.

- Клієнтська логіка. У сучасних веб-додатках з великою кількістю JavaScript, крім веб-сторінок, що використовують інші типи клієнтських технологій (наприклад, Silverlight, Flash, Java-аплети), цей тип функцій стає все більш поширеним.

Отже, тестування веб-безпеки спрямоване на виявлення вразливостей у веб-додатках та їх конфігураціях. Первинною метою є прикладний рівень (тобто те, що виконується за протоколом HTTP). Тестування безпеки веб-програми часто включає відправку різних типів вхідних даних, щоб спровокувати помилки і змусити систему поводитися несподіваним чином. Ці так звані негативні тести перевіряють, чи робить система те, для чого вона не призначена [11].

Також важливо розуміти, що тестування веб-безпеки - це не лише тестування функцій безпеки (наприклад, аутентифікації та авторизації), які можуть бути реалізовані у додатку. Не менш важливо перевірити, що інші функції реалізовані безпечним способом (наприклад, бізнес-логіка та використання правильної перевірки введення та кодування виведення). Ціль полягає в тому, щоб забезпечити безпеку функцій, представлених у веб-додатку.

Згідно з дослідженнями OWASP [8] найбільш ефективним способом виявлення вразливостей web-додатків є експертний аналіз вихідних кодів web-додатку (code review). Цей спосіб дуже трудомісткий, вимагає високої кваліфікації експерта та не захищений від помилок експерта.

Тому активно також розвиваються методи автоматичного виявлення вразливостей web-додатків.

Методи автоматичного виявлення вразливостей web-сайтів можна розділити на дві основні групи:

- Методи, що аналізують роботу розгорнутого на стенді web-сайту без звернення до вихідних кодів web-сайтів;

- Методи, що аналізують вихідні коди web-сайтів та конфігураційні налаштування. Перша група методів розглядає веб-сайти з погляду зовнішнього користувача, тобто потенційного зловмисника

Згідно з класифікацією, наведеною в [8,11], види тестів безпеки веб-додатків діляться на:

- Тест динамічної безпеки програм (DAST). Цей автоматичний тест безпеки програм найкраще підходить для внутрішніх програм з низьким рівнем

ризику, які повинні відповідати нормативним вимогам до безпеки. Для додатків із середнім ступенем ризику та критичних додатків, що зазнають незначних змін, найкращим рішенням є поєднання DAST із деяким ручним тестуванням веб-безпеки на загальні вразливості.

- Статичний тест безпеки додатків (SAST). Цей підхід до забезпечення безпеки програм пропонує автоматизовані та ручні методи тестування. Він найкраще підходить для виявлення помилок без необхідності запускати програми у виробничому середовищі. Це також дозволяє розробникам сканувати вихідний код та систематично знаходити та усувати уразливості безпеки програмного забезпечення.

- Тест на проникнення. Цей ручний тест безпеки додатків найкраще підходить для критично важливих додатків, особливо тих, які зазнають серйозних змін. Оцінка включає бізнес-логіку та тестування зловмисників для виявлення складних сценаріїв атак.

- Самозахист програм під час виконання (RASP). Цей підхід до безпеки програм, що розвивається, включає в себе ряд технологічних прийомів для інструментарію програми, щоб можна було відстежувати атаки в міру їх виконання і, в ідеалі, блокувати в режимі реального часу.

Детально методи автоматичного тестування будуть розглянуті далі у рамках магістерської дисертації.

Виявивши основну причину вразливостей, на ранніх етапах тестування можна реалізувати заходи для пом'якшення наслідків, щоб запобігти будь-яким проблемам. Крім того, знання того, як ці атаки працюють, можна використовувати під час тестування безпеки веб-додатків.

Визнання впливу атаки також є ключем до управління ризиками, оскільки результати успішної атаки можна використовувати для оцінки загальної серйозності вразливості. Якщо проблеми виявляються під час перевірки безпеки, визначення їхньої серйозності дозволяє організації ефективно розставити пріоритети у зусиллях виправлення.

Перед виявленням проблеми оцінка потенційного впливу на кожну програму в бібліотеці додатків може полегшити пріоритет тестування безпеки додатків. Маючи встановлений список висококласних програм, тестування безпеки web може бути заплановане так, щоб в першу чергу націлити критично важливі програми компанії з більш цілеспрямованим тестуванням, щоб знизити ризики [12].

2.2 Застосування сканерів та їх можливості

Для пошуку вразливостей використовують спеціальні сканери вразливостей. До основних завдань сканерів уразливостей відносяться [13]:

- ідентифікація та аналіз загроз;
- інвентаризація ресурсів (операційна система, програмне забезпечення, мережеві пристрої);
- формування звітів з описом уразливостей та варіанти виправлення уразливостей системи.

Існує два основних механізми роботи сканерів уразливостей [13]:

- сканування - пасивний аналіз, що являє собою збір інформації про порти, операційні системи, версії програмного забезпечення, отримані дані порівнюються з правилами визначення інформації про порти, програмне забезпечення та інші компоненти системи та формується висновок про наявність чи відсутність уразливостей;
- зондування - активний аналіз, що є імітацією атаки вразливість, яка перевіряється.

Існують різні засоби пошуку уразливостей для різних етапів перевірки систем на наявність уразливостей, від сканерів портів до комплексних систем, які складаються із сканерів портів, засобів пошуку експлойтів для вразливостей [13].

Прикладами засобів пошуку уразливостей можуть бути:

- програма для дослідження мережі Nmap – дозволяє визначати хости в мережі, встановлені служби та їх версію, операційні системи та версії, які вони використовують, пакетні фільтри/міжмережові екрани [13];

- комплекс засобів перевірки веб-додатків Burp Suite - має власний проксі-сервер, сканер уразливостей, засіб автоматизації атак;

- Metasploit Framework – інструмент для перевірки та експлуатації вразливостей.

Засоби пошуку та експлуатації вразливостей можуть бути зібрані у спеціальних операційних системах, призначених для аналізу захищеності та проведення тестувань комп'ютерних систем на проникнення.

Існують такі операційні системи для проведення тестування комп'ютерних систем на проникнення:

- ОС Kali Linux;

- ОС BlackArch Linux;

- ОС Parrot Security OS;

- ОС BlackBox.

Розглянемо приклади існуючих сканерів вразливостей (таблиця 2.1).

Таблиця 2.1 – Існуючі сканери вразливостей та їх порівняння

Назва	Defect Tracking Integration	IAST Module Hybrid Analysis	SAST Module Hybrid Analysis	Flash Scanner	CGI Scanner	Enterprise Console Management Features	Demo
Rapid appspider	+	-	-	+	-	+/-	+
Portswigger Burp Suite	+/-	+	-	+	+	+/-	+
Fortify WebInspect	+	+	+	+	+	+	+

Продовження таблиці 2.1

IBM Security AppScan	+	+	+	+	+	+	+
Accunetix Vulnerability Scanner	+	+	-	-	+	+	+
Netsparker Web Application Security Scanner	+	-	-	-	+	+	+
Janusec WebCruiser	-	-	-	-	+	-	+

Джерело: авторська розробка із застосуванням даних з [12], [13], [14], [15], [16], [17], [18].

Розглянемо коротко кожен із запропонованих сканерів.

1) Продукт компанії Rapid7 – це функціональний засіб тестування веб- та мобільних додатків. Крім виявлення вразливостей, Appspider вміє надавати конкретні рекомендації щодо їх усунення та розставляти пріоритети.

Є 95 видів атак, завдяки чому програми можна перевірити на стійкість до всіх сучасних поширених загроз. До того ж тут є можливість запускати певні атаки окремо, щоб перевірити актуальність захисту від них.

Інструмент чудово працює з усіма сучасними технологіями. Є підтримка Ajax, JSON, GWT та інших стандартів, різноманітних форматів та протоколів, що використовуються у сучасних веб-додатках та браузерах. Також є перевірка на відповідність сучасним стандартам безпеки.

Rapid7 може виводити інтерактивні звіти, які подаються у вигляді веб-сторінок.

Їхня головна зручність — це можливість заглибитись у конкретну вразливість та деталізувати її найдрібніші подробиці для вирішення проблеми. Інструмент вміє інтегруватися з наявними засобами безпеки (наприклад, Web Application Firewall), що істотно економить час і ресурси. Спробувати інструмент можна безкоштовно протягом обмеженого часу.

Інтерфейс сканера наведений на рисунку 2.1.

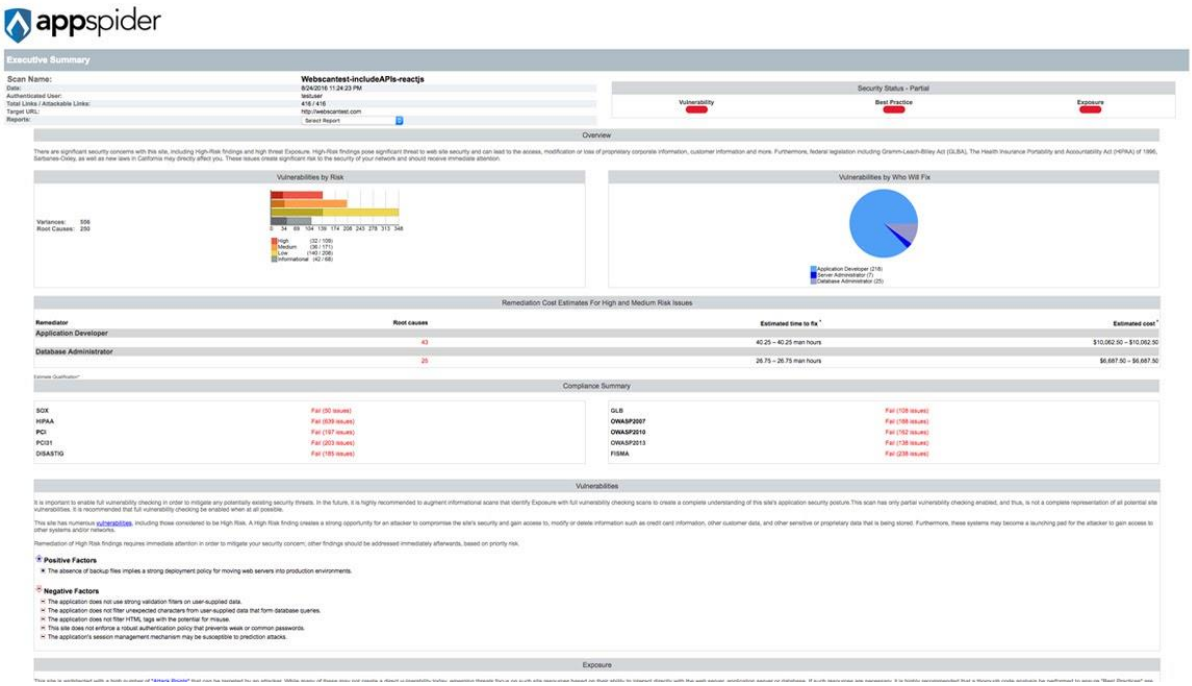


Рисунок 2.1 – Інтерфейс сканера Rapid appspider

Джерело[12]

2) Portswigger Burp Suite. Цей сканер дозволяє тестувати безпеку веб-додатків як в ручному, так і в автоматичному режимі. Але головний упор робиться на ручні перевірки. Для цього в Burp Suite є низка інструментів. Наприклад, Intruder дозволяє виявляти незвичайні вразливості, а Repeater використовується для маніпуляцій та повторного надсилання індивідуальних запитів. Інтерфейс Burp Suite інтуїтивно зрозумілий, можливо швидко розібратися в програмі.

Однією з переваг інструменту є наявність безлічі сторонніх плагінів і доповнень, які серйозно розширюють його базову функціональність. Багато хто

з них розроблений самими програмістами, які використовували Burp Suite у своїй роботі і точно знали, чого саме не вистачає оригінального продукту. Якщо потрібного плагіна знайти не вдалося, його можна написати самостійно.

Інтерфейс програми наведений на рисунку 2.2.

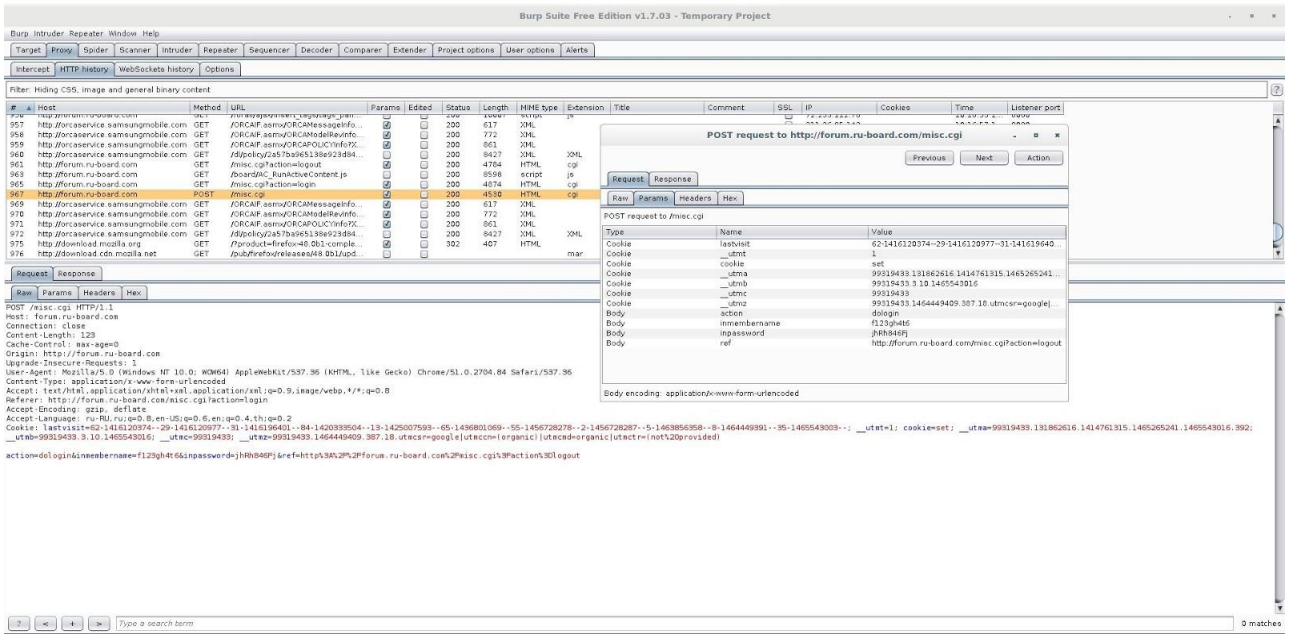


Рисунок 2.2 – Інтерфейс Portswigger Burp Suite
Джерело[12]

3) Fortify WebInspect. Fortify WebInspect – це один із найфункціональніших інструментів. Він може поставлятися як ліцензоване ПЗ або використовуватися за моделлю SaaS (програмне забезпечення як послуга), а також працювати певний час як демонстраційна версія.

