Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Технічна оцінка захищеності веб-сайту фітнес-клубу "Каруна"

Виконав(ла): студент(ка) 4 курсу, групи СБ-41
спеціальності 125 кібербезпека
(шифр і назва спеціальності)

(підпис) Береза І.В. (прізвище та ініціали)

Керівник (підпис) Александер Марек Б. (прізвище та ініціали)

Нормоконтроль (підпис) (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна О.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«___» _____ 2023 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Березі Івану Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Технічна оцінка захищеності веб-сайту фітнес-клубу "Каруна"

Керівник роботи д.т.н., професор Александер Марек Б.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «3» 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець М.У., д.т.н., професор каф. МТ		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи		

Студент _____ Береза І.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Александер Марек Б.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Технічна оцінка захищеності веб-сайту фітнес-клубу "Каруна"// Кваліфікаційна робота ОР «Бакалавр» // Береза Іван Віталійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // с. 49, рис. – 6, табл. – 1, бібліогр. – 13.

Метою даної роботи виявити та оцінити потенційні вразливості безпеки веб-сайту "Каруна" , який використовується для інформаційно-бронювальних послуг, розробити рекомендації щодо усунення, уникнення чи пом'якшення знайдених вразливостей.

Об'єкт дослідження – веб-сайт фітнес-клубу "Каруна"

Ключові слова: технічна оцінка, вразливості, аналіз безпеки, веб-сайт Karuna.

Предмет дослідження – потенційні вразливості безпеки, існуючі на веб-сайті фітнес-клубу "Каруна"

В кваліфікаційній роботі проведено аналіз об'єкта оцінювання, побудовано структуру системи захисту, проведено діагностику безпеки веб-сайту, яка передбачає створення вимог безпеки, вибір необхідних інструментів для сканування та налаштування конфігурації, проведено проактивні заходи для забезпечення безпеки, а також створено план та рекомендації щодо майбутнього оцінювання захищеності.

Результатом роботи є виявлення та оцінення вразливостей безпеки веб-сайту "Каруна", та розроблено рекомендації для усунення знайдених вразливостей .

Для отримання успіху в даній роботі було використано такі програмні продукти: OWASP ZAP.

ANNOTATION

Technical security assessment of the fitness club “Karuna” website// Qualification work for a Bachelor's degree // Bereza Ivan Vitaliyovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer and Information Systems and Software Engineering, Department of Cybersecurity, SB-41 group // Ternopil, 2023 // p. 49, fig. - 6, tab. - 1, bibl. - 13.

The purpose of this study is to identify and assess potential security vulnerabilities of the "Karuna" fitness club website, which is used for informational and booking services, and to develop recommendations for addressing, avoiding, or mitigating the identified vulnerabilities.

The research object is the website of the "Karuna" fitness club.

Keywords technical assessment, vulnerabilities, security analysis, Karuna website.

The research subject is the potential security vulnerabilities existing on the website of the "Karuna" fitness club.

The qualification work includes an analysis of the evaluation object, the construction of a security system structure, a diagnosis of the website's security, which involves establishing security requirements, selecting necessary scanning tools and configuring them, proactive measures for ensuring security, as well as creating a plan and recommendations for future security assessments.

The result of this work is the identification and assessment of security vulnerabilities on the "Karuna" website, and the development of recommendations for addressing the identified vulnerabilities.

To achieve success in this study, the following software products were used: OWASP ZAP.

ЗМІСТ

ВСТУП

Актуальність безпеки у веб-сайтах в сучасному світі є надзвичайно важливою темою, яка заслуговує нашої уваги. Веб-сайти забезпечують такий спектр функцій: обмін інформацією, здійснення транзакцій, спілкування та представлення бізнесу.

Однак, із прогресом технологій і зростанням кіберзагрози безпека веб-сайтів стає надзвичайно важливою проблемою. Перш за все, безпека веб-сайтів є важливою для захисту конфіденційної інформації користувачів. Багато веб-сайтів збирають та зберігають особистість користувачів такі як: імена, адреси, електронні пошти та фінансові дані. Ця інформація може бути цінним активом для злочинців, які можуть використовувати її для шахрайства, крадіжки особистості та інших злочинних дій. Тому веб-сайти повинні застосовувати інші заходи безпеки, такі як шифрування даних, захищені протоколи, передачі даних і захист від несанкціонованого доступу щоб гарантувати захист конфіденційності даних користувачів.

Однак, користувачам також необхідно бути обережними та вживати заходи для захисту своєї особистої інформації, наприклад, використовуючи складні паролі, не ділячись особистою інформацією з незнайомцями та завжди перевіряючи достовірність веб-сайтів перед введенням особистих даних. Тому, приділення належної уваги захисту інформації стає стратегічною потребою для організацій, установ та індивідуальних користувачів.

Основні причини актуальності захисту інформації та комп'ютерних систем: зростаюча кількість кібератак, зловмисники постійно розробляють нові методи атак на інформаційні системи. Вони використовують шкідливі програми, фішинг, соціальний інжиніринг та інші техніки для отримання несанкціонованого доступу до даних. Актуальний захист допомагає запобігти та захистити конфіденційну інформацію - збільшення обсягу цифрових даних.

У сучасному світі обсяг цифрової інформації швидко зростає, як бізнес-даних так і особистої інформації користувачів. Забезпечення адекватного захисту

цих даних стає важливим завданням, оскільки, їх втрата або розголошення може призвести до таких наслідків: фінансові втрати, порушення приватності, пошкодження репутації. Законодавство та вимоги до захисту даних: у багатьох країнах існують закони та регуляторні вимоги, що стосуються захисту інформації. Організації повинні відповідати цим вимогам щоб уникнути штрафів, санкцій, правових проблем. Такі вимоги стосуються конфіденційності, цілісності, доступності даних а також резервного копіювання та відновлення. Збільшення використання хмарних технологій та мобільних пристроїв: з хмарними технологіями та мобільними пристроями стає легше зберігати та обмінюватись даними. Проте, це також створює нові виклики у сфері безпеки, такі як: захист інформації на хмарних серверах, забезпечення безпечного доступу до даних з різних пристроїв, захист від загроз які пов'язанні з мобільними пристроями, є важливими завданнями.

Важливість довіри та репутації: захист інформації і комп'ютерних систем має безпосереднє відношення до довіри і репутації. Компанії та організації, які демонструють високий рівень безпеки та добре захищені системи здатні зберегти довіру клієнтів та співробітників. Втрата даних або порушення безпеки може значно підірвати довіру та негативно вплинути на репутацію. Враховуючи ці фактори актуальність захисту інформації та комп'ютерних систем стає невід'ємною частиною успішного функціонування організацій та забезпечення безпеки користувачів.

Ефективний захист даних та захист систем вимагає комплексного підходу, що включає технічні, організаційні, психологічні заходи і також постійне оновлення та підвищення кваліфікації спеціалістів з інформаційної безпеки.

Оцінка веб-сайту є основним процесом для визначення його ефективності, функціональності та безпеки. Оцінка ефективності веб-сайту може бути здійснена за допомогою веб-аналітики яка надає важливі дані про веб-сайт, такі як: кількість відвідувачів, джерело трафіку, сторінки які найбільш популярні, час перебування на сайті.

Функціональність сайту оцінюється через такі критерії: перевірка основних функцій (важливо перевірити, чи працюють основні функції веб-сайту без будь-яких помилок або несправностей).

Оцінка безпеки веб-сайту включає проведення різних заходів для виявлення потенційних загроз і вразливостей. Основні кроки, які можна виконати для оцінки безпеки веб-сайту: проаналізувати архітектуру (включаючи сервера), бази даних, перевірити чи належним чином налаштовані ці компоненти з точки зору безпеки. Також використовуючи різні інструменти для перевірки сайту на вразливості можна запобігти їх шкоді та для ідентифікації можливих слабких місць. Важливо переконатися, що веб-сайт має останні оновлення для всіх використовуваних програмних засобів і платформ.

Останнім і не менш важливим кроком є проведення повного аудита безпеки, щоб перевірити дотримання найкращих практик безпеки, таких як: використання сильних паролів, налаштування прав доступу, шифрування даних. Всі ці теоретичні аспекти оцінювання веб-сайту спрямовані на забезпечення високого рівня захисту інформації, конфіденційності та недоступності для несанкціонованих осіб. Результати оцінки дозволять ідентифікувати потенційні проблеми безпеки та вжити відповідних заходів для їхнього вирішення, щоб забезпечити безпечну та надійну роботу веб-сайту фітнес-клубу "Каруна".

РОЗДІЛ 1 АНАЛІЗ ОБ'ЄКТА ОЦІНЮВАННЯ

1.1 Аналіз системи управління веб-сайту фітнес-клубу

Аналіз системи веб-сайту фітнес-клубу "Каруна" показав привабливий дизайн, який відповідає бренду клубу. Чітка структура навігації дозволяє легко знайти необхідну інформацію. Графічні елементи і фотографії використовуються ефективно, підкреслюючи спортивний характер клубу. В асортименті функціональності можна побачити ряд основних функцій, включаючи можливість запису на тренування, перегляду розкладу, онлайн-сплати абонементів, створення особистого профілю та зміну особистих налаштувань. Крім того, можуть бути додаткові функції: підписка на новини, бронювання тренерів або онлайн-тренування.

Користування сайтом можливе з усіх пристроїв включаючи комп'ютери, смартфони, планшети. Він зручно відображається на будь-якому пристрої та забезпечує легкий доступ до функцій та інформації незалежно від розміру екрану. Демонстрація швидкого відкривання сторінок та функціювання без затримок на різних пристроях та розмірах екранів показують високу продуктивність сайту на всіх платформах.

Системи безпеки веб-сайту використовують SSL - шифрування для захисту конфіденційних даних користувачів таких як: особисті дані, платіжна інформація, використання паролів, обмеження доступу та регулярне оновлення системи допомагають запобігти несанкціонованому доступу до сайту. Також перевірка продемонструвала наявність Search Engine Optimization, яка включає ряд технічних, вмістових, зовнішніх факторів вони впливають на ранжування сайту в пошукових системах. Search Engine Optimization – це комплекс заходів, спрямованих на покращення видимості та позицій веб-сайту в результатах пошукових систем, таких як Google, Bing, Yahoo головна мета SEO-оптимізації

полягає в залученні більшої органічної (неоплаченої) аудиторії на сайт шляхом поліпшення ранжування в пошукових системах.

