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)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Технічна оцінка захищеності вебсайту Vandal Академії

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

(підпис) Лісняк М.С (прізвище та ініціали)

Керівник (підпис) Лечаченко Т.А (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б (прізвище та ініціали)

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

Рецензент (підпис) Петрик М.Р. (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
(підпис) Загородна Н.В.
(прізвище та ініціали)
«19» червня 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Лісняк Максим Сергійович
(прізвище, ім'я, по батькові)

1. Тема роботи Технічна оцінка захищеності вебсайту Vandal Академії

Керівник роботи Іваненко Тарас Анатолійович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «03» жовтня 2023 року № 4/7-349
2. Термін подання студентом завершеної роботи 17.06.2023
3. Вихідні дані до роботи технічна оцінка захищеності

4. Зміст роботи (перелік питань, які потрібно розробити)
Мета та завдання дослідження, актуальність теми
Методи та інструменти аналізу захищеності вебсайту Vandal Академії
Технічна оцінка захищеності вебсайту Vandal Академії, рекомендації
Безпека вебсайту.
Безпека інтернет-діяльності, основні ознаки фрод

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна. 2 Мета та завдання дослідження 3 Види загроз. Вектор і техніки захисту 5 Процедури захисту 6 Основні заходи 7 Переваги автоматизації перевірки 8 Інструменти забезпечення безпеки 9 Основні функції Vandal Академії 10 Вразливості кібербезпеки 11 Результати тестування OWASP ZAP 12 Результати тестування Nessus 13 Рекомендації щодо покращення

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата: завдання видав	Підпис, дата: завдання прийняв
Безпека життєдіяльності основи охорони праці	Лимінець П.І. д.т.н. професор кафедри НТ	18.06.23	18.06.23

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення з завданням до кваліфікаційної роботи	16.01 - 19.01	Виконано
2	Підбір джерел про технічну оцінку вебсайту, методи оцінки	20.01 - 05.02	Виконано
3	Опрацювання джерел в галузі дослідження технічної оцінки вебсайту	06.02 - 22.02	Виконано
4	Технічна оцінка захищеності вебсайту	23.02 - 20.03	Виконано
5	Створення рекомендацій щодо захисту	21.03 - 05.04	Виконано
6	Оформлення розділу "Мета та завдання дослідження, актуальність теми"	06.03 - 17.04	Виконано
7	Оформлення розділу "Методи та інструменти оцінки захищеності вебсайту Vanda Академії	18.04 - 29.04	Виконано
8	Оформлення розділу "Технічна оцінка захищеності вебсайта Vanda Академії	30.04 - 13.05	Виконано
9	Виконання завдання до підрозділу "Безпека життєдіяльності основи охорони праці"	14.05 - 21.05	Виконано
10	Оформлення кваліфікаційної роботи	22.05 - 05.06	Виконано
11	Нормоконтроль	06.06 - 11.06	Виконано
12	Рецензія на роботу	12.06 - 15.06	Виконано
13	Попередній захист кваліфікаційної роботи	16.06 - 19.06	Виконано
14	Захист кваліфікаційної роботи	22.06.2023	

Студент _____ (підпис) Лісняк М.С. (прізвище та ініціали)

Керівник роботи _____ (підпис) Лимінець Г.А. (прізвище та ініціали)

АНОТАЦІЯ

Технічна оцінка захищеності вебсайту Vandal Академії 1”// Кваліфікаційна робота освітнього рівня «Бакалавр» // Лісняк Максим Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль 2023 // С.50 , рис. - 4, посил. – 9.

Ключові слова: ТЕХНІЧНА ОЦІНКА ЗАХИЩЕНОСТІ ВЕБСАЙТУ, ВИДИ ЗАГРОЗ І АТАК НА ВЕБСАЙТИ, МЕТОДИ ТЕСТУВАННЯ ЗАХИЩЕНОСТІ ВЕБСАЙТУ, АВТОМАТИЧНА ПЕРЕВІРКА.

Кваліфікаційна робота присвячена технічній оцінці захищеності вебсайту, використовуючи метод автоматичної перевірки для проведення технічної оцінки. В роботі проведено технічну оцінку захищеності вебсайту та запропоновані рекомендації щодо її покращення.

При проведені технічної оцінки вебсайту було виявлено загрози та запропоновано рекомендації, щодо захисту від них. Продемонстровано використання автоматичного методу перевірки захищеності вебсайту.

ANNOTATION

Technical security assessment of the Vandal Academy 1 LLC // Thesis of educational level “Bachelor” // Lisniak Maksym Serhiyovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, group SBs-41 // Ternopil 2023 // P.50 , fig. - 4, links - 9.

Keywords: TECHNICAL ASSESSMENT OF WEBSITE SECURITY, THREATS AND ATTACKS ON WEBSITES, METHODS OF WEBSITE SECURITY TESTING, AUTOMATED SCANNING.

The qualification work is dedicated to the technical assessment of the website's security, using an automated checking method to conduct the technical evaluation. The paper carries out a technical assessment of the website's security and proposes recommendations for its improvement.

During the technical evaluation of the website, threats were identified, and recommendations were made on how to protect against them. The use of an automated method for checking website security was demonstrated.

ЗМІСТ

ВСТУП. 7
1 МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ, АКТУАЛЬНІСТЬ ТЕМИ 8
1.1 Основні поняття та теоретичні аспекти захищеності вебсайтів 8
1.2 Види загроз і атак на вебсайти 11
1.3 Заходи захисту вебсайтів 13
2 МЕТОДИ ТА ІНСТРУМЕНТИ АНАЛІЗУ ЗАХИЩЕНОСТІ ВЕБСАЙТУ VANDAL АКАДЕМІЇ 16
2.1 Автоматична перевірка 16
2.2 Ручна перевірка 24
2.3 Вибір методу перевірки захищеності сайту 32
3 ТЕХНІЧНА ОЦІНКА ЗАХИЩЕНОСТІ ВЕБСАЙТУ VANDAL АКАДЕМІЇ 33
3.1 Опис вебсайту та його основних функцій 33
3.2 Аналіз потенційних загроз та вразливостей 34
3.3 Проведення тестування безпеки та аналіз результатів 36
4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ 44
4.1 Долікарська допомога при обмороженні 44
4.2 Санітарно-гігієнічні вимоги до умов праці в офісі 46
ВИСНОВКИ 49
ПЕРЕЛІК ПОСИЛАНЬ 50

ВСТУП

У світлі стрімкого розвитку інформаційних технологій та їх все більшого впливу на всі сфери нашого життя, питання інформаційної безпеки, особливо в контексті веб-ресурсів, набуває нових обертів. Досить часто організації, особливо освітні, якими є Vandal Академія, стають об'єктом кібератак з метою викрадення важливої інформації або завдання шкоди їх репутації.

Такий стан речей робить актуальним завдання проведення технічної оцінки захищеності вебсайтів, зокрема Vandal Академії, з метою виявлення потенційних слабких місць і розробки рекомендацій по їх усуненню. Існує чимало сучасних розробок у цій сфері, але все ще відсутній єдиний стандартний підхід, що робить цю тему вельми перспективною для дослідження.

Спроектовані та впроваджені положення щодо оцінки та зміцнення безпеки вебсайту Vandal Академії матимуть значний науковий і практичний вплив. З одного боку, вони дозволять покращити теоретичні знання в даній області, а з іншого - забезпечать конкретні кроки для покращення безпеки конкретного вебсайту, що може бути застосовано для інших схожих ресурсів.

Проблема захисту вебсайтів активно вивчається вченими та фахівцями з кібербезпеки, але через постійний розвиток технологій та зміну тактик кібератак, постійно з'являються нові виклики. У цій роботі буде проведено оцінку захищеності вебсайту Vandal Академії, виявлення слабких місць і вироблення рекомендацій щодо їх усунення, що може стати основою для подальших наукових досліджень та практичних застосувань.

1 МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ, АКТУАЛЬНІСТЬ ТЕМИ

Сучасний стан розвитку інформаційних технологій та все більше впливу їх на різні сфери життєдіяльності суспільства зумовлює необхідність забезпечення безпеки веб-ресурсів. Особливо це стає актуальним у контексті освітніх організацій, які мають значну кількість користувачів та обробляють великі обсяги інформації. Вебсайт Vandal Академії відноситься до таких ресурсів.

Мета цього розділу полягає в узагальненні основних теоретичних понять та принципів, що стосуються захисту вебсайтів, а також у визначенні актуальних проблем та завдань у даній галузі. Це необхідно для розуміння поточного стану захищеності вебсайту Vandal Академії та визначення способів його покращення.

1.1 Основні поняття та теоретичні аспекти захищеності вебсайтів

Захист вебсайтів - це набір технологій, процедур та практик, спрямованих на запобігання несанкціонованому доступу, використанню, зміні, перегляду або знищенню інформації. Він також включає в себе захист від різноманітних видів загроз, таких як віруси, витоки даних, DDoS-атаки й інші.

Основні теоретичні аспекти захищеності вебсайтів включають розуміння принципів конфіденційності, цілісності та доступності (CIA). Принцип конфіденційності означає, що інформація доступна тільки для тих, хто має на це право. Цілісність вимагає, щоб інформація та системи були захищені від змін або знищення в неавторизований спосіб. Доступність означає, що інформація та ресурси повинні бути доступні тим, хто їх потребує.

Давайте детальніше розглянемо теоретичні аспекти захищеності вебсайтів:

- Конфіденційність в контексті кібербезпеки означає, що інформація має бути доступна та видима лише для тих осіб, хто має на це відповідні права доступу. Це означає, що захист конфіденційності вимагає запобігання неавторизованому доступу до даних. Методи для забезпечення конфіденційності включають в себе шифрування даних, контроль доступу, двофакторну аутентифікацію та інше.

- Цілісність стосується забезпечення того, що дані та системи залишаються цілими, консистентними та точними. Це означає, що дані не можуть бути змінені або знищені в неавторизований спосіб. Методи забезпечення цілісності даних включають в себе контроль хеш-сум, цифрові підписи, системи відновлення даних та інше.
- Доступність означає, що ресурси (інформація, системи, сервіси) повинні бути доступні для використання при потребі. Це включає забезпечення стабільності роботи вебсайтів, запобігання перебоям в роботі, резервне копіювання та відновлення даних, боротьба з DDoS-атаками.

Кожен з цих принципів важливий для забезпечення безпеки вебсайту. Вони служать основою для визначення політик та процедур безпеки, а також для розробки та впровадження технічних заходів захисту.

Захист вебсайтів також включає в себе розробку та впровадження політик безпеки, проведення періодичного аудиту та моніторингу системи на наявність зловмисних дій, та реагування на інциденти безпеки.

Розробка та впровадження політик безпеки є важливим кроком у захисті вебсайтів. Ці політики служать основою для всіх процедур та технічних заходів, що вживаються для забезпечення безпеки вебсайту. Вони можуть включати правила користування ресурсами, вимоги до паролів, процедури резервного копіювання, правила відповіді на інциденти безпеки та інше. Політики безпеки повинні бути чітко сформульовані, легкими для розуміння та доступними для всіх користувачів вебсайту.

Періодичний аудит та моніторинг системи є іншим критично важливим аспектом захисту вебсайтів. Аудит безпеки допомагає визначити поточний стан безпеки, виявити слабкі місця, відстежити виконання політик та процедур безпеки. Моніторинг, в свою чергу, допомагає виявити зловмисні дії або аномальну поведінку в реальному часі, що дає можливість вживати відповідних дій, перш ніж виникне реальна загроза.

