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

(повна назва факультету)

(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

(назва освітнього ступеня)

на тему:

Виконав(ла): студент(ка) _____ курсу, групи _____

спеціальності

(шифр і назва спеціальності)

(підпис) (прізвище та ініціали)

Керівник

(підпис) (прізвище та ініціали)

Нормоконтроль

(підпис) (прізвище та ініціали)

Завідувач кафедри

(підпис) (прізвище та ініціали)

Рецензент

(підпис) (прізвище та ініціали)

Тернопіль
20___

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

Факультет _____
(повна назва факультету)

Кафедра _____
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ _____
(підпис) (прізвище та ініціали)
« » 20___ р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня _____
(назва освітнього ступеня)

за спеціальністю _____
(шифр і назва спеціальності)

студенту _____
(прізвище, ім'я, по батькові)

1. Тема роботи _____

Керівник роботи _____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 20___ року № _____

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

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

АННОТАЦІЯ

Дослідження захищеності веб сервісу електронного навчання Atutor // Кваліфікаційна робота ОР «Бакалавр» // Слупський Богдан Васильович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // с. 66, рис. – 5, табл. – 3.

Метою даної роботи є системний аналіз та дослідження рівня безпеки та захисту веб-сервісу Atutor, який використовується для електронного навчання, виявлення потенційних вразливостей, оцінка ризиків, а також рекомендації та заходи щодо підвищення безпеки системи.

Об'єкт дослідження – Веб сервіс електронного навчання Atutor.

Предмет дослідження – дослідження захищеності веб сервісу електронного навчання Atutor з використання сканера вразливостей.

В кваліфікаційній роботі проведено аналіз системи електронного навчання Atutor, її функціональних можливостей та систем захисту, виконано класифікацію критичної інформації для оцінки впливу знайдених вразливостей на неї з надання рекомендації по їх усуненню та надано додаткові поради по зміцненню безпеки.

Результатом роботи є оцінка виявлених вразливостей з наданням рекомендацій щодо їх усунення.

Для реалізації даної роботи були використані такі програмні продукти: Acunetix.

ANNOTATION

Research on the security of the Atutor e-learning web service // Qualification work for a Bachelor's degree // Slupskyi Bohdan Vasylovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer and Information Systems and Software Engineering, Department of Cybersecurity, SB-41 group // Ternopil, 2023 // p. 66, fig. - 5, tab. - 3.

The purpose of this work is a systematic analysis and study of the level of security and protection of the Atutor web service, which is used for e-learning, identification of potential vulnerabilities, risk assessment, as well as recommendations and measures for enhancing the security of the system.

The object of study - Atutor e-learning web service.

The subject of the study - investigation of the security of the Atutor e-learning web service using a vulnerability scanner.

In the qualification work, an analysis of the Atutor e-learning system, its functional capabilities and security systems was conducted, a classification of critical information was made for assessing the impact of found vulnerabilities on it, recommendations were given for their elimination, and additional advice was provided to strengthen security.

The result of the work is an evaluation of the identified vulnerabilities with the provision of recommendations for their elimination.

To implement this work, the following software products were used: Acunetix.

ЗМІСТ

ВСТУП

Актуальність та значимість дослідження захищеності веб-сервісів не може бути переоціненою в сучасному цифровому світі. Щороку веб-сервіси стають мішенями масових кібератак, які призводять до значних збитків для їхніх власників.

Атаки можуть бути різноманітними - від простих спроб вдарити по репутації до складних інфраструктурних вторгнень з метою крадіжки даних або використання ресурсів для виконання нелегальних операцій. Такі атаки можуть призвести до втрати цінної інформації, втрати довіри з боку користувачі, а також до не прямих фінансових збитків, які пов'язані з відновленням послуг.

Про всю глибину цієї проблеми свідчать дані з різних досліджень та звітів. Один з них - звіт держспецзв'язку, у якому показано тенденції зростання у сфері кіберзлочинності. Згідно з цим звітом, кількість атак на веб-сервіси продовжує зростати, і це вимагає відповідної реакції [1].

Щоб протистояти цим загрозам, власники веб-сервісів використовують різні методи оцінки та покращення захищеності. Одним із них є проведення дослідження захищеності веб-сервісів, включаючи тестування на проникнення, аудит коду, а також оцінку інфраструктури на відповідність стандартам безпеки.

Використання цих підходів стало загальноприйнятою практикою, яка дозволяє оцінити стан захищеності веб-сервісів, виявити потенційні слабкі місця, а також розробити план дій для їх усунення. Наразі існує безліч відомих компаній, що надають послуги в сфері оцінки та покращення захищеності веб-сервісів, що свідчить про великий попит на надання даних послуг.

Основним метою є дослідження захищеності веб-сервісі для електронного навчання Atutor, що використовує Тернопільський національний технічний університет.

Atutor - це потужна система управління навчанням, яка використовується для організації і проведення електронного навчання. Це інструмент, що забезпечує безперебійну взаємодію між студентами та викладачами, що дозволяє

проводити онлайн-заняття, оцінювати роботи студентів, обмінюватися файлами та багато іншого.

Однак, подібно до будь-якого іншого веб-ресурсу, Atutor може стати мішенню для кібератак. Зловмисники можуть спробувати зламати систему для крадіжки конфіденційних даних, пошкодження репутації університету, або навіть для перешкоджання навчальному процесу.

Така потенційна загроза має серйозні наслідки. Втрата або витік конфіденційних закладу, даних студентів чи викладачів може призвести до порушення прав на конфіденційність і може нанести значну шкоду репутації ТНТУ. Також, будь-які перебої у роботі Atutor можуть вплинути на процес навчання, що може мати негативні наслідки для студентів та викладачів.

У зв'язку з цим, важливо провести дослідження захищеності Atutor. Це дозволить оцінити поточний стан безпеки, виявити та усунути потенційні слабкі місця, а також зробити внесок в розвиток системи безпеки, яка захистить сервіс від можливих кібератак. Такий підхід забезпечить надійну роботу сервісу, захист даних закладу і користувачів та безперебійний навчальний процес.

Мета даного дослідження полягає в систематичному аналізі та вивченні рівня безпеки веб-сервісу Atutor. Це включає в себе розбір структури та роботи сервісу, його поточного стану безпеки, та можливих дірок в захисті, які можуть стати цільовими для зловмисників.

Основним завданням є виявлення потенційних вразливостей в системі. Це допоможе зрозуміти, які аспекти безпеки Atutor потребують удосконалення або покращення. По завершенню цієї частини дослідження, наступним кроком буде розробка рекомендацій та заходів, спрямованих на підвищення захищеності системи.

Ці рекомендації та заходи будуть спрямовані на створення більш стійкої до атак системи, яка захистить дані закладу та користувачів і гарантує безперебійну роботу сервісу.

Для досягнення цих цілей, необхідно використовувати обґрунтовану методологію та методи дослідження, які дозволять оцінити безпеку Atutor у всіх його аспектах.

Перше, важливим аспектом є аналіз політики інформаційної безпеки сервісу. Це дасть змогу оцінити, наскільки правила і процедури безпеки, які вже застосовуються, відповідають сучасним вимогам і стандартам. Буде перевірено, наскільки ці політики враховують потенційні загрози і вразливості, та як вони сприяють забезпеченню захищеності системи.

Далі, щоб знайти потенційні вразливості, будуть використовуватися як автоматизовані, так і ручні методи. Автоматизовані інструменти, такі як сканери вразливостей, можуть швидко провести сканування сервісу на наявність відомих вразливостей. З іншого боку, ручне тестування дозволяє більш глибоко аналізувати систему, використовуючи творчий підхід та досвід експертів в галузі безпеки, щоб виявити вразливості, які можуть бути неочевидні для автоматизованих інструментів.

Такий багатоаспектний підхід до дослідження допоможе забезпечити повноту аналізу, виявити і усунути вразливості, а також зробити внески у підвищення загального рівня безпеки веб-сервісу Atutor.