Система управління веб-сайтом є ключовим компонентом для його ефективності, система надає різноманітні функції для редагування, створення та оновлення вмісту веб-сайту без необхідності вміння програмування (див. рисунок 1.1). Це включає можливість додавання та редагування сторінок, завантаження медіафайлів, створення блогів, керування меню. Оснащена зручними інструментами для організації та управління вмістом це надає можливості для налаштування метатегів, URL-структури, мап сайту та інших факторів, які впливають на пошукову видимість веб-сайту. Наявність інструментів для збору даних про відвідуваність, показники конверсії, популярність сторінок показує аналітичну та звітову роботу.

Рисунок 1.1 – CMS системи

1.2 Структура системи захисту фітнес-клубу

Оцінка структури захисту системи веб-сайту є важливим кроком безпеки різного виду сайтів, адже в процесі роботи визначається наскільки захищеною є система і виявлення потенційно слабких місць.

В системі захисту фітнес-клубу використовуються механізми аутентифікації для перевірки ідентичності користувачів перед наданням доступу до ресурсів. Додатково, механізми авторизації забезпечують, що користувачам надається доступ лише до необхідних функцій та даних. У захисті мережі є застосовані механізми для виявлення та блокування не бажаного мережевого трафіку, таких як фаєрволи і системи виявлення вторгнень (IDS), приватна мережа (VPN) дозволяє забезпечити безпечне з'єднання між різними вузлами мережі фітнес-клубу. Забезпечення конфіденційності даних має в собі такі методи, як шифрування TLS/SSL, це забезпечує безпечний обмін інформацією між клієнтами і сервером, а також захищає дані від перехоплення зловмисниками.

Регулярне створення резервних копій даних та їх збереження на захищених серверах або в хмарному сховищі є важливим елементом структури захисту - це дозволяє відновлювати дані в разі випадкового видалення або пошкодження. Система захисту включає механізми моніторингу, які постійно контролюють активність на веб-сайті фітнес-клубу, це може бути включення аналізу лог-файлів, моніторинг мережевої активності, виявлення незвичайних або підозрілих дій. Такий моніторинг дозволяє оперативно виявляти загрози та вживати заходів для їх запобігання.

Загалом, структура системи захисту фітнес-клубу об'єднує фізичну, логічну та мережеву безпеку, а також управління ризиками, для створення надійного і безпечного середовища для клієнтів та фітнес-клубу в цілому.

1.3 Перегляд політики інформаційної безпеки

Політика інформаційної безпеки - це важливий документ, який визначає, як організація зберігає, обробляє та захищає свої дані. Вона включає положення, що стосуються зберігання, передачі, обробки та знищення даних, а також контроль доступу, використання паролів, фізичну безпеку, шифрування та багато іншого. Під час перегляду політики інформаційної безпеки, перш за все, необхідно оглянути та оновити цілі та цінності організації, що стосуються безпеки інформації. Це включає оцінку ризиків, що становлять загрозу безпеці даних, аналіз інцидентів, звітність про безпеку, а також прослуховування вимог та рекомендацій стосовно інформаційної безпеки. Далі, важливо переглянути і оновити правила та процедури, пов'язані з захистом інформації. Це може включати політику паролів, доступ до систем, захист мережі, контроль доступу, шифрування даних та інші важливі аспекти. Під час перегляду політики варто забезпечити відповідність її з міжнародними стандартами та нормативними вимогами з безпеки інформації. Також необхідно оцінити ефективність існуючих заходів безпеки, здійснюючи аудит та тестування системи безпеки, щоб виявити можливі слабкі місця і вразливості. Це допоможе виявити можливі ризики та знайти шляхи для їх усунення.

У результаті перегляду політики інформаційної безпеки, будуть визначені нові заходи та стратегії для підвищення безпеки інформації в організації. Важливо розробити план впровадження оновленої політики, забезпечити відповідне навчання, ознайомлення персоналу з новими правилами та процедурами. Загальною метою перегляду політики інформаційної безпеки є забезпечення захисту даних та інформації організації, запобігання витокам даних, несанкціонованому доступу та іншим загрозам. Правильно розроблена та актуалізована політика інформаційної безпеки є ключовим елементом успішного управління безпекою веб-сайту та інших інформаційних систем.

Загальний огляд: політика безпеки веб-сайту фітнес-клубу "Каруна" створена для забезпечення захисту інформації клієнтів, співробітників та самого

клубу. Її ціль - забезпечити конфіденційність, цілісність та доступність даних на веб-сайті. Адміністрація відповідає за забезпечення безпеки веб-сайту. Вона приділяє особливу увагу захисту персональних даних клієнтів та виконанню вимог законодавства щодо конфіденційності.

Веб-сайт має систему аутентифікації та авторизації, щоб контролювати доступ до різних функцій та даних. Доступ до конфіденційної інформації, такої як: особисті дані клієнтів, фінансові відомості, обмежується лише авторизованим співробітникам клубу, які мають необхідні права доступу.

Фітнес-клуб "Каруна" вживає заходів для захисту даних на веб-сайті. Це включає використання шифрування SSL для захищеної передачі інформації, регулярне резервне копіювання даних для запобігання втраті, встановлення брандмауерів та інших захисних заходів для запобігання несанкціонованому доступу та використанню даних.

Контроль вразливостей проводить аудит безпеки веб-сайту та регулярно оновлює програмне забезпечення для виправлення вразливостей. Вони також виконують сканування на виявлення можливих вразливостей та вчасно вживають заходів для їх усунення. Навчання забезпечує співробітників з питань безпеки даних та свідомого використання веб-сайту. Це включає навчання щодо сильних паролів, фішингу та інших загроз, а також нагадування про важливість зберігання конфіденційної інформації та дотримання політики безпеки.

РОЗДІЛ 2 ДІАГНОСТИКА БЕЗПЕКИ ВЕБ-САЙТУ ФІТНЕС-КЛУБУ "КАРУНА"

2.1Створення вимог інформаційної безпеки для веб-сайту

Створення вимог інформаційної безпеки для веб-сайту є важливим етапом у забезпеченні захисту даних та запобіганні можливим кібератакам. Ось кілька ключових вимог, які можна включити до політики інформаційної безпеки для веб-сайту: аутентифікація та авторизація є важливими аспектами, які необхідно врахувати. Вони забезпечують контроль доступу до веб-сайту та його ресурсів, гарантуючи, що лише правомірні користувачі мають доступ до конфіденційної інформації та функціональності сайту.

Аутентифікація - визначає процес ідентифікації користувача та перевірки його правильності. У веб-сайтах це може означати введення логіна та пароля, використання біометричних даних або інших методів ідентифікації. Вимоги щодо аутентифікації повинні бути настільки сильними, щоб ускладнити несанкціонований доступ до системи. Це може включати вимогу використовувати складні паролі, встановлення обмежень на кількість невдалих спроб входу та використання механізмів двофакторної аутентифікації.

Авторизація - з іншого боку, визначає, які дії та ресурси можуть бути доступні користувачеві після успішної аутентифікації. Це означає встановлення прав доступу для окремих користувачів або груп користувачів. Вимоги щодо авторизації мають визначати, які функції та області сайту можуть бути доступні для кожного користувача, залежно від його ролі та повноважень. Наприклад, адміністратор має мати широкі повноваження для керування сайтом: установки та налаштування, керування користувачами, завантаження контенту, тоді як звичайному користувачеві можуть бути доступні лише обмежені функції: перегляд контенту, реєстрація та авторизація, взаємодія зі сторінкою, пошук певної, потрібної інформації з даного сайту.

Важливо також забезпечити, щоб механізми аутентифікації та авторизації були надійними та захищеними від атак. Це може включати шифрування передачі даних, використання безпечних протоколів комунікації та забезпечення захисту від перехоплення інформації. Для веб-сайту важливим аспектом є захист від недоліків безпеки.

Вразливості можуть використовуватись зловмисниками для отримання несанкціонованого доступу до сайту, виконання шкідливого коду або викрадення конфіденційної інформації. Один з перших кроків у захисті від вразливостей - це оновлення всіх програмних компонентів, використовуваних на веб-сайті. Це включає операційну систему, веб-сервер, базу даних, фреймворки та інші сторонні бібліотеки. Регулярні оновлення допомагають усувати виявлені вразливості та запобігати можливим атакам. Також важливо встановити механізми захисту від вразливостей - фільтрація введення користувача (input validation), що дозволяє перевірити та блокувати небезпечний або некоректний ввід даних. Це допомагає запобігти атакам, таким як введення SQL-запитів або скриптів у веб-форми.

Додатковим заходом захисту є використання механізмів шифрування для захисту передачі конфіденційної інформації, такої як логіни, паролі та інші чутливі дані. Це допомагає уникнути можливості перехоплення інформації зловмисниками під час її передачі по мережі.

Крім того, важливо проводити регулярні аудити безпеки, щоб виявляти потенційні вразливості, слабкі місця та неправильні налаштування, які можуть бути використані для атаки. Аудити допомагають своєчасно виявляти проблеми та вживати відповідних заходів для їх усунення.

Вразливості можуть використовуватись зловмисниками для отримання несанкціонованого доступу до сайту, виконання шкідливого коду або викрадення конфіденційної інформації. Один з перших кроків у захисті від вразливостей - це оновлення всіх програмних компонентів, використовуваних на веб-сайті. Це включає операційну систему, веб-сервер, базу даних, фреймворки та інші сторонні бібліотеки. Регулярні оновлення допомагають усувати виявлені

вразливості та запобігати можливим атакам. Також, важливо встановити механізми захисту від потенційних проблем, такі як фільтрація введення користувача (input validation), що дозволяє перевірити та блокувати небезпечний або некоректний ввід даних. Це допомагає запобігти атакам, таким як введення SQL-запитів або скриптів у веб-форми.