Реагування на інциденти безпеки — це процес, що включає в себе виявлення, аналіз, виправлення та відновлення роботи системи після інциденту. Важливо мати чіткий план реагування на інциденти, що містить конкретні дії у випадку виявлення

можливої або реальної загрози. Це може включати ізоляцію компрометованих систем, видалення зловмисного ПО, виправлення вразливостей, відновлення з резервних копій та звітність про інцидент.

Система захисту вебсайту, як правило, включає в себе ряд компонентів, таких як брандмауери, системи виявлення вторгнень, антивіруси, фільтри спаму, системи захисту від DDoS-атак, інструменти для шифрування даних та інші.

Існує також ряд стандартів та рекомендацій, спрямованих на підвищення рівня захисту вебсайтів. Одним з них є рекомендації OWASP (Open Web Application Security Project), які включають перелік найчастіших вразливостей веб-додатків, та рекомендації щодо їх усунення.

Впровадження заходів захисту вебсайтів потребує знань та навичок не тільки в галузі інформаційних технологій, але і в галузі кібербезпеки. Також важливим є розуміння специфіки роботи конкретного вебсайту, його архітектури, використовуваних технологій, потенційних ризиків та вразливостей.

У наступних розділах буде проведено детальний аналіз специфіки захисту вебсайту Vandal Академії, ідентифіковано потенційні загрози та вразливості, та розроблено рекомендації щодо їх усунення.

Слід пам'ятати, що кіберзахист - це не одноразове завдання, а постійний процес. Технології швидко змінюються, а зловмисники неперервно розробляють нові методи атак. Тому необхідно не тільки регулярно оновлювати захисні механізми, але й проводити їх аудит, моніторинг, тестування та налаштування. Також важливо проводити тренінги з безпеки для користувачів сайту, оскільки вони часто є найслабкішим ланцюгом в системі захисту.

Щодо Vandal Академії, велику увагу необхідно приділити захисту особистих даних користувачів, а також інформації, що є інтелектуальною власністю цієї компанії. Оскільки академія проводить онлайн-навчання, особливо важливим є захист інформації про навчальний процес, включаючи оцінки, домашні завдання та інші навчальні матеріали.

У кінцевому підсумку, оцінка захищеності вебсайту Vandal Академії має на меті не тільки виявлення потенційних слабких місць, але й розробку конкретних

рекомендацій щодо їх усунення, що сприятиме поліпшенню захисту даного веб-ресурсу.

1.2 Види загроз і атак на вебсайти

Сучасний цифровий світ переповнений різними видами загроз і атак, які можуть підірвати безпеку вебсайтів. Наприклад:

- Віруси та зловмисне ПО (malware): це шкідливі програми, що зазвичай потрапляють на вебсайт через інфіковані файли або додатки. Вони можуть шкодити сайту, викрадати даних, руйнувати файли або навіть перетворити ваш комп'ютер на частину ботнету для подальших атак.
- SQL Injection (впровадження SQL): це тип атаки, при якій зловмисник вводить шкідливі SQL команди через форми на сайті, що призводить до несанкціонованого доступу до бази даних, викрадення, зміни або видалення даних.
- Cross-Site Scripting (XSS): цей тип атаки відбувається, коли зловмисник вставляє шкідливий JavaScript-код в веб-сторінки, які переглядають інші користувачі. Це може призвести до крадіжки особистої інформації, як-от сесійних куків, або навіть до взлому облікового запису користувача.
- Відмова в обслуговуванні (DoS) та Розподілена відмова в обслуговуванні (DDoS): це атаки, які перегружають систему або мережу, роблячи вебсайт недоступним для користувачів. Зловмисники цілеспрямовано перевантажують сервер великою кількістю запитів, через що нормальний трафік не може дійти до сайту.
- Крадіжка даних і фішинг: це атаки, спрямовані на викрадення особистої або фінансової інформації користувачів. У фішингових атаках зловмисники створюють вебсайти, які виглядають як популярні сервіси, щоб обманом змусити користувачів ввести свої дані.
- Атаки "людина посередині" (Man-in-the-Middle, MitM): під час такої атаки зловмисник перехоплює та може змінювати комунікацію між двома сторонами без їхнього відома. Це може призвести до витоку конфіденційної інформації, включаючи облікові дані, номери кредитних карт і багато іншого.

- Zero-day атаки: це атаки, які використовують невідомі вразливості в програмному забезпеченні, які ще не були виявлені або виправлені розробником. За допомогою таких атак зловмисник може отримати несанкціонований доступ до системи або даних.
- Атаки на бокові канали: ці атаки використовують інформацію, отриману з фізичного середовища системи (наприклад, спостереження за споживанням енергії, звуками, електромагнітним випромінюванням тощо), щоб отримати доступ до конфіденційної інформації.
- Соціальна інженерія: це мета-атаки, які використовують психологічні трюки та маніпуляції, щоб змусити людей діяти проти своїх інтересів, наприклад, віддати свої облікові дані або встановити шкідливе програмне забезпечення.
- Криптографічні атаки: ці атаки мають на меті порушити алгоритми шифрування та безпеки, що використовуються для захисту даних і комунікації[1].

За даними звітів з кібербезпеки за 2021 рік, три найбільш поширених типи атак на вебсайти були атаки з відмовою в обслуговуванні (DoS або DDoS), атаки шкідливим програмним забезпеченням (Malware) і атаки на SQL ін’єкції (SQL Injection)[2].

Атаки з відмовою в обслуговуванні (DoS або DDoS): За даними різних джерел, до 33% усіх атак на вебсайти в 2021 році були атаки DoS або DDoS. Ці атаки використовують велику кількість трафіку для перевантаження серверів та роблять вебсайт недоступним для користувачів.

Атаки шкідливим програмним забезпеченням (Malware): Згідно з даними Cisco, близько 27% атак на вебсайти в 2021 році були пов'язані з шкідливим програмним забезпеченням. Шкідливе ПЗ може включати в себе віруси, черв'яки, трояни та програми-вимагачі.

Атаки на введення SQL (SQL Injection): Поряд з двома першими, атаки SQL Injection також є поширеними і складають приблизно 23% всіх атак на вебсайти, за даними звіту OWASP за 2021 рік. У таких атаках зловмисники використовують вразливості в веб-додатках для виконання шкідливих SQL-запитів, що може призвести до витоку, зміни або видалення даних.

Враховуючи цю статистику, можна зробити висновок, що для адекватного захисту вебсайтів необхідно розглядати різні види атак і розробляти комплексні стратегії захисту, що враховують специфіку кожного з цих типів загроз.

1.3 Заходи захисту вебсайтів

Захист вебсайтів вимагає комплексного підходу, який включає ряд різноманітних заходів. Ці заходи охоплюють технічні, процедурні та освітні аспекти.

Технічні заходи:

- Використання HTTPS: HTTPS використовує SSL/TLS протокол для шифрування інформації, яка передається між клієнтом і сервером, запобігаючи прослуховуванню або "Man-in-the-Middle" атакам.
- Брандмауери (Firewalls): Веб-брандмауери можуть бути встановлені для фільтрації шкідливого трафіку та блокування загроз, таких як SQL Injection або XSS атаки.
- Системи виявлення та запобігання вторгненню (IDS/IPS): Ці системи моніторять трафік, виявляють підозрілу активність та можуть автоматично вживати заходів для блокування загроз.
- Оновлення та патчі: Регулярне оновлення програмного забезпечення вебсайту, включаючи його CMS, плагіни, теми та інші складові, є важливим для усунення відомих вразливостей.
- Процедурні заходи:
- Політики безпеки: Важливо мати чітко сформульовані політики безпеки, які описують прийнятні та неприйнятні поведінки, вимоги до паролів, процедури резервного копіювання та відновлення та інше.
- Резервне копіювання та відновлення: Регулярне резервне копіювання даних вебсайту та здатність швидко відновити їх у випадку атаки або технічного збою є критично важливими для забезпечення безпеки.
- Реагування на інциденти: Організації повинні мати чіткі плани реагування на інциденти, включаючи процедури сповіщення, відключення та

відновлення послуг, аналіз причин і наслідків інциденту та вживання запобіжних заходів для майбутнього запобігання.

Освітні заходи:

- Навчання персоналу: Освічення персоналу про правила безпеки використання вебсайту, розпізнавання фішингових атак, створення міцних паролів та інших базових практик безпеки є важливим кроком у запобіганні атак.
- Свідомість користувачів: Залучення користувачів до безпеки вебсайту шляхом надання чітких інструкцій, повідомлень про потенційні загрози та освітніх матеріалів про захист може сприяти зниженню ризиків.

Загальна мета цих різноманітних заходів полягає в забезпеченні безпеки вебсайту шляхом впровадження технічних рішень, встановлення правил та процедур, а також підвищення свідомості персоналу та користувачів. Цей комплексний підхід допомагає запобігати атакам, вразливостям та несанкціонованому доступу до вебсайту, забезпечуючи надійний рівень захисту та захищаючи конфіденційність, цілісність та доступність даних. Послідовне застосування технічних, процедурних та освітніх заходів створює надійну базу для захисту вебсайту та зменшення ризиків веб-загроз.

1.4 Аналіз сучасних підходів до технічної оцінки захищеності вебсайтів

Технічна оцінка захищеності вебсайту включає у себе велику кількість стратегій та методологій, використання яких залежить від конкретних цілей та потреб організації. В основному, вони можуть бути поділені на дві категорії: автоматизовані та ручні методи оцінки.

Автоматизовані методи оцінки захищеності вебсайтів передбачають використання спеціалізованих програм та інструментів, які автоматично сканують вебсайт на наявність вразливостей. Ці інструменти можуть швидко просканувати великі об'єми коду і виявити поширені вразливості, такі як SQL-ін'єкції, XSS-атаки, CSRF-атаки та інше. Наприклад, до таких інструментів відносяться OWASP ZAP, Nessus, Acunetix та інші[3].

Ручні методи оцінки захищеності вебсайтів передбачають ретельний аналіз коду та структури вебсайту спеціалістами з кібербезпеки. Вони можуть виявити складніші та специфічні вразливості, які автоматизовані інструменти можуть не виявити. Ручна перевірка включає такі методи, як перегляд коду, тестування на проникнення, фазування вхідних даних та інше[4].

Обидва підходи мають свої переваги та недоліки, і найкращий підхід, як правило, включає комбінацію автоматизованого та ручного тестування.

Важливою частиною процесу оцінки захищеності вебсайту є також розуміння його контексту: хто його користувачі, які дані він обробляє, які загрози йому найбільш релевантні, як він взаємодіє з іншими системами тощо.

На даний момент, із розвитком штучного інтелекту та машинного навчання, активно розробляються та тестуються нові підходи до оцінки захищеності вебсайтів. Це включає в себе автоматизоване виявлення нових типів вразливостей, адаптивні системи захисту, які можуть навчатися та адаптуватися до нових загроз, а також інструменти для автоматизації процесів відповіді на інциденти безпеки.

Отже, обрання підходу до технічної оцінки захищеності вебсайту вимагає глибокого розуміння конкретного контексту вебсайту, доступних ресурсів та потенційних загроз.

2 МЕТОДИ ТА ІНСТРУМЕНТИ АНАЛІЗУ ЗАХИЩЕНОСТІ ВЕБСАЙТУ VANDAL АКАДЕМІЇ

Процес технічної оцінки захищеності вебсайту вимагає використання великої кількості підходів та методик, вибір яких диктується специфікою та потребами конкретної організації. У загальному вигляді, ці методики можна розділити на дві великі групи: автоматизовані та ручні методи оцінки захищеності.