Засіб вміє імітувати реальні атаки та техніки злому, які найчастіше застосовують кіберзлочинці. Сканер підтримує всі сучасні технології, що дозволяє працювати з додатками без огляду на його архітектуру. Серед найпопулярніших — Adobe Flash та JavaScript/Ajax, які на сьогоднішній день використовуються при створенні веб-застосунків дуже часто.

До переваг цього продукту також належать простота установки, налаштування та можливість масштабування. Після закінчення тестів Fortify WebInspect видає найдокладніші звіти, які будуть корисні та зрозумілі як

менеджменту компанії, так і розробникам. У них показується статистика знайдених уразливостей, їхня пріоритетність (на що потрібно звернути увагу перш за все), демонструються докладні відомості про кожну проблему. У програмі є набір готових шаблонів для звітів, але можна також створювати свої власні.

Інтерфейс наведений на рисунку 2.3.

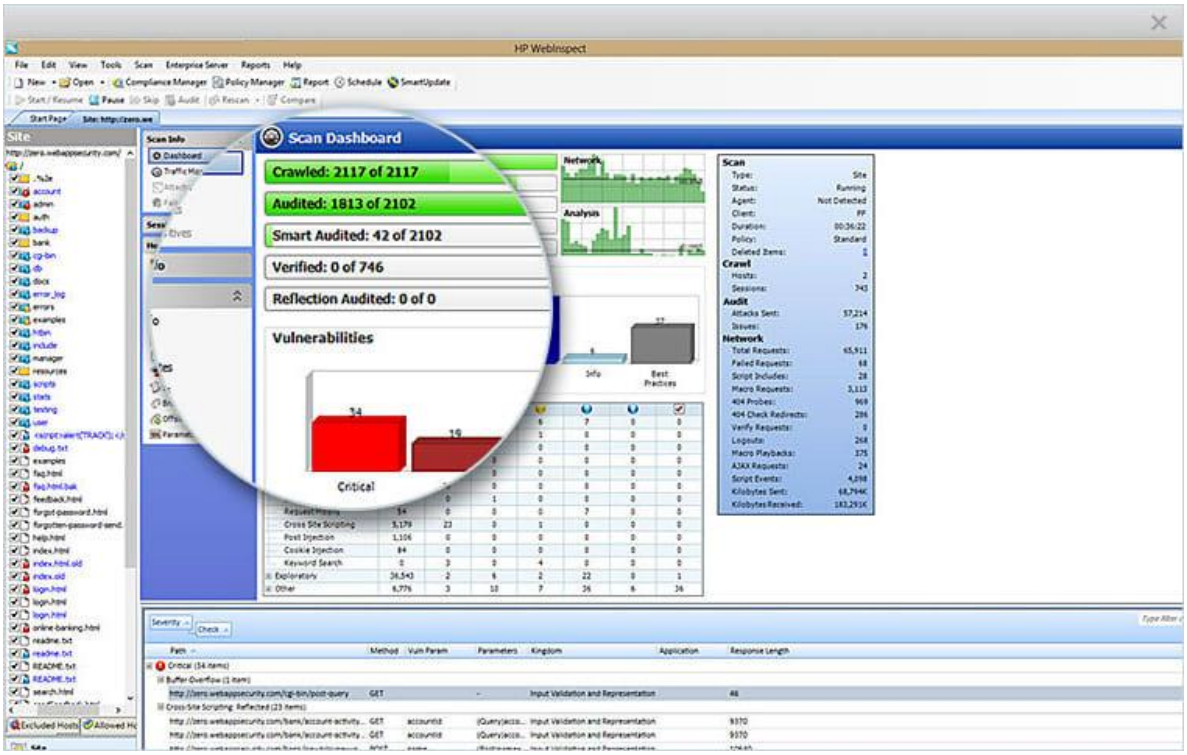


Рисунок 2.3 – Інтерфейс Fortify WebInspect

Джерело[13]

4) IBM Security AppScan. В арсеналі Security AppScan є різноманітні інструменти для проведення статичних та динамічних тестів, а також перевірки Open Source компонентів.

Програма підтримує більшість сучасних протоколів, стандартів та архітектур, у тому числі JavaScript/Ajax та Adobe Flash. Хоча упор для IBM Security AppScan зроблений на автоматичних перевірках, є можливість проводити і ручні тести додатків. Алгоритми перевірки для максимальної

схожості з реальними атаками використовують адаптивні процедури, що імітують людську поведінку.

Виявлені проблеми подаються у вигляді зручних звітів. У базі програми є понад 40 шаблонів звітів про відповідність різноманітним стандартам: ISO 27001, ISO 27002, Basel II, т.д.

Для кожної виявленої вразливості наводиться докладне пояснення та рекомендації щодо оперативного усунення проблеми.

У цих порадах використовуються підготовлені етапи роботи, що включають приклади коду та список завдань, які необхідно виконати першочергово. Продукт постачається в кількох редакціях, перед покупкою можна спробувати безкоштовну версію.

Інтерфейс наведений на рисунку 2.4.

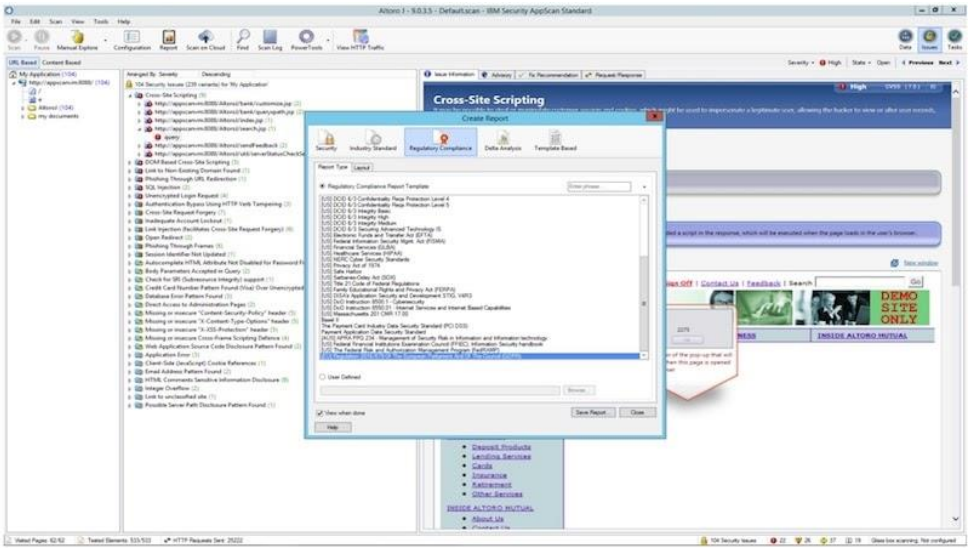


Рисунок 2.4 – Інтерфейс IBM Security AppScan
Джерело[14]

5) Accunetix Vulnerability Scanner. Захисні продукти Acunetix користуються заслуженою популярністю серед таких клієнтів, як, Visa або American Express. Серед цих продуктів і сканер захищеності веб-застосунків Acunetix Vulnerability Scanner. Цей інструмент має великий набір функцій для забезпечення автоматичного контролю безпеки програм.

Він виявляє всі поширені типи вразливостей, серед яких SQL-ін'єкції, виконання шкідливих скриптів та кодів. Наприклад, для популярної платформи WordPress цей продукт може виявити до 1200 відомих уразливостей. При цьому він може працювати у багатопотоковому режимі, що дозволяє перевіряти тисячі об'єктів різних платформ без перерви.

Усі виявлені проблеми відображаються у зручних звітах. Вони підходять як для фахівців, які безпосередньо усуватимуть проблеми, так і для керівників, яким потрібно бути в курсі того, що відбувається, і розуміти загальну картину. Підсумкові звіти можуть бути скомпоновані у загальному файлі. Ці результати можуть бути звірені з аналогічними даними після минулих перевірок, щоб визначити, які уразливості усунуті, а які ще залишилися.

Пробна версія програми (з деякими обмеженнями) доступна протягом 14 днів. Також сервіс має хмарний сканер, який передбачає деяку кількість безкоштовних перевірок.

Інтерфейс програми наведений на рисунку 2.5.

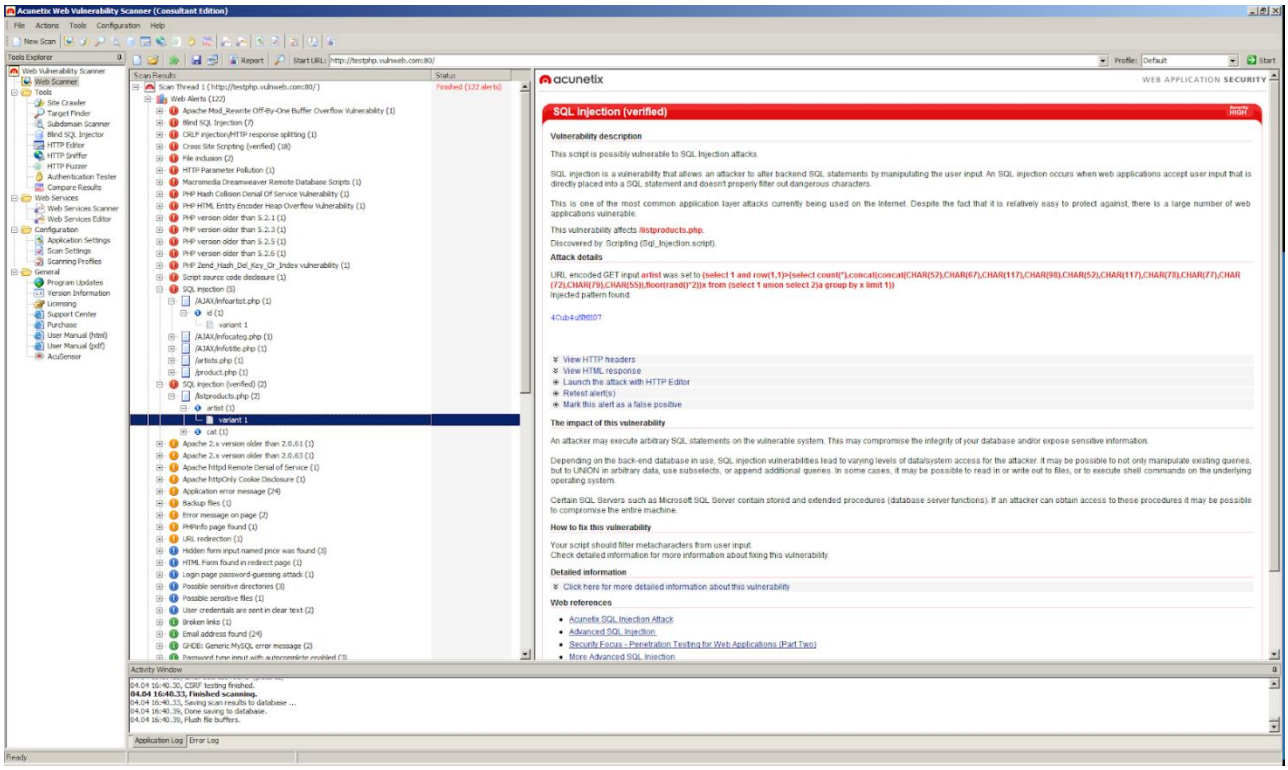


Рисунок 2.5 - Accunetix Vulnerability Scanner
Джерело[15]

6) Netsparker Web Application Security Scanner. Цей повністю автоматичний сканер відрізняється високим рівнем виявлення вразливостей та мінімальною кількістю помилкових спрацьовувань. Такий результат досягається завдяки фірмовому інструменту Proof-Based Scanning, який не лише сигналізує про загрозу, а й одразу ж надає докази, що це не хибне спрацювання.

Таким чином економиться багато часу та ресурсів, адже виявлені загрози не потрібно повторно перевіряти вручну, а можна одразу приступати до їх усунення.

Netsparker Web Application Security Scanner вміє аналізувати веб-програми та сервіси на всіх поширених платформах, серед яких Java Script, HTML 5, .NET та багато інших. Перевірка проводиться у всіх поширених типах атак.

Інструмент може одночасно працювати з сотнями та тисячами ресурсів, при цьому легко інтегрується у вже існуючі системи безпеки. Продукт поставляється в десктопному, корпоративному та хмарному варіанті. Також є пробна версія.

Інтерфейс наведений на рисунку 2.6.