Додатковим заходом захисту є використання механізмів шифрування для захисту передачі конфіденційної інформації: логіни, паролі та інші чутливі дані. Це допомагає уникнути можливості перехоплення інформації зловмисниками під час її передачі по мережі. Крім того, важливо проводити регулярні аудити безпеки, щоб виявляти потенційні вразливості, слабкі місця та неправильні налаштування, які можуть бути використані для атаки. Аудити допомагають своєчасно виявляти проблеми та вживати відповідних заходів для їх усунення.

Захист даних включає заходи, що мають на меті збереження конфіденційності, цілісності та доступності інформації, яка зберігається на веб-сайті. Перш за все, важливо встановити механізми аутентифікації та авторизації. Це означає, що лише користувачі з правом доступу мають змогу переглядати та редагувати дані на веб-сайті. Вимоги до паролів, використання двофакторної аутентифікації та контроль доступу до адміністративних функцій сайту є важливими компонентами захисту даних.

Далі, необхідно забезпечити шифрування даних. Важлива інформація, така як особисті дані користувачів, фінансові відомості або конфіденційні документи, має бути зашифрована під час передачі між клієнтом і сервером. Використання протоколу HTTPS з використанням SSL/TLS забезпечує шифрування даних та захист від перехоплення зловмисниками.

Також, важливо регулярно резервувати дані на веб-сайті. Це допомагає забезпечити можливість відновлення даних в разі випадкового видалення, системних збоїв або кібератак. Резервні копії даних слід зберігати в безпечному місці, віддалено від основного сервера, і регулярно перевіряти їх цілісність. Крім цього, необхідно використовувати механізми контролю доступу та обмеження прав користувачів. Рівні доступу до різних типів даних мають бути належно

налаштовані, забезпечуючи, що лише необхідна кількість людей має доступ до конфіденційної інформації. Це допомагає знизити ризик витоку даних та несанкціонованого доступу.

Нарешті, варто звернути увагу на постійну моніторинг і оновлення безпекових заходів. Виявлення нових загроз і вразливостей, регулярні патчі та оновлення програмного забезпечення, аудит безпеки та проведення пенетраційних тестів допоможуть підтримувати веб-сайт на високому рівні захищеності. Свідомість користувачів є важливою складовою створення вимог інформаційної безпеки для веб-сайту. Навіть найсильніша технічна захист може бути компрометована, якщо користувачі несвідомо діють і не приділяють належної уваги своїм діям та безпеці інформації.

Одним із аспектів створення вимог щодо свідомості користувачів є надання достатньої освіти та навчання з питань безпеки в інтернеті. Веб-сайт повинен пропонувати чіткі та доступні рекомендації щодо безпечного використання сайту, створення міцних паролів, усвідомлення потенційних ризиків та заходів, що можна прийняти для їх запобігання. Крім того, важливо підтримувати постійну комунікацію з користувачами щодо актуальних загроз та способів їх запобігання. Це може бути здійснене шляхом надання оновлень, новин та порад щодо безпеки через електронну пошту, соціальні мережі або спеціальні розділи на веб-сайті. Загалом, свідомість користувачів є необхідною складовою вимог інформаційної безпеки для веб-сайту. Це передбачає надання освіти та навчання користувачам, забезпечення ефективної комунікації щодо безпеки, встановлення механізмів контролю доступу та аутентифікації та підтримку актуальних політик безпеки. Тільки спільними зусиллями можна забезпечити надійний рівень захисту веб-сайту та зменшити ризик компрометації інформації.

2.2 Вибір сканера вразливостей для проведення повного сканування

Вибір сканера вразливостей є важливим кроком у процесі діагностики безпеки веб-сайту. Сканер вразливостей є інструментом, який автоматично

перевіряє веб-сайт на наявність потенційних проблем і недоліків у системі безпеки. функціональні можливості є одним із ключових критеріїв, які варто враховувати, оскільки метою повного сканування є виявлення різноманітних типів недоліків безпеки, важливо, щоб обраний сканер мав широкий спектр функціональних можливостей.

Виявлення вразливостей у веб-додатках: сканер повинен мати здатність виявляти різні типи потенційних проблем, такі як кросс-сайтовий скриптінг (XSS), SQL-ін'єкції, недостатні перевірки доступу та інші. Він повинен використовувати різні методи, щоб виявити вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до системи. Виявлення слабких місць в мережевих компонентах: Деякі сканери вразливостей також мають здатність сканувати мережеві компоненти, такі як мережеві маршрутизатори, комутатори та файрволи, для виявлення можливих проблем з безпекою. Це дозволяє ідентифікувати потенційні слабкі місця в мережі, які можуть бути використані зловмисниками для злому системи.

Перевірка наявності захисту від відомих уразливих аспектів: сканер повинен мати базу даних з відомими недоліками безпеки та патчами, щоб перевірити, чи встановлені необхідні заходи безпеки на веб-сайті. Це дозволяє виявити вразливості, для яких вже існують відповідні патчі або заходи забезпечення.

Аналіз результатів сканування: сканер повинен надати детальні звіти та аналіз результатів сканування. Це дозволить зрозуміти, які вразливості були виявлені, їх серйозність та рекомендації щодо виправлення. Чим більш детальні та зрозумілі звіти, тим ефективніше буде процес виправлення виявлених проблем.

Користувацький інтерфейс: важливо, щоб сканер мав зручний інтерфейс, який дозволяє зручно керувати процесом сканування, переглядати результати та виконувати необхідні дії. Перевірка сумісності означає, наскільки добре сканер може працювати з різними типами веб-сайтів, платформами та технологіями. Підтримка різних веб-платформ: сканер повинен мати можливість працювати з

різними веб-платформами, такими як WordPress, Drupal, Joomla, Magento та інші популярні CMS. Він повинен розпізнавати структуру сайту та його особливості, щоб ефективно виявляти вразливості, що пов'язані з конкретними платформами.

Підтримка різних технологій: веб-сайти можуть використовувати різні технології, такі як PHP, ASP.NET, Java, JavaScript та інші. Сканер повинен мати можливість виявляти вразливості, що пов'язані з цими технологіями, та адаптуватися до їх особливостей. Розпізнавання API та веб-сервісів: деякі веб-сайти можуть мати відкриті API або веб-сервіси, які використовуються для взаємодії з іншими додатками або системами. Сканер повинен бути здатним розпізнавати та аналізувати ці API та веб-сервіси, щоб виявляти можливі вразливості, пов'язані з ними. Сумісність зі стандартами безпеки: сканер повинен відповідати відповідним стандартам безпеки, таким як OWASP Top 10 або CWE/SANS Top 25, що дозволить ефективно виявляти вразливості, які відповідають цим стандартам.

Сумісність з обмеженнями сайту: веб-сайти можуть мати різні обмеження, такі як часові обмеження, обмеження швидкості запитів або обмеження доступу. Сканер повинен бути здатним працювати в межах цих обмежень, не порушуючи правил сайту та не завдаючи шкоди його функціональності. Враховуючи перевірку сумісності при виборі сканера вразливостей, можна забезпечити його ефективну роботу з різними типами веб-сайтів та технологіями, що дозволить виявляти й виправляти потенційні проблеми безпеки.

Сканер повинен бути надійним і точним в виявленні слабких місць. Він повинен мати актуалізовану базу даних з відомими недоліками безпеки, регулярно оновлюватися та виявляти потенційні проблеми безпеки з високою точністю. Надійний сканер мінімізує помилкові позитиви та негативи, що дозволяє зосередитись на реальних загрозах.

Швидкодія: швидкодія сканера є важливим фактором, особливо при скануванні великих веб-сайтів або веб-сайтів з великою кількістю сторінок. Чим швидше сканер виявляє вразливості, тим швидше можна прийняти відповідні

заходи для їх виправлення. При виборі сканера варто звернути увагу на його продуктивність та швидкість сканування.

Сканування в реальному часі: ідеальним варіантом є сканер, який може працювати в режимі реального часу, перевіряючи веб-сайт на вразливості під час його активної роботи. це дозволяє виявляти нові вразливості та реагувати на них миттєво. Такий підхід забезпечує постійний контроль за безпекою веб-сайту.

Масштабованість: сканер повинен бути здатним працювати з великими проектами та масштабуватись залежно від потреб організації. Він повинен мати можливість працювати з різними типами веб-сайтів, платформами та технологіями. Сканер повинен забезпечувати зрозумілі та лаконічні звіти про виявлені вразливості. Звіти повинні бути організовані і структуровані таким чином, щоб було легко знайти необхідну інформацію і оцінити її важливість. Вони можуть включати деталі про вразливості, рекомендації щодо виправлення, рівень серйозності та інші важливі показники.

Графіки та діаграми: подання результатів сканування у вигляді графіків та діаграм допомагає зрозуміти обсяг та розподіл вразливостей на веб-сайті. Це дозволяє швидко оцінити загальну стан безпеки та виявити основні тенденції та проблемні області.

Персоналізація звітів: сканер повинен надавати можливість персоналізувати звіти та аналітику залежно від потреб користувача. Наявність різних фільтрів, сортування, групування та налаштувань допомагає зосередитись на конкретних аспектах безпеки, які є найбільш важливими для організації. Тривалість сканування: звіти повинні містити інформацію про час, необхідний для проведення повного сканування веб-сайту. Це допомагає оцінити продуктивність та ефективність сканера, а також планувати роботу з недоліків безпеки та їх усунення. Аналітика результатів: повний сканер вразливостей повинен забезпечувати можливість аналізу та інтерпретації результатів сканування. Це може включати призначення пріоритетів для недоліків безпеки, рекомендації щодо виправлення, статистику з попередніх сканувань та іншу інформацію, яка допомагає зрозуміти поточний стан безпеки веб-сайту.