Це дослідження надійності веб-сервісу електронного навчання Atutor має як теоретичне, так і практичне значення.

З теоретичного боку, дослідження допоможе розширити знання про механізми захисту веб-сервісу, специфічні типи вразливостей, які можуть виникнути в таких системах, і методи їх виявлення та усунення. Результати цього дослідження можуть стати основою для подальших наукових досліджень і розвитку методології аналізу безпеки веб-сервісів.

З практичного боку, прямим результатом цього дослідження буде підвищення рівня безпеки веб-сервісу Atutor. Виявлення та оцінювання вразливостей, а також рекомендації щодо їх усунення допоможуть зміцнити систему і зменшити ймовірність успішної атаки зловмисників. Це, у свою чергу,

зменшить потенційні збитки, що можуть виникнути в результаті порушення безпеки.

Отже, це дослідження є важливим кроком не тільки для забезпечення безпеки веб-сервісу Atutor, але й для розвитку галузі інформаційної безпеки в цілому. Зрештою, оцінка та зміцнення безпеки Atutor — це процес, що підтримує його стабільність, надійність та стійкість до майбутніх загроз.

РОЗДІЛ 1 АНАЛІЗ ОБ'ЄКТА ДОСЛІДЖЕННЯ

1.1 Аналіз системи управління навчанням Atutor

Atutor - це веб-сервіс електронного навчання, який був розроблений командою Adaptive Technology Resource Centre на базі університету Торонто, Канада. Це відбулося на початку 2000-х років з метою створення зручного і доступного інструменту для електронного навчання, який міг би задовольнити потреби навчальних закладів різних рівнів [2].

Atutor розроблено з використанням відкритого вихідного коду, що дозволяє будь-якому користувачеві або організації безкоштовно встановлювати, використовувати і модифікувати цю систему. Призначення Atutor - це надання зручних інструментів для створення онлайн-курсів та управління навчанням. Завдяки своїй гнучкості і адаптивності, Atutor застосовується в широкому спектрі установ, включаючи університети, коледжі, школи та корпоративні організації по всьому світу.

З часом Atutor знайшов своє місце на міжнародному ринку електронного навчання. Сьогодні його використовують сотні навчальних закладів і організацій по всьому світу, і він перекладений на десятки мов. Спільнота користувачів Atutor продовжує зростати, що свідчить про високу цінність цього продукту в галузі електронного навчання.

Після ближчого ознайомлення з історією та поширенням Atutor, перейдемо до огляду його можливостей.

Atutor вирізняється широким набором можливостей, які роблять цю систему зручною та функціональною для викладачів, студентів, а також адміністраторів системи.

Спочатку, зручність встановлення та налаштування Atutor вирізняє його серед інших систем електронного навчання. Atutor легко інсталюється на більшість веб-серверів, що підтримують PHP та MySQL.

Більш детально розглянемо можливості, які Atutor надає своїм користувачам [3].

Можливості для адміністраторів:

– Керування користувачами: адміністратори можуть додавати нових користувачів, видаляти або блокувати існуючих, налаштовувати права доступу.

– Керування курсами: адміністратори мають змогу створювати нові курси, редагувати або видаляти існуючі.

– Налаштування системи: можливість налаштування різних параметрів системи, включаючи вигляд, мову, налаштування безпеки тощо.

– Можливості для викладачів:

– Створення курсів: викладачі можуть створювати нові курси, заповнювати їх контентом, включаючи різні типи медіа, створювати тести і завдання для самостійної роботи.

– Управління курсами: викладачі мають можливість налаштовувати параметри курсів, додавати або видаляти матеріали, оновлювати інформацію, переглядати статистику курсу.

– Оцінювання: викладачі можуть встановлювати критерії оцінювання для кожного завдання і тесту, переглядати роботи студентів та виставляти оцінки.

– Взаємодія зі студентами: система надає зручні засоби для комунікації зі студентами, включаючи форуми, чати, особисті повідомлення.

– Можливості для студентів:

– Перегляд курсів: студенти мають змогу переглядати всі доступні для них курси, переходити по розділах, читати навчальні матеріали, дивитися відео, слухати аудіо-файли та виконувати тести.

– Система оцінювання: студенти отримують оцінки за виконані завдання і тести, а також можуть переглядати загальну успішність в курсі.

– Інтерактивні елементи: використання форумів, чатів і інших засобів комунікації дозволяє студентам обговорювати матеріали курсу, задавати питання та обмінюватися думками з однокурсниками і викладачами.

– Персоналізація: можливість налаштування свого профілю, включаючи зображення профілю, контактну інформацію тощо.

Крім того, завдяки відкритому вихідному коду, Atutor можна легко розширювати і модифікувати за допомогою плагінів, що дозволяє адаптувати систему до специфічних потреб користувачів, що дозволяє розширювати його функціонал.

Тим не менш, разом з цими зручними і потужними інструментами, необхідно розглянути і питання безпеки. Так, як будь-яка інша велика система, Atutor мала вразливості які були додані до загальної бази вразливостей CWE. Розглянемо кількість та тип вразливостей які були виявлені за час існування Atutor, та на основі цього зробимо деякі висновки щодо якості створеного продукту в плані захищеності.

Наявність вразливостей в програмному забезпеченні, такому як Atutor, може здатись спочатку небезпечною, але варто розуміти, що виявлення та усунення вразливостей є нормальною частиною процесу розвитку програмного забезпечення. Така активність свідчить про те, що програма є "живою" та активною, що над нею працюють і вона привертає увагу спільноти розробників і експертів з безпеки.

Розглянувши виявлені вразливості Atutor на веб-сайті CVE Details на рисунку 1.1, можна зробити декілька висновків. Всього було виявлено понад 20 різних вразливостей, з яких більшість відносяться до виконання коду, переповнення буфера, XSS, CSRF та інших загальних веб-вразливостей [4].

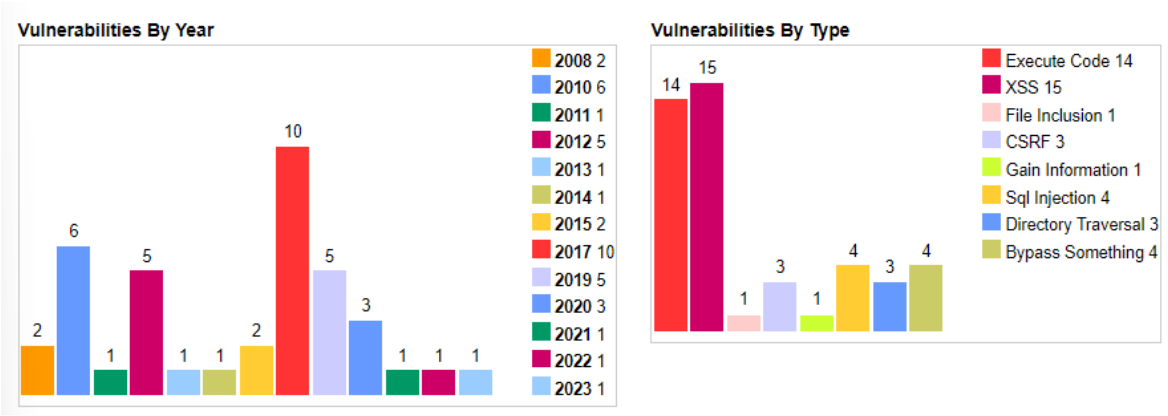


Рисунок 1.1 – Статистика старих виявлених вразливостей

При цьому, деякі з цих вразливостей мали високий рівень серйозності та мали великий вплив на систему. Однак, важливо зазначити, що кількість виявлених вразливостей з часом зменшується, що свідчить про те, що команда розробників активно працює над усуненням існуючих проблем.