2.1 Автоматичні методи перевірки

Автоматична перевірка вебсайтів є важливою складовою процесу забезпечення безпеки і захищеності. Вона дозволяє виявляти потенційні вразливості та проблеми безпеки вебсайту шляхом автоматизованого аналізу його коду, конфігурацій, ресурсів та інших складових.

Основна мета автоматичної перевірки вебсайтів - це ідентифікація вразливостей, які можуть бути використані зловмисниками для злому, крадіжки даних, атак на користувачів або недоступності вебсайту. Цей процес може включати різні види сканування, аналізу коду, перевірку конфігурації сервера та інші техніки для виявлення потенційних проблем.

Основні переваги автоматичної перевірки вебсайтів:

- Швидкість та ефективність: Автоматичні інструменти можуть просканувати великі об'єми коду та ресурсів вебсайту швидше, ніж це можливо зробити вручну. Вони виявляють загрози та вразливості в автоматизованому режимі, що дозволяє зекономити час та зусилля.
- Об'єктивність: Автоматичні інструменти виконують аналіз на основі заданих правил, настанов та критеріїв безпеки. Це дозволяє отримати об'єктивну оцінку стану безпеки вебсайту, уникнути людських помилок та забезпечити однаковий стандарт оцінки.
- Виявлення різноманітних вразливостей: Автоматичні інструменти можуть виявляти широкий спектр вразливостей, таких як SQL-ін'єкція, XSS-атаки,

CSRF-атаки, вразливості конфігурації сервера та інші. Вони здатні перевіряти вебсайт на дотримання кращих практик безпеки та використання стандартів.

- Маштабованість: Автоматичні інструменти можуть бути легко масштабовані для виконання перевірки безпеки на великій кількості вебсайтів. Це особливо важливо для організацій з великою кількістю проектів або мережевих ресурсів.

Однак автоматична перевірка має також свої обмеження:

- Обмежена виявлення нових вразливостей: Автоматичні інструменти можуть бути менш ефективні в виявленні нових та невідомих вразливостей, які можуть виникнути через унікальні конфігурації, розроблені на замовлення або специфічний код.

- Необхідність перевірки результатів: Важливо проаналізувати результати автоматичної перевірки, оцінити їх достовірність та врахувати особливості конкретного вебсайту. Іноді помилково позитивні виявлення можуть виникати через складнощі або специфіку веб-додатків.

- Відсутність контексту: Автоматична перевірка не завжди враховує специфічні особливості бізнес-процесів, вимог до безпеки та інших факторів, які можуть вплинути на загрози та рівень ризику.

Автоматична перевірка вебсайтів може включати різні типи сканування та тестування, що спрямовані на виявлення вразливостей та потенційних загроз. Ось деякі з них:

Сканування вразливостей: Це процес автоматичного перебору вебсайту з метою виявлення вразливостей, таких як вразливості в програмному забезпеченні, некоректно налаштовані сервери, витоки інформації та інші. Сканери вразливостей використовують бази даних з відомими вразливостями, а також евристичні методи для виявлення нових атак.

Тестування на переповнення буфера: Цей вид тестування спрямований на виявлення вразливостей, пов'язаних з переповненням буфера, що може призвести до виконання зловмисного коду або збоїв в роботі програми. Автоматичні інструменти можуть намагатися перевищити максимальну межу буфера або викликати певні вразливі функції, щоб виявити ці проблеми.

Перевірка валідності введених даних: Цей вид перевірки виконується для перевірки коректності та безпечності введених даних, перед тим як вони будуть оброблені веб-додатком. Інструменти можуть відправляти різноманітні вхідні дані, включаючи спеціальні символи, SQL-запити, HTML-теги та інше, для перевірки, чи виконується належна фільтрація та валідація.

Аналіз конфігурації сервера: Автоматичні інструменти можуть перевіряти конфігурацію веб-сервера та додатків на наявність неправильних налаштувань або слабких точок. Наприклад, вони можуть перевіряти налаштування SSL/TLS, обмеження доступу до файлів, налаштування файлів конфігурації та інші параметри, які можуть стати джерелом вразливостей.

Перевірка дотримання стандартів безпеки: Інструменти можуть перевіряти вебсайт на дотримання стандартів безпеки, таких як OWASP Top 10 або інші відомі керівництва та рекомендації. Вони можуть виявляти загрози, що входять до цих стандартів, і надавати рекомендації щодо виправлення виявлених проблем.

Моніторинг безпеки: Інструменти можуть постійно моніторити вебсайт на наявність нових загроз і вразливостей, а також виявляти активні атаки або незвичну активність. Це може допомогти рано виявити потенційні проблеми та негайно прийняти відповідні заходи безпеки.

Додатковою можливістю автоматичної перевірки вебсайтів є використання систем управління вразливостями (Vulnerability Management Systems). Ці системи включають в себе сканери та інструменти, які автоматично сканують вебсайт на наявність вразливостей і надають звіти з рекомендаціями щодо виправлення.

Системи управління вразливостями можуть проводити регулярні перевірки вебсайту згідно заданого графіку або навіть в режимі реального часу, аналізуючи зміни в коді та конфігурації. Вони виявляють вразливості, порівнюючи сканований вебсайт з базою даних відомих вразливостей і застосовуючи різноманітні техніки аналізу.

Деякі системи управління вразливостями також підтримують автоматичне виправлення виявлених проблем, використовуючи механізми автоматизованої підміни вразливого коду або налаштування.

Крім того, в автоматичну перевірку вебсайтів можуть включатися такі елементи, як перевірка безпеки мережі, виявлення збоїв безпеки, сканування веб-додатків на відповідність стандартам безпеки та інші. Крім того, автоматична перевірка вебсайтів може включати такі компоненти, як сканування веб-додатків на відповідність стандартам безпеки, перевірка конфігурації сервера та додатків, аналіз журналів подій та моніторинг активності на вебсайті. Ці функції допомагають виявити потенційні проблеми безпеки, такі як некоректні налаштування сервера, вразливості у коді веб-додатків чи незвичайну активність, що може вказувати на атаку.

Однак, важливо враховувати, що автоматична перевірка вебсайтів має свої обмеження. Вона може виявляти лише відомі вразливості, а нові атаки чи невідомі вразливості можуть залишатися непоміченими. Крім того, деякі вразливості можуть бути контекстуальними і потребувати ручного аналізу для їх виявлення.

Тому, оптимальний підхід до перевірки захищеності вебсайту полягає в комбінації автоматичних та ручних методів. Автоматична перевірка може значно збільшити швидкість та ефективність оцінки, виявляючи загрози, що широко поширені або мають відомі сценарії атак. Ручна перевірка, у свою чергу, забезпечує детальний аналіз коду, конфігурації та контексту вебсайту, дозволяючи виявити складні та специфічні вразливості.

Враховуючи постійний розвиток технологій кібербезпеки, методи автоматичної перевірки стають більш потужними та розширеними. Нові інструменти, що використовують штучний інтелект та машинне навчання, можуть виявляти невідомі вразливості, аналізувати поведінку веб-додатків та відстежувати потоки даних для виявлення аномалій. Використання таких інструментів покращує ефективність автоматичної перевірки та дозволяє швидше реагувати на нові загрози.

П'ять найпопулярніших способів автоматичної перевірки вебсайтів у 2021 році:

- OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) є одним з найбільш відомих інструментів для тестування веб-додатків на безпеку.

Він надає можливість сканувати веб-додатки на наявність різних вразливостей, таких як SQL-ін'єкції, XSS атаки, CSRF-атаки та інші.

- Nessus є популярним інструментом для автоматичного сканування вебсайтів на вразливості та забезпечення безпеки мережі. Він виявляє широкий спектр вразливостей, включаючи вразливості ОС, сервісів та додатків, які можуть бути використані зловмисниками.

- Burp Suite - це інтегрована платформа для тестування безпеки веб-додатків. Вона надає широкі можливості для сканування, аналізу та виявлення вразливостей веб-додатків, включаючи перехоплення трафіку, перевірку параметрів URL, атаки на сесії та багато іншого.

- Acunetix є потужним інструментом для автоматичного сканування веб-додатків на наявність вразливостей безпеки. Він виявляє широкий спектр атак, включаючи SQL-ін'єкції, XSS атаки, вразливості в аутентифікації та авторизації, ін'єкції коду та багато іншого.

- Nikto є відкритим інструментом для сканування веб-серверів на наявність вразливостей. Він спеціалізується на виявленні вразливостей конфігурації веб-сервера, таких як налаштування аутентифікації, директорії перегляду та інші потенційні проблеми безпеки.

Ці інструменти отримали визнання у галузі кібербезпеки та активно використовуються для автоматичної перевірки безпеки вебсайтів, тому давайте детальніше розглянемо кожен із них.

OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) є відкритим (безкоштовним) інструментом для тестування безпеки веб-додатків [5].

Він розроблений спільнотою проекту OWASP, яка працює над підвищенням безпеки веб-додатків шляхом розробки відкритого програмного забезпечення та розповсюдження знань про кібербезпеку.

OWASP ZAP надає можливість автоматичного сканування веб-додатків на наявність різних вразливостей та потенційних загроз безпеці. Його основні функції включають:

Сканування вразливостей: OWASP ZAP виявляє різноманітні вразливості, такі як SQL-ін'єкції, XSS атаки, CSRF-атаки, недостатні контролі авторизації,

недостатні контролі доступу до файлів та інші. Він аналізує веб-сторінки, форми, параметри URL, куки та інші складові веб-додатка для виявлення потенційних проблем безпеки.

Перехоплення трафіку: OWASP ZAP може перехоплювати трафік між браузером і сервером, що дозволяє аналізувати та модифікувати дані, що передаються. Це дозволяє виявляти і використовувати потенційні проблеми безпеки, такі як незашифрований обмін даними, небезпечні параметри запитів та інші.

Генерація звітів: OWASP ZAP надає зручні інструменти для створення детальних звітів про виявлені вразливості. Звіти містять інформацію про знайдені проблеми безпеки, рекомендації щодо виправлення та посилання на релевантні джерела знань для додаткової інформації.

Розширюваність: OWASP ZAP підтримує розширення та додатки, що дозволяють розширювати його функціональність та використовувати власні модулі аналізу та перевірки. Це дозволяє використовувати інструмент для специфічних потреб і вимог безпеки.

OWASP ZAP є безкоштовним інструментом з відкритим вихідним кодом, доступним для використання всім без обмежень. Його можна завантажити з офіційного вебсайту проекту OWASP. Оскільки OWASP ZAP є проектом з відкритим кодом, він не має платних версій та не вимагає плати за використання. Весь функціонал інструменту доступний користувачам безкоштовно.

OWASP ZAP є популярним інструментом в галузі тестування безпеки веб-додатків завдяки своїм функціональним можливостям, простоті використання та активній підтримці спільнотою проекту OWASP.

Nessus є одним з найпопулярніших інструментів для автоматичного сканування вебсайтів та забезпечення безпеки мережі. Розроблений компанією Tenable, Nessus надає можливість виявляти широкий спектр вразливостей, включаючи вразливості операційних систем, сервісів та додатків, які можуть бути використані зловмисниками [6].

Nessus має потужний сканер, який дозволяє автоматично перевіряти вебсайти на вразливості, використовуючи різні техніки, такі як активне сканування портів,

виявлення слабких паролів, перевірка на наявність вразливостей веб-додатків і багато іншого. Він також надає можливість аналізувати результати сканування, забезпечуючи детальну інформацію про виявлені вразливості та рекомендації щодо їх виправлення.