В моєму випадку було обрано сканер OWASP ZAP (Zed Attack Proxy), тому що він є потужним інструментом для виявлення потенційних проблем у веб-додатках. Основні функціональні можливості цього сканера активне сканування веб-додатків шляхом надсилання запитів та аналізування відповідей. Він дозволяє виявити різноманітні вразливості, такі як перекриття авторизації, кросс-сайтовий скриптинг (XSS), SQL-ін'єкції та багато інших. OWASP ZAP також підтримує пасивне сканування, при якому він аналізує вхідний трафік між клієнтом та сервером для виявлення можливих вразливостей. Це дозволяє виявити проблеми, які не вимагають активних взаємодій з додатком, такі як витік конфіденційної інформації через HTTP-заголовки або незахищені кукі. Він вміє перебирати різні сторінки та виконувати сканування на основі встановлених правил та шаблонів. Це дозволяє ефективно виявляти потенційні проблеми без необхідності ручного втручання, надає зручні інструменти для створення звітів та аналізу результатів сканування, можна отримати детальну інформацію про виявлені вразливості, включаючи їх тип, вплив та рекомендовані заходи з усунення. Це дозволяє легко оцінити рівень безпеки веб-сайту та прийняти відповідні заходи для виправлення проблем. Сканер є розширюваною платформою, яка підтримує плагіни та розширення можна використовувати наявні розширення або створити власні, щоб розширити функціональність сканера та налаштувати його під свої потреби.

2.3 Налаштування конфігурації сканера та підготовка до сканування

Налаштування конфігурації сканера та підготовка до сканування є важливим етапом процесу оцінки безпеки веб-сайту. Для забезпечення ефективного та точного сканування, необхідно виконати наступні кроки: встановлення сканера. Перш ніж розпочати сканування, необхідно встановити сканер уразливих аспектів на потрібну платформу або систему. Зазвичай, сканери надаються у вигляді програмного забезпечення, яке можна встановити на локальному комп'ютері або використовувати як онлайн-сервіс.

Налаштування параметрів сканування. Перед початком сканування, необхідно налаштувати параметри сканера вразливостей. Це включає вибір типів недоліків безпек, які потрібно перевірити, глибину сканування, швидкість сканування та інші важливі параметри. Для кращої точності та ефективності, рекомендується вибрати налаштування, які найкраще відповідають особливостям вашого веб-сайту.

Конфігурація автентифікації. Якщо ваш веб-сайт має обмежений доступ або вимагає аутентифікації, необхідно налаштувати сканер таким чином, щоб він мав можливість увійти в систему і сканувати захищені частини веб-сайту. Це може включати встановлення користувача та пароля для автентифікації або використання API-ключів.

Вказівка цільової аудиторії. Перед початком сканування, необхідно вказати цільову аудиторію для сканера. Це означає вказати URL-адресу або діапазон URL-адрес, які мають бути перевірені. Це дозволяє сканеру зосередитися на конкретних сторінках та функціях вашого веб-сайту.

Перевірка сумісності. Переконайтеся, що сканер вразливостей сумісний з технологіями, які використовуються на вашому веб-сайті. Він повинен підтримувати розпізнавання технологій, таких як HTML, бази даних та інші, щоб забезпечити належне сканування та виявлення вразливостей.

Планування та підготовка ресурсів. Перед запуском сканування, варто планувати його відповідно до потреб вашої організації. Забезпечте достатні

ресурси (пам'ять, процесор, мережеві ресурси)для ефективного виконання сканування. Також важливо врахувати час, необхідний для сканування, і призначити його в зручний для вас час, щоб уникнути перебоїв в роботі веб-сайту. Правильна конфігурація сканера та підготовка до сканування гарантують ефективну оцінку безпеки вашого веб-сайту.

Перший етап сканування запускаємо сканер (див. рисунок 2.2).

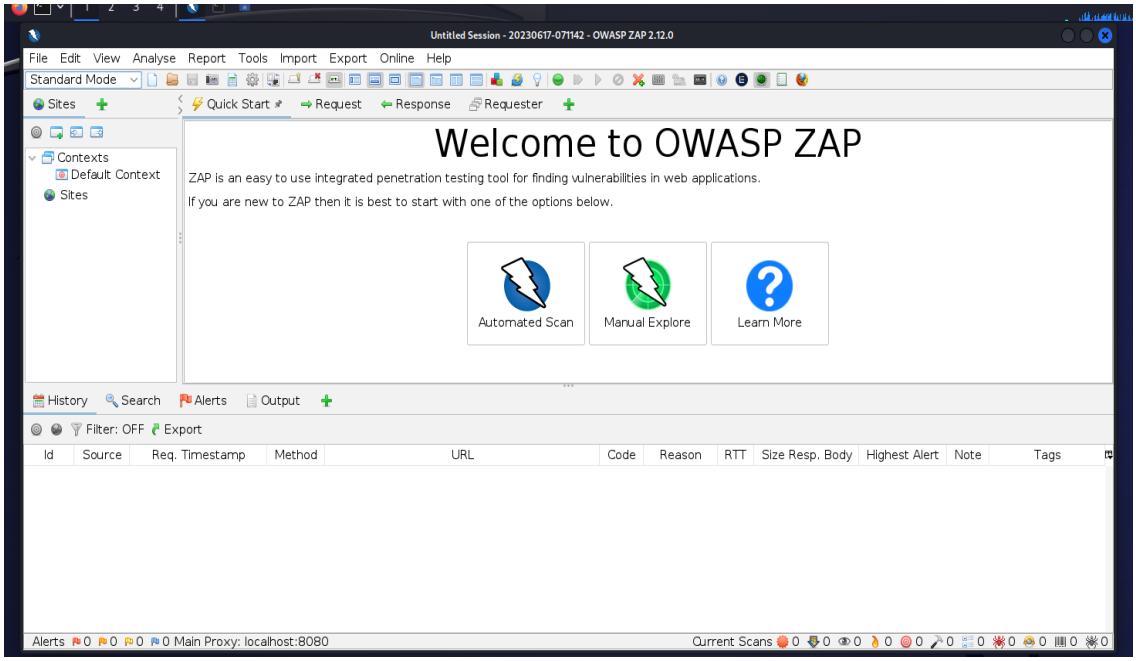

Рисунок 2.2 – активне положення сканера

Розібравшись з панеллю керування переходимо до налаштування, обираємо автоматизоване сканування, (див. Рисунок 2.3).

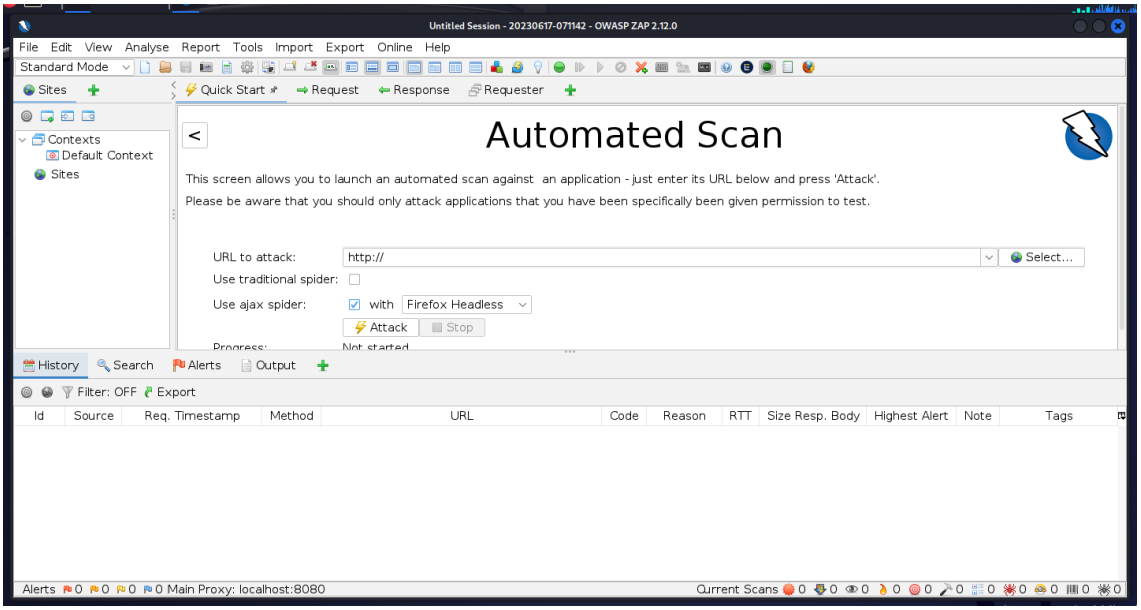

Рисунок 2.3 – панель керування

Далі встановлюємо адресу веб-сайту для сканування,(див. Рисунок 2.4)

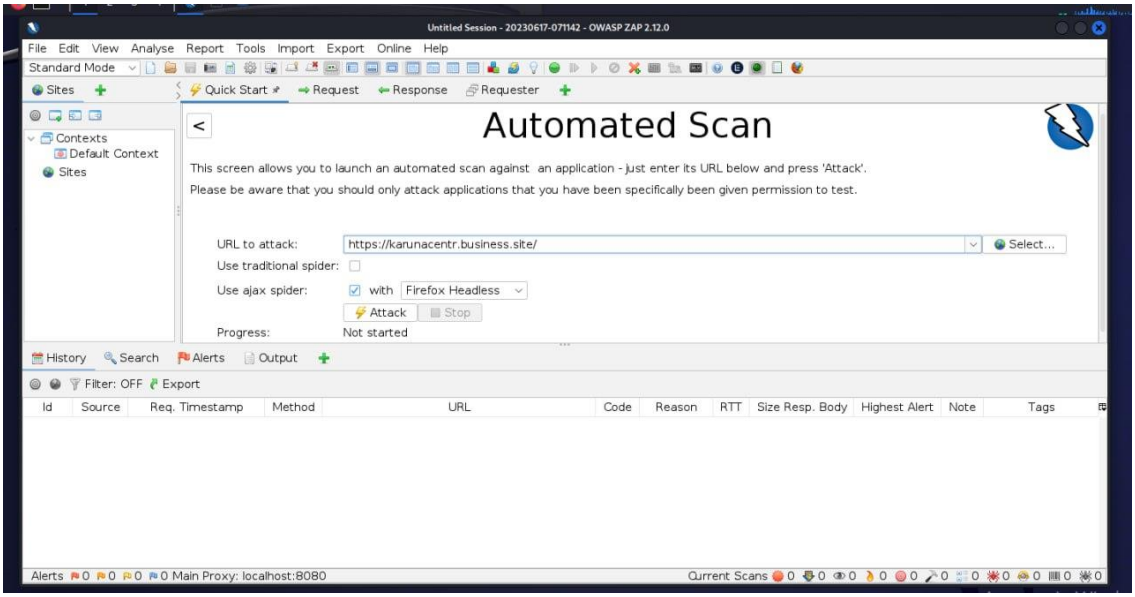

Рисунок 2.4 – налаштування сканера

Натиснувши команду Attack, з’явиться вікно з 4 режимами налаштування, (див. рисунок 2.5), я обрав standart mode, тому що він не є дуже інтенсивним і тому не зможе причинити шкоду сайту.