В порівнянні з іншими подібними системами, такими як Moodle чи Blackboard, в Atutor було виявив менше критичних вразливостей. Це може свідчити про високу якість коду Atutor та його тестування розробниками та спільнотою.

Отже, на основі цих даних, можна зробити висновок, що Atutor, хоч і мав деякі вразливості, він є безпечною системою для електронного навчання. Команда розробників активно працює над виявленням та усуненням вразливостей, що підтверджується зменшенням кількості виявлених вразливостей з часом. Не дивлячись на це, рекомендується завжди використовувати останню версію програмного забезпечення та своєчасно виконувати всі оновлення безпеки.

1.2 Реалізація Atutor у навчальному закладі ТНТУ

Тернопільський національний технічний університет (ТНТУ) активно використовує систему електронного навчання Atutor для впровадження інноваційних та ефективних методів навчання. Це обгрунтовується рядом вагомих переваг власної платформи управління навчанням. Зокрема, така система дозволяє університету мати повний контроль над даними, їхнім обробленням та захистом. Також, з точки зору навчання, Atutor надає гнучкі можливості налаштування навчальних процесів та матеріалів, відповідно до особливостей та потреб кожного курсу або дисципліни.

Atutor в ТНТУ розгорнуто локально на серверах університету і підключено до LDAP-сервера. Локальне розгортання дає університету можливість володіти повним контролем над системою, включаючи даними користувачів та змістом курсів. Захист даних користувачів також забезпечується на вищому рівні,

оскільки усі дані зберігаються внутрішньо, а не передаються третім сторонам. Інтеграція з LDAP в свою чергу дозволяє забезпечити єдиний механізм аутентифікації та управління правами доступу для всіх систем університету, що включає і Atutor [5] .

Atutor у ТНТУ тісно взаємодіє з автоматизованою системою управління "Університет". Ця система має ключове значення для функціонування університету, оскільки вона зберігає всі важливі дані про студентський контингент, освітні програми, академічний прогрес та інше. Інтеграція Atutor з АСУ "Університет" відкриває додаткові можливості для ефективного управління навчальним процесом.

Завдяки цьому обміну даними, Atutor автоматично отримує актуальну інформацію про студентів та їхні академічні результати, а також може враховувати зміни в освітніх програмах. Це не лише полегшує роботу адміністраторів і викладачів, але і дозволяє студентам отримувати максимально актуальну інформацію та ресурси для навчання в реальному часі.

Що стосується використання веб-сервера nginx, він відомий своєю надійністю, високою продуктивністю та гнучкістю. Він дозволяє ефективно обробляти велику кількість одночасних з'єднань, що особливо важливо для освітнього установи, де учні та викладачі мають одночасний доступ до системи.

Структуру Atutor можна побачити на рисунку 1.2.

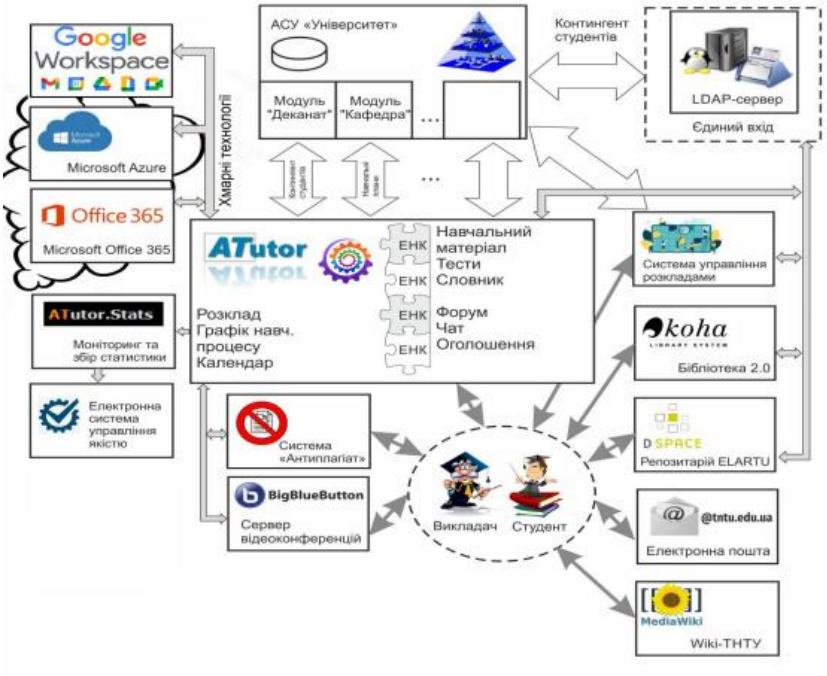


Рисунок 1.2 – Структура сервісу

В Atutor у ТНТУ реалізовано широкий спектр функцій, включаючи різноманітні модулі для проведення тестів, створення курсів, обговорень, завантаження навчальних матеріалів та ін.. Наступна частина нашого огляду детальніше розкриє який саме функціонал Atutor було реалізовано в ТНТУ, та як він використовується для підтримки навчального процесу.

Однією з ключових особливостей Atutor в ТНТУ є навчальні курси, що включають як теоретичний матеріал, так і віртуальні лабораторні установки. Студенти мають змогу вивчати теорію, а потім застосовувати здобуті знання на практиці в безпечному віртуальному середовищі. Це дозволяє отримати глибоке розуміння предмета і набути практичних навичок.

Для зручності користувачів в системі реалізовані такі інструменти, як тести для перевірки знань, скринька для завдань та електронна залікова книжка. Викладачі можуть створювати тести для оцінки прогресу студентів, приймати та оцінювати завдання, а студенти - відслідковувати свій академічний прогрес

Крім того, в Atutor є інструменти для комунікації. Середовище відеоконференцій дозволяє проводити онлайн-лекції, семінари, консультації, а також вести обговорення і співпрацю в групах.

Засоби відеоконференцій в Atutor дозволяють викладачам і студентам взаємодіяти один з одним в режимі реального часу, використовуючи аудіо- та відео-трансляцію, а також текстовий чат. Це означає, що викладачі можуть проводити онлайн-заняття, під час яких вони можуть демонструвати презентаційні матеріали, використовувати інструменти малювання для виділення ключових моментів на слайдах та проводити обговорення зі студентами.

Можливість демонстрації екрану, включаючи окремі вікна програм або браузера, дозволяє викладачам ефективно показувати навчальні матеріали або процеси. Вони також можуть транслювати відеоматеріали, включаючи відео з YouTube, що робить заняття більш динамічними і цікавими.

Важливо відзначити, що викладачі мають можливість записувати відеозаписи занять та інтегрувати ці відео у матеріал курсу. Це означає, що студенти можуть переглядати ці відеозаписи після занять для додаткового вивчення матеріалу.

Студенти і викладачі можуть переглядати свої навчальні плани та розклади прямо в системі. Це робить процес планування та організації навчання більш зручним та ефективним.

Atutor також має засоби для контролю якості електронного навчання та моніторингу перебігу онлайн-занять. Викладачі можуть відслідковувати виконання завдань студентами, їх активність та прогрес у навчанні, що дозволяє своєчасно виявляти та вирішувати проблеми.

1.3 Система захисту Atutor

Atutor, як система управління навчанням, використовує цілий комплекс методів і принципів, спрямованих на захист інформації та даних користувачів [6]. Наведемо декілька ключових з них:

– Фільтрація вводу: є важливою частиною захисту інформації, що зосереджена на перевірці та обробці даних, введених користувачами в систему.

Мета полягає в тому, щоб виявити та видалити або замінити потенційно шкідливий контент, що може пошкодити систему або викликати її неналежне функціонування.

В системі Atutor фільтрація вводу використовується для забезпечення безпеки даних, введених користувачами. Це включає перевірку даних, введених через веб-форми, адреси URL та інші інтерфейси. Фільтрація вводу є важливим елементом захисту від різноманітних атак, включаючи SQL-ін'єкції та XSS-атаки, які можуть використовувати ненадійний ввід для внесення шкідливих запитів або скриптів в систему.