Що стосується вартості Nessus, то це комерційний продукт, який пропонується в різних варіантах ліцензування. Вартість Nessus залежить від потреб користувача та обсягу функціональності, який вони бажають отримати. Мінімальний план підписки буде коштувати 13.99$ в місяць.

Burp Suite є популярним інструментом для тестування на проникнення та веб-додатків. Він розроблений компанією PortSwigger і має широкий спектр функцій, які дозволяють виявляти вразливості веб-додатків, аналізувати трафік, модифікувати запити та багато іншого [7].

Burp Suite складається з декількох модулів, які працюють разом для забезпечення повноцінного тестування веб-додатків. Основні модулі включають:

- Proxy (проксі): Цей модуль дозволяє перехоплювати трафік між веб-браузером та цільовим веб-сервером. Користувач може переглядати, змінювати та повторювати запити, що надходять та відправляються, що дозволяє виявляти потенційні вразливості.
- Scanner (сканер): Цей модуль автоматично сканує веб-додатки на наявність різних типів вразливостей, включаючи SQL-ін'єкції, XSS-атаки, перехоплення сесій, недостатній контроль доступу та багато інших.
- Intruder (вторгнення): Цей модуль дозволяє здійснювати автоматизовані атаки на веб-додатки, включаючи перебор паролів, фазування параметрів та введення власних даних для виявлення вразливостей.
- Repeater (повторювач): Цей модуль дозволяє повторно відправляти і змінювати запити до сервера, щоб перевірити реакцію веб-додатка на різні сценарії та виявити вразливості.

Burp Suite доступний у двох версіях: Community Edition та Professional Edition. Community Edition - це безкоштовна версія Burp Suite, яка містить базовий набір функцій. Вона призначена для особистого використання та досліджень, але має обмежені можливості порівняно з Professional Edition.

Professional Edition: Це комерційна версія Burp Suite, яка надає розширений функціонал та інструменти для професіонального тестування на проникнення. Ціна на Professional Edition варіюється залежно від типу ліцензії та обсягу функціональності. Мінімальна підписка буде коштувати 449$ в рік, тобто 37$ в місяць.

Acunetix є відомим інструментом для автоматичного тестування на проникнення веб-додатків. Він розроблений компанією Acunetix Ltd. і має потужний набір функцій для виявлення вразливостей в веб-додатках та забезпечення їх безпеки:

- Сканування вразливостей: Acunetix автоматично сканує веб-додатки на наявність різних типів вразливостей, таких як SQL-ін'єкції, XSS-атаки, недостатні контролі доступу, перехоплення сесій, небезпечні конфігурації сервера та багато інших.
- Перевірка безпеки мережі: Acunetix також може проводити сканування безпеки мережі для виявлення вразливостей на рівні мережевих пристроїв, таких як маршрутизатори, комутатори, мережеві фаєри та інші.
- Виявлення вразливостей у веб-сервері: Acunetix допомагає виявляти вразливості, пов'язані з конфігурацією веб-сервера, такі як неправильні налаштування, небезпечні директорії, виток інформації та інші.
- Інтеграція з інструментами розробників: Acunetix підтримує інтеграцію з популярними інструментами розробників, такими як Jenkins, JIRA, GitHub та інші, що дозволяє автоматизувати процес виявлення та виправлення вразливостей.

Acunetix є комерційним інструментом, що означає, що він має платну ліцензію. Ціна на Acunetix залежить від типу ліцензії, обсягу функціональності та потреб користувача. Мінімальна ціна за сканування сайту 4495$ [8].

Nikto - це відкрите програмне забезпечення, призначене для автоматичного сканування веб-серверів з метою виявлення потенційних вразливостей. Він розроблений з використанням мови Perl і має простий у використанні інтерфейс командного рядка [9].

Основні функції та можливості Nikto включають:

- Сканування вразливостей: Nikto сканує веб-сервери на наявність різних типів вразливостей, включаючи недостатні контролі доступу, виток інформації, потенційні проблеми безпеки на рівні конфігурації сервера та багато інших.
- Виявлення прихованих файлів та директорій: Nikto шукає приховані файли та директорії на веб-сервері, які можуть бути доступні несанкціонованим користувачам.
- Аналіз конфігурації сервера: Nikto перевіряє налаштування веб-сервера на наявність потенційних проблем безпеки, таких як використання застарілих версій програмного забезпечення, відключений контроль доступу до файлів тощо.
- Розширені налаштування: Nikto надає користувачу можливість настроювати параметри сканування, включаючи обмеження швидкості, ігнорування певних вразливостей або файлів, вказівку кастомних заголовків тощо.

Nikto є безкоштовним програмним забезпеченням з відкритим вихідним кодом, доступним на умовах ліцензії GNU General Public License (GPL). Це означає, що його можна використовувати, змінювати та поширювати Nikto безкоштовно.

Автоматична перевірка вебсайтів є важливим етапом технічної оцінки захищеності. Вона допомагає виявити широко поширені та відомі вразливості, а також швидко просканувати великі об'єми коду. Однак, комбінація автоматичної та ручної перевірки є оптимальним підходом для отримання більш повної та точної оцінки захищеності вебсайту.

2.2 Ручна перевірка

Ручна перевірка вебсайту є важливим етапом у процесі оцінки та забезпечення безпеки веб-додатків. Вона виконується спеціалістами з кібербезпеки, які проводять детальний аналіз коду, функцій та структури вебсайту з метою виявлення потенційних вразливостей та інших проблем безпеки. Основними метою ручної перевірки є ідентифікація слабких місць, які можуть бути

пропущені автоматизованими інструментами, а також оцінка загроз та ризиків, що виникають з використання веб-додатку.

Процес ручної перевірки вебсайту включає наступні кроки:

- Аналіз коду: Спеціалісти з кібербезпеки переглядають вихідний код веб-додатку з метою виявлення потенційних проблем безпеки, таких як вразливості вводу/виводу даних, недостатнє перевірка валідності вхідних даних, незахищені протоколи комунікації тощо.
- Перехоплення та аналіз трафіку: Спеціалісти використовують інструменти, які дозволяють перехоплювати та аналізувати трафік, що переходить між клієнтом та сервером. Це дозволяє виявити можливі проблеми безпеки, такі як вразливості міжсайтового скриптінгу (XSS), міжсайтового запросу (CSRF), витоки конфіденційної інформації тощо.
- Тестування авторизації та аутентифікації: Спеціалісти перевіряють механізми авторизації та аутентифікації веб-додатку, виявляючи можливі слабкі місця, які можуть дозволити несанкціонований доступ до облікових записів користувачів або обмежити їхню ефективність.
- Перевірка конфіденційності та захищеності даних: Спеціалісти перевіряють, як веб-додаток обробляє та зберігає конфіденційну інформацію користувачів, таку як паролі, особисті дані, фінансова інформація тощо. Вони переконуються, що дані належним чином шифруються, зберігаються у безпечному місці та пересилаються через захищені протоколи.
- Тестування зламу та проникнення: Спеціалісти можуть виконувати тестування зламу (hacking) та проникнення, щоб перевірити, наскільки веб-додаток вразливий до атак. Це дозволяє виявити можливі шляхи атаки, проникнення до системи та несанкціонований доступ до даних.

Ручна перевірка вебсайту є більш гнучким та спеціалізованим підходом, оскільки спеціалісти з кібербезпеки можуть виявляти складні та контекстуальні вразливості, які автоматизовані інструменти можуть пропустити. Проте вона вимагає додаткового часу та експертизи, а також може бути дорожчою у порівнянні з автоматизованими методами, тому давайте розглянемо кожен крок детальніше.

Аналіз коду є одним з ключових етапів перевірки безпеки вебсайту та використовується для виявлення потенційних вразливостей, помилок програмування та можливих проблем безпеки, які можуть бути використані зловмисниками для атак на веб-додаток.

Аналіз коду може виконуватись як автоматизовано, за допомогою спеціалізованих інструментів та сканерів, так і вручну, залучаючи експертів з кібербезпеки. Основна мета аналізу коду - перевірити, чи дотримуються найкращі практики програмування та безпеки, чи використовуються надійні механізми обробки вхідних даних та чи виявлені потенційні вразливості, такі як SQL-ін'єкції, XSS-атаки, доступ до неправомірних файлів та інші.

Під час автоматизованого аналізу коду використовуються спеціальні інструменти, які сканують вихідний код веб-додатку та виявляють потенційні вразливості. Ці інструменти можуть перевіряти дотримання стандартів безпеки, перевіряти правильність обробки вхідних даних, аналізувати логіку програми та виявляти можливі проблеми безпеки. Прикладами популярних інструментів для автоматичного аналізу коду є SonarQube, Fortify, Checkmarx та інші.

В ручному аналізі коду залучаються експерти з кібербезпеки, які ретельно досліджують вихідний код веб-додатку, перевіряють його структуру, логіку та можливі вразливості. Вони виявляють потенційні проблеми безпеки, які можуть бути пропущені автоматизованими інструментами. Ручний аналіз коду дозволяє виявити складні та специфічні вразливості, встановити контекстуальні зв'язки та оцінити загрози.

Аналіз коду має кілька переваг. Він дозволяє виявити вразливості, які не можуть бути виявлені автоматизованими засобами, та допомагає забезпечити високий рівень безпеки веб-додатку. Крім того, аналіз коду допомагає виявити помилки програмування, що можуть впливати на продуктивність та якість роботи вебсайту. Однак аналіз коду може бути часо- та ресурсомістким процесом, особливо при ручному аналізі, і вимагає спеціалізованих знань та досвіду в галузі кібербезпеки.

У підсумку, аналіз коду є важливим етапом перевірки безпеки вебсайту. Він доповнює автоматичну перевірку, дозволяючи виявити складні та специфічні

вразливості. Комбінація автоматизованого та ручного аналізу коду допомагає забезпечити надійний рівень безпеки та попередити можливі атаки на веб-додаток.

Перехоплення та аналіз трафіку є важливою складовою частиною перевірки безпеки вебсайту. Цей процес включає перехоплення та аналіз мережевого трафіку, що передається між клієнтами і серверами, з метою виявлення потенційних загроз та вразливостей.

Перехоплення трафіку може виконуватись за допомогою спеціалізованих інструментів, таких як проксі-сервери, сніфери (sniffers) або програмне забезпечення аналізу мережевого трафіку. Ці інструменти дозволяють отримувати доступ до мережевого трафіку, перехоплювати пакети даних, які передаються між клієнтами і серверами, та аналізувати їх.

Після перехоплення трафіку виконується аналіз отриманих даних. Мета аналізу трафіку полягає в виявленні потенційних загроз та вразливостей, таких як перехоплення аутентифікаційних даних, вразливості протоколів, нешифрований обмін конфіденційною інформацією та інше. Аналіз трафіку може включати перевірку наявності шифрування, валідацію вхідних даних, перевірку цілісності та достовірності даних, а також виявлення підозрілого або незвичного зв'язку.

Один із важливих аспектів аналізу трафіку - це виявлення атак "людина посередині" (Man-in-the-Middle, MitM), де зловмисник перехоплює і змінює комунікацію між двома сторонами без їхнього відома. Це може призвести до витоку конфіденційної інформації, включаючи облікові дані, номери кредитних карт та інші конфіденційні дані.

Інші види загроз, які можуть бути виявлені через перехоплення та аналіз трафіку, включають вразливості в протоколах, атаки на сесійні куки, маніпуляцію змістом веб-сторінок (наприклад, впровадження шкідливого JavaScript-коду) та багато іншого.