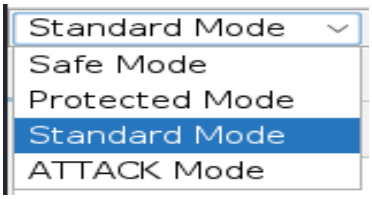

Рисунок 2.5 – вибір атаки

Сканування веб-сайту розпочато! Під час сканування веб-сайту важливо слідкувати за прогресом сканування, щоб переконатися, що він виконується успішно і без перешкод.

РОЗДІЛ 3 ПРОАКТИВНІ ЗАХОДИ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВЕБ-САЙТУ "КАРУНА"

3.1 Оцінка виявлених вразливостей після проведення сканування

Оцінка виявлених загроз допомагає визначити серйозність та потенційний вплив вразливостей на безпеку вашого веб-сайту.

Декілька кроків, які можна виконати для оцінки виявлених вразливостей - класифікація вразливостей є важливим етапом у процесі аналізу та управління безпекою. Дозволяючи групувати вразливості за певними категоріями або класами, вона сприяє більш структурованому підходу до розуміння та реагування на потенційні проблеми. Ось кілька загальних категорій для класифікації вразливостей: - категорія атаки, - розділення вразливостей на основі типу атаки, яку вони можуть викликати. Наприклад, вразливості можуть бути класифіковані як вразливості введення даних, маніпулювання параметрами, перехоплення сесії, впровадження коду або вразливості мережевого протоколу.

Рівень серйозності - розподіл вразливостей за їхньою важливістю або серйозністю. Це може включати категорії, такі як критичні, високоризикові, помірковані або низькоризикові вразливості, залежно від потенційного впливу на безпеку системи.

Компонент або система - класифікація недоліків безпеки за відповідними компонентами або системами, до яких вони належать. Наприклад, ви можете мати вразливості, пов'язані з веб-додатками, базами даних, серверами, мережевими протоколами тощо. Тип вразливості: Розподілення уразливих аспектів на основі їхнього конкретного типу або дефекту. Це може включати вразливості, пов'язані з недостатнім контролем доступу, незахищеними вводами, уразливостями в коді програми, недостатньою шифруванням даних тощо.

Видимість - класифікація вразливостей залежно від їхньої відомості або відомостей, які можуть бути використані для їхнього використання. Вразливості

можуть бути відкриті (відомі публічно), закриті (відомі лише обмеженому колу осіб) або невідомі (поки не виявлені або досліджені).

Ранжування вразливостей - це процес призначення пріоритетів для потенційних проблем, які були виявлені під час сканування або аналізу безпеки. Це дозволяє визначити, які вразливості потребують негайного виправлення або усунення, а які можуть бути відкладені на пізніший час. При ранжуванні вразливостей можна використовувати різні методики та критерії. Деякі з них включають: віддалена доступність, оцінка, наскільки легко атакувач може скористатися вразливістю з-зовні мережі без авторизації або аутентифікації.

Вразливості, які дозволяють виконання віддалених атак, часто мають високий пріоритет. Локальна експлуатація: оцінка, наскільки складно атакувачеві експлуатувати вразливість, якщо він вже має фізичний доступ до системи або мережі. Вразливості, які потребують фізичного доступу або спеціальних привілеїв, можуть мати менший пріоритет. Потенційний вплив: врахування потенційного впливу вразливості на систему або бізнес-процеси. Вразливості, які можуть призвести до серйозних наслідків, таких як витік конфіденційної інформації або відмова в обслуговуванні, часто мають вищий пріоритет. Витрати на виправлення: оцінка складності та витрат на виправлення вразливості. Вразливості, які можуть бути легко виправлені шляхом встановлення патча або змін у конфігурації системи, можуть мати нижчий пріоритет. Документування результатів є важливою частиною процесу сканування вразливостей. Це допомагає зберегти інформацію про виявлені вразливості, їх характеристики, ступінь важливості та рекомендації щодо усунення.

Основні елементи документування результатів сканування вектора атак включають: опис вразливостей. Кожна виявлена вразливість повинна бути описана детально, включаючи її назву, опис, можливі наслідки та шляхи експлуатації. Класифікація порушення безпеки: вразливості можуть бути класифіковані за типом (наприклад, SQL-ін'єкція, переповнення буфера, хробаки тощо) або за рівнем важливості (наприклад, критична, висока, середня, низька).

Вплив і ризик: Документування потенційного впливу слабких місць на систему або бізнес-процеси. Це включає оцінку наслідків, які можуть виникнути при експлуатації потенційних проблем, і ризиків для безпеки системи.

Рекомендації щодо виправлення: надання конкретних рекомендацій щодо усунення недоліків безпеки або зменшення ризиків. Це можуть бути патчі, оновлення програмного забезпечення, налаштування конфігурації або рекомендації щодо змін у політиках безпеки.

Приорітети та терміни: встановлення пріоритетів для усунення уразливих аспектів на основі їх важливості та потенційного ризику. Вказівка рекомендованих термінів для виправлення вразливостей.

Документація процесу: запис всіх етапів проведення сканування потенційних проблем, включаючи дати, використані інструменти, налаштування сканування та іншу важливу інформацію. Документування результатів сканування недоліків безпеки допомагає зберегти інформацію для подальшого аналізу, планування виправлень і моніторингу безпеки. Це також може бути корисним при аудитах безпеки, внутрішніх оглядах та комунікації зі зацікавленими сторонами. Оцінка виявлених потенційних проблем дозволяє вам зробити обґрунтовані рішення щодо подальших кроків, включаючи виправлення проблем з захищеністю, встановлення пріоритетів та планування заходів щодо підвищення безпеки вашого веб-сайту. По завершенню сканування було отримано такі результати, (див. рисунок 3.6).

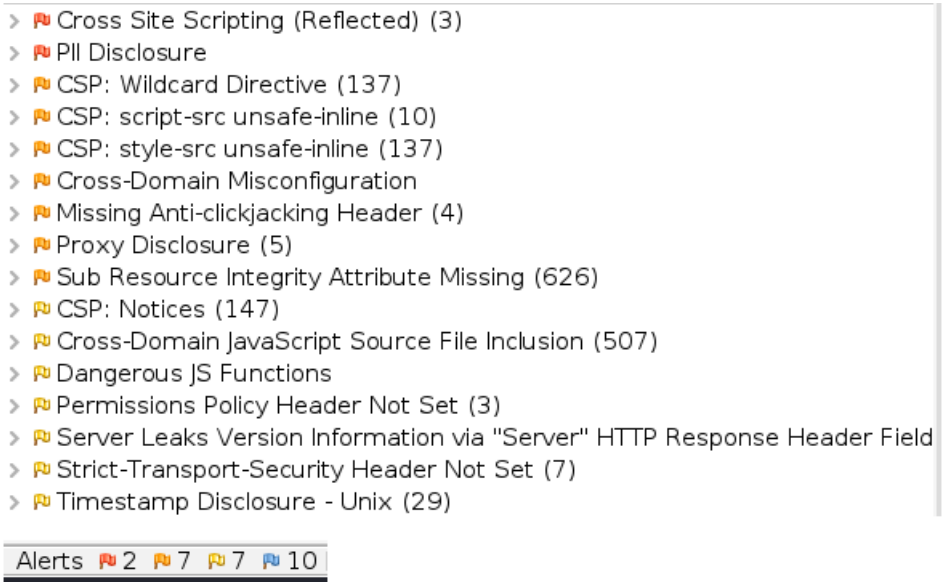

Рисунок 3.6 – результат сканування

Міжсайтовий скриптинг (XSS) - це метод атаки, при якому зловмисник передає свій код у веб-браузер користувача. Це може статися через спеціальне посилання зі шкідливим кодом або через відвідування зловмисної веб-сторінки зі шкідливою веб-формою. Код зазвичай написаний на HTML/JavaScript, але може використовувати інші технології, такі як VBScript, ActiveX, Java, Flash і т. д. Коли зловмисник отримує можливість виконати свій код у браузері користувача, він отримує доступ до чутливих даних, які доступні для браузера. Це може призвести до крадіжки облікових записів, перенаправлення браузера на інші сторінки або відображення шахрайського вмісту. Атаки XSS порушують довіру між користувачем і веб-сайтом. Додатки, які використовують вбудовані браузери, можуть виконувати код з машини користувача і компрометувати систему.

Існують три типи атак XSS: непостійні, постійні та DOM-базовані. Непостійні атаки та DOM-базовані атаки вимагають від користувача переходу за посиланням зі шкідливим кодом або відвідування веб-сторінки зі шкідливою веб-формою. Шкідлива форма може бути автоматично відправлена без відома жертви (наприклад, за допомогою JavaScript). Після натискання на шкідливе посилання або відправки шкідливої форми, XSS-код буде виконаний у браузері користувача. Ще один спосіб відправки запитів (GET і POST) полягає використанні

вбудованого клієнта, такого як Adobe Flash. Постійні атаки відбуваються, коли шкідливий код надсилається на веб-сайт, де він зберігається протягом певного часу.