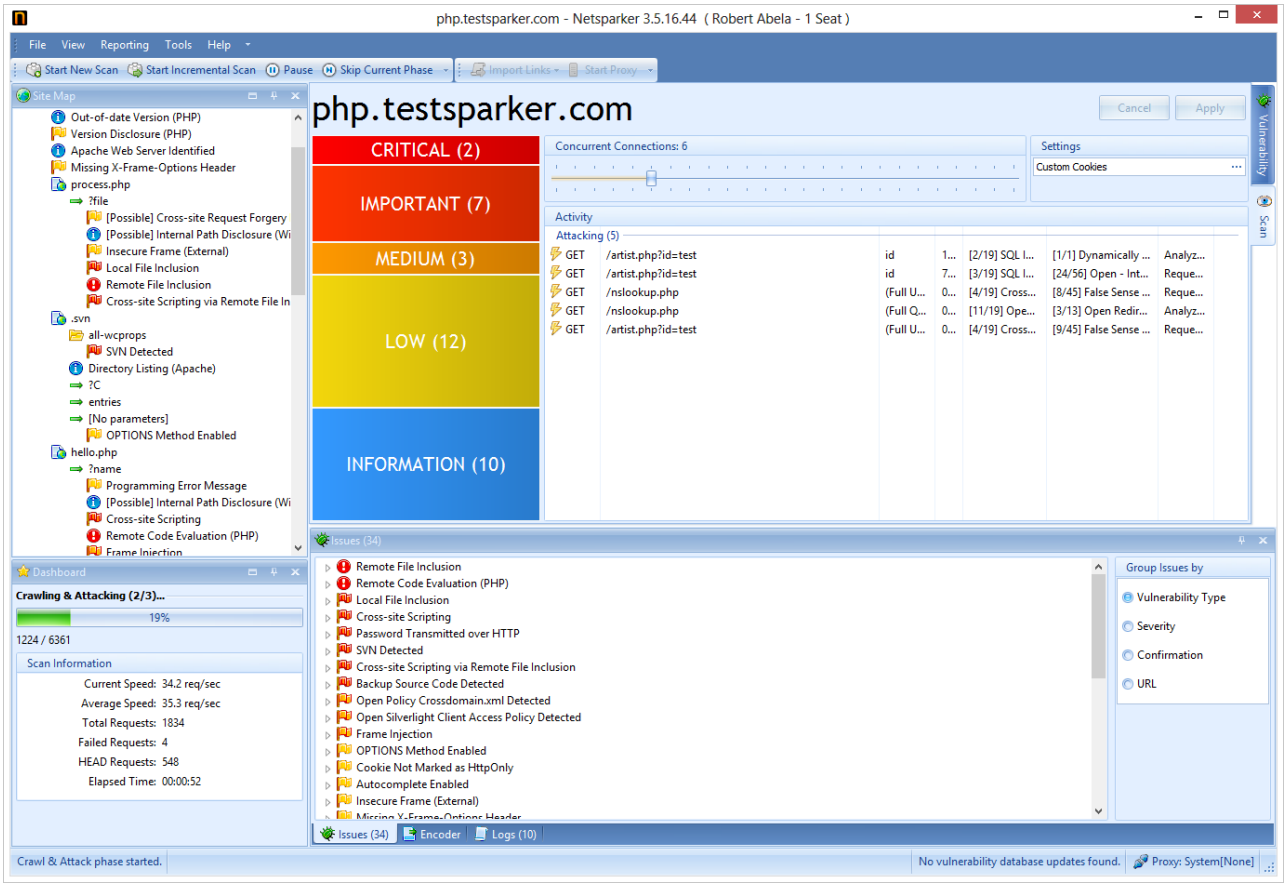


Рисунок 2.6 – Інтерфейс Netsparker Web Application Security Scanner
Джерело[16]

7) Janusec WebCruiser. Сканер заточений головним чином на проведення SQL-ін'єкцій на різних платформах, наприклад, SQL Server, Oracle і Access. У ньому також є інструменти для роботи з cookie, міжсайтовим криптингом, PHP-ін'єкціями та іншими найпоширенішими загрозами.

Інтерфейс наведений на рисунку 2.7.

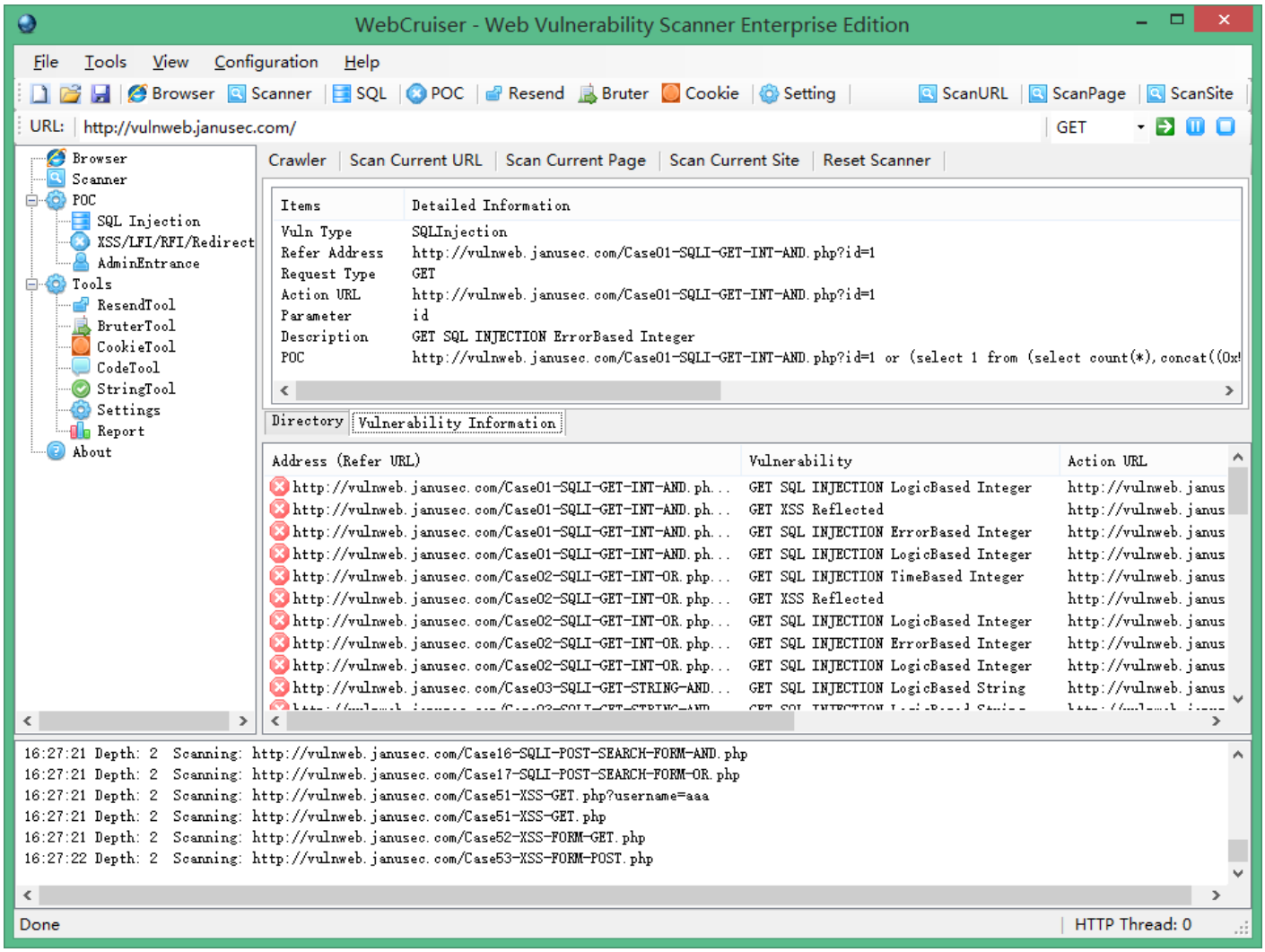


Рисунок 2.7 – Інтерфейс Janusec WebCruiser

Джерело[17]

8) Nessus. Це добре відомий та популярний сканер уразливостей, який надається безкоштовно для особистого некомерційного використання.

Його було вперше випущено в 1998 році Ренурдом Дерасоном і в даний час опубліковано Tenable Network Security. Існує також додатковий проект Nessus 2 під назвою OpenVAS, який публікується за ліцензією GPL.

Використовуючи велику кількість перевірок уразливостей, які називаються плагінами в Nessus, можна ідентифікувати велику кількість добре відомих уразливостей. Metasploit приймає файли результатів сканування вразливостей як від Nessus, і від OpenVAS у форматі файлу nbe .

Інтерфейс сканера наведений на рисунку 2.8.

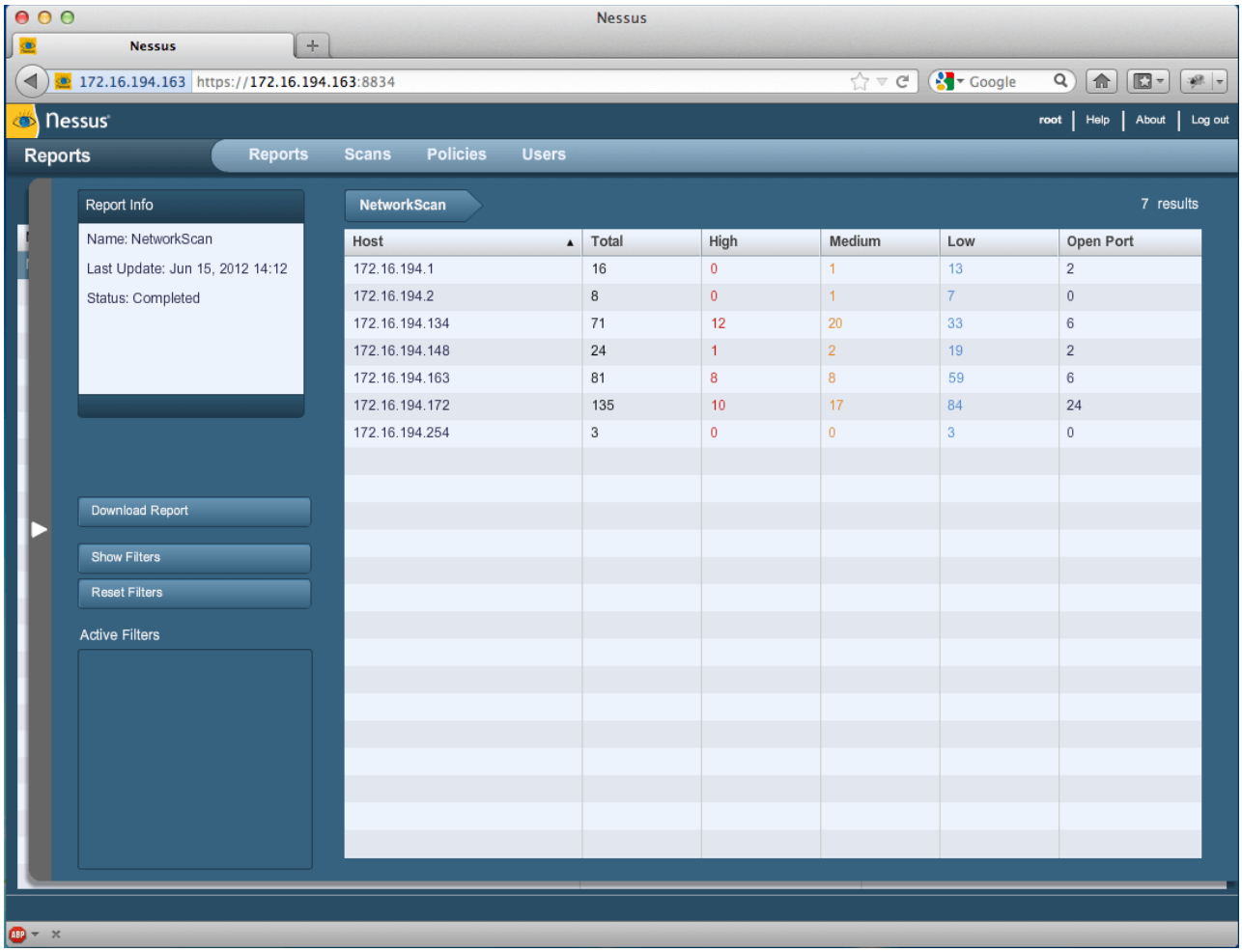


Рисунок 2.8 - Інтерфейс сканера Nessus

Джерело[18]

Nessus може сканувати наступні вразливості:

- Вразливості, які можуть дозволити неавторизований контроль або доступ до конфіденційних даних у системі;

- Неправильна конфігурація (наприклад, відкритий поштовий ретранслятор):

- Відмова в обслуговуванні (DOS) вразливості;

- Стандартні паролі, кілька спільних паролів та порожні / відсутні паролі для деяких системних облікових записів

Збої в програмному забезпеченні, відсутні виправлення, шкідливе програмне забезпечення та помилки неправильної конфігурації в широкому

спектрі операційних систем, пристроїв та програм вирішуються за допомогою Nessus.

Сервер Nessus в даний час доступний для:

- Unix;
- Linux;
- FreeBSD.

Також сканер доступний для:

- Операційних систем на основі Unix;
- Операційних системи на базі Windows;

Істотні можливості Nessus включають:

- Заплановані аудити безпеки;
- Виявлення «дірок» у безпеці на локальних чи віддалених хостах;
- Імітація атак виявлення вразливостей;
- Виявлення відсутніх оновлень безпеки та патчів;

Nessus Professional виконує сканування внутрішньої мережі відповідно до вимог PCI DSS 11.2.1.

Приклад результатів сканування наведений на рисунку 2.9.

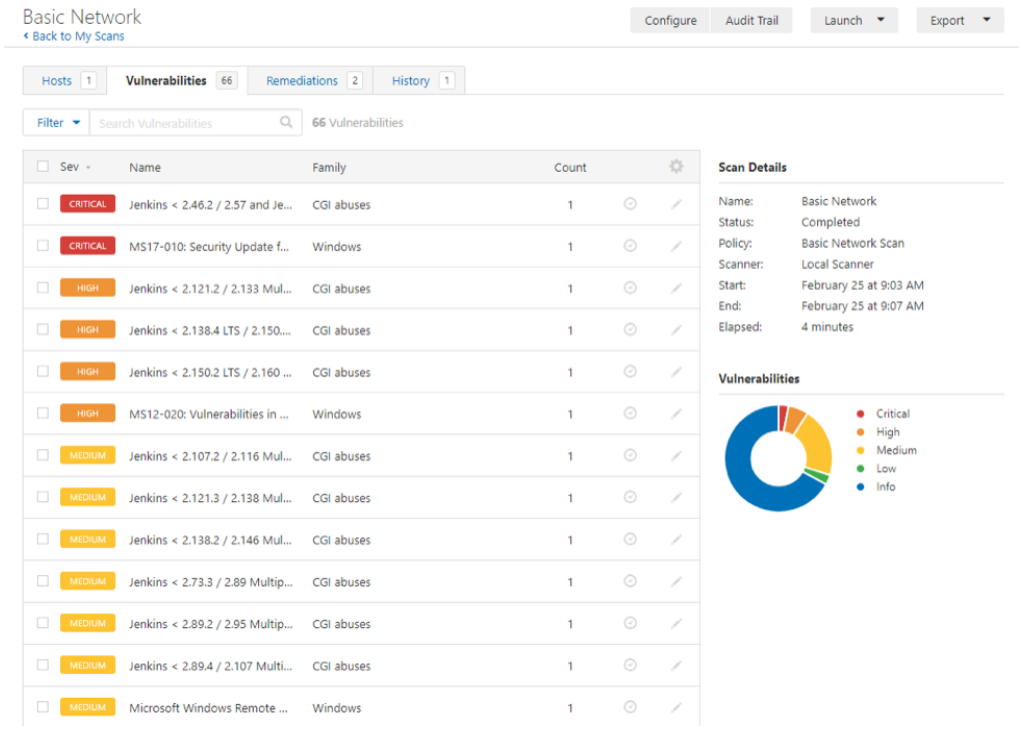


Рисунок 2.9 – Приклад результатів сканування Nessus

Джерело[18]

Таким чином, існують наступні варіанти пошуку вразливостей - використання комплексних комерційних рішень, таких як Nessus, або використання засобів, що входять до спеціальних ОС, таких як Kali Linux та ін.