Фільтрація вводу в Atutor дуже ефективна, оскільки допомагає запобігти низці загроз інформаційної безпеки. Проте, важливо зауважити, що жодна одна захисна заходи не може гарантувати 100% захисту, тому фільтрація вводу має використовуватися в комбінації з іншими стратегіями захисту для досягнення найбільшої можливої безпеки.

– Захист від CSRF-атак: є ще одним важливим елементом системи безпеки Atutor. CSRF, або атаки на перехресну підміну запитів сайтів, - це метод, за допомогою якого зловмисники можуть змусити користувача виконати дії на веб-сайті без його відома, що може призвести до несанкціонованого доступу до даних або зміни стану системи.

Ці атаки зазвичай використовуються в тих випадках, коли користувач вже аутентифікований на сайті. Якщо користувач натискає на зловмисне посилання або відкриває зловмисний веб-сайт, його браузер може надіслати запит на аутентифікований веб-сайт, використовуючи їхній діючий сеанс.

Atutor запобігає цим атакам шляхом використання CSRF-токенів. Кожен запит, що вносить зміни, повинен містити цей токен, який генерується сервером і пов'язаний із сеансом користувача. Цей токен перевіряється сервером при отриманні запиту, що вносить зміни. Якщо токен відсутній або не відповідає токену в сеансі, запит відхиляється.

Цей підхід дуже ефективний для захисту від CSRF-атак, оскільки зловмисникам важко отримати доступ до цих токенів або передбачити їх. Таким

чином, Atutor забезпечує безпеку користувача від потенційних атак на перехресну підміну запитів.

– Сесійний менеджмент: Управління сесіями є суттєвою складовою безпеки в будь-якій веб-платформі, і Atutor тут не є винятком. Веб-сесії створюються, коли користувач автентифікується на сайті, і їх використовують для відслідковування стану користувача на протязі різних запитів. Вони дозволяють серверу ідентифікувати користувача та запам'ятовувати його дії.
В Atutor ідентифікатори сесій регулярно оновлюються для запобігання їх перехоплення, а також встановлюється таймаут неактивності для автоматичного видалення старих сесій. Це є важливою мірою безпеки, яка допомагає зменшити ризик несанкціонованого доступу до аккаунтів користувачів та відповідних даних. Наприклад, якщо зловмисник намагається скопіювати ідентифікатор сесії, він може виявитися вже недійсним через механізм оновлення, запобігаючи таким чином потенційному зловмисному використанню.

– Хешування паролів: це процес перетворення вихідних даних (в даному випадку пароля) у відмінний від оригіналу набір символів, що має фіксовану довжину незалежно від розміру вихідних даних. Хеш-функції розроблені таким чином, що будь-яке незначне змінення вхідних даних призведе до зовсім іншого хеш-значення.

– Atutor використовує цей метод для безпечного зберігання паролів користувачів. Коли користувач вводить свій пароль, він перетворюється в хеш-значення, яке потім зберігається в базі даних. Під час авторизації введений пароль знову перетворюється в хеш, і це значення порівнюється з хешем, збереженим в базі даних.

Цей метод є ефективним, оскільки реальні паролі не зберігаються, і, таким чином, навіть у разі витоку бази даних паролі не можуть бути використані зловмисниками безпосередньо. Однак, потрібно використовувати сучасні і надійні хеш-функції, які важко зламати. Atutor усвідомлює цю потребу та використовує відповідні алгоритми для забезпечення найвищого рівня безпеки паролів користувачів.

– Рольова модель доступу: це метод контролю доступу, при якому права на доступ до ресурсів визначаються на основі ролі користувача в системі. Це означає, що користувачам надається доступ до певних ресурсів або функцій відповідно до їх ролі, а не індивідуально.

Atutor використовує рольову модель доступу, надаючи різні рівні доступу до ресурсів і функцій системи в залежності від ролі користувача. Наприклад, студенти можуть мати доступ до матеріалів курсу, але не можуть змінювати їх, тоді як викладачі мають права на редагування цих матеріалів.

Цей метод захищає від невідповідного або несанкціонованого доступу до інформації і функцій. Він також сприяє збалансованому розподілу прав і обов'язків, забезпечуючи, що кожен користувач має доступ лише до тих ресурсів, які він потребує для виконання своєї ролі.

– TLS: Transport Layer Security (TLS) - це криптографічний протокол, що забезпечує захищене з'єднання між двома сторонами, зазвичай між клієнтом (користувачем) та сервером. TLS працює шляхом створення зашифрованого каналу, через який передаються дані, забезпечуючи конфіденційність і цілісність даних під час передачі.

– Atutor активно використовує TLS для захисту даних користувача під час передачі між користувачем та сервером. Наприклад, коли користувач вводить свої облікові дані для входу в систему, TLS забезпечує, що ці дані не можуть бути прочитані або змінені зловмисниками під час передачі.

Такий захист є особливо важливим у сучасному цифровому світі, де зловмисники постійно шукають нові шляхи перехоплення і використання чужих даних. TLS вважається ефективним та надійним методом захисту, який став стандартом для багатьох онлайн-систем, включаючи Atutor. Через використання TLS користувачі Atutor можуть бути впевнені в безпеці своїх даних під час взаємодії з системою.

– Функції аудиту: це процес слідкування і запису дій, що виконуються в системі. Вони використовуються для виявлення несанкціонованої активності, аналізу безпеки та виявлення можливих слабких місць.

Atutor має вбудовані функції аудиту, що дозволяють адміністраторам відстежувати дії користувачів. Вони можуть бачити, хто виконав певну дію, коли це було зроблено, та інші відповідні деталі. Це може бути корисним при розслідуванні інцидентів безпеки, а також для підтримки загальної відповідності правилам і стандартам безпеки.

Ця функція важлива для запобігання та виявлення зловмисних дій в системі. Якщо адміністратор побачить підозрілу активність, таку як незвичайно велику кількість вхідних запитів або спроби доступу до ресурсів, він зможе відповідно відреагувати, що може включати зміну налаштувань безпеки, зміну паролів користувача або повне блокування користувача.

Загалом, функції аудиту є важливим інструментом для забезпечення безпеки в Atutor. Вони допомагають виявляти зловмиснику вчасно і попереджати можливі порушення безпеки, що робить їх високоефективним методом захисту.

– Обмеження на кількість вхідних запитів: це важлива частина захисної стратегії, яка має на меті запобігти атакам типу DoS (Denial of Service) або Brute Force. Атака DoS полягає в надсиланні великої кількості запитів до сервера з метою перевантаження його та порушення нормального функціонування. Brute Force – це метод, при якому зловмисник намагається зламати пароль шляхом постійного введення різних комбінацій.

Atutor використовує обмеження на кількість вхідних запитів для того, щоб протистояти цим типам атак. Якщо система виявляє, що від одного користувача або IP-адреси надходить надмірна кількість запитів за короткий проміжок часу, вона може тимчасово заблокувати додаткові запити від цього користувача або IP.

Цей метод є досить ефективним для запобігання перевантаженню сервера або незаконному доступу до облікових записів користувачів. Він впливає на здатність зловмисників використовувати автоматизовані скрипти для вгадування паролів або відправки надмірних запитів до сервера, що допомагає забезпечити стабільність та безпеку системи.

Система захисту Atutor включає цілу низку стратегій та технологій, які спільно працюють для забезпечення безпеки користувачів та їх даних. Сесійний менеджмент, хешування паролів, протокол TLS, обмеження на кількість вхідних запитів, функції аудиту, рольова модель доступу та фільтрація вводу - все це елементи системи безпеки Atutor, кожен з яких виконує свою важливу роль.