Для забезпечення безпеки вебсайту важливо регулярно проводити перехоплення та аналіз трафіку, особливо при передачі конфіденційної інформації, такої як облікові дані користувачів чи фінансові дані. Цей процес допомагає виявити потенційні загрози та вразливості та прийняти відповідні заходи для забезпечення безпеки та захисту вебсайту та його користувачів.

Тестування авторизації та аутентифікації є важливою частиною процесу перевірки безпеки вебсайту. Цей вид тестування спрямований на перевірку механізмів, які використовуються для ідентифікації та авторизації користувачів, з метою виявлення можливих вразливостей та викриття потенційних шляхів атак.

Аутентифікація - це процес перевірки, що користувач, який намагається отримати доступ до системи або ресурсів, є дійсною ідентичністю, яку він/вона стверджує бути. Авторизація - це процес надання визнання та дозволу користувачеві на доступ до конкретних ресурсів або функцій системи, після успішної аутентифікації.

Під час тестування авторизації та аутентифікації розглядаються різні аспекти, включаючи:

- Валідація введених даних: Перевірка, які дані вводяться під час процесу аутентифікації та авторизації, і чи здійснюється належна валідація цих даних. Недостатня або неправильна валідація може призвести до зламу системи.
- Складність паролів: Перевірка, які вимоги встановлені для паролів користувачів і які механізми захисту використовуються, такі як хешування та соління паролів. Слабкі паролі можуть бути легко вгадані або підібрані зловмисниками.
- Механізми сесій: Аналіз механізмів, що використовуються для керування сесіями, таких як сесійні ідентифікатори, тайм-аут сесій та валідація сесій. Недостатній захист сесій може призвести до крадіжки аутентифікаційних даних та несанкціонованого доступу до системи.
- Вимоги до прав доступу: Перевірка, які права доступу встановлені для різних ролей користувачів і які механізми контролю доступу використовуються. Неправильно налаштовані права доступу можуть призвести до неконтрольованого доступу до конфіденційних даних або виконання несанкціонованих операцій.
- Перевірка на перехоплення сесій: Тестування вразливостей, пов'язаних з перехопленням сесій, які можуть дозволити зловмиснику використовувати чужі сесійні ідентифікатори для отримання доступу до системи.

Існує багато інструментів та технік, які використовуються для тестування авторизації та аутентифікації, включаючи ручну перевірку, використання

спеціалізованих програм, наприклад, браузерних розширень та проксі-серверів. Під час тестування важливо враховувати різні сценарії, перевіряти вхідні та вихідні дані, проводити тестування на вразливості, такі як слабкі паролі, недостатню валідацію даних, недіючі механізми блокування та інші. Це допомагає виявити потенційні проблеми та рекомендувати вдосконалення механізмів авторизації та аутентифікації для покращення безпеки вебсайту.

Перевірка конфіденційності та захищеності даних є важливою складовою процесу тестування безпеки вебсайту. Цей вид тестування спрямований на перевірку механізмів, що використовуються для збереження та обробки конфіденційної інформації, з метою виявлення можливих вразливостей та захищеності даних від несанкціонованого доступу.

Під час перевірки конфіденційності та захищеності даних розглядаються різні аспекти, включаючи:

Шифрування даних: Перевірка, які механізми шифрування використовуються для захисту конфіденційних даних під час передачі або зберігання. Важливо перевірити правильне використання сильних алгоритмів шифрування та відповідне управління ключами.

Управління доступом: Аналіз механізмів, що використовуються для контролю доступу до конфіденційних даних. Перевірка належності доступу, рівнів привілеїв, аудиту доступу та застосування принципу найменшого привілею.

Захист від перехоплення даних: Тестування вразливостей, пов'язаних з перехопленням трафіку або витоком даних. Це включає перевірку наявності шифрування на протокольному рівні, захист від атак типу Man-in-the-Middle та застосування безпечних протоколів передачі даних.

Обробка помилок та виключних ситуацій: Перевірка, які механізми обробки помилок використовуються при роботі з конфіденційними даними. Важливо переконатися, що деталі помилок не розкривають неприпустиму інформацію або не викривають систему до атак.

Захищений зберігання даних: Оцінка механізмів збереження конфіденційних даних, включаючи захищені бази даних, шифровані сховища та механізми

хешування паролів. Важливо перевірити, чи використовуються належні методи для зберігання та захисту даних від несанкціонованого доступу.

Виток інформації: Аналіз системи на наявність можливих шляхів витоку конфіденційної інформації, включаючи некоректне виведення помилок, небезпечні налаштування, недостатні контролі та інші вразливості.

Для перевірки конфіденційності та захищеності даних використовуються різноманітні техніки, включаючи ручний аналіз коду, використання спеціалізованих інструментів сканування вразливостей, проведення тестування на проникнення та аудит безпеки. Це допомагає виявити потенційні проблеми та рекомендувати вдосконалення механізмів захисту даних для забезпечення конфіденційності та захищеності вебсайту.

Тестування зламу та проникнення (Penetration Testing або Pentesting) - це процес активного тестування безпеки вебсайту з метою виявлення потенційних вразливостей та інших слабких місць, що можуть бути використані для несанкціонованого доступу, зламу системи або викрадення даних.

Тестування зламу та проникнення передбачає моделювання атак зловмисників на вебсайт з метою виявлення і експлуатації вразливостей у реальному середовищі. Основна мета - виявити проблеми безпеки та надати організації рекомендації щодо покращення захисту.

Процес тестування зламу та проникнення може включати наступні етапи:

- Збір інформації: Збір даних про вебсайт, його архітектуру, розташування серверів, використовувані технології, доступні сервіси та інше. Це допомагає скласти карту сайту та визначити потенційні вразливі точки входу.
- Виявлення вразливостей: За допомогою спеціалізованих інструментів та ручного аналізу коду, перевірка вебсайту на наявність різних вразливостей, таких як SQL-ін'єкції, XSS-атаки, некоректне виведення помилок, недостатні контролі доступу, слабкі паролі та інші.
- Експлуатація вразливостей: Якщо виявлені вразливості, тестувальник може спробувати експлуатувати їх, використовуючи різні методи атак. Це може включати злам аутентифікації, отримання несанкціонованого доступу, модифікацію даних, перехоплення сесій та інше.

- Аналіз результатів: Оцінка впливу виявлених вразливостей на безпеку вебсайту та даних, виявлення можливих наслідків атак та рекомендації щодо виправлення проблем. Результати тестування документуються і передаються власнику вебсайту для подальшого вдосконалення системи безпеки.

Ціль ручної перевірки вебсайту полягає не тільки у виявленні вразливостей, але й у розумінні контексту веб-додатку, ідентифікації потенційних загроз та розробці індивідуальних стратегій захисту. Експерти з кібербезпеки можуть виявляти нові атаковані вектори та використовувати творчий підхід для імітації атак, які важко автоматизувати.

Під час ручної перевірки вебсайту, спеціалісти з кібербезпеки можуть використовувати різноманітні інструменти, наприклад, проксі-сервери, перехоплення трафіку, розширення браузера та інші, для аналізу та маніпуляції взаємодії з веб-додатком. Це дозволяє їм досліджувати вразливості, проводити злочинні сценарії та оцінювати рівень захищеності.

Крім того, ручна перевірка вебсайту доповнює автоматичні методи тестування, оскільки експерти можуть зосередитись на унікальних аспектах веб-додатку, які не можуть бути виявлені автоматичними інструментами. Вони можуть проводити аналіз дизайну, перевіряти правильність конфігурації, а також перевіряти дієвість запроваджених заходів безпеки.

Щодо вартості ручної перевірки вебсайту, вона може бути значно вищою, порівняно з автоматичними методами, через необхідність висококваліфікованих фахівців та більш тривалу роботу. Вартість ручної перевірки може варіюватися в залежності від складності веб-додатку, його розміру та інших факторів. Зазвичай ціни формуються на основі годинної ставки або проектної оцінки, і можуть бути різними для кожної компанії або експерта з кібербезпеки.

Ручна перевірка вебсайту є необхідною складовою процесу забезпечення безпеки. Вона доповнює автоматичні методи, дозволяючи виявити складні та контекстуальні вразливості, оцінити рівень захищеності та розробити індивідуальні стратегії захисту. Це важлива інвестиція, яка допомагає попередити серйозні наслідки внаслідок атак та забезпечити надійний рівень безпеки веб-додатку.

2.3 Вибір методу перевірки захищеності сайту

При виборі методу перевірки захищеності вебсайту Vandal Академії, необхідно враховувати переваги та обмеження автоматичного та ручного методів. Обидва підходи мають свої особливості та можуть бути використані в комбінації для досягнення більш повного огляду безпеки вебсайту.

Переваги автоматичного методу перевірки захищеності сайту:

- Ефективність та швидкість: Автоматичні інструменти дозволяють проводити швидке сканування великих обсягів коду та ідентифікувати поширені вразливості, що дозволяє економити час та ресурси.
- Покриття: Автоматичні інструменти можуть просканувати широкий спектр вразливостей та загроз безпеки, включаючи SQL-ін'єкції, XSS-атаки, недостатні контролі доступу та інші. Це дозволяє швидко виявити загрози та вразливості, які можуть бути пропущені при ручному аналізі.
- Легкість використання: Багато автоматичних інструментів мають інтуїтивно зрозумілий інтерфейс та можуть бути використані навіть без глибоких знань у сфері кібербезпеки.

Переваги ручного методу перевірки захищеності сайту:

- Глибокий аналіз: Ручна перевірка дозволяє провести більш детальний аналіз коду, структури та компонентів вебсайту, виявити складні та специфічні вразливості, які можуть бути пропущені автоматичними інструментами.
- Контекстуальний аналіз: Ручний підхід дозволяє спеціалістам з кібербезпеки більш глибоко зрозуміти контекст вебсайту, його функціональність, потенційні загрози та специфічні вразливості, що дозволяє забезпечити більш точну оцінку загроз. Автоматичний метод перевірки захищеності сайту є ефективним для швидкого виявлення поширених загроз та вразливостей, тому кваліфікаційна робота бакалавра буде включати автоматичну перевірку захисту вебсайту Vandal Академії.

3 ТЕХНІЧНА ОЦІНКА ЗАХИЩЕНОСТІ ВЕБСАЙТУ VANDAL АКАДЕМІЇ

3.1 Опис вебсайту та його основних функцій

Компанія VandalVape заснована в 2015 році, спочатку як магазин не продуктових товарів, а саме, електронних сигарет. Компанія росла, а разом з нею сформувався IT-відділ, який займався створенням веб-додатків та їх підтримкою. На даний момент, надає повний спектр послуг з веб-розробки, включаючи розробку з нуля, редизайн і покращення наявних сайтів, створення електронних магазинів, корпоративних порталів, лендінгів та інших типів веб-додатків. Vandal Vape працює з різними технологіями та веб-фреймворками, щоб забезпечити найкращі рішення для клієнтів. Одним з таких сайтів, який компанія використовує сама, є Vandal Академія.

Vandal Академія є вебсайтом компанії VandalVape, який служить для навчання нових працівників компанії. Основною метою вебсайту є підготовка та навчання нових співробітників для подальшої роботи в компанії VandalVape.