Використання спеціальних ПЗ для пошуку вразливостей та проведення тестувань на проникнення передбачає дотримання певного алгоритму застосування вбудованих в ПЗ засобів з метою підвищення ефективності пошуку вразливостей.

2.3 Системи автоматизированого тестування як ефективні засоби захисту персональних даних

При ручному тестуванні захисту персональних даних витрачається багато людських ресурсі для проведення повного циклу тестування безпеки під час виконання наступних етапів:

- Збір інформації;

- Ручне сканування вразливостей захисту персональних даних;

- Виявлення та перевірка вразливості;

- Складання звітів;

- Виправлення [13].

У будь-якій організації ці етапи зазвичай пов'язані з залученням безлічі людей: розробників, аналітиків якості, менеджерів проектів, адміністраторів мережі, розробників веб-додатків, менеджерів інформаційної безпеки, аудиторів та керівників. Навіть сторонні постачальники залучаються до проектів оцінки веб-безпеки. З такою кількістю співробітників, які працюють заради спільної мети, необхідно максимально автоматизувати пошук вразливостей персональних даних учнів навчального закладу.

Є певні переваги автоматизованого тестування захисту персональних даних. По-перше, є ризик дублювання зусиль під час надлишкових тестів. Коли є безліч складних веб-додатків, як більшість сучасних онлайн-компаній, це може призвести до значного обсягу непотрібної роботи [13].

Ще одна проблема, полягає в тому, що не вистачає знань або часу для постійного ручного тестування вразливостей усіх персональних даних. Якщо тестування безпеки веб-застосунків не автоматизовано з використанням перевіреного автоматизованої системи безпеки персональних даних, які можуть перевірити тисячі потенційних недоліків безпеки, при цьому деякі, якщо не всі серйозні вразливості веб-додатків можуть бути втрачені.

В якості прикладу можна розглянути індивідуалізовану веб-систему планування ресурсів підприємства (ERP). Така система буде мати сотні видимих точок входу або поверхонь для атак, а також безліч інших прихованих вразливостей, які необхідно перевірити на наявність вразливостей персональних даних, таких як SQL-ін'єкції та міжсайтові сценарії.

Нехай ERP має 200 точок входу, які необхідно перевірити на предмет 100 різних варіантів вразливості веб-додатків. Це означає, що тестеру на проникнення необхідно запустити щонайменше 20 000 тестів безпеки. Якби

кожен тест займав всього 5 хвилин, спеціалісту з веб-безпеки знадобилося б близько 208 робочих днів, щоб завершити належний аудит безпеки персональних даних в ERP-системі.

Система автоматизованого захисту персональних даних може сканувати набагато більші ERP-системи на предмет набагато більшої кількості варіантів уразливостей персональних даних за декілька годин. І, на відміну від людини, автоматичний сканер безпеки не забуде просканувати вхідний параметр.

Виконуючи ручний тест безпеки веб-застосунків, виникає обмеження проникнення рядом відомих уразливостей, відомих тестеру на проникнення. З іншого боку, при використанні автоматичного сканера веб-вразливостей, вможливо переконаєтеся, що всі параметри перевіряються на відповідність усім типам варіантів безпеки персональних даних.

Використовуючи системи автоматизованого захисту, можна гарантувати гарантуєте, що в результатах сканування безпеки персональних даних не буде повідомлень про помилкові спрацьовування, тому не потрібно виділяти час на перевірку виявлених уразливостей.

Важливість автоматизації тестування вразливостей підкреслюється популярними дослідженнями у сфері інформаційної безпеки. Рік за роком це дослідження вказує на ті самі основні причини інформаційних ризиків, такі як брак ресурсів, недостатня прозорість і непоінформованість керівництва. Кожен із цих елементів може бути вирішений шляхом автоматизації процесів тестування безпеки [13].

Як відмічається в [13], немає ідеального способу перевірити вразливість персональних даних. Однак робити це вручну і покладатися тільки на досвід співробітників не може гарантувати повну достовірність отриманих результатів тестування.

Існують різні інструменти автоматичного тестування безпеки персональних даних учнів навчльного закладу, розглянемо список із найкращих

інструментів систем тестування персональних даних станом на 2022 рік згідно з інформацією, представленою в [12,13].

1. WebLOAD. WebLOAD - це ефективний інструмент тестування продуктивності веб-застосунків для веб-додатків, який показує здатність програми обробляти навантаження. Цей інструмент має потужний потенціал створення сценаріїв, який спрощує комплексне тестування. Більш того, за його допомогою можна визначити аспекти продуктивності, вузькі місця та можливі вразливості у додатку. Це відповідний інструмент, який може допомогти у досягненні необхідної ефективності відгуку для веб-додатку. Крім цього, WebLOAD також інтегрований з Selenium, Jenkins та іншими інструментами, щоб підвищити його можливості тестування.

Інтерфейс наведений на рисунку 2.10.

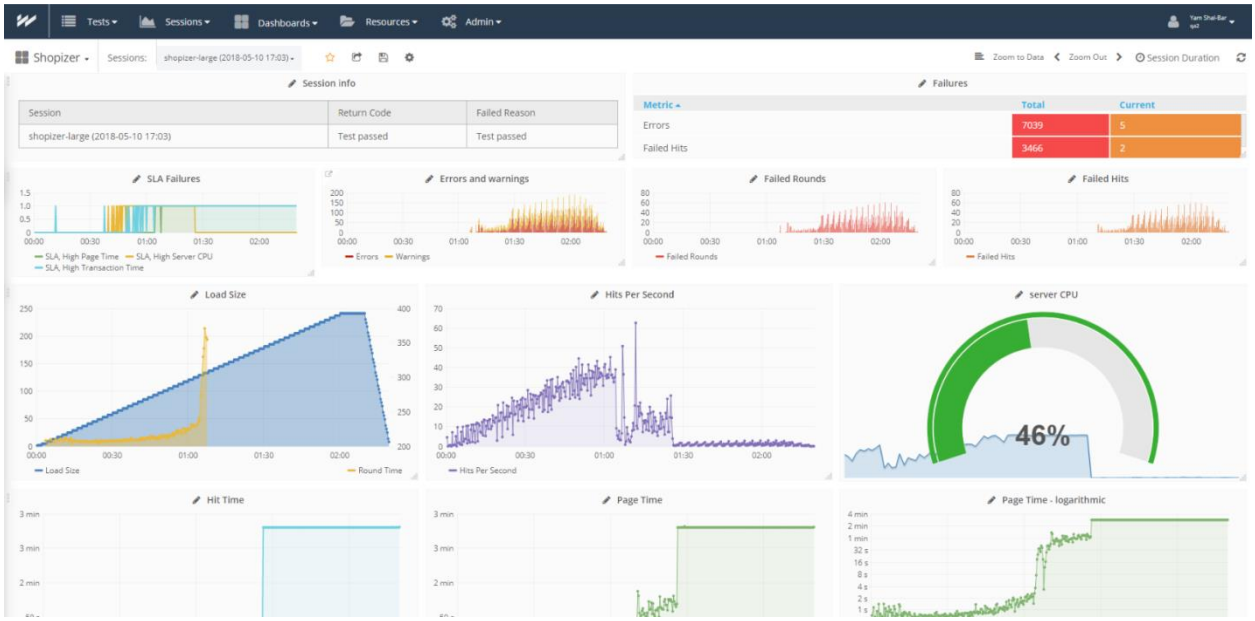


Рисунок 2.10 – Інтерфейс інструменту WebLOAD

Джерело[12]

2. Acunetix. Acunetix - це автоматизований варіант інструментів тестування безпеки веб-додатків, в який вбудований сканер безпеки, який був розглянутий раніше для виявлення навіть незначних вразливостей більш ніж 4500 веб-додатків.

Інтерфейс наведений на рисунку 2.11.

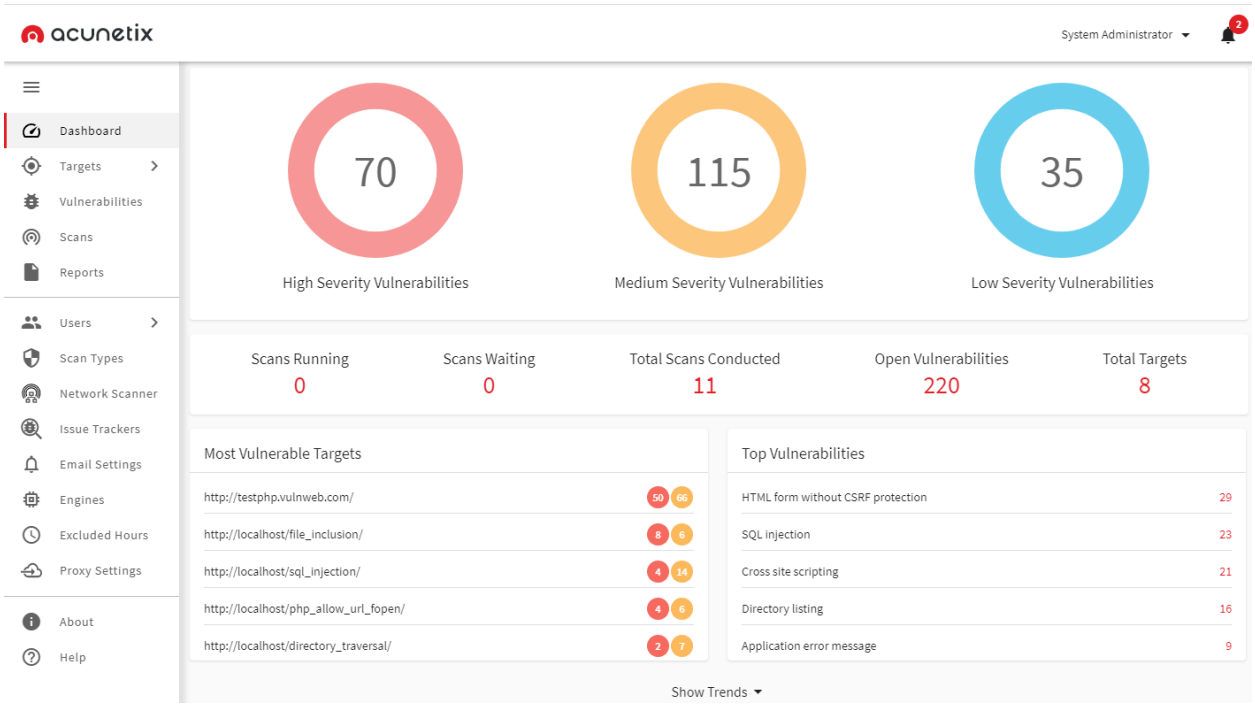


Рисунок 2.11 – Інтерфейс автоматизованої системи Acunetix

Джерело[13]

3. Netsparker. Інструмент тестування веб-додатків Netsparker відомий своєю точністю. Він також має вбудований сканер безпеки для виявлення дрібних та серйозних уразливостей майже у всіх веб-API, який був розглянутий раніше. Цей інструмент виявляє помилки і перевіряє, чи вони справжні або помилкові. Це допоможе заощадити час у порівнянні з ручною перевіркою та переглядом кожної виявленої несправності після сканування. Можна використовувати інструмент Netsparker як програмне забезпечення Windows або як постачальник послуг онлайн. Функції та ефективність залишаються однаковими в обох версіях.

Інтерфейс наведений на рисунку 2.12.

Рисунок 2.12 – Інтерфейс автоматизованої системи Netsparker

Джерело[14]

4. Experitest. Experitest дозволяє користувачам тестувати веб-додатки на більш ніж 1000 пристроїв одночасно у хмарі. Існують як інструкції, так і автоматизовані інструменти для перегляду веб-додатків, призначені для тестування веб-застосунків.

З Experitest буде достатньо протестувати програму в будь-якому браузері. Більш того, він інтегрований з Appium та Selenium для досягнення найкращих результатів. Шаблон тестування цього інструменту працює в режимі реального часу та налагоджує його для отримання найкращих результатів. Experitest може провести більше 100 тестів одночасно. На додаток до цього також можна пройти візуальне тестування, щоб визначити ефективність відгуку інтерфейсу користувача при різних дозволах.

Інтерфейс наведений на рисунку 2.13.