PII Disclosure (розкриття особисто визначеної інформації) відбувається, коли зловмисник намагається отримати, використовувати або розкрити конфіденційні особисті дані людей без їхнього дозволу або згоди. Це може статися через незахищені механізми зберігання або передачі даних, недостатній рівень безпеки або недбалість з боку організацій, які збирають і обробляють ці дані.

Атака PII Disclosure може мати серйозні наслідки для постраждалих осіб, так як особисті дані можуть бути використані для крадіжки ідентичності, шахрайства, спаму, фішингу та інших злочинних дій. Зловмисники можуть отримати доступ до таких конфіденційних даних, як імена, адреси, номери соціального страхування, банківські реквізити, медична інформація тощо.

Вразливість "CSP: script-src unsafe-inline" відноситься до політики безпеки веб-сайту, встановленої за допомогою Content Security Policy (CSP). CSP використовується для захисту веб-додатків від різних видів атак, включаючи атаки Cross-Site Scripting (XSS). Опція "script-src unsafe-inline" в CSP вказує, що веб-сайт дозволяє виконання скриптів, включаючи вбудований JavaScript, з використанням інлайнових (встроєних) скриптів без додаткової перевірки або санітізації. Це означає, що якщо зловмисник здатен впровадити шкідливий скрипт безпосередньо у веб-сторінку, він буде виконуватись безпосередньо в контексті сторінки, що відкриває двері для можливих атак XSS. Ця вразливість створює потенційний ризик для безпеки веб-сайту і користувачів. Злоумисники можуть використовувати цю вразливість для впровадження шкідливого коду, крадіжки даних, перехоплення сесій або впливу на поведінку веб-сторінки.

"CSP: style-src unsafe-inline" відноситься до політики безпеки веб-сайту, встановленої за допомогою Content Security Policy (CSP). CSP використовується для захисту веб-додатків від різних видів атак, включаючи атаки Cross-Site Scripting (XSS). Опція "style-src unsafe-inline" в CSP вказує, що веб-сайт дозволяє

використання встроєних (інлайнових) стилів без додаткової перевірки або санітізації. Це означає, що якщо зловмисник здатен впровадити шкідливий стиль безпосередньо у веб-сторінку, він буде виконуватись безпосередньо в контексті сторінки, що може створювати потенційні проблеми безпеки. Ця вразливість створює ризик для безпеки веб-сайту і користувачів. Злоумисники можуть використовувати цю вразливість для впровадження шкідливого коду, зміни візуального оформлення сторінки або впливу на її поведінку.

Cross-Domain Misconfiguration (неправильна конфігурація міждоменного доступу) - це вразливість, яка виникає, коли веб-додаток неправильно налаштований для обміну ресурсами між різними доменами. Зазвичай ця вразливість виникає внаслідок недостатньо строгих політик безпеки, які дозволяють небезпечний обмін даними між доменами. Коли веб-додаток дозволяє доступ до своїх ресурсів (наприклад, сценарії, стилі, фрейми) з іншого домену без належних обмежень, це може створити ризик безпеки. Злоумисники можуть скористатись цим, щоб отримати доступ до конфіденційної інформації користувачів або виконати атаку на самого користувача, таку як атака типу Cross-Site Scripting (XSS) або Cross-Site Request Forgery (CSRF).

Missing Anti-clickjacking Header (відсутність захисного заголовка проти clickjacking) - це вразливість, яка виникає, коли веб-сайт не встановлює або не правильно налаштовує заголовок захисту від clickjacking. Clickjacking є атакою, при якій зловмисники намагаються зманіпулювати користувачем, щоб вони ненавмисно виконували небезпечні дії на веб-сайті без їхньої усвідомленості. Заголовок захисту проти clickjacking, відомий також як X-Frame-Options, вказує браузеру, як обробляти вкладені фрейми на сторінці. Встановлення правильного заголовка X-Frame-Options дозволяє обмежити можливість clickjacking атак і захистити користувачів. Відсутність або неправильна конфігурація заголовка X-Frame-Options може призвести до того, що злоумисники зможуть вкладати веб-сторінку в фрейм на своєму зловмисному сайті і отримувати контроль над взаємодією користувача з цією сторінкою. Це може призвести до виконання небажаних дій від імені користувача, таких як виконання фінансових операцій,

розкриття конфіденційної інформації або виконання дій, що можуть завдати шкоди користувачеві.

Proxy Disclosure (розкриття проксі) - це вразливість, яка виникає, коли інформація про проксі-сервери, що використовуються для доступу до веб-сайту, неправильно розкривається або витікає. Проксі-сервери використовуються для проміжного з'єднання між клієнтом і сервером, і вони можуть впливати на приватність і безпеку комунікації. Якщо інформація про проксі-сервери неправильно налаштована або некоректно відображається, це може призвести до розкриття конфіденційних даних або допуску несанкціонованого доступу до системи. Наприклад, зловмисник може отримати доступ до внутрішньої мережі або серверів за допомогою неправильно налаштованого проксі-сервера.

Sub Resource Integrity Attribute Missing (відсутність атрибуту цілісності підресурсу) - це вразливість, яка виникає, коли на веб-сайті відсутні атрибути цілісності (integrity attributes) для підресурсів, таких як зовнішні сценарії (scripts), стилі (stylesheets) або інші ресурси, що завантажуються з інших джерел. Атрибути цілісності, які використовуються у веб-розробці, дозволяють перевіряти, чи були ресурси не змінені під час їх завантаження. Вони генеруються за допомогою хеш-функцій і включаються в теги завантажуваних ресурсів. При завантаженні ресурсу браузер перевіряє його цілісність шляхом порівняння отриманого хешу з оригінальним хешем. Якщо хеші не співпадають, це може свідчити про зміну ресурсу, що може бути ознакою атаки або несанкціонованої модифікації. Відсутність атрибутів цілісності підресурсів створює ризик того, що зловмисник може змінити ці підресурси без відома власника веб-сайту або відвідувачів. Це може призвести до виконання шкідливого коду, включення шкідливого вмісту або зміни функціональності веб-сторінки.

CSP: Notices (повідомлення Content Security Policy) - це механізм, що використовується для виявлення та повідомлення про порушення політики безпеки контенту на веб-сайті. Політика безпеки контенту (Content Security Policy, CSP) встановлює набір правил і обмежень для веб-сторінок, що мають на

меті запобігання атакам, таким як внедрення скриптів (Cross-Site Scripting, XSS) або використання небезпечних джерел ресурсів.

CSP: Notices дозволяє веб-розробникам отримувати повідомлення про можливі порушення політики безпеки контенту, які відбуваються на веб-сайті. Це може включати сповіщення про заборонені джерела ресурсів, невідповідність політиці безпеки, спроби виконання небезпечних операцій, використання вразливих параметрів і багато іншого.

Повідомлення CSP: Notices надають важливу інформацію про можливі вразливості або порушення безпеки, що допомагає виявити проблеми та прийняти відповідні заходи для їх усунення. Веб-розробники можуть використовувати ці повідомлення для аналізу безпеки веб-сайту, виявлення потенційних вразливостей і вдосконалення політики безпеки контенту.

Cross-Domain JavaScript Source File Inclusion (включення JavaScript-файлів з іншого домену) - це вразливість, яка виникає, коли веб-сторінка дозволяє підключати зовнішні JavaScript-файли з інших доменів без належних обмежень. Ця вразливість може бути використана зловмисниками для впровадження шкідливого коду зі зловживанням довіри користувача до домену, з якого підключається файл. Зазвичай веб-браузери застосовують політику схоронності, відому як Same-Origin Policy (SOP), яка обмежує доступ скриптів до ресурсів (таких як JavaScript-файли) з інших доменів. Це робиться для запобігання атакам, таким як Cross-Site Scripting (XSS) і зловживання привілеїв. Проте, якщо веб-сторінка встановлює некоректні або недостатні обмеження, зловмисник може зловживати цим і впроваджувати шкідливий код з інших доменів. Це може призвести до виконання небажаних операцій на веб-сторінці, збору конфіденційної інформації, перехоплення сесійних файлів та інших шкідливих дій.

Відсутність заголовка Strict-Transport-Security (STS) (Нестрога безпека транспорту) є вразливістю, яка виникає, коли веб-сервер не встановлює цей заголовок у відповіді. STS є механізмом безпеки, який забезпечує захист від атак, пов'язаних з атаками "Man-in-the-Middle" та "SSL-Stripping". Заголовок Strict-

Transport-Security надає вказівку веб-браузеру використовувати тільки захищений канал (HTTPS) для взаємодії з веб-сайтом. Це означає, що браузери, які підтримують STS, будуть автоматично переходити на HTTPS-з'єднання, навіть якщо користувач введе незахищену версію URL-адреси. Відсутність заголовка Strict-Transport-Security може залишити веб-сайт вразливим до атак, таких як атаки перехоплення з'єднання та перенаправлення HTTP на HTTPS. Зловмисники можуть спробувати використовувати ці атаки для зламування зв'язку між користувачем і веб-сайтом, отримання конфіденційної інформації або зламування сесійних файлів.

Вразливість "Timestamp Disclosure - Unix" відноситься до ситуації, коли система розкриває інформацію про часовий штамп (timestamp) або деякі деталі щодо розрахунку часу на Unix-подібних системах. Це може включати відображення точного часу, останніх модифікацій файлів або інших подібних інформаційних даних. Ця вразливість може мати наслідки в ситуаціях, коли відомості про час можуть бути використані зловмисниками для аналізу або виявлення слабких місць в системі. Наприклад, зловмисники можуть використовувати інформацію про точний час для синхронізації атак або встановлення часових рамок для виконання певних дій.

3.2 Пропозиції щодо покращення безпеки враховуючи виявлені вразливості

Зважаючи на виявлені проблеми з безпекою на веб-сайті, ми пропонуємо наступні рекомендації для покращення загального рівня безпеки:

Виправлення вразливостей: основною метою є усунення виявлених вразливостей на веб-сайті табл.1. Це може включати виправлення помилок в коді, встановлення оновлень платформи або фреймворка, оновлення сторонніх компонентів і плагінів, а також перевірку налаштувань сервера і бази даних на наявність потенційних проблем. Захист від зловмисних атак: встановлення додаткових заходів безпеки для запобігання зловмисним атакам, таким як використання файрволу для блокування небажаного трафіку, використання системи виявлення вторгнень (IDS) або виявлення зловмисного програмного забезпечення (MDS) для виявлення незвичайної активності, а також використання системи фільтрації веб-запитів для блокування відомих атак.