Основні функції вебсайту Vandal Академії включають:

- Реєстрація нових працівників: Після проходження співбесіди з hr-менеджером, нові працівники можуть зареєструватись на вебсайті Vandal Академії, використовуючи свою електронну пошту або номер телефону.
- Курси та навчальні листи: Вебсайт надає доступ до різних курсів та навчальних листів. Нові співробітники можуть переглядати навчальні матеріали, включаючи текстові листи та відеоуроки.
- Тести та відповіді: Після кожного навчального листа розміщені тести, які нові працівники повинні пройти. Тести можуть містити як закриті запитання, так і відкриті відповіді, на які співробітник повинен відповісти.
- Кураторські функції: Куратори, які відповідають за навчання нових працівників, мають особливі привілеї. Вони можуть надавати доступ до курсів та навчальних листів, створювати, редагувати та видаляти навчальні матеріали.
- Перевірка відповідей та оцінювання: Куратори мають можливість переглядати відповіді нових співробітників та оцінювати їх проходження курсів.

Вони можуть приймати або відхиляти проходження уроків залежно від якості відповідей.

- Профіль користувача: Кожен користувач має свій особистий профіль, де він може переглядати свій навчальний прогрес, досягнення та отримані оцінки. Це дозволяє кожному користувачеві відстежувати свої успіхи та вдосконалювати свої навички.
- Комунікація та співпраця: Вебсайт надає можливості для комунікації між співробітниками та кураторами. Користувачі можуть обмінюватись повідомленнями, задавати питання та отримувати відповіді, співпрацювати над проектами та ділитись знаннями.

Цільова аудиторія вебсайту Vandal Академії включає:

- Нових співробітників: Вебсайт призначений для навчання нових співробітників компанії VandalVape. Вони можуть використовувати ресурси сайту для отримання необхідних знань і навичок для роботи в компанії.
- HR-менеджерів: HR-менеджери компанії VandalVape відповідають за навчання нових працівників та мають доступ до кураторських функцій на вебсайті.
- IT відділ: IT відділ компанії VandalVape відповідає за моніторинг та покращення вебсайту Vandal Академії, забезпечуючи його безпеку та функціональність.

3.2 Аналіз потенційних загроз та вразливостей

Вебсайт Vandal Академії може стикатися з різними видами загроз, які можуть впливати на його безпеку та надійність. Загрози можуть виникати з різних джерел, ось декілька категорій зацікавлених осіб та загроз:

- Зловмисники - особи або групи, які намагаються незаконно отримати доступ до вебсайту, вкрасти конфіденційну інформацію, спотворити або зруйнувати дані, використати сайт для зловживань або встановити шкідливе програмне забезпечення.

- Конкуренти або недоброзичливі сторони - інші компанії або особи можуть мати інтерес у завданні шкоди бізнесу або вебсайту, зокрема шляхом зламу, спаму, відмови в обслуговуванні або інших злочинних дій.
- Внутрішні загрози - можуть виникати зсередини організації, від співробітників або колишніх співробітників, які мають несанкціонований доступ або зловживають своїми привілеями.
- Вразливості програмного забезпечення - якщо вебсайт використовує різні програмні рішення, наявність вразливостей в цьому програмному забезпеченні може стати причиною атак і зламів.
- Соціальна інженерія - зловмисники можуть намагатися отримати доступ до вебсайту, використовуючи методи маніпулювання або обманування людей, які мають доступ до системи, наприклад, через фішингові атаки, шахрайство з використанням електронної пошти або соціальні мережі.

Ось деякі види загрози, які можуть бути актуальними для Vandal Академії:

- Атаки злому аутентифікації: Зловмисники можуть намагатися зламати аутентифікаційні механізми Vandal Академії, спробуючи вгадати або підбирати паролі, використовуючи методи, такі як брутфорс або словники паролів. Якщо успішно, це може дозволити їм отримати несанкціонований доступ до системи.
- Між сайтовий скриптинг (XSS): Ця загроза полягає у вбудовуванні зловмисного скрипту на веб-сторінці Vandal Академії, який може використовувати браузер користувача для виконання шкідливих дій, таких як крадіжка сесійних файлів або виконання дій в ім'я користувача.
- Фішингові атаки: Зловмисники можуть спробувати використовувати методи соціальної інженерії для обману користувачів Vandal Академії і отримання їхніх особистих даних, таких як ім'я, пароль або фінансова інформація.
- Атака на відмову в обслуговуванні (DoS) або розподілена атака на відмову в обслуговуванні (DDoS) атаки: У цих атаках зловмисники перевантажують сервер Vandal Академії або мережеві ресурси, надсилаючи велику кількість запитів або використовуючи ботів для залучення багатьох комп'ютерів до атаки. Це може призвести до перебоїв у роботі сайту або його повного відключення для користувачів.

3.3 Проведення тестування безпеки та аналіз результатів

Першим методом тестування захищеності вебсайту Vandal Академії є OWASP ZAP. Тестування проводилось в attack mode (див.рис. 3.3.1).

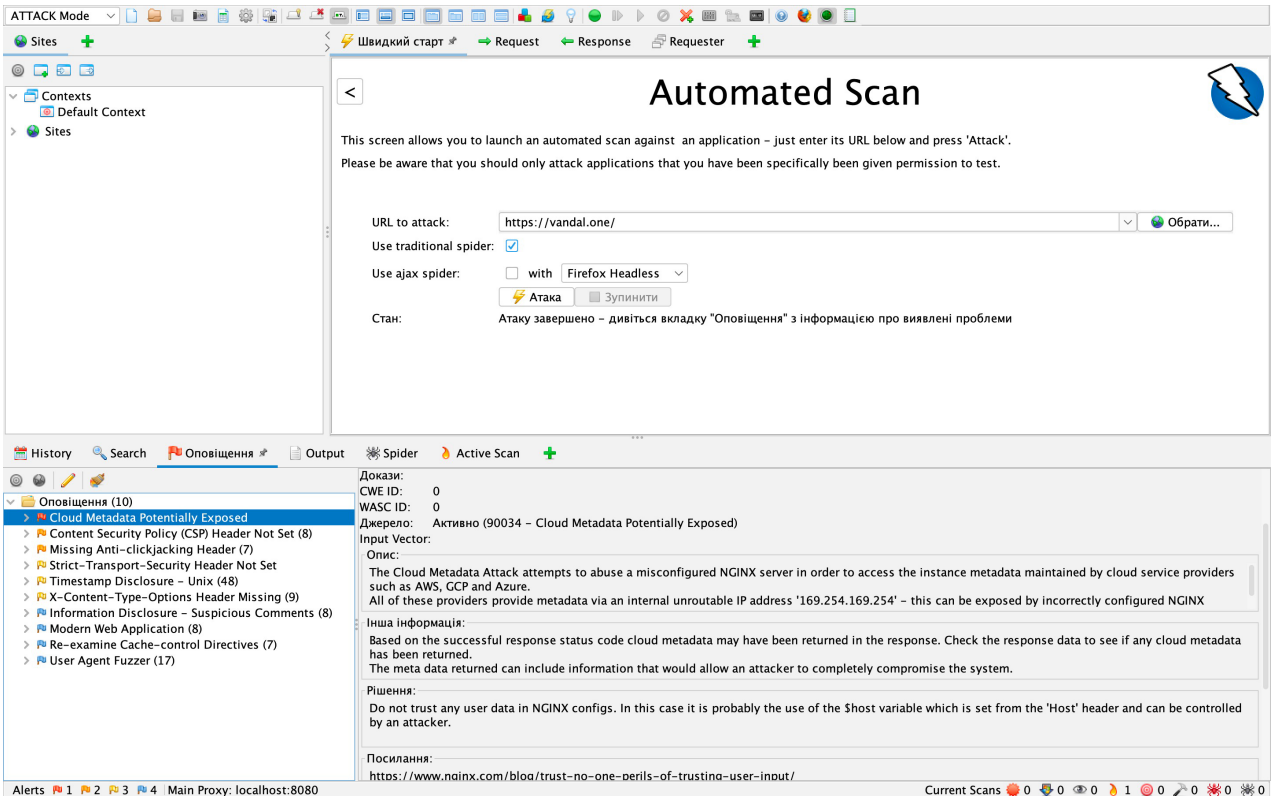

Рисунок 3.3.1 – Результат тестування OWASP ZAP

У результаті тестування виявлено десять загроз, вони виведені в лівій нижній частині програми.

У програмі OWASP ZAP кольори прапорців загроз сайту використовуються для позначення рівня серйозності і типу виявлених потенційних загроз безпеці. Основні кольори прапорців загроз і їх значення в ZAP такі:

Червоний прапорець: показує критичні потенційні загрози безпеці, які варто негайно виправити. Це можуть бути уразливості, що дозволяють зловмисникам отримати повний контроль над системою або компрометувати дані.

Помаранчевий прапорець: позначає серйозні потенційні загрози безпеці, які варто виправити. Це можуть бути уразливості, що дозволяють здійснювати обмежений доступ або отримувати обмежену інформацію.

Жовтий прапорець: вказує на помірні потенційні загрози безпеці, які можуть потребувати додаткової перевірки та виправлення.

Синій прапорець: позначає інформативні повідомлення, які не є загрозами безпеці, але містять корисну інформацію про конфігурацію, налаштування або структуру веб-додатка.

Ці кольорові прапорці допомагають визначити та розставити за пріоритетом виявлені потенційні загрози безпеки у веб-додатку.

У результаті тестування були виявлені такі загрози:

Cloud Metadata Potentially Exposed (червоний прапорець) - атака на метадані хмари спрямована на зловживання неправильно налаштованим сервером NGINX з метою доступу до метаданих екземпляра, які зберігаються провайдерами хмарних сервісів, такими як AWS, GCP та Azure. Усі ці провайдери надають метадані за допомогою внутрішньої непереносної IP-адреси "169.254.169.254". Ця адреса може бути розкрита через неправильно налаштовані сервери NGINX та отримана за допомогою цієї IP-адреси в полі заголовка "Host".

Content Security Policy (CSP) Header Not Set (8) (помаранчевий прапорець) – не встановлений заголовок CSP. Content Security Policy (CSP) це додатковий рівень безпеки, який допомагає виявляти та запобігати певним видам атак, включаючи міжсайтовий скриптинг (XSS) та атаки ін'єкції даних. Ці атаки використовуються для викрадення даних, дефейсу вебсайтів або поширення шкідливого програмного забезпечення. CSP надає набір стандартних заголовків HTTP, які дозволяють власникам вебсайтів визначити джерела затвердженого вмісту, який браузери можуть завантажувати на цій сторінці. Серед типів вмісту, які можуть бути охоплені, є JavaScript, CSS, HTML-фрейми, шрифти, зображення та вкладені об'єкти, такі як Java аплети, ActiveX, аудіо- та відеофайли. Дана загроза знайдена у вісьмьох місцях.

Missing Anti-clickjacking Header (7) (помаранчевий прапорець) - у відповіді відсутній заголовок Content-Security-Policy з директивою 'frame-ancestors' або X-Frame-Options для захисту від атак типу захоплення кліка (ClickJacking).

Strict-Transport-Security Header Not Set (жовтий прапорець) - не встановлений заголовок HSTS. HTTP Strict Transport Security (HSTS) - це механізм

політики безпеки веб-сервера, при якому веб-сервер заявляє, що взаємодія відповідних користувацьких агентів (наприклад, веб-браузерів) з ним повинна відбуватися тільки через безпечне з'єднання HTTPS (тобто HTTP, що використовується разом з TLS/SSL). HSTS є протоколом, що входить до стандартів IETF, і його специфікація описана в RFC 6797.

Timestamp Disclosure (жовтий прапорець) - часова мітка була розкрита додатком або веб-сервером - Unix.