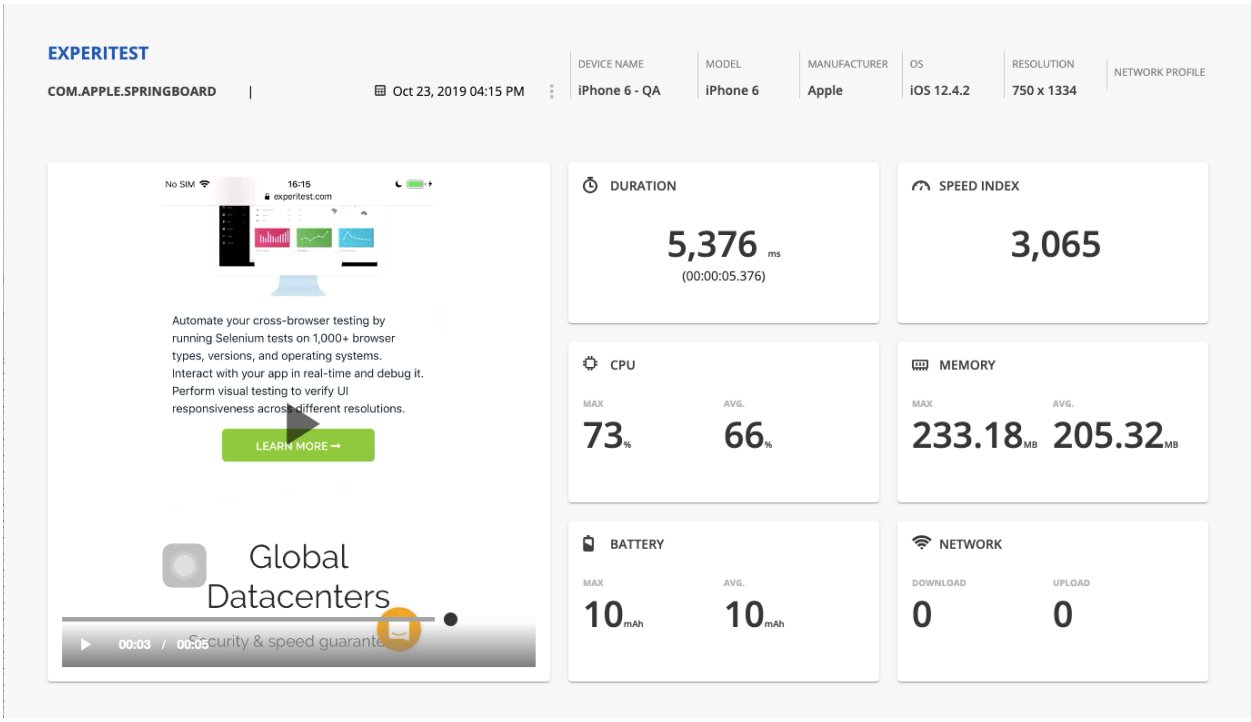


Рисунок 2.13 – Інтерфейс автоматизованої системи Experitest

Джерело[15]

5. Lambda Test. Інструмент Lambda Test призначений для забезпечення безперебійної роботи всіх елементів веб-застосунків, таких як CSS, HTML5 та інших, на всіх пристроях. Цей інструмент слідує за схемою тестування: ручне, візуальне, а також автоматичне тестування або прогресивні результати. Він використовує хмарну інфраструктуру для одночасного паралельного запуску кількох тестів.

Інтерфейс наведений на рисунку 2.13.

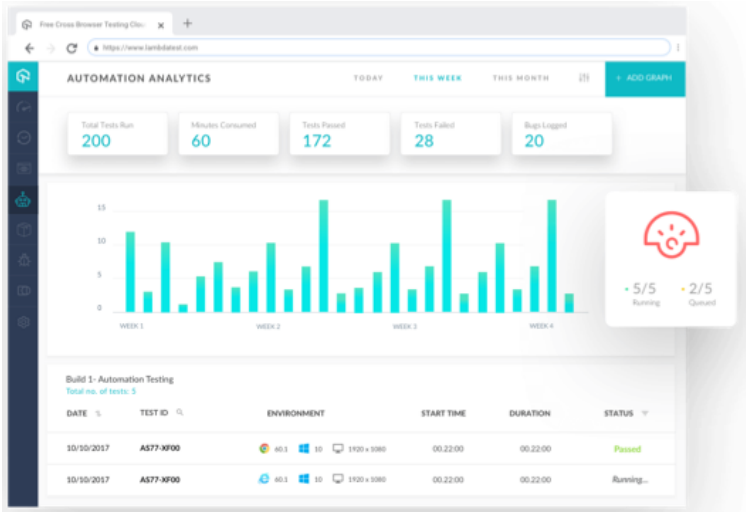


Рисунок 2.13 – Інтерфейс автоматизованої системи Lambda Test

Джерело[16]

6. Selenium. У списку інструментів автоматизації тестування з відкритим кодом для веб-додатків це один із найбільш широко застосовуваних інструментів тестувальників. Selenium широко відомий як один із найкращих інструментів регресійного тестування, який без проблем працює у різних браузерах та платформах.

Автоматизація тестування – одна з найкращих переваг Selenium, і в нього вбудовано безліч окремих інструментів. Кожен інструмент Selenium призначений для обробки різних аспектів тестування веб-додатків. Selenium IDE, Selenium Web Driver, Selenium RC та Selenium Grid – це чотири компоненти Selenium.

Інтерфейс системи наведений на рисунку 2.14.

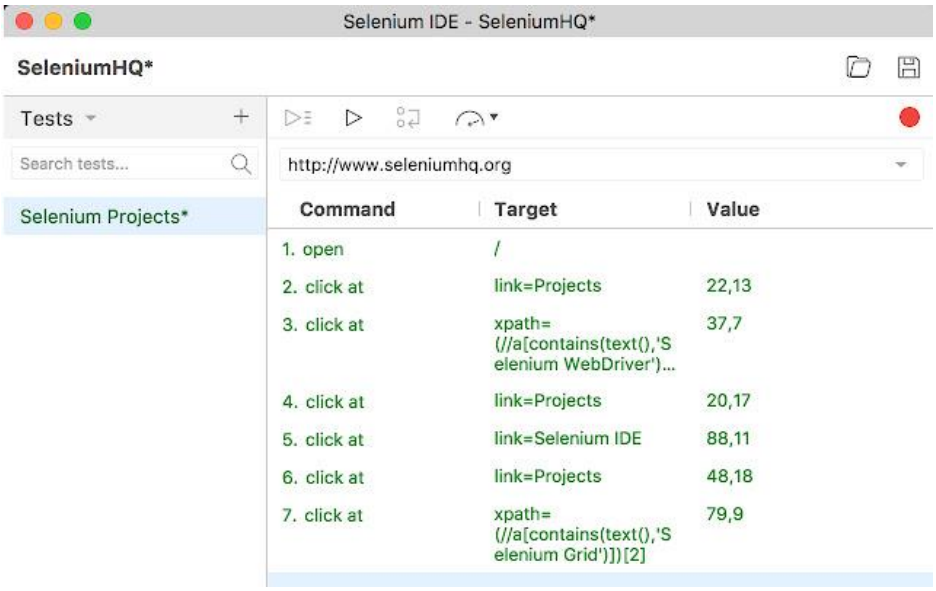


Рисунок 2.14 – Інтерфейс автоматизованої системи Selenium

Джерело[17]

7. Watir. Watir – це абревіатура від слова «тестування веб-додатків у Ruby». Найкраще в Watir - те, що він тестує веб-програми так само, як і люди. Цей інструмент тестування використовує такі ідеології, як перехід за посиланнями, перевірка текстів, заповнення форм та інші аспекти для тестування веб-додатків у реальному часі для виявлення основних лазівок. Система досить проста у використанні і без проблем працює на різних платформах чи браузерах.

Інтерфейс представлений на рисунку 2.15.

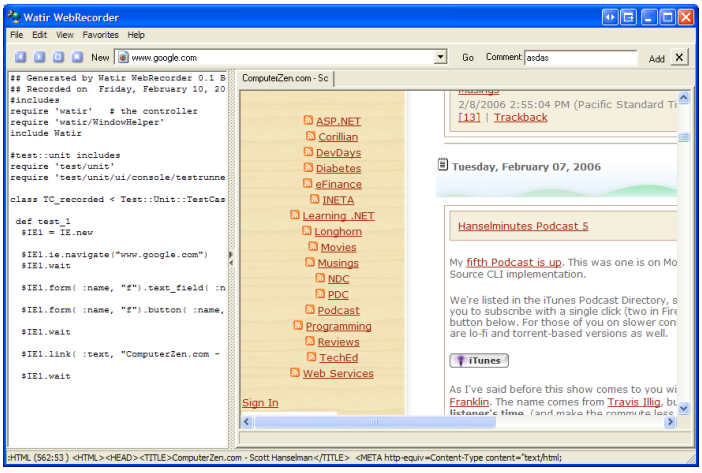


Рисунок 2.15 - Інтерфейс автоматизованої системи Watir

Джерело[18]

8. Ranorex Studio. Ranorex розроблений для максимального збільшення ресурсів підтримки методів автоматизованого тестування. Це відповідний інструмент для початку наскрізного тестування з використанням симуляторів або реальних пристроїв для більш помітних результатів. Він чудово працює практично з усіма браузерами, такими як Safari, Microsoft Edge, Chrome та іншими.

Інтерфейс представлений на рисунку 2.16.

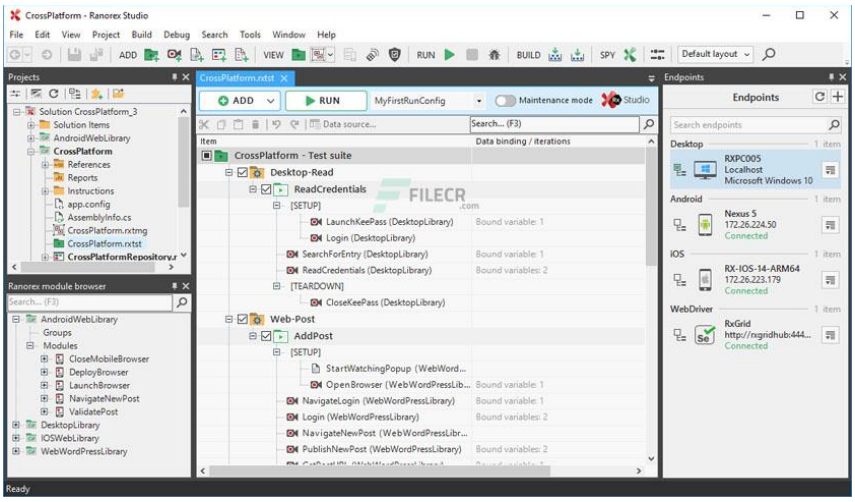


Рисунок 2.16 – Інтерфейс автоматизованої системи Ranorex Studio

Джерело[19]

9. Serenity. Інструмент тестування Serenity гарантує, що написані тести простіше в обслуговуванні та досить гнучкі для різних програм. Крім того, Serenity складає докладні звіти про тестування, щоб дати уявлення про продуктивність веб-додатку. Більше того, він також відстежує весь прогрес проекту.

Вище наведено 9 найкращих інструментів для тестування персональних даних, які широко використовуються компаніями. При адекватних результатах робота над модифікацією додатків стане простішою та зручнішою.

2.4 Висновки до другого розділу

Існують різні засоби пошуку уразливостей для різних етапів перевірки систем на наявність уразливостей, від сканерів портів до комплексних систем, які складаються із сканерів портів, засобів пошуку експлойтів для вразливостей.

Для захисту персональних даних існує окрема ідеологія тестування, і цей процес охоплює безліч аспектів. Під час тестування захисту персональних даних перевіряються такі аспекти, як безпека веб-сайту, функціональність, зручність використання, доступність, продуктивність та інші. У разі будь-яких проблем чи лазівок інструменти тестування захисту персональних даних вкажуть розробникам їх усунення в найкоротші терміни.

Актуально використовувати автоматизовані системи тестування захисту персональних даних. Проте аналіз існуючих рішень показав, що деякі з них є недостатньо ефективними щодо нових виникаючих загроз, є нешвидко дійними та не застосовують сучасних технологій тестування. В межах написання роботи пропонується розробка власної системи автоматизованого тестування з застосуванням нейронних мереж з метою підвищення ефективності виявлення сучасних загроз інформаційної безпеки.

3 РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ УЧНІВ НАВЧАЛЬНОГО ЗАКЛАДУ

3.1 Методика аналізу основних мір від актуальних загроз безпеки персональних даних

Для нейтралізації та зниження ймовірності прояву тих чи інших загроз на всіх стадіях життєвого циклу вузлів необхідно використовувати комплекс заходів та засобів захисту:

- організаційних та організаційно-технічних;
- інженерних та інженерно-технічних;
- технічних; програмних, апаратних та програмно-апаратних.

Клас спеціальної інформаційної системи персональних даних присвоюється згідно з експертною оцінкою спеціаліста із захисту інформації. Оскільки для розподіленої інформаційної системи персональних даних підприємства порушення заданої характеристики безпеки персональних даних, оброблюваних у яких, може призвести до значних негативних наслідків для суб'єктів персональних даних, інформаційної системи персональних даних присвоюється клас спеціальний. Вибір засобів захисту персональних даних має здійснюватися кілька етапів. На першому етапі виконується експертний аналіз ринку засобів захисту та проведення попереднього відбору виробника та лінійки продуктів засобів захисту інформації, що задовольняють вимогам до системи захисту персональних даних.

За результатами першого етапу складається перелік засобів захисту, у якому вказувалися всі лінійки продуктів засобів захисту інформації аналізованого типу та його виробники. За наявності або відсутності сертифіката засобу захисту в таблиці порівняння проставлялася відповідно «1» або «0».

На другому етапі для вибору засобів захисту з попереднього переліку використовується факторний аналіз. У факторному аналізі використовуються

суттєві характеристики засобів захисту інформації, ваговий коефіцієнт характеристики, рівень відповідності продукту – опису характеристики.

Перелік характеристик визначається на основі всіх істотних властивостей засобів захисту інформації, пов'язаних з функціональними та системними можливостями продуктів, можливостями, пов'язаними з управлінням та моніторингом, характеристик пов'язаних із довірою та вартістю продуктів. При цьому враховувалися ті властивості, про наявність або відсутність яких можна дати відповідь «є» або «ні», а також ті, для яких можна експертним шляхом вибрати значення з діапазону від 0 до 1.

Ваговий коефіцієнт характеристики визначає, наскільки дана можливість чи характеристика продукту важлива реалізації системи захисту персональних даних. Він може приймати значення:

1 та більше – дуже важлива;

0,5 – важлива;

0 – не важлива.

Ступінь відповідності продукту визначає, наскільки продукт відповідає необхідній для системи захисту персональних даних можливості або характеристиці. Позиції матриці в факторній таблиці заповнювалися логічними значеннями «0» або «1» відповідно за відсутності або наявності засобів захисту інформації можливості або якості, що описується характеристикою. Якщо рівень відповідності характеристиці в різних засобів може бути оцінена, то застосовується градація значень параметра цієї характеристики, який може набувати значення від 0 до 1.

Для включення в факторну таблицю кількісних показників, наприклад, вартості, вони приводилися до нормального вигляду. Показники характеристик, для яких найкращими є максимальні значення, обчислюються за такою формулою:

$$П_n = \frac{C_n}{C_{max}}, \quad (2)$$

де $П_n$ - нормований кількісний показник характеристики n-го засобів захисту інформації,

C_n - Значення показника характеристики n-го засобів захисту інформації,

C_{max} - Максимальне значення показника характеристики з усіх аналізованих засобів захисту інформації.