Шифрування даних: застосування шифрування для захисту конфіденційної інформації, яка передається між користувачем і сервером. Це може включати використання протоколу HTTPS з встановленим SSL / TLS сертифікатом, що забезпечує захищене з'єднання, а також шифрування чутливих даних, які зберігаються на сервері. Аудит безпеки: регулярне проведення аудиту безпеки для виявлення нових потенційних вразливостей та слабких місць на веб-сайті. Це може бути виконано зовнішніми експертами з безпеки або внутрішнім командою безпеки, які проводять тестування на проникнення, перевірку конфігурацій сервера, перевірку виконання найкращих практик і перевірку наявності оновлень. Користувачська свідомість: навчання користувачів про безпечне користування веб-сайтом та свідоме виконання безпечних практик. Це може включати надання пояснень щодо слабких паролів, перевірку пошти на фішингові листи, підказки про безпечні методи передачі особистих даних та попередження щодо небезпечних веб-сайтів або завантажень. Резервне копіювання даних: регулярне створення резервних копій даних веб-сайту для

забезпечення можливості відновлення в разі випадкового видалення або пошкодження даних. Резервні копії повинні зберігатися на окремих серверах або в хмарних сховищах з обмеженим доступом. Моніторинг та виявлення інцидентів: постійний моніторинг активності на веб-сайті для виявлення підозрілої активності, незвичних підключень або спроб несанкціонованого доступу. Швидка реакція на потенційні інциденти та вжиття заходів для їх припинення та запобігання подальшим порушенням безпеки. Ці рекомендації допоможуть покращити безпеку веб-сайту і забезпечити захист від можливих загроз, знизити ризики вразливості та зберегти конфіденційність, цілісність та доступність даних.

Таблиця 3.1 – розбір вразливостей

Вразливості	Усунення
Cross Site Scripting (Reflected)	Валідувати та екранизувати вхідні дані, екранизувати вихідні дані.
PII Disclosure	Видаліть зайві конфіденційні дані, застосуйте шифрування.
CSP: Wildcard Directive	Wildcard Directive, замініть символ "" у директиві на конкретні джерела ресурсів на вашому веб-сайті.
CSP: script-src unsafe-inline	Видаліть директиву "unsafe-inline" з налаштувань script-src.
CSP: style-src unsafe-inline	Видаліть директиву "unsafe-inline" з налаштувань style-src.
Cross-Domain Misconfiguration	Слід перевірити і налаштувати правильні конфігурації безпеки.
Missing Anti-clickjacking Header	Слід додати відповідний заголовок "X-Frame-Options" до HTTP-відповідей вашого веб-сервера.
Proxy Disclosure	Рекомендується налаштувати ваш проксі-сервер або веб-сервер таким чином, щоб він не розкривав конфіденційну інформацію про проксі-сервер, таку як версія або інші ідентифікуючі дані.

Продовження таблиці 3.1

Sub Resource Integrity Attribute Missing	Необхідно додати атрибут integrity до всіх зовнішніх ресурсів (таких як скрипти, стилі, зображення), які завантажуються на веб-сторінку.
CSP: Notices	Необхідно ретельно переглянути та налаштувати політику Content Security Policy (CSP) для веб-сайту.
Cross-Domain JavaScript Source File Inclusion	необхідно перевірити та налаштувати правильну політику Same-Origin Policy (SOP) для веб-сайту. Забезпечити, щоб скрипти були завантажені лише з довірених та валідних джерел, а доступ до них з інших доменів був обмежений.
Strict-Transport-Security Header Not Set	Необхідно встановити заголовок Strict-Transport-Security (HSTS) на вашому веб-сервері.
Timestamp Disclosure - Unix	Необхідно відключити відображення системного часу (Unix timestamp) на веб-сайті або замінити його загальним або локалізованим форматом дати і часу.

3.3 Створення плану та рекомендації щодо повторного та періодичного оцінювання захищеності

План та рекомендації щодо повторного та періодичного оцінювання захищеності веб-сайту фітнес-клубу:

План оцінювання захищеності веб-сайту:

Цілісність даних - переконатися, що дані клієнтів, співробітників і фітнес-клубу зберігаються без змін. Конфіденційність даних: Захистити конфіденційну інформацію від несанкціонованого доступу.

Доступність - забезпечити безперебійний доступ до веб-сайту для користувачів.

Вибір методів оцінювання - використання спеціалізованих інструментів для сканування веб-сайту на наявність вразливостей. Аудит безпеки для перевірки дотримання стандартів і рекомендацій безпеки. Проведення пенетраційного тесту для виявлення слабких місць і можливих атак. Розробка графіка оцінювання: Встановлення регулярності оцінювання, яка відповідає змінам на веб-сайті, новим загрозам і внутрішнім політикам безпеки. Визначення термінів проведення оцінювання та призначення відповідальних осіб.

Виконання оцінювання - запуск інструментів оцінювання та виконання аудиту безпеки згідно з планом. Збір і аналіз даних, отриманих під час оцінювання.

Аналіз результатів та розробка рекомендацій - оцінка виявлених небезпечних точок та проблем безпеки. Розробка конкретних рекомендацій для виправлення виявлених проблем і підвищення загальної захищеності.

Рекомендації щодо покращення захищеності веб-сайту: встановлення регулярного оновлення системи, виконання оновлення оперативної системи, веб-сервера та платформи веб-сайту для усунення відомих вразливостей. Використання безпечних паролів: захистіть акаунта адміністраторів, співробітників і клієнтів від несанкціонованого доступу, вимагаючи складні

паролі. Захист даних - використовуйте шифрування для зберігання та передачі конфіденційних даних. Встановлення механізмів моніторингу – встановіть систему моніторингу безпеки, щоб вчасно виявляти підозрілу активність і атаки. Навчання персоналу - забезпечте навчання співробітників щодо безпекових практик і свідомості щодо потенційних загроз. Резервне копіювання даних - регулярно створюйте резервні копії даних, щоб уникнути втрати і відновити веб-сайт у разі інциденту. Впровадження системи контролю доступу - використовуйте механізми аутентифікації та авторизації для обмеження доступу до веб-сайту тільки для авторизованих користувачів.

Ці рекомендації допоможуть забезпечити покращення захищеності вашого веб-сайту. Регулярне повторне оцінювання та виконання рекомендацій є важливими етапами для забезпечення надійної захисту даних і довіри користувачів.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при ураженні електричним струмом

При ураженні електричним струмом необхідно якомога швидше звільнити потерпілого від струмопровідних частин обладнання. Дотик до струмопровідних частин (мережі під напругою) у більшості випадків призводить до судом м'язів, тобто людина самостійно не в змозі відірватися від провідника. Тому необхідно швидко відключити ту частину електрообладнання, до якої доторкається людина. Будь-яке зволікання при наданні допомоги, а також невміння того, хто допомагає, надати кваліфіковану допомогу, призводить до загибелі людини, яка знаходиться під дією струму.

При звільненні потерпілих від струмопровідних частин або проводу в електроустановках напругою до 1000 В відключають струм, використовуючи сухий одяг, палицю, дошку, шапку, сухі рукавиці, рукав одягу, діелектричні рукавиці. Провідники перерізають інструментом з ізольованими ручками, перерубують сокирою з дерев'яним сухим топорищем.

Потерпілого можна також відтягнути від струмопровідних частин за одяг, уникаючи дотику до навколишніх металевих предметів та до відкритих частин тіла потерпілого. Відтягуючи потерпілого за ноги, не можна торкатися його взуття, оскільки воно може бути сирим і стає провідником електричного струму. Той, хто надає допомогу, повинен одягнути діелектричні рукавиці або обмотати їх шарфом, натягнути на них рукав піджака або пальта. Можна також ізолювати себе, ставши на гумовий килимок, суху дошку тощо.

Після звільнення потерпілого від дії струму потрібно відразу ж надати йому необхідну медичну допомогу. Виділяють три стани людського організму внаслідок дії електроструму:

– I стан – потерпілий при свідомості. Слід забезпечити повний спокій, 2-3 годинне спостереження, виклик лікаря.

– II стан – потерпілий непритомний, але дихає. Людину покласти горизонтально, розстебнути комір і пасок, дати нюхати нашатирний спирт, викликати лікаря.

– III стан – потерпілий не дихає або дихає з перервами, уривчасто. Роблять штучне дихання і непрямий масаж серця.

Якщо потерпілий після звільнення від дії електричного струму і надання медичної допомоги прийшов до тями, його не слід одного відправляти додому або допускати до роботи. Такого потерпілого слід доставити в лікувальний заклад, де за ним буде встановлено спостереження, так як наслідки від впливу

електричного струму можуть проявитися через кілька годин і привести до більш важких наслідків.

4.2 Організація ведення робіт в аварійних умовах.

Організація ведення робіт в аварійних умовах є надзвичайно важливим аспектом забезпечення безпеки та ефективності в небезпечних ситуаціях. Одні із основних кроків такій ситуації:

- оцінка ризиків: Перед початком будь-яких аварійних робіт необхідно провести оцінку ризиків. Визначте потенційні небезпеки, що виникають у зв'язку з аварійною ситуацією, і розробіть план заходів для зниження цих ризиків.

- створення команди: Сформуйте команду, яка буде відповідальна за проведення аварійних робіт. Команда повинна складатися з кваліфікованих фахівців з необхідними навичками та досвідом в роботі з аварійними ситуаціями.

- встановлення комунікації: Забезпечте ефективну систему комунікації всередині команди та з іншими відповідними структурами (пожежна служба, поліція, медична допомога тощо). Засоби зв'язку повинні бути надійними та доступними, щоб забезпечити швидкий обмін інформацією.