X-Content-Type-Options Header Missing (жовтий прапорець) - заголовок X-Content-Type-Options з атрибутом 'nosniff' не був встановлений. Це дозволяє старим версіям Internet Explorer і Chrome виконувати MIME-пошук на тілі відповіді, що потенційно може спричинити тлумачення тіла відповіді та його відображення як контенту іншого типу, ніж заявлений тип контенту. Старі версії Firefox будуть використовувати заявлений тип контенту (якщо він встановлений), а не виконувати MIME-пошук. Ця проблема так само стосується сторінок з помилками (401, 403, 500 і т. д.), оскільки такі сторінки часто також можуть бути підтверджені проблемам ін'єкції, що може спричинити те, що браузери будуть тлумачити сторінки як контент іншого типу, ніж фактичний тип контенту.

Information Disclosure - Suspicious Comments (синій прапорець) - відповідь містить підозрілі коментарі, які можуть допомогти зловмиснику.

Re-examine Cache-control Directives (синій прапорець) - заголовок "cache-control" не встановлено належним чином або відсутній, що дозволяє браузеру та проксі-серверам кешувати не тільки статичні ресурси.

Другий метод тестування захищеності вебсайту Vandal Академії є Vega Scanner
(див.рис. 3.3.2).

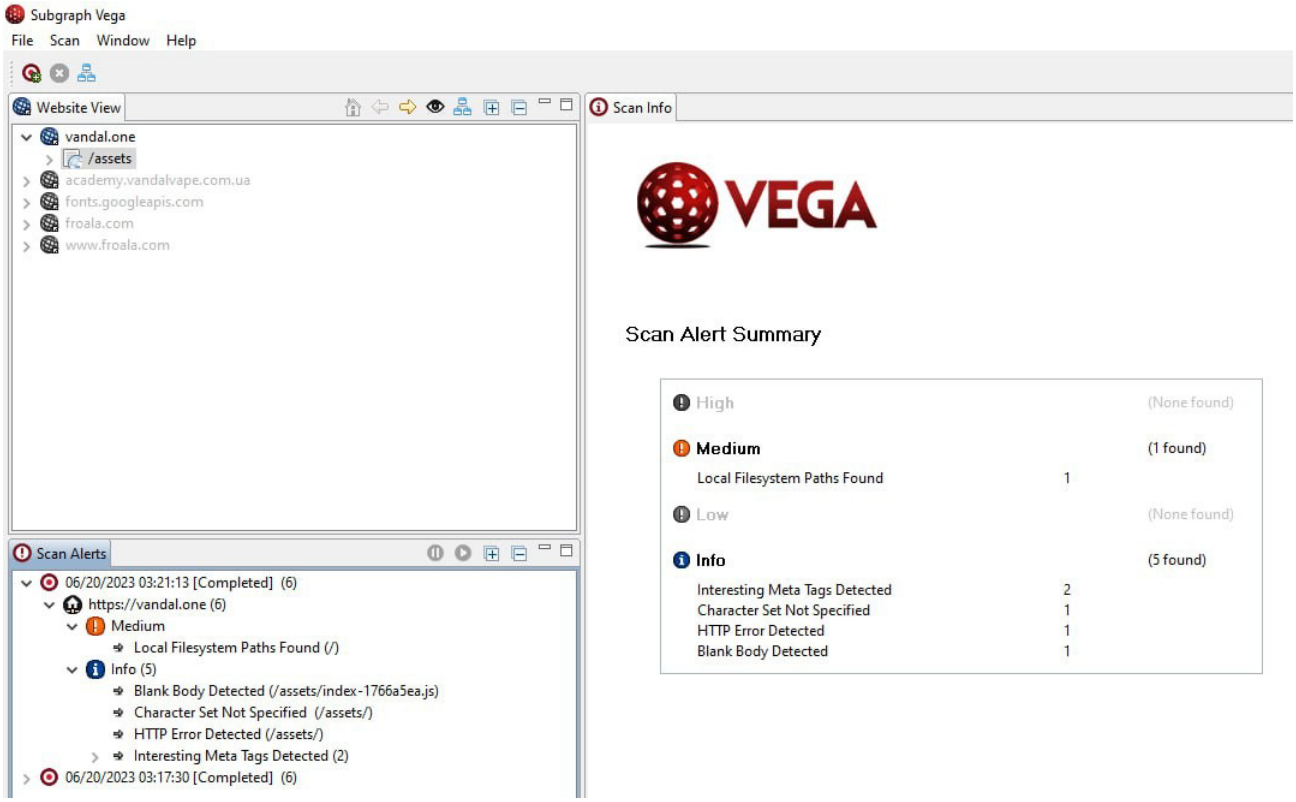

Рисунок 3.3.2 – Результат тестування Vega Scanner

Vega Scanner знайшла менше вразливостей, ніж OWASP ZAP. "Local filesystem paths found" від сканера Vega означає, що під час сканування були знайдені посилання або посилання на локальні системні файли. Це може вказувати на потенційну проблему безпеки або некоректну конфігурацію вебсайту. Знайдення шляхів до локальних файлів може бути небезпечним, оскільки це може витікати конфіденційну інформацію або дозволяти зловмиснику отримати доступ до файлів на сервері.

Повідомлення "Blank node detected" від сканера Vega означає, що під час сканування було виявлено пустий вузол (blank node). Це може вказувати на проблему безпеки або некоректну структуру вебсайту. У семантичних мережах або RDF (Resource Description Framework) пустий вузол (blank node) є вузлом, який не має унікального ідентифікатора або URI. Це може вказувати на некоректне використання або відсутність визначення вузлів у структурі даних вебсайту.

Character set not specified - значає, що під час сканування не було вказано кодування символів (character set) для веб-сторінок. Це може вказувати на відсутність або некоректну конфігурацію кодування символів на вебсайті.

HTTP error detected - під час сканування було виявлено помилку HTTP. Це вказує на проблему або неправильну відповідь сервера під час взаємодії з певними запитами.

Повідомлення "Interesting meta tags detected" від сканера Vega означає, що під час сканування були виявлені цікаві мета-теги на веб-сторінках. Це може вказувати на наявність додаткової інформації або конфігураційних параметрів, які можуть бути цікавими з точки зору безпеки або аналізу вашого веб-сайту. Мета-теги є частинами HTML-коду веб-сторінки, які надають додаткову інформацію про сторінку, таку як метадані, опис, автор, ключові слова та інше. Цікаві мета-теги можуть містити інформацію, яка може бути використана зловмисниками для аналізу веб-сайту або знайдення потенційних вразливостей.

Nessus – третій метод тестування захищеності вебсайту Vandal Академії (див.рис. 3.3.3).

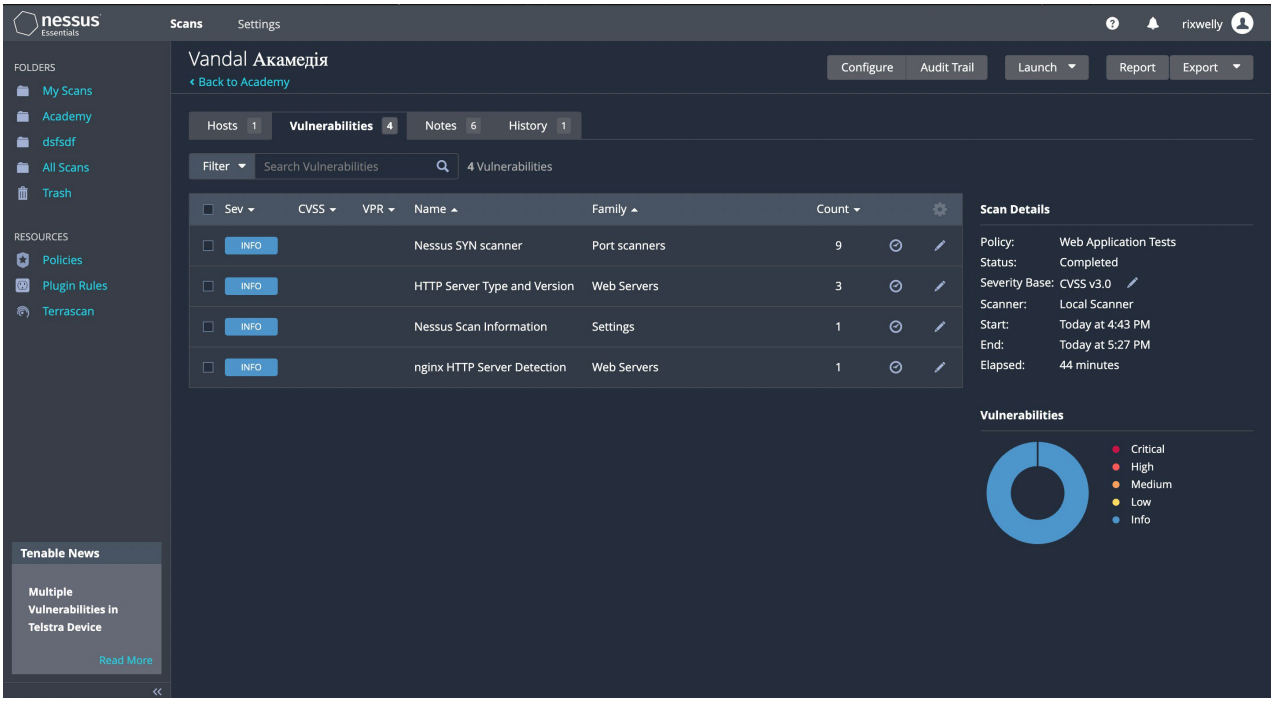

Рисунок 3.3.3 – Результат тестування Nessus

При тестуванні сайту застосунком Nessus не було виявлено критичних загроз. Детальніші результати тесту:

- Nginx HTTP Server Detection - Nessus зміг виявити веб-сервер NGINX, переглянувши HTTP-банер на віддаленому хості.

- HTTP Server Type and Version - значає, що Nessus зміг визначити тип веб-сервера, який використовується на вказаному веб-сайті, а також його версію.
- Nessus SYN scanner – виявив відкриті порти на веб-сервері.
- Nessus Scan Information виводить загальну інформацію про результати сканування (див.рис. 3.3.4)

Output

```
Information about this scan :

Nessus version : 10.5.2
Nessus build : 20009
Plugin feed version : 202306201003
Scanner edition used : Nessus Home
Scanner OS : DARWIN
Scanner distribution : macosx
Scan type : Normal
Scan name : Vandal Акамедія
Scan policy used : Web Application Tests
Scanner IP : 192.168.1.220
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 36.629 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2023/6/20 16:43 EEST
Scan duration : 2640 sec
Scan for malware : no
less...
```

Рисунок 3.3.4 – Загальна інформація про сканування

3.4 Рекомендації щодо поліпшення захисту

На основі аналізу тестування безпеки, вебсайту Vandal Академії рекомендується:

- Не довіряти жодній користувацькій інформації в конфігураціях NGINX. У випадку з тесту змінній $host, яка встановлюється з заголовка 'Host' і може бути контрольована зловмисником.
- Переконатись, що веб-сервер сервер застосунків, балансувальник навантаження та інші компоненти налаштовані для встановлення заголовка Content-Security-Policy з метою оптимальної підтримки браузерів: Chrome 25+, Firefox 23+ та Safari 7+, "X-Content-Security-Policy" для Firefox 4.0+ та Internet Explorer 10+, і "X-WebKit-CSP" для Chrome 14+ та Safari 6+.
- Переконатись, що заголовок HTTP Content-Security-Policy або X-Frame-Options встановлено на всіх веб-сторінках, які повертає вебсайт.
- Перевірити чи веб-сервер, сервер застосунків, балансувальник навантаження та інші компоненти налаштовані для використання Strict-Transport-Security (STS) забезпечення.
- Вручну перевірити чи мітки часу не є динамічними і дані не можуть бути агреговані для розкриття експлуатованих шаблонів. Це означає, що потрібно перевірити, чи не містять дані мітки часу конфіденційної або приватної інформації, такої як особисті дані, паролі, фінансові дані тощо. Також переконатись, що немає можливості агрегування цих даних для виявлення шаблонів або вразливостей, які можуть бути використані зловмисниками. Це можна зробити шляхом аналізу типів даних, які зберігаються в мітках часу, та переконавшись, що немає інформації, яка може бути використана для ідентифікації або використана в шкідливих цілях. Також слід перевірити, чи вжиті заходи для забезпечення анонімності та безпеки даних мітки часу.
- Переконатись, що програма/веб-сервер належним чином встановлює заголовок Content-Type і встановлює заголовок X-Content-Type-Options зі значенням "nosniff" для всіх веб-сторінок, вказує браузеру, який тип контенту передається.