Спільно ці компоненти формують потужний бар'єр проти більшості загроз безпеки, що виникають в онлайн-освітніх середовищах. Вони не тільки активно запобігають атакам, але й відслідковують активність, що допомагає виявити та нейтралізувати потенційні проблеми. Всі ці елементи, взяті разом, свідчать про високий рівень захисту, що його надає Atutor, та гарантують користувачам безпечне та захищене середовище для навчання.

1.4 Аналіз політики інформаційної безпеки Atutor

Темою дослідження є захищеність веб-сервісу електронного навчання Atutor. Частиною такого дослідження є аналіз політики інформаційної безпеки цієї системи. Політика інформаційної безпеки - це документований набір правил та процедур, що регулюють те, як організація управляє, захищає та розподіляє свої інформаційні ресурси. Але для роботи буде необхідний розділ де буде промаркована критична інформація, так звана процедура лейблінгу [7].

Маркування критичної інформації означає ідентифікацію та визначення рівня важливості або чутливості даних. Цей процес важливий, оскільки він допомагає організації розуміти, які дані потребують найвищого рівня захисту. Без відповідного маркування критичної інформації, організація може ризикувати надмірним або недостатнім захистом своїх даних [8].

Там же описується на основі промаркованої інформації те який поріг впливу вразливості на цю інформацію є критичним та недопустимим.

Поріг критичності впливу на інформацію - це важливий концепт у сфері інформаційної безпеки. Він визначає рівень впливу потенційної вразливості на

конфіденційність, цілісність або доступність промаркованої критичної інформації, який вважається неприйнятним.

При визначенні порогу критичності впливу на інформацію, враховуються різні фактори. По-перше, це важливість інформації для організації. Наприклад, якщо інформація є життєво важливою для бізнесу, як от корпоративні секрети або персональні дані клієнтів, поріг критичності впливу на цю інформацію буде нижчим.

Коли вплив потенційної вразливості перевищує встановлений поріг, організація повинна вжити заходів для виправлення вразливості або зменшення її потенційного впливу. Це може включати в себе патчування програмного забезпечення, зміну конфігурації або зміну процесів управління ризиками.

Використання порогу критичності впливу на інформацію є важливим елементом управління ризиками інформаційної безпеки, оскільки воно допомагає організаціям виявити та відреагувати на найбільш серйозні вразливості вчасно. Всі вразливості, які перевищують цей поріг, повинні бути виявлені та виправлені в найкоротший термін, щоб забезпечити неперервність служби та захист користувачів.

У процесі дослідження документації сервісу електронного навчання Atutor, специфічної частини, яка відповідає за маркування критичної інформації, не було виявлено, така інформація не присутня або відсутня в доступних документаційних ресурсах.

Втім, в різних частинах документації згадується інформація, яка може бути вважана критичною в контексті безпеки інформації, але ці вказівки не сформульовані як чіткі маркування. Замість цього, ця інформація, в основному, вказує на різні види даних в системі, але не дає чіткого розуміння того, як ці ролі або дані маркуються або визначаються як критичні в рамках політики інформаційної безпеки Atutor.

Відсутність чіткого маркування критичної інформації може ускладнити розуміння того, як Atutor визначає і захищає свої найбільш важливі активи інформації, а також оцінює ризики, пов'язані з можливими вразливостями

РОЗДІЛ 2 ЗАХОДИ З ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ATUTOR

2.1 Розробка політики інформаційної безпеки для Atutor

У процесі дослідження інформаційної безпеки веб-сервісу електронного навчання Atutor, виникає питання щодо відсутності чіткого класу критичної інформації. Це може перешкоджати ефективному оцінюванню потенційного впливу вразливостей, що були або могли б бути виявлені в рамках даної системи.

Невідомість, які види інформації в системі є критичними, і як вони маркуються, ускладнює оцінювання того, наскільки серйозною може бути потенційна вразливість для цієї системи. Без знання про те, які дані в системі є найбільш цінними або найбільш чутливими, важко визначити, як вразливості можуть впливати на ці дані, а також на загальну безпеку системи [9].

У зв'язку з цим, як спеціаліст з інформаційної безпеки, я бачу необхідність самостійного маркування критичної інформації в системі Atutor, як частини цього дослідження. Цей процес буде включати аналіз інформації, що обробляється в системі, їх потенційної важливості для організації або користувачів, а також потенційного впливу, якщо ця інформація буде компрометована або змінена через вразливості в системі.

Перш ніж здійснити маркування критичної інформації в системі електронного навчання Atutor, важливо визначити, яка інформація циркулює в даній системі. Цей процес включає розуміння різних видів даних, які обробляються, зберігаються або передаються через систему.

В першу чергу, Atutor є платформою для електронного навчання, тому вона зберігає велику кількість освітніх даних. Це може включати навчальні матеріали, такі як навчальні модулі, тести, відео, аудіо та інші мультимедійні ресурси. Ця інформація є важливою, адже вона становить основний контент, який надається для навчання студентів.

Наступним важливим типом інформації, який обробляється в Atutor, є персональні дані користувачів. Це може включати імена, адреси електронної

пошти, дати народження, інформацію про контактні дані та інші особисті дані, які користувачі надають при реєстрації або використанні сервісу. Ця інформація є чутливою, оскільки вона може бути використана для ідентифікації конкретних осіб.

Крім того, система обробляє дані про взаємодію користувачів із системою та їхнім навчальним процесом. Це може включати дані про перегляди сторінок, результати тестів, відповіді на завдання, діалоги в чатах та форумах, інформацію про відвідування курсів та інше.

До інформації, яка циркулює в системі Atutor, також відносяться дані про саму систему та її налаштування. Це включає інформацію про версію системи, конфігурацію, налаштування різних модулів та компонентів, параметри безпеки, логи системи та інше.

Ця інформація допомагає управлінню системою, відстеженню її стану, виявленню та розробці стратегії реагування на інциденти безпеки. Вона також є важливою для оптимізації роботи системи та забезпечення її стабільної роботи.

Усі ці види даних створюють загальну картину інформації, яка зберігається та циркулює в системі Atutor, і є основою для детального маркування критичної інформації в межах системи. На основі цих даних можна виділити основну інформацію та провести її класифікацію.

Data Classification, або класифікація даних, - це процес, що включає ідентифікацію активів (інформації) та їх важливості для організації. В даному випадку, ми визначаємо чотири основні активи в системі Atutor, які впливають на її цілісність і безпеку:

– Навчальні матеріали: Ці дані мають високий рівень важливості, оскільки є ключовими для навчального процесу. Їх цілісність, доступність та конфіденційність мають бути надійно захищені. Втрата таких матеріалів є недопустимою, так як по факту це і є тим що продає заклад.

– Матеріали для оцінювання знань студентів, тести: Мають високу важливість, оскільки вони допомагають вимірювати прогрес навчання та здобутки студентів. Ця інформація має бути конфіденційною, і її цілісність та

доступність мають бути гарантовані. Здебільшого ця інформація є унікальною, і не знаходиться у відкритому до ступі, що свідчить про її високу цінність, втрата якої може мати серйозні наслідки, так як унеможливить точне оцінювання знань здобувачів вищої освіти, що призведе до проблем із визначенням місця студента в рейтингу, та подальшим присвоєнням йому певних бонусів за посідання верхньої її частини.

– Персональна інформація користувачів: Ця інформація має надзвичайно високу важливість. Порушення конфіденційності, цілісності або доступності цих даних може призвести до порушення законодавства про захист даних та негативно вплинути на репутацію системи. Втрата такої інформації матиме серйозні наслідки не тільки для репутації системи а і для її користувачів, так як зловмисники зможуть отримати більше інформації про конкретну людину та на основі цього з більшою вірогідністю зможуть обманути її чи виконати інші зловмисні дії.