- планування та координація: Розробіть детальний план робіт, включаючи послідовність дій, розподіл завдань, використання необхідного обладнання та ресурсів. Координуйте дії команди таким чином, щоб досягти ефективного вирішення проблеми.

- навчання та підготовка працівників: Працівники, які беруть участь у роботах в аварійних умовах, повинні мати необхідні навички та знання. Забезпечте їм належне навчання з процедур безпеки, використання спеціального обладнання та заходів, які слід вживати під час аварій.

Складовою частиною процесу ліквідації наслідків НС є рятування людей. Цей процес представляє собою взаємопов'язаний комплекс робіт, які за характером виконання діляться на три специфічні групи: рятувальні, спеціальні і допоміжні.

Рятувальні роботи, що безпосередньо пов'язані із рятуванням людей включають у себе:

- пошук постраждалих у місцях їхнього можливого блокування;
- деблокування постраждалих (забезпечення доступу до них);
- надання постраждалим домедичної допомоги;
- евакуація постраждалих із місць блокування.

Спеціальні роботи включають:

- гасіння пожеж;
- ліквідацію аварії на комунально-енергетичних і технологічних мережах;
- улаштування проїздів (проходів) у завалах;
- зміцнення (обвалення) нестійких конструкцій.

У результаті виконання спеціальних робіт створюються умови найбільш сприятливі для виконання рятувальних робіт і запобігання додаткового ураження людей. Допоміжні роботи пов'язані з інженерною та організаційною підготовкою ділянки рятувальних робіт та робочих місць. До них відносяться:

- розчищення майданчиків;
- установлення на них техніки;
- огородження, попереджувальних знаків;
- освітлення робочих місць.

Час, необхідний для виконання технологічних операцій, є основним критерієм, що характеризує доцільність їх застосування у технологічному процесі порятунку людей, у певних організаційнотехнологічних умовах.

У практиці рятування постраждалих при обваленні будівель використовуються наступні рятувальні технології:

- пошук постраждалих за допомогою спеціально навчених собак (кінологічний спосіб);
- пошук постраждалих за допомогою спеціальних приладів;
- деблокування постраждалих із завалу, що складається із дрібних уламків, способом розбирання завалу зверху;
- деблокування постраждалих із завалу, що складається із великих уламків, способом розбирання завалу зверху;
- деблокування постраждалих із завалу способом суцільного горизонтального розбирання;
- деблокування постраждалих способом улаштування лазу у завалі;
- деблокування постраждалих із завалених приміщень;
- деблокування постраждалих з верхніх поверхів будівлі з використанням вертольоту;
- деблокування постраждалих з верхніх поверхів будівлі із застосуванням автодрабин;

- порятунок постраждалих з верхніх поверхів будівлі за допомогою автовишок та автопідйомників;

- порятунок постраждалих з верхніх поверхів будівлі по збереженим або тимчасово відновленим сходовим маршам;

- порятунок постраждалих з верхніх поверхів будівлі з використанням канатної дороги;

- порятунок постраждалих з верхніх поверхів будівлі із застосуванням рятувального рукава;

- деблокування постраждалих з верхніх поверхів будівлі з використанням альпіністських засобів.

У загальному вигляді процес рятування постраждалих може бути представлений як комплексний технологічний процес, що включає наступні етапи:

- загальна спеціальна розвідка осередку ураження та об'єкта робіт;

- підготовчі роботи;

- аварійно-технічні роботи;

- пошуково-рятувальні роботи;

- роботи з деблокування та витягання постраждалих;

- надання домедичної та лікарської допомоги, медична евакуація поранених;

- евакуація, упізнання та поховання загиблих.

На кожному з наведених технологічних етапів здійснюються відповідні види робіт, а вони, у свою чергу виконуються певними способами. Найбільш складним технологічним етапом при обваленні будівель і споруд є інженерні роботи з деблокування та витягання постраждалих.

Роботи з деблокування та витягання постраждалих доцільно розділити на види робіт:

- деблокування та витягання постраждалих, що перебувають у завалах будівельних конструкцій;

- деблокування та витягання постраждалих, що перебувають у замкнутих, ізольованих приміщеннях;

- деблокування та порятунок постраждалих, що перебувають на верхніх поверхах (рівнях) напівзруйнованих і палаючих будівель.

Роботи з деблокування та витягання постраждалих, що перебувають у завалах будівельних конструкцій є самими трудноміськими і складними.

Деблокування потстраждалих у завалах виконується у два етапи: на першому — забезпечується доступ до постраждалого, проникнення рятувальників до місця блокування; на даному етапі допускається виконання технологічних операцій, пов'язаних з руйнуванням, дробленням уламків завалів; на другому — здійснюється вивільнення постраждалих від елементів завалу, при цьому операції, пов'язані з ударними навантаженнями, що створюють загрозу зсуву елементів завалу повинні бути виключені, тому що являють собою підвищену небезпеку для постраждалих, що перебувають у завалі.

Деблокування постраждалих у завалах здійснюється такими способами:

- послідовно-поетапного горизонтального розбирання;
- послідовно-поетапного вертикального розбирання;
- проходки галерей у завалі;
- улаштування галерей у ґрунті під завалом;
- улаштування вертикальних або похилих колодязів;
- улаштуванню лазу.

Кожний спосіб може виконуватися із застосуванням різних комплектів аварійно-рятувального інструменту, видів інженерної техніки, матеріалів та обладнання.

Роботи можуть проводитись силами різних за складом підрозділів (розрахунків, ланок, груп)

ВИСНОВКИ

Отже, при проведенні повного дослідженні веб-сайту "Каруна" були виявлені різні потенційні вразливості безпеки. Кожна виявлена вразливість була оцінена з точки зору потенційного впливу на безпеку веб-сайту та конфіденційність, цілісність та доступність даних користувачів. Були визначені високоризикові вразливості, які можуть призвести до серйозних наслідків, а також низькоризикові вразливості, які потребують меншої уваги.

Виявлені результати мають велику значимість для безпеки системи веб-сайту "Каруна". Вони вказують на наявність потенційних проблем, які можуть бути використані зловмисниками для атак та порушення безпеки інформації. Залежно від характеру виявлених вразливостей, наслідки можуть бути серйозними. Наприклад, Cross-Site Scripting (XSS) може дозволити зловмиснику внедрити шкідливий код на веб-сторінках, що призведе до виконання шкідливих дій на браузерах користувачів. SQL Injection може дозволити зловмиснику отримати несанкціонований доступ до бази даних та витягнути конфіденційну інформацію. Інші вразливості можуть призвести до втрати чутливих даних, викриття особистої інформації користувачів або порушення функціональності системи.

Тому, виявлення цих слабких точок та їх вирішення мають вирішальне значення для забезпечення безпеки веб-сайту "Каруна". Вони надають можливість здійснити необхідні заходи для усунення потенційних проблем та запобігання можливим атакам. Захищена система забезпечує конфіденційність, цілісність та доступність інформації, а також довіру користувачів до веб-сайту. Враховуючи важливість безпеки, рекомендації щодо усунення проблеми з захищеністю та підвищення безпеки системи повинні бути виконані якомога швидше.

В результаті проведення оцінки безпеки веб-сайту фітнес-клубу "Каруна", було досягнуто важливих результатів, спрямованих на забезпечення захищеності системи. Основна ціль оцінки полягала в виявленні потенційних

слабких місць та розробці рекомендацій щодо усунення, уникнення чи пом’якшення цих вразливостей. Проведений аудит безпеки виявив ряд недолік безпек, що можуть стати потенційними точками входу для зловмисників або спричинити порушення безпеки системи.

На основі цих результатів були розроблені конкретні рекомендації, спрямовані на вирішення виявлених проблеми з захищеністю. Виконання цих рекомендацій дозволить підвищити рівень захищеності веб-сайту та зменшити ймовірність успішних атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. http://dspace.kntu.kr.ua/jspui/handle/123456789/11436
2. **https://sci.ldubgd.edu.ua/bitstream/123456789/11456/1/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%972019%20%D0%9B%D0%B0%D0%B3%D1%83%D0%BD%20%D0%A0%D1%83%D0%B4%D0%B8%D0%BA.pd**
3. **https://web.s.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=22235744&AN=115853245&h=%2bqMG8OIAPyqupG23op8SM4UDo%2fpebbFEWneJxTmfaT5P6iXgKI4kKxaEYZj3Fr6oxdHR%2bFQYjV69aPPUCoqsPg%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d22235744%26AN%3d115853245**
4. **https://knute.edu.ua/file/NjY4NQ==/250dafc576ffd3c6a92546eebacc834d.pdf#page=130**
5. **https://openarchive.nure.ua/items/ff6a37df-c279-4c47-94f7-1bf53ddd4f57**
6. **http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/33917/%D0%A4%D1%80%D0%BE%D0%BB%D0%BE%D0%B2.pdf?sequence=1&isAllowed=y**
7. **http://ir.stu.cn.ua/handle/123456789/26668**
8. **https://elartu.tntu.edu.ua/handle/lib/35554**
9. **http://mdu.edu.ua/wp-content/uploads/agit2018proceeding.pdf#page=196**
10. **https://ir.nmu.org.ua/bitstream/handle/123456789/148764/masal_kolisn.pdf?sequence=1&isAllowed=y**
11. **https://corewin.ua/blog/how-scanners-find-vulnerabilities/**
12. **https://uk.shram.kiev.ua/progs/scaners.shtml**
13. **https://medium.com/@svyatoslavlogyn/%D1%82%D0%B5%D1%81%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%**

B8%D0%B5-%D0%BD%D0%B0-xss-%D0%B8-%D0%B4%D1%80%D1%83%D0%B3%D0%B8%D0%B5-%D1%83%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D0%B8-c-%D0%BF%D0%BE%D0%BC%D0%BE%D1%89%D1%8C%D1%8E-owasp-zap-a99183c32013

14. https://futurenow.com.ua/shho-take-veb-sajt-yaka-istoriya-yih-vynyknennya-ta-vydy-veb-sajtiv-shho-take-veb-storinka/