Показники характеристик, для яких найкращими є мінімальні значення, обчислювалися за такою формулою:

$$П_n = 1 - \frac{C_n}{C_{max}}, \quad (3)$$

де $П_n$ - нормований кількісний показник характеристики n-го засобів захисту інформації,

C_n - Значення показника характеристики n-го засобів захисту інформації,

C_{max} - Максимальне значення показника характеристики з усіх аналізованих засобів захисту інформації.

Наприклад, якщо вартість 1-го, 2-го, 3-го та 4-го засобів захисту інформації дорівнює відповідно 100, 150, 200 і 250 грн, то дорівнюватиме 250 грн, а C_{max} нормовані значення показників для всіх засобів: 1 – 0 ,4 = 0,6, 1 - 0,6 = 0,4, 1 - 0,8 = 0,2 і 1 - 1 = 0.

Після заповнення факторної таблиці проводиться розрахунок та отримання значень показників ефективності засобів захисту інформації аналізованого типу.

Показник ефективності (рейтинг) засобів захисту інформації розраховувався за такою формулою:

$$Э_n = \frac{\sum_m z_n x_m}{M}, \quad (4)$$

Де $Э_n$ - показник ефективності n-го засобів захисту інформації,

z_n - Показник наявності властивості у n-го засобів захисту інформації, що приймає значення від 0 до 1,

x_m - ваговий коефіцієнт m-го властивості засобів захисту інформації, що приймає значення від 0 до 10,

n – порядковий номер (індекс) засобів захисту в матриці факторної таблиці,

m – порядковий номер (індекс) характеристики якості у матриці факторної таблиці,

M - загальна кількість характеристик засобів захисту інформації.

Одним із найактуальніших на поточний момент питанням у галузі захисту інформації в Україні є захист персональних даних відповідно до законодавства та актуальних загроз безпеки інформаційної системи персональних даних. Особливо гостро стоїть питання забезпечення безпеки в персональних даних у великих розподілених інформаційних системах персональних даних.

Особливістю розподіленої інформаційної системи персональних даних є передача персональних даних по неконтрольованому каналу, що найчастіше представляє собою мережу зв'язку загального користування або Інтернет. Ця особливість впливає на всі основні характеристики безпеки інформаційна система персональних даних, у тому числі на необхідність криптографічного захисту даних, що передаються. Зважаючи на розподіл і різнорідність засобів інформатизації та захисту інформаційна система персональних даних, гостро стає питання вибору система захисту інформації, питання централізації механізмів моніторингу та управління.

У розподіленій інформаційній системі персональних даних найчастіше обробляються персональні дані.

Розподілена інформаційна система персональних даних завжди є спеціальною, тому що для неї крім забезпечення конфіденційності необхідно також забезпечити цілісність і доступність. Клас спеціальної інформаційної системи персональних даних визначається на основі моделі загроз безпеки персональних даних.

Відповідно до моделі загроз, розподілена інформаційна система персональних даних має низький рівень вихідної захищеності та низку актуальних загроз.

Клас спеціальної інформаційна система персональних даних присвоюється згідно з експертною оцінкою спеціаліста із захисту інформації. Оскільки для розподіленої Інформаційна система персональних даних підприємства порушення заданої характеристики безпеки персональних даних, що обробляються в них, не може призвести до значних негативних наслідків для суб'єктів персональних даних, розподілена

Для нейтралізації та зниження ймовірності прояву тих чи інших загроз на всіх стадіях життєвого циклу інформаційної системи необхідно використовувати комплекс заходів та засобів захисту:

- організаційних та організаційно-технічних;
- інженерних та інженерно-технічних;
- технічних;
- програмних, апаратних та програмно-апаратних.

Проектована система захисту персональних даних згідно з проведеним аналізом повинна складатися з наступних підсистем:

- підсистема захисту від несанкціонованого доступу;
- підсистема антивірусного захисту;
- підсистема міжмережевого екранування;
- підсистема криптографічного захисту;
- підсистема виявлення вторгнень;
- підсистема аналізу захищеності.

3.2 Дослідження розробленої системи і аналіз отриманих результатів

Підсистема захисту від несанкціонованого доступу реалізується засобами управління знімними носіями та забезпечення посиленої аутентифікації.

При виборі засобами управління знімними носіями розглядалися виробники та їх продукти, які відповідають вимогам системи захисту персональних даних, зазначені в таблиці 2.2.

Таблиця 2.2 - Аналізовані засоби управління знімними носіями

Назва засоби захисту інформації	Сертифікат	Інші	Примітка
Security Studio (Информзахист).	1	0	4 НДВ 4, 5 СВТ.
Device Lock (Смарт Лайн Инк).	1	0	4 НДВ, ЗБ.
Lumension Device Control (Lumension).	0	0	
McAfee Device Control (McAfee).	0	0	
Cisco Security Agent (Cisco Systems).	1	1	ТУ, EAL2.
Symantec Endpoint Protection 11.0 (Symantec Corporation).	1	1	ТУ, 4 НВД.

Було проведено порівняння основних функціональних, системних можливостей товарів, показників пов'язані з довірою та вартістю товарів. Як засіб посиленої аутентифікації був обраний продукт eToken Network Logon, який використовується спільно з eToken PRO (Java)/72K/CERT-1883. Для створення централізованої системи управління, призначеної для впровадження, управління, використання та обліку апаратних засобів аутентифікації користувачів eToken PRO (Java), рекомендується розгорнути комплекс eToken TMS.

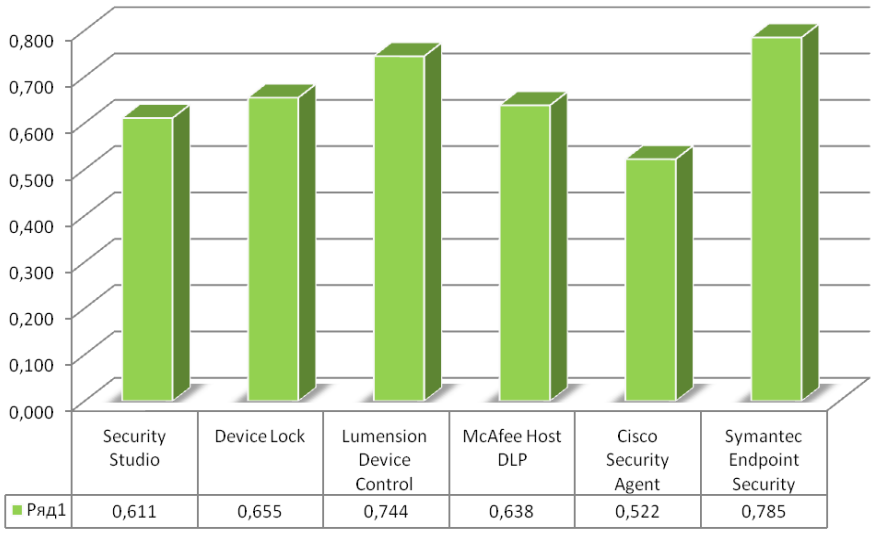


Рисунок 3.1 – Графік рейтингів засобів управління знімними носіями

Джерело[21]

Як засіб антивірусного захисту інформаційні системи персональних даних пропонується використовувати засоби антивірусної Symantec Endpoint Protection виробництва компанії Symantec, так як цей комплексний засіб реалізує функції декількох підсистем і має високі показники ефективності.

Обробка персональних даних здійснюється технічними засобами, тому безпека персональних даних може бути досягнута лише у разі, якщо буде виключена можливість несанкціонованого доступу до інформаційної системи, у якій обробляються персональні дані.

Як правило, виділяють чотири класи методів захисту персональних даних в інформаційних системах. По-перше, фізичні методи, по-друге, апаратні, по-третє, програмні, нарешті, по-четверте, організаційні.

На організаційному рівні захист персональних даних відбувається у вигляді розробки та впровадження відповідних нормативно-правових актів, проведення організаційно-технічних заходів.

Фізичний захист здійснюється за рахунок таких засобів як служба охорони, система захисту вікон та дверей, лазерні та оптичні системи, які реагують на

перетин зловмисником світлових променів. Тобто фізичні методи захисту мають на увазі під собою фізичну перешкоду доступу до персональних даних.

Апаратні способи захисту можна реалізувати за допомогою спеціальних пристроїв. До таких засобів можна віднести різноманітні схеми блокування від несанкціонованого використання персональних даних. Апаратні засоби використовуються у складі ЕОМ.

Нарешті програмний захист здійснюється за допомогою програм, до яких можна віднести операційну систему, антивіруси, спеціальні програми захисту та інші.

Мабуть, саме апаратно-програмні засоби захисту персональних даних максимально дозволяють захищати персональні дані від несанкціонованого доступу до них.

Апаратно-програмний захист досягається застосуванням таких способів захисту як:

1. Захист від несанкціонованого використання персональних даних з боку користувачів та програм, у тому числі за наявності доступів.

2. Захист від некоректного використання наявних ресурсів.

3. Високий рівень якості апаратно-програмних засобів, що використовуються.

Загалом перелік технічних заходів щодо захисту персональних даних в інформаційній системі виглядає так:

— недопущення несанкціонованого доступу до персональних даних за допомогою антивірусного програмного забезпечення та системи паролів;

- діяльність з виявлення фактів несанкціонованого доступу та використання персональних даних (наприклад, оновлення антивірусного програмного забезпечення);

- Охорона, а також регламентування використання технічних засобів, за допомогою яких відбувається обробка персональних даних з метою недопущення порушення їх функціонування;

- Наявність можливості відновлення персональних даних у разі знищення персональних даних (зберігання резервних копій на знімних носіях) [3].

3.3 Розробка та впровадження технічної безпеки

Отже, що стосується захисту ЛОМ, то її необхідно поділити на 4 рівні:

1) загальний (зберігає тільки загальні відомості про П.І.Б., дату народження, поле, домашню адресу);

2) спеціальний (зберігає інформацію про номер ІПН, пенсійне медичне страхування-СНІЛЗ, дані трудової книжки);

3) Як відомо, бухгалтерія та кадри зберігають інформацію про співробітників;

4) Звичайний, де є всі інші абоненти мережі.

Оскільки організація мережі змінюється, слід висновок, що зміниться організація бази даних, яка буде складатися з кількох частин:

1) На файловому сервері (СРВ2), де зберігаються різні файли користувача, буде створена база даних, що складається з таблиць, що не мають зв'язку між собою і зберігають довідкову інформацію. У цій базі будуть розміщені:

- довідники прізвищ, імен, по батькові;
- довідники суб'єктів України, населених пунктів, адміністративно-територіальних одиниць суб'єктів, вулиць;
- довідники ветеранів міжнародного рівня;
- довідники адміністрації районів Краснодарського краю та їх населених пунктів.

Отже, ця БД містить лише знеособлену інформацію, тобто. між таблицями немає жодного зв'язку.

2) Сервер зберігання загальної інформації (SRV4) міститиме такі дані:

- Дата народження;
- Стать;
- Індекс, прізвище, ім'я, по батькові, місце проживання;
- Номер телефону;

Інша інформація, необхідна для роботи менеджменту, але не відноситься до ПДН.

Усі дані беруться з довідників SRV2, що зрештою призводить до зменшення обсягу персональних даних без шкоди для роботи установи. Зв'язок між таблицями встановлюється за принципом «ПД+індекс».

Сервер, на якому зберігається спеціальна інформація управління (SRV5), міститиме такі дані:

- номер ІПН;
- серія та номер СНІЛ;
- відомості із трудової книжки;

Та й інші відомості, необхідних трудової діяльності, які стосуються особливої категорії персональних даних.

Усі номери також взяті із довідників SRV2. Зв'язок між таблицями встановлюється за принципом «ПДН + ІПН».

База даних бухгалтерії та відділу кадрів включає весь набір інформації про співробітників, так як використовується програмне забезпечення з певною внутрішньою структурою, наприклад, «1С Підприємство».

Окремо знеособлені бази на SRV2, SRV4 і SRV5, що дозволить знизити клас ISPD.

Проектована мережа складається з різноманітного обладнання, що виконує різні функції для забезпечення працездатності та безпеки мережі.

Сервери SRV2, SRV4, SRV5 керуються операційною системою Debian GNU/Linux 5.0. Ця операційна система заснована на ядрі Linux, є стабільною та

гнучкою операційною системою, підтримує велику кількість архітектур та поширюється під ліцензією General Public License (GPL).

Як СУБД використовується MySQL 5.5. MySQL має багато переваг, у тому числі:

- Висока продуктивність.
- Бюджетний
- Простота використання.
- Портативність.
- Підтримка SSL. SSL – це криптографічний протокол, який забезпечує безпечне з'єднання між клієнтом та сервером. Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером за протоколом TCP/IP, а шифрування використовується асиметричний алгоритм відкритого ключа. У шифруванні з відкритим ключем використовуються два ключі, кожен із яких можна використовувати для шифрування повідомлення. Таким чином, якщо для шифрування використовується один ключ, то для дешифрування повинен використовуватися інший ключ. У такій ситуації можна отримати захищені повідомлення, публікуючи відкритий ключ і зберігаючи секретний ключ у секреті.

Протокол SSL складається з двох підпротоколів:

-SSL запис та протокол рукостискання. Протокол запису SSL визначає формат, який використовується для передачі даних. Протокол SSL включає рукостискання з використанням протоколу запису SSL для обміну серією повідомлень між сервером та клієнтом під час першого з'єднання. SSL вимагає, щоб сервер мав SSL-сертифікат, що надає канал з трьома основними властивостями:

1) Аутентифікація. Сервер завжди аутентифікується, а клієнт аутентифікується залежно від алгоритму.

2) Цілісність. Обмін повідомленнями включає перевірку цілісності.

3) Конфіденційність каналу.