– Інформація про систему та її налаштування: Ця інформація є важливою для безпеки системи. Вона включає в себе дані, що допомагають управляти системою, налаштуваннями, розробкою стратегії реагування на інциденти безпеки, тощо. Порушення її цілісності, конфіденційності або доступності може призвести до серйозних проблем з безпекою системи. Розповсюдження такої інформації може негативно вплинути на загальну безпеку системи, так як вона несе інформацію про роботу системи та її налаштування, володіючи такою інформацією зловмисник може більш детальніше припрацьовувати атаки на систему що піднімає вірогідність успішної експлуатації вразливості та втрати даних.

Цей процес допомагає у визначенні критичності різних типів даних і допоможе в подальшому розробити ефективні стратегії їх захисту.

Ця таблиця 1.1допомагає краще зрозуміти ступінь важливості різних аспектів безпеки для кожного типу інформації. У всіх випадках, порушення цілісності, доступності або конфіденційності є недопустимими, що підкреслює

високий рівень важливості цих даних для нормального функціонування системи Atutor.

Таблиця 1.1 – Критерії впливу на критичні активи

Актив	**Цілісність**	**Доступність**	**Конфіденційність**
Навчальні матеріали	Недопустима	Недопустима	Недопустима
Матеріали для оцінювання знань	Недопустима	Недопустима	Недопустима
Персональна інформація користувачів	Недопустима	Недопустима	Недопустима
Інформація про систему та її налаштування	Недопустима	Недопустима	Недопустима

По завершенню аналізу політики інформаційної безпеки, я зробив декілька важливих висновків. Перше і найважливіше, було розроблено систему маркування критичної інформації закладу. Це включає навчальні матеріали, матеріали для оцінювання знань студентів, персональну інформацію користувачів та інформацію про систему та її налаштування.

Кожен з цих активів був оцінений на важливість з точки зору цілісності, доступності та конфіденційності. В кожному випадку, втрата будь-якого з цих аспектів була визначена як недопустима, що підкреслює високу важливість цих даних для функціонування системи

На основі цього маркування критичної інформації, ми можемо проводити більш глибокий аналіз захищеності веб-сервісу електронного навчання Atutor. Ми можемо оцінити потенційний вплив різних видів вразливостей на цю критичну інформацію і, відповідно, на загальну безпеку системи.

Цей аналіз дозволяє нам краще розуміти, які аспекти безпеки важливі для Atutor, і буде використано як основа для подальшого дослідження і вдосконалення безпеки системи.

2.2 Підходи до визначення захищеності веб-ресурсів

В сучасному цифровому світі захист веб-ресурсів є одним з найважливіших елементів успішної діяльності організацій. Існує множина практик та методологій, що допомагають оцінити і підтримувати рівень захищеності веб-ресурсів. Ці методики використовуються не лише крупними корпораціями, але і малими організаціями, нон-профітними установами та навіть окремими особами.

Зростаюча кількість кібератак та постійне еволюціювання загроз робить регулярну оцінку захищеності не просто рекомендованою, а майже обов'язковою процедурою. Ця перевірка захищеності зазвичай включає в себе щорічний аудит, що допомагає ідентифікувати потенційні вразливості та вдосконалити заходи щодо інформаційної безпеки [10] .

Використовуючи сучасні підходи до оцінки захищеності, організації можуть гарантувати безпеку своїх веб-ресурсів, захищаючи свою інформацію, активи та, що найважливіше, довіру своїх користувачів. Ось декілька ключових методів, які використовуються для визначення рівня захищеності веб-ресурсів:

– Аудит безпеки: це комплексний процес, в якому проводиться детальний аналіз політики безпеки, процедур та контролю, які застосовуються до веб-ресурсу. Ця систематична оцінка допомагає ідентифікувати потенційні вразливості, ризики або недоліки в інформаційній безпеці організації.

Основна мета аудиту безпеки полягає в забезпеченні захисту важливих активів організації, в тому числі даних, інформації та технологій. Він допомагає переконатися, що заходи безпеки впроваджені правильно, діють ефективно і що всі потенційні вразливості та ризики відповідно управляються.

Переваги аудиту безпеки включають здатність виявляти вразливості та слабкі місця у системі, перевіряти дотримання нормативних вимог, політик та процедур безпеки, а також надавати рекомендації щодо покращення контролю безпеки.

Водночас, існують також недоліки аудиту безпеки. Це, в першу чергу, може бути витрати часу та ресурсів, що потрібні для проведення аудиту. Інший недолік полягає в тому, що результати аудиту часто можуть бути технічно складними та незрозумілими для неспеціалістів. Крім того, аудит безпеки є лише "моментним знімком" стану безпеки в конкретний момент часу і не може гарантувати захист від майбутніх загроз.

Незважаючи на ці недоліки, аудит безпеки вважається критично важливим кроком в управлінні інформаційною безпекою та допомагає організаціям підтримувати рівень захисту, який відповідає їхнім потребам та вимогам.

– Тестування на проникнення (Penetration Testing): це метод оцінки безпеки веб-ресурсу шляхом спроби його "взлому" або "проникнення". Мета цього підходу - імітувати дії потенційного зловмисника, щоб виявити та виправити вразливості перед тим, як вони будуть експлуатовані в реальному світі. Техніки тестування на проникнення можуть включати соціальну інженерію, експлуатацію відомих вразливостей, фазінг (випадкове введення даних для виявлення вразливостей) та багато іншого.

Однією з головних переваг тестування на проникнення є те, що воно дає можливість побачити реальні наслідки потенційних вразливостей, а також допомагає оцінити ефективність існуючих механізмів захисту. Водночас, одним із недоліків цього підходу є те, що він може бути дорогим і часозатратним, а також він вимагає високого рівня експертизи для ефективного проведення. Крім того, результати тестування на проникнення відображають лише стан безпеки в конкретний момент часу і можуть не враховувати майбутні вразливості або загрози.

– Сканування вразливостей: є автоматизованим процесом пошуку та виявлення потенційних слабких місць або "вразливостей" в системах та мережах. Це здійснюється за допомогою спеціалізованого програмного забезпечення, яке аналізує різні аспекти системи, включаючи програмне забезпечення, налаштування, версії патчів та інше. Основна мета цього процесу - виявити та

виправити будь-які вразливості перед тим, як вони можуть бути використані зловмисниками.

Серед переваг сканування вразливостей варто відзначити здатність швидко та ефективно ідентифікувати велику кількість потенційних проблем безпеки. Це також може допомогти організаціям визначити пріоритети своїх зусиль з безпеки, концентруючись на найбільш критичних вразливостях. Однак, цей підхід також має свої недоліки. Наприклад, сканування вразливостей може не виявити всі потенційні вразливості, особливо ті, які вимагають складного контексту або взаємодії з користувачем. Крім того, цей процес може спричинити помилкові спрацювання (false positives), що вимагає додаткового часу та ресурсів на їх перевірку.

– Інспекція коду. Інспекція коду відноситься до процесу перегляду та аналізу вихідного коду програми з метою виявлення потенційних проблем та вразливостей. Це може включати пошук небезпечних функцій, недостатніх перевірок безпеки або ненадійних протоколів. Ціль такого перегляду полягає в тому, щоб виявити та виправити будь-які вразливості або помилки в коді, перш ніж вони стануть проблемою в продуктивному середовищі.

Однією з основних переваг інспекції коду є здатність виявити та виправити проблеми на ранніх стадіях розробки, що може врешті решт допомогти зекономити час та ресурси. Вона також може допомогти виявити та виправити проблеми, які можуть бути пропущені в процесі тестування.

Однак, існують і недоліки. Інспекція коду може бути час затратною, особливо для великих систем. Також, цей процес залежить від знань та досвіду людей, які проводять перегляд, і тому може не виявити всі потенційні проблеми, особливо слабкі місця, пов'язані з найновішими техніками атаки.

– Оцінка ризику. це систематичний процес ідентифікації та аналізу потенційних загроз та вразливостей, які можуть позначитися на веб-ресурсі. Основна мета полягає в оцінці вірогідності та потенційного впливу цих загроз, що допомагає виробити пріоритети в аспектах безпеки та розробити стратегію їх вирішення.