- Видалити всі коментарі, які містять інформацію, яка може допомогти зловмиснику, виправити проблеми, на які вони посилаються.

- Переконатись, що встановлений заголовок HTTP cache-control зі значенням "no-cache, no-store, must-revalidate". Якщо актив повинен бути закешованим, розглянути встановлення директив "public, max-age, immutable". Ці налаштування допоможуть забезпечити належне управління кешуванням та зберегти безпеку контенту на вебсайті.

Додаткові поради: встановити двофакторну аутентифікацію для додаткового рівня безпеки, регулярно оновлювати програмне забезпечення, плагіни та додатки вебсайту, щоб виправити вразливості, які можуть бути використані зловмисниками, заохочувати студентів встановлювати сильні, унікальні паролі, регулярно їх оновлювати.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при обмороженні

Обмороження - це травма, яка виникає через дію низької температури на тканини тіла. Обмороження вражає різні частини тіла, особливо ноги, руки, вуха, ніс та губи. Це стан потребує швидкої долікарської допомоги.

Перша допомога при обмороженні включає наступні етапи:

- укриття від холоду: перше, що треба зробити, це негайно віддалити людину від холодового оточення, щоб запобігти подальшому зниженню температури тіла;
- зігрівання: для зігрівання тканин, які піддавалися впливу холоду, потрібно використовувати теплу, але не гарячу воду (від 37°C до 42°C). Важливо пам'ятати, що гаряча вода або відкритий вогонь спричиняють подальші ушкодження тканини. Потрібно уникати активного тертя або масажу області обмороження, оскільки це спричинить додаткове ушкодження тканин;
- медична допомога: навіть якщо перша допомога була надана вчасно і правильно, важливо звернутися до медичного працівника для оцінки та подальшого лікування. Обмороження може мати серйозні ускладнення, включаючи інфекції і некроз тканин;
- анальгетики: біль під час обмороження є сильним, особливо під час процесу зігрівання. Застосування безрецептурних анальгетиків, таких як парацетамол або ібупрофен, допомогає зменшити біль;
- тимчасове знерухомлення: ушкоджену ділянку потрібно тримати якомога нерухомою, щоб запобігти подальшому ушкодженню тканин. Наприклад, використати шарф для фіксації обмороженої руки;
- обезводнення: жертва обмороження може відчувати обезводнення, тому необхідно вживати достатньо рідини. Однак алкоголь та кава сприяють втраті тепла, тому не потрібно їх вживати.

Обмороження класифікуються за ступенем важкості. Важливо розуміти ці відмінності, щоб визначити найкращий план дій:

- обмороження першого ступеня: при обмороженні першого ступеня шкіра стає блідою, білою або жовтою. Часто супроводжується болем, свербінням або поколюванням. Після зігрівання може з’явитися червоний висип;
- обмороження другого ступеня: при обмороженні другого ступеня, шкіра стає темно-червоною або синюватою, з появою пухирів, наповнених прозорою або мутною рідиною. Це стан вимагає негайного медичного втручання;
- обмороження третього і четвертого ступеня: це найсерйозніші стадії обмороження, які вражають глибокі шари шкіри, м'язи, нерви та навіть кістки. Шкіра стає темно-синьою або чорною. Це вимагає негайного госпіталізації;

При важких випадках обмороження, перша допомога є недостатньою, і потребуються негайні медичні втручання, тому потрібно якнайшвидше викликати швидку допомогу. Після того, як особа отримала першу медичну допомогу, її госпіталізують для подальшого лікування, включаючи антибіотики для запобігання інфекціям, біль знижують препарати та іноді, хірургічне втручання.

При обмороження не можна:

- використовувати гарячу воду, відкритий вогонь, грілки або опалювальні пристрої для прогрівання обморожених ділянок, оскільки вони спричиняють опіки;
- розтирати обморожену шкіру;
- робити масаж обморожених ділянок;
- використовувати пряму теплоту до обмороженої ділянки тіла, поки медична допомога не прибуде;
- проколювати пухирі, які утворилися внаслідок обмороження;
- жертва обмороження має уникати куріння та алкоголю, оскільки вони знижують кровообіг та загрожують процесу відновлення.

Слід врахувати, що швидкість і ефективність першої допомоги при обмороженні суттєво впливають на процес відновлення та здоров'я потерпілого. Чим швидше буде надана допомога медичних спеціалістів, тим кращі шанси на повне відновлення.

4.2 Санітарно-гігієнічні вимоги до умов праці в офісі

Санітарно-гігієнічні вимоги до умов праці в офісі мають на меті забезпечення комфорту та безпеки працівників, зниження рівня стресу і покращення продуктивності. Вони включають ряд різноманітних аспектів роботи, від освітлення і температури до вологості та рівня шуму. Основні вимоги до санітарно-гігієнічних умов:

- освітлення: освітлення в офісі є достатнім, щоб працівники могли виконувати свої обов'язки без напруження очей. Застосування природного світла має бути оптимізоване, але також передбачені додаткові джерела світла для роботи в темний час доби або в хмарну погоду. Штучне освітлення приміщення має бути обладнане системою загального рівномірного освітлення. Забороняється застосування світильників без розсіювачів та екрануючих сіток. Рівень освітленості на робочому столі має бути в межах 300 – 500 лк;
- температура та вологість: температура в офісі є комфортною для праці (22 – 25 °С), а вологість знаходитися в межах 40-60%, швидкість руху повітря – не більше 0,1 м/с. Ці умови потребують використання кондиціонерів, обігрівачів або зволожувачів повітря;
- ергономіка: меблі та обладнання є ергономічними, щоб запобігти розвитку професійних захворювань, таких як синдром зап’ясткового каналу або проблеми з хребтом. Це означає, що стільці, столи та інше обладнання налаштовані так, щоб працівники могли сидіти або стояти у правильному положенні;
- вентиляція: офісні приміщення достатньо вентильовані, щоб забезпечити свіже повітря і відвести забруднене повітря;
- рівень шуму: рівень шуму є контрольованим (не перевищує 65 дБа), щоб не відволікати працівників від їх обов'язків і не спричиняти стресу. Заходи, такі як використання шумоізоляції або навушників, є корисними для працівників;
- санітарні умови: туалети та кухонні приміщення є чистими та відповідають санітарним нормам. Працівники мають доступ до достатньої кількості питної води;

- контроль за випромінюванням: в офісах, де використовується багато електронного обладнання, важливо контролювати рівні електромагнітного випромінювання, щоб вони були в межах безпечних норм;
- пожежна безпека: офіси обладнані належними засобами пожежогасіння, такими як вогнегасники та автоматичні системи пожежогасіння. Також важливою є розробка та проведення навчання з пожежної безпеки, щоб працівники знали, що робити у випадку пожежі;
- психологічна атмосфера: забезпечення здорової психологічної атмосфери на робочому місці є не менш важливим для забезпечення здоров'я та продуктивності працівників. Включаючи такі заходи, як регулярні перерви на відпочинок, заохочення здорового способу життя, надання психологічної підтримки та вирішення конфліктів на робочому місці;
- чистота та порядок: робочі місця є чистими, а все обладнання та матеріали - організовані і легко доступні. Це не тільки підвищує продуктивність, але також зменшує ризик нещасних випадків;
- регулярні медичні обстеження: регулярні медичні обстеження допомогають виявити та запобігти професійні захворювання. Роботодавці організовувють такі обстеження для своїх працівників;
- обов'язкові перерви та відпустки: щоб запобігти перевтомі та професійному вигоранню, важливо, щоб працівники регулярно робили перерви протягом дня та мали достатньо часу на відпочинок від роботи;
- надання першої допомоги: на робочому місці є набір для надання першої допомоги, а працівники навчені основам надання першої допомоги;
- безпека приміщень: при вході та виході, а також усередині офісу є відповідні заходи безпеки, включаючи вихідні двері для евакуації, відеоспостереження та безпекове освітлення;
- доступність: офісні приміщення є доступними для всіх працівників, включаючи людей з обмеженими можливостями. Це включає в себе наявність пандусів, підйомників та інших засобів для людей з фізичними обмеженнями.

Санітарно-гігієнічні вимоги до умов праці в офісі відіграють вирішальну роль у забезпеченні здорового та безпечного робочого середовища. Вони

включають широкий спектр аспектів, від контролю за вологістю та освітленням до психологічної атмосфери. Дотримання цих вимог не тільки забезпечує добробут працівників, але й сприяє підвищенню їхньої продуктивності та загальної ефективності організації.

ВИСНОВКИ

У першому розділі було розглянуто основні аспекти безпеки вебсайтів, включаючи найпоширеніші види атак, методи захисту та сучасні підходи до технічної оцінки захищеності вебсайтів. Було зроблено акцент на необхідності комплексного підходу до захисту вебсайтів, який об'єднує технічні, процедурні та освітні заходи.

У другому розділі описано автоматичний і ручний методи перевірки захищеності вебсайтів, їхні особливості, переваги та недоліки. Розглянуто найпопулярніші методи автоматичної перевірки захищеності вебсайтів та вразливості, які вони перевіряють. Описаний ручний метод перевірки, головні кроки
у ньому.

У третьому розділі проведений опис вебсайту Vandal Академії, його основних функцій. Досліджена технічна оцінка захищеності вебсайту, а саме: аналіз потенційних загроз, тестування безпеки та аналіз результатів, а також написані рекомендації щодо поліпшення захисту.

У четвертому розділі були розглянуті питання долікарської допомоги при обморожені та Санітарно-гігієнічні вимоги до умов праці в офісі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Які існують типи кібератак і загроз? [Електронний ресурс] – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack

2. 5 Найпоширеніших атак на веб-сайти [Електронний ресурс] – Режим доступу: https://www.websiterating.com/uk/online-security/most-common-website-attacks-how- to-defend-against-them/

3. Проведення ручного аудиту безпеки [Електронний ресурс] – Режим доступу: https://cybermolfar.io/services/it-security-audit/

4. Перевірка безпеки сайту: чек-лист [Електронний ресурс] – Режим доступу: https://www.ukraine.com.ua/uk/blog/hosting_ukraine/proverka-bezopasnosti-vashego-sajta-chek-list.html

5. OWASP ZAP Getting Started [Електронний ресурс] – Режим доступу: https://www.zaproxy.org/getting-started/

6. Tenable Nessus [Електронний ресурс] – Режим доступу: https://www.tenable.com/products/nessus

7. Burp Suite Community Edition [Електронний ресурс] – Режим доступу: https://portswigger.net/burp/communitydownload

8. Acunetix Vulnerability Scanner [Електронний ресурс] – Ресурс доступу: https://www.acunetix.com/vulnerability-scanner/

9. Features Nikto [Електронний ресурс] – Режим доступу: https://cirt.net/Nikto2