Найбільш поширеним та найкращим рішенням для захисту трафіку від перехоплення є шифрування з'єднання за допомогою SSL. Кросплатформовий продукт OpenSSL інтегрується в багато критично важливих програм, таких як СУБД MySQL, веб-сервер Apache. Для забезпечення сумісності з російським законодавством (за замовчуванням OpenSSL реалізує лише зарубіжні алгоритми шифрування DES/3DES, RC4, Blowfish, IDEA, AES, MD5, SHA/SHA-1, RSA, DSA та інші) необхідно включити підтримку вітчизняних стандартів шифрування. У OpenSSL версії 1.0.0 використання російських алгоритмів вимагає модифікації бібліотек OpenSSL.

Адміністратор безпеки володіє інформацією про те, хто намагається отримати доступ до системи та намагається в даний момент, а також може визначити, чи переплутав співробітник ім'я реального сервера і випадково потрапив у пастку чи діяв навмисно і в мережі дійсно є порушники, намагаючись знайти сервери чи служби, які працюють з даними, що становлять цінність для компанії.

Основними перевагами метода є:

– імітація реальних систем зберігання даних;

– Виявлення та реєстрація фактів ВД до даних, що імітуються системою;

– оповіщення заінтересованих осіб про спроби несанкціонованого доступу до цих даних;

– можливість відновлення зміненої зловмисником системи у вихідний стан;

– Формування звітів про роботу системи за певні періоди часу;

– централізоване керування кількома пастками (датчиками);

– авторизація та контроль доступу до управління системою;

– механізм контролю за працездатністю (діагностика);

– гнучке настроювання правил реагування на спроби UA;
– генерація даних моделювання, що виглядають як реальні;
– періодична зміна IP-адрес пасток (сенсорів).

Для підвищення надійності захисту необхідно контролювати всю мережеву архітектуру, розміщуючи зонди (комп'ютери з NIDS) у кожному сегменті мережі. Ці комп'ютери не обов'язково мають бути серверами; NIDS можна встановити на звичайну робочу станцію.

3.4 Висновки до третього розділу

Для нейтралізації та зниження ймовірності прояву тих чи інших загроз на всіх стадіях життєвого циклу інформаційної системи необхідно використовувати комплекс заходів та засобів захисту:

– організаційних та організаційно-технічних;
– інженерних та інженерно-технічних;
– технічних;
– програмних, апаратних та програмно-апаратних.

Система захисту персональних даних має складатися з наступних підсистем:

– підсистема захисту від несанкціонованого доступу;
– підсистема антивірусного захисту;
– підсистема міжмережевого екранування;
– підсистема криптографічного захисту;
– підсистема виявлення вторгнень;
– підсистема аналізу захищеності.

ВИСНОВКИ

Основною метою є розробка системи захисту персональних даних учнів навчального закладу під час якої необхідно в процесі проектування та розробки виявити будь-які вразливості або загрози, що можуть поставити під загрозу безпеку або цілісність персональних даних.

З огляду на це проведено дослідження та проектування автоматизованої системи тестування захисту персональних даних учнів навчального закладу. Встановлено, що тестування використовується веб-розробниками та адміністраторами безпеки для тестування та вимірювання рівня безпеки веб-додатка з використанням ручних та автоматизованих методів тестування безпеки.

В ході написання роботи встановлено, що існуючі системи автоматизованого тестування не є в достатній мірі ефективними та функціональними щодо виявлення сучасних загроз та вразливостей.

В результаті написання роботи були виконані наступні задачі:

1. Виконано огляд літератури з теми дослідження. Досліджено проблеми захисту персональних даних учнів навчального закладу та визначено актуальність автоматизованого тестування;

2. Здійснено огляд засобів захисту персональних даних та розглянуто системи автоматизованого тестування;

3. Виконано розробку та дослідження системи захисту персональних даних учнів навчального закладу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безопасность веб-приложений: от уязвимостей до мониторинга [Електронний ресурс]: Режим доступу: https://habr.com/en/company/pentestit/blog/526878/ (дата звернення: 01.11.2021).

2. О.Бондаренко, І.Ушкалено. Безпека web-додатків: Актуальні проблеми та їх аналіз. Формування ринкової економіки в Україні. 2017. Вип. 38. С. 28-36.

3. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.

4. The Web Application Security Consortium [Електронний ресурс]: Режим доступу: https://www. academia. Edu /11623665/ Web_ Application_ Security_ Consortium_ Threat_ Classification_WASC-TC_and_ISECOM_ Open_ Source_ Security_ Testing_ Methodology_Manual_OSSTMM_ (дата звернення: 07.11.2021).

5. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.

6. 2021 CWE Top 25 Most Dangerous Software Weaknesses [Електронний ресурс]: Режим доступу: http://cwe.mitre.org/ top25/archive/2021/2021_cwe_top25.html (дата звернення: 11.11.2021).

7. OWASP Top 10:2021 [Електронний ресурс]: Режим доступу: https://owasp.org/Top10/ (дата звернення: 15.11.2021).

8. OWASP Top 10:2021 List [Електронний ресурс]: Режим доступу: https://owasp.org/Top10/0x00-notice/ (дата звернення: 20.11.2021).

9. OWASP Top 10: 10 самых опасных уязвимостей [Електронний ресурс]: Режим доступу: https://cisoclub.ru/owasp-top-10-10-samyh-opasnyh-uyazvimostej/ (дата звернення: 22.11.2021).

10. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.

11. Бенкен, Елена AJAX. Программирование для Интернета (+ CD-ROM) / Елена Бенкен , Геннадий Самков. - М.: БХВ-Петербург, 2017. - 464 с.

12. Будилов, В. Основы программирования для Интернета. Самоучитель / В. Будилов. - М.: БХВ-Петербург, 2016. - 634 с.

13. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.

14. ДСанПІН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. Затверджено Постановою Головного державного санітарного лікаря України 10 грудня 1998 р. №7.

15. ДСН 3.3.6.037-99. Державні санітарні норми. Шум. Загальні вимоги безпеки. – К.: Затверджено Постановою Головного державного санітарного лікаря України 1 грудня 1999 р. №37.

16. ДБН В.2.5.-28-2006. Державні будівельні норми. Природне і штучне освітлення. – К.: Інститут "Київпромелектропроект". Наказ від 30.12.2011 № 438.

17. Правила улаштування електроустановок. – Видання офіційне. Міненерговугілля України. – Х.: Видавництво «Форт», 2017. – 760 с.

18. ДБН В.2.5-67:2013 Опалення, вентиляція та кондиціонування. Наказ 25.01.2013 № 24.

19. ДБН В.1.1.7-2016. Захист від пожежі. Пожежна безпека об'єктів будівництва. Наказ від 31.10.2016 № 287.

20. ДСТУ EN 62305-1:2012 Захист від блискавки. Частина 1. Загальні принципи (EN 62305-1:2011, IDT). Наказ від 28.05.2012 № 640 Про прийняття міжнародних та європейських нормативних документів як національних нормативних документів методом підтвердження».

21. Наказ від 16.06.2014 № 398 «Порядок надання домедичної допомоги постраждалим при ураженні електричним струмом та блискавкою».

Додаток А

Зауваження нормоконтролера

Таблиця А.1 – Зауваження нормоконтролера

Сторінка	Позначення	Зміст зауваження
Вступ, ПЗ		Невірні переліки вдовж всієї ПЗ
Зміст		Прописні літери для назв розділі, відсутність назви додатку Б
ПЗ		Більшість рисунків не виділено порожнім рядком зверху, не розташовано по центру
ПЗ		Нещільне заповнення сторінок ПЗ
		Продовження таблиці 2.1
Розділ 3		Змінні у формулах та в тексті різні, нумерація формул невірна

Додаток Б

ДВНЗ «ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

Факультет комп'ютерних наук і технологій

Кафедра прикладної математики і інформатики

Випускна кваліфікаційна робота
бакалавра

на тему

«Комплексний захист конфіденційної інформації в учбовому закладі»
зі спецчастиною
«Розробка системи захисту персональних даних учнів закладу»

Виконав: студент 4 курсу, групи КІБ-18

напряму підготовки (спеціальності) 125 «Кібербезпека»

•

Студент: Огоновський Євгеній Володимирович

Керівник **д.т.н., проф. Башков Є.О.**

АКТУАЛЬНІСТЬ ТЕМИ ДОСЛІДЖЕННЯ

Актуальність теми. У бакалаврській роботі розроблена система захисту персональних даних учнів навчального закладу

Проведено аналіз теоретичних основ забезпечення інформаційної безпеки в навчальних закладах. Виконано аналіз основних механізмів захисту інформації від несанкціонованого доступу та проблем, що виникають при цьому в навчальних закладах. Розроблено пропозиції з питань забезпечення інформаційної безпеки в навчальних закладах.

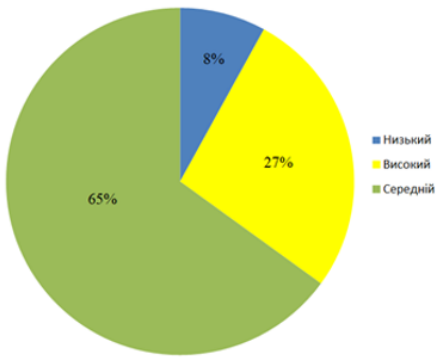
Наукова новизна отриманих результатів полягає у тому, що вдосконалено існуючі системи автоматизованого тестування безпеки навчальних закладів з застосуванням модуля прогнозування.

Метою роботи є показати шляхи подолання труднощів та запропонувати розробку щодо інформаційної безпеки загальноосвітнього навчального закладу.

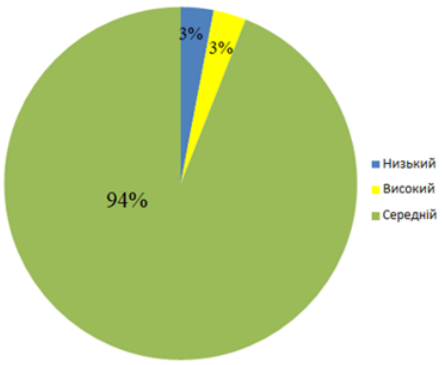
2

Аналіз статистики атак на навчальні заклади

Розподіл вразливостей за рівнем ризику



Розподіл систем за максимальним рівнем ризику виявлених вразливостей

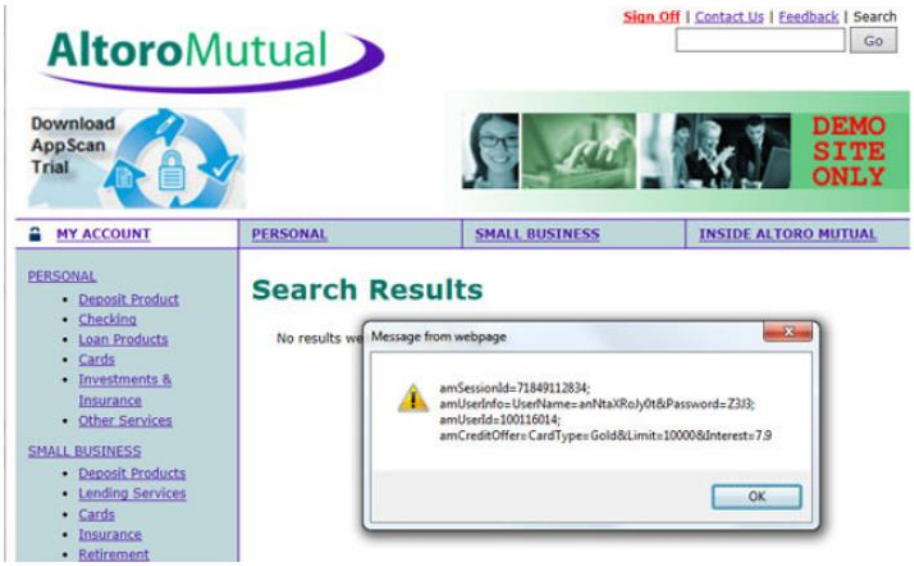


3

Типовий інтерфейс тестової веб-програми

4

Приклад роботи тестового скрипту



5

Приклади організації атак засобами аналізу XML

Request

```
POST http://example.com/xml HTTP/1.1

<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar "World">
]>
<foo>
  Hello &bar;
</foo>
```

Response

```
HTTP/1.0 200 OK

Hello World
```

Request

```
POST http://example.com/xml HTTP/1.1

<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar "World ">
  <!ENTITY t1 "&bar;&bar;">
  <!ENTITY t2 "&t1;&t1;&t1;&t1;">
  <!ENTITY t3 "&t2;&t2;&t2;&t2;&t2;">
]>
<foo>
  Hello &t3;
</foo>
```

Response

```
HTTP/1.0 200 OK

Hello World World World World World World Wor
ld World World World World World World
World World World World World World Wor
ld World World World World World World
World World World World World World Wor
ld World World World
```

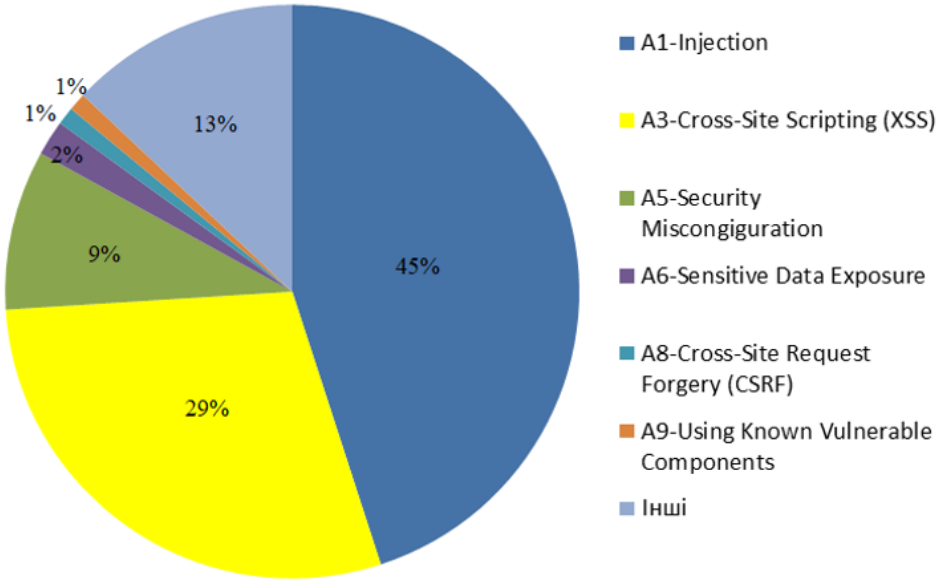
Request

```
POST http://example.com/xml HTTP/1.1

<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar SYSTEM
  "file:///etc/lsb-release">
]>
<foo>
  &bar;
</foo>
```