Однією з основних переваг оцінки ризику є можливість передбачити та чітко реагувати на потенційні проблеми безпеки. Це може допомогти уникнути втрати даних, перебоїв в роботі або інших негативних наслідків.

Проте, метод оцінки ризику також має недоліки. Він може бути трудомістким та складним, особливо для великих організацій зі складними системами. Також, його ефективність значною мірою залежить від точності та повноти використаних даних. Наприклад, оцінка ризику може не врахувати нові або невідомі загрози, що може призвести до недооцінки ризику.

Важливо зазначити, що кращий підхід до оцінки захищеності веб-ресурсу включає комбінацію всіх або декількох цих методів. Такий комплексний підхід допомагає забезпечити, що всі потенційні вразливості будуть виявлені та вирішені.

У моєму майбутньому дослідженні я планую використати такі методики, як сканування вразливостей та тестування на проникнення. Вибір цих методик зумовлений їх високою практичністю та широким використанням у світі інформаційної безпеки.

Сканування вразливостей дозволяє автоматизовано виявляти слабкі місця, які можуть бути використані зловмисниками. Завдяки цьому методу можна швидко виявити та усунути потенційні загрози.

Тестування на проникнення, з свого боку, дає можливість не просто знайти вразливості, але й перевірити, наскільки вони реально можуть бути експлуатовані. Цей метод дозволяє провести більш глибокий аналіз безпеки, імітуючи дії потенційного зловмисника.

Обидва ці методи доповнюють одне одного і, застосовані разом, дають змогу провести комплексний аналіз безпеки веб-ресурсу.

2.3 Вибір сканера вразливостей для проведення тестування

Після вибору методик для дослідження захищеності, однією з ключових складових стає сканування вразливостей. Для його проведення

використовуються спеціалізовані програмні інструменти, так звані сканери вразливостей. Вони виконують автоматичний пошук слабких місць у веб-ресурсах, які можуть бути потенційними точками проникнення для зловмисників.

При виборі сканера вразливостей я буду врахувати кілька ключових критеріїв:

– Покриття вразливостей: це важливий критерій для вибору сканера вразливостей. Під цим терміном мається на увазі здатність сканера виявляти широкий спектр вразливостей, що включає, але не обмежується стандартними вразливостями в програмному забезпеченні, такими як SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) та іншими.

Детальна база даних вразливостей важлива для забезпечення того, що сканер може виявити велику кількість потенційних слабких місць. Ця база даних повинна регулярно оновлюватися, оскільки нові вразливості виявляються дуже швидко. Це забезпечує те, що сканер вразливостей може виявити найновіші вразливості, навіть ті, що були виявлені нещодавно.

Також важливо, щоб сканер мав здатність адаптуватися до різних типів архітектури веб-ресурсів і технологій, включаючи нові та менш розповсюджені. Він повинен бути здатний сканувати веб-додатки, створені на основі різних мов програмування, і виявляти специфічні для цих технологій вразливості.

– Точність діагностики: це інший важливий критерій при виборі сканера вразливостей. Це відноситься до здатності сканера правильно ідентифікувати та класифікувати вразливості.

"Хибно позитивні" результати - це ситуації, коли сканер помилково ідентифікує безпечну ситуацію як вразливу. Це може стати проблемою, оскільки такі результати відволікають ресурси від справжніх проблем та можуть змусити команду безпеки витрачати час та зусилля на виправлення проблем, яких насправді не існує.

З іншого боку, "хибно негативні" результати теж становлять проблему. Це відбувається, коли сканер не виявляє дійсної вразливості, що може створити ілюзію безпеки та призвести до пропуску серйозних проблем.

Тому при виборі сканера вразливостей важливо розглянути, наскільки точно він може виявити і класифікувати вразливості, а також його історію виявлення хибно позитивних та хибно негативних результатів. Краще вибрати сканер, який має високий рівень точності та низький рівень хибно позитивних та хибно негативних результатів.

– Зручність використання: це важливий критерій вибору сканера вразливостей. Це відноситься до ступеня, до якого користувач може легко та ефективно використовувати сканер.

Інтерфейс сканера повинен бути інтуїтивно зрозумілим і простим у навігації, дозволяючи користувачам легко визначати й конфігурувати параметри сканування, розпочинати процес сканування та переглядати й аналізувати результати.

Документація є іншим важливим аспектом зручності використання. Вона повинна бути зрозумілою, добре організованою та доступною для користувача. Документація має надавати чіткі вказівки щодо використання сканера, включаючи детальні інструкції щодо його налаштування та використання, а також пояснення результатів сканування.

Вибір сканера вразливостей є важливим етапом в процесі оцінки безпеки веб-ресурсу. Правильно вибраний інструмент може значно покращити якість та ефективність цього процесу [11].

Після визначення основних критеріїв вибору сканера вразливостей, можна приступити до порівняльного аналізу потенційних інструментів. В нашому випадку, ми розглянемо чотири популярні сканера вразливостей: Nessus, Acunetix, Burp Scanner та OWASP ZAP.

– Nessus - це один із найбільш відомих та широко використовуваних сканерів вразливостей в індустрії кібербезпеки. Цей інструмент здатний

виявляти тисячі вразливостей, які входять до його регулярно обновлюваної бази даних.

Сканер Nessus розроблений з метою виявлення вразливостей, що стосуються широкого спектру областей, включаючи мережі, системи, веб-додатки та бази даних. Додатково, Nessus включає також функції оцінки відповідності стандартам, що дозволяє перевірити, чи відповідають ваші системи встановленим стандартам індустрії.

Точність сканування Nessus є одним із його ключових переваг. Дякуючи спеціалізованим плагінам та регулярним оновленням, цей інструмент може здійснити глибокий аналіз і надати детальну інформацію про виявлені вразливості. Крім того, Nessus включає в себе модулі, які дозволяють виявити і неправильні конфігурації систем, що можуть стати потенційними вхідними точками для атак.

– Acunetix - це першокласний сканер вразливостей веб-додатків, який випускається компанією Acunetix Ltd. Його основна спеціалізація - виявлення вразливостей, специфічних для веб-додатків, включаючи такі небезпечні загрози як SQL Injection, Cross-Site Scripting (XSS), CSRF (Cross-Site Request Forgery) та інші.

Acunetix пропонує глибокий аналіз безпеки, включаючи автоматизоване сканування, а також підтримку ручного тестування для виявлення більш складних вразливостей. Зокрема, Acunetix використовує передову технологію глибокого сканування, що дозволяє ідентифікувати вразливості, які можуть бути пропущені менш суворими сканерами.

Додатково, Acunetix інтегрується з рядом інших систем безпеки та інструментів управління проектами, що дозволяє зручно організовувати процес виявлення та усунення вразливостей. Він також включає інструменти для автоматичного створення звітів, що значно спрощує процес документації та аналізу результатів сканування.

– Burp Scanner - це потужний компонент пакета Burp Suite, який розроблений компанією PortSwigger. Його основне призначення - це

автоматизоване тестування вразливостей веб-додатків, проте він також може використовуватися для ручного тестування.

Burp Scanner здатний виявляти різноманітні типи вразливостей, включаючи Cross-Site Scripting (XSS), SQL Injection, неналежні конфігурації безпеки, потенційні вразливості в сесіях та багато іншого. Це досягається за допомогою деталізованого аналізу відповідей сервера та використанням розширених методів сканування.

Однією з ключових особливостей Burp Scanner є його здатність до налаштування та гнучкості. Користувачі можуть налаштовувати процес сканування, вибираючи, які типи вразливостей шукати, як глибоко сканувати, та які області веб-додатку необхідно проаналізувати. Це робить Burp Scanner відмінним вибором для спеціалістів з інформаційної безпеки, які потребують високого рівня контролю над процесом тестування.

– OWASP ZAP (Zed Attack Proxy) - це відкритий та безкоштовний сканер вразливостей веб-додатків, що розробляється глобальною спільнотою OWASP (Open Web Application Security Project). Цей інструмент забезпечує комплексний набір функцій для тестування безпеки веб-додатків, починаючи від автоматичного сканування та виявлення вразливостей, закінчуючи інструментами для проведення атак типу "людина посередині".

OWASP ZAP володіє потужними засобами для виявлення вразливостей, включаючи Cross-Site Scripting (XSS), SQL Injection, Path Traversal, та багато інших типів вразливостей. Крім того, він пропонує різноманітні інструменти для активного та пасивного сканування, які дозволяють налаштувати процес тестування відповідно до конкретних потреб та контексту.

Однією з важливих особливостей ZAP є його модульність і гнучкість. Він дозволяє додавати додаткові плагіни та скрипти, що розширюють його можливості. Це означає, що інструмент можна налаштувати так, щоб він відповідав конкретним вимогам кожного проекту.

Оскільки OWASP ZAP є відкритим програмним забезпеченням, він має активну спільноту розробників та користувачів, які постійно вносять

покращення та оновлення. Це означає, що інструмент постійно розвивається та покращується, що допомагає забезпечити його актуальність у контексті змінюваних загроз безпеки.

Після ретельного вивчення характеристик кожного з представлених сканерів вразливостей, необхідно зробити осмислений вибір інструмента для проведення тестування. Вибір буде залежати від специфіки проекту, його вимог до безпеки, а також від ресурсів, що доступні для проведення тестування.

Кожен з розглянутих сканерів вразливостей — Nessus, Acunetix, Burp Scanner і OWASP ZAP — має свої унікальні особливості, переваги та недоліки. Деякі з них спеціалізуються на конкретних типах вразливостей або сферах застосування, інші надають більш універсальний набір інструментів.

Таблиця 1.2 представляє собою порівняльний аналіз чотирьох популярних сканерів вразливостей - Nessus, Acunetix, Burp Scanner та OWASP ZAP - за трьома ключовими параметрами: покриття вразливостей, точність діагностики та зручність використання. Кожен сканер оцінюється за шкалою від "погано" до "дуже добре".

Таблиця 1.2 – Критерії вимоги сканера

Назва / Вимоги	**Nessus**	**Acunetix**	**Burp Scanner**	**OWASP ZAP**
Покриття вразливостей	Добре	Дуже добре	Добре	Нормально
Точність діагностики	Добре	Дуже добре	Добре	Нормально
Зручність використання	Добре	Дуже добре	Нормально	Дуже добре

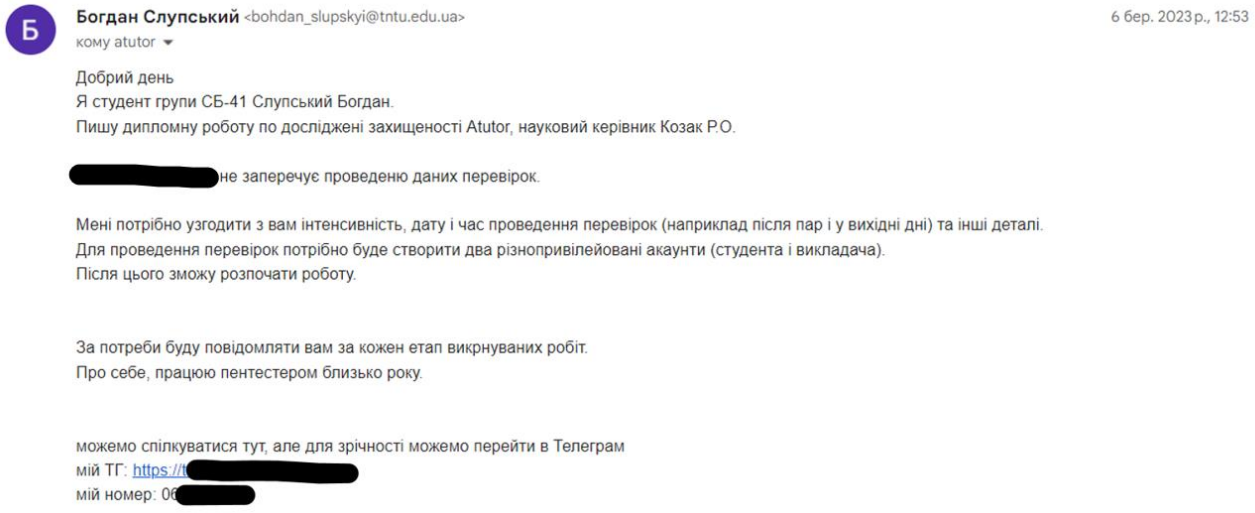
З урахуванням цього аналізу та особливостей мого дослідження, я вирішив вибрати Acunetix як інструмент для сканування вразливостей. Acunetix виявився особливо ефективним у виявленні веб-вразливостей, має добре покриття вразливостей та точність діагностики, а також забезпечує високий рівень зручності користування.

2.4 Підготовчі етапи до сканування

Одразу після вибору інструменту для сканування вразливостей, наступний важливий крок - підготовка цілі для сканування та отримання відповідних дозволів для проведення цього дослідження.

Виконання сканування без відповідного дозволу може призвести до небажаних наслідків, включаючи правові проблеми. Тому перед початком дослідження важливо з'ясувати, хто відповідає за систему, що підлягає тестуванню, та отримати від них відповідний дозвіл.

У моєму випадку, ціль дослідження - це система Atutor, яка використовується в Тернопільському національному технічному університеті. Я з'ясував, хто в університеті відповідає за Atutor, та з допомогою завідуючого кафедрою кібербезпеки, я зміг зв'язатися з відповідальною особою. Вони надали мені дозвіл на проведення дослідження захищеності системи Atutor, Після чого я зв’язався з адміністратором сервісу для більш детального обговорення робіт це показано на рисунку 1.3.


Б

Богдан Слупський <bohdan_slupskyi@tntu.edu.ua> 6 бер. 2023 р., 12:53

кому atutor

Добрий день
Я студент групи СБ-41 Слупський Богдан.
Пишу дипломну роботу по дослідженні захищеності Atutor, науковий керівник Козак Р.О.

[redacted] не заперечує проведеню даних перевірок.

Мені потрібно узгодити з вам інтенсивність, дату і час проведення перевірок (наприклад після пар і у вихідні дні) та інші деталі.
Для проведення перевірок потрібно буде створити два різнопривілейовані акаунти (студента і викладача).
Після цього зможу розпочати роботу.

За потреби буду повідомляти вам за кожен етап викрнуваних робіт.
Про себе, працюю пентестером близько року.

можемо спілкуватися тут, але для зрічності можемо перейти в Телеграм
мій ТГ: https://[redacted]
мій номер: 0[redacted]

Рисунок 1.3 – Повідомлення адміністратору

Після узгодження цілі для тестування, так і перед початком самого процесу сканування, критично важливо забезпечити відповідну комунікацію з усіма

зацікавленими сторонами. В моєму випадку, це було зроблено шляхом прямого звернення до адміністратора системи Atutor через електронну пошту.

На скріншоті нижче можна бачити, як я зв'язався з адміністратором та повідомив його про мої наміри провести дослідження захищеності. Я також поставив перед ним ряд важливих питань, що потребували узгодження перед початком процесу. Це включало такі питання, як створення додаткових акаунтів з яких буде проводитись перевірка внутрішнього периметра сервісу, та узгодження часу роботи та інтенсивності сканування.

Вже на наступний день я отримав відповідь від адміністратора, в якій він погодився на проведення тестування. Він також відповів на всі поставлені мною питання, що дозволило нам визначити конкретні параметри для подальшої роботи. На рисунку 1.4 показано що буде розгорнуто дзеркало системи з якої буде прибрана критична інформація. З цієї відповіді я отримав зелене світло для початку підготовчих дій до сканування вразливостей системи Atutor.