Response

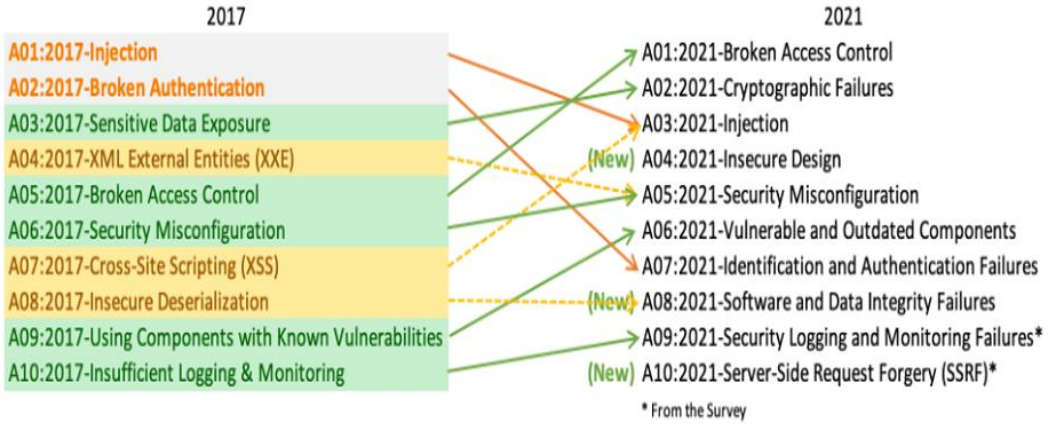
```
HTTP/1.0 200 OK

DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04 LTS"
```

Розподіл виявлених вразливостей відповідно до класифікації OWASP Top 10



7

Зміни в огляді вразливостей веб-сайтів OWASP Top 10



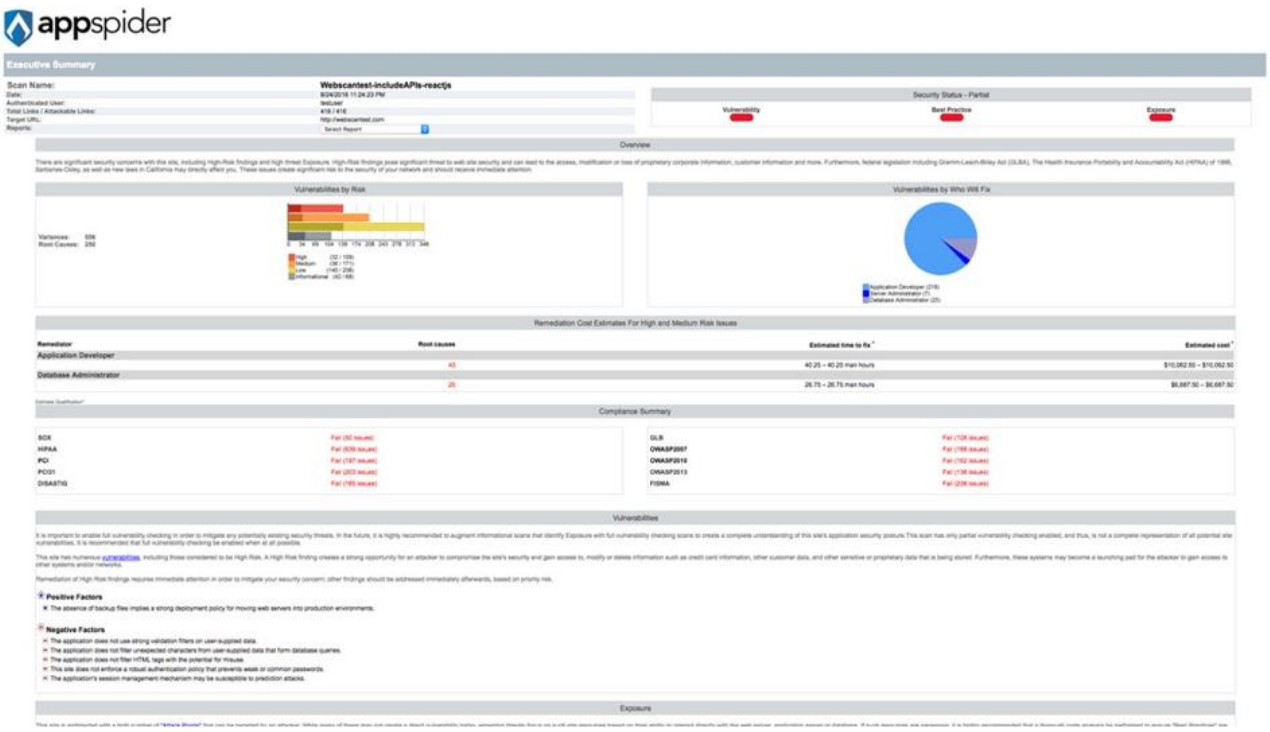
8

Існуючі сканери вразливостей та їх порівняння

Назва	Defect Tracking Integration	IAST Module Hybrid Analysis	SAST Module Hybrid Analysis	Flash Scanner	CGI Scanner	Enterprise Console Management Features	Demo
Rapid appspider	+	-	-	+	-	+/-	+
Portswigger Burp Suite	+/-	+	-	+	+	+/-	+
Fortify WebInspect	+	+	+	+	+	+	+
IBM Security AppScan	+	+	+	+	+	+	+
Accunetix Vulnerability Scanner	+	+	-	-	+	+	+
Netsparker Web Application Security Scanner	+	-	-	-	+	+	+
Janusec WebCruiser	-	-	-	-	+	-	+

9

Інтерфейс сканера Rapid appspider



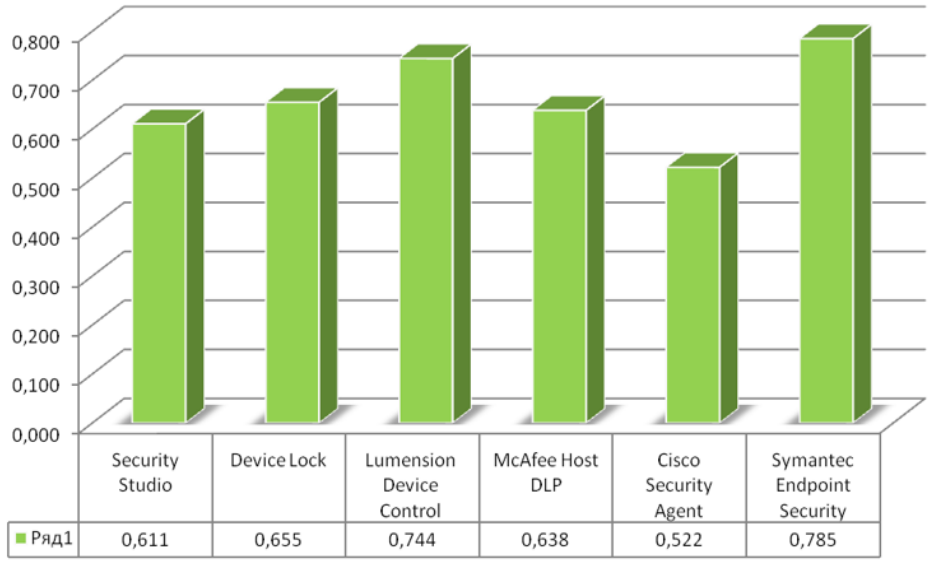
10

Аналізовані засоби управління знімними носіями

Назва засоби захисту інформації	Сертифікат	Інші	Примітка
Security Studio (Информзахист).	1	0	4 НДВ 4, 5 СВТ.
Device Lock (Смарт Лайн Инк).	1	0	4 НДВ, 3Б.
Lumension Device Control (Lumension).	0	0	
McAfee Device Control (McAfee).	0	0	
Cisco Security Agent (Cisco Systems).	1	1	ТУ, EAL2.
Symantec Endpoint Protection 11.0 (Symantec Corporation).	1	1	ТУ, 4 НВД.

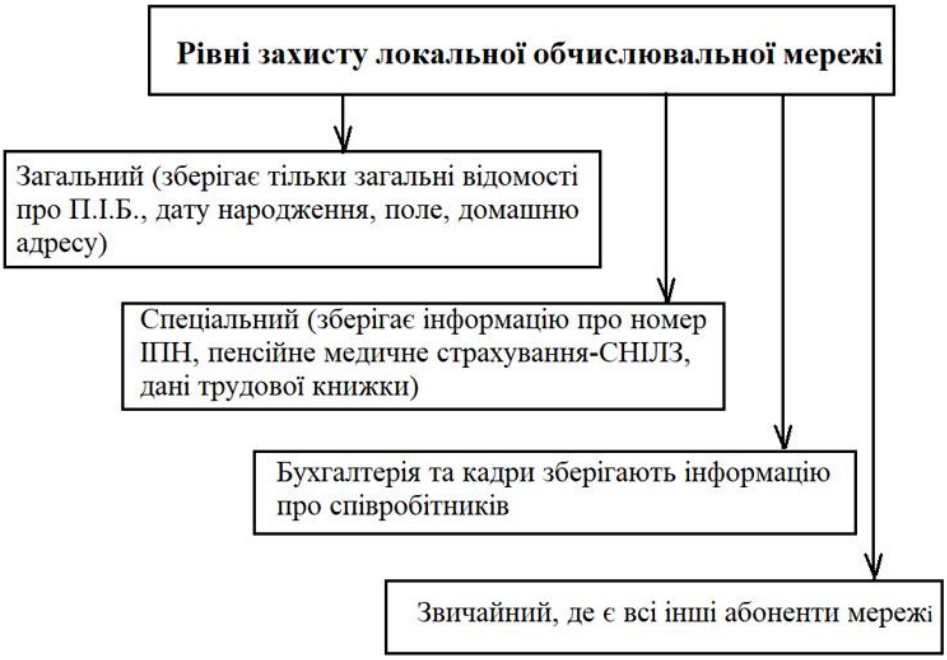
11

Графік рейтингів засобів управління знімними носіями



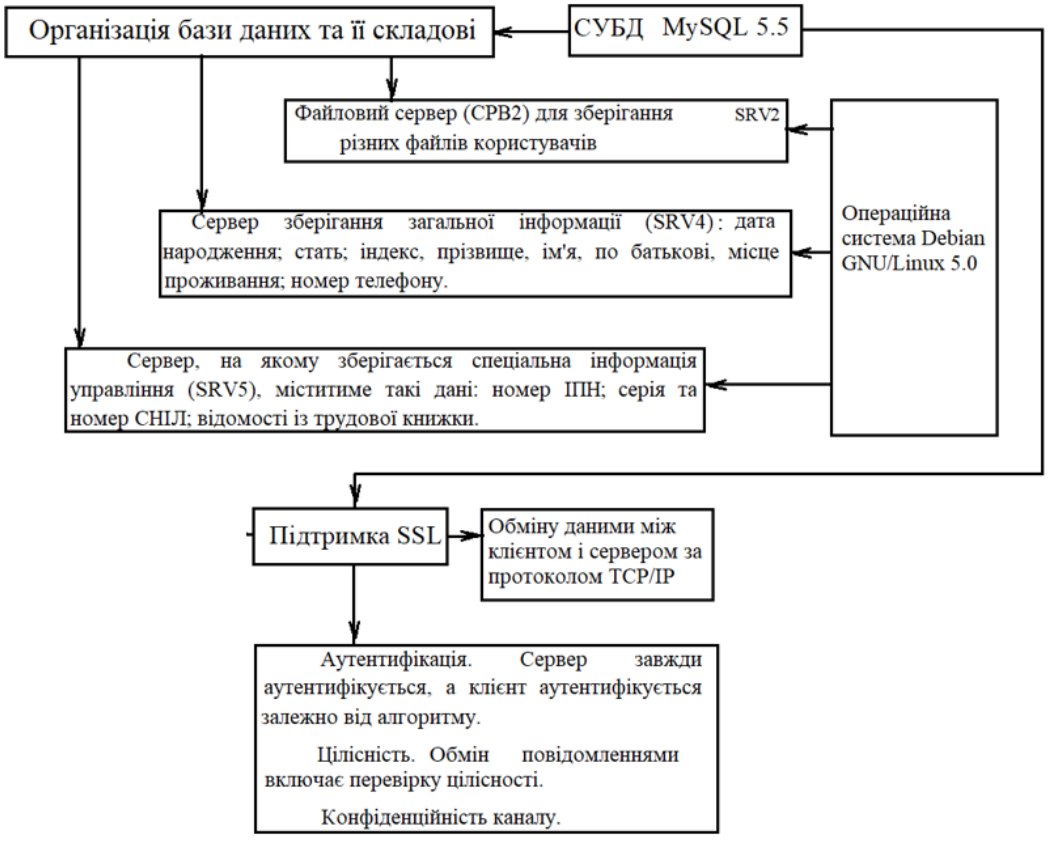
12

Аналіз рівнів захисту системи технічної безпеки даних учнів



13

Розробка та впровадження системи технічної безпеки даних учнів



14

ВИСНОВКИ

Основною метою є розробка системи захисту персональних даних учнів навчального закладу під час якої необхідно в процесі проектування та розробки виявити будь-які вразливості або загрози, що можуть поставити під загрозу безпеку або цілісність персональних даних.

З огляду на це проведено дослідження та проектування автоматизованої системи тестування захисту персональних даних учнів навчального закладу. Встановлено, що тестування використовується веб-розробниками та адміністраторами безпеки для тестування та вимірювання рівня безпеки веб-додатка з використанням ручних та автоматизованих методів тестування безпеки.

В ході написання роботи встановлено, що існуючі системи автоматизованого тестування не є в достатній мірі ефективними та функціональними щодо виявлення сучасних загроз та вразливостей.

В результаті написання роботи були виконані наступні задачі:

1. Виконано огляд літератури з теми дослідження. Досліджено проблеми захисту персональних даних учнів навчального закладу та визначено актуальність автоматизованого тестування;

2. Здійснено огляд засобів захисту персональних даних та розглянуто системи автоматизованого тестування;

3. Виконано розробку та дослідження системи захисту персональних даних учнів навчального закладу.

15

Дякую за увагу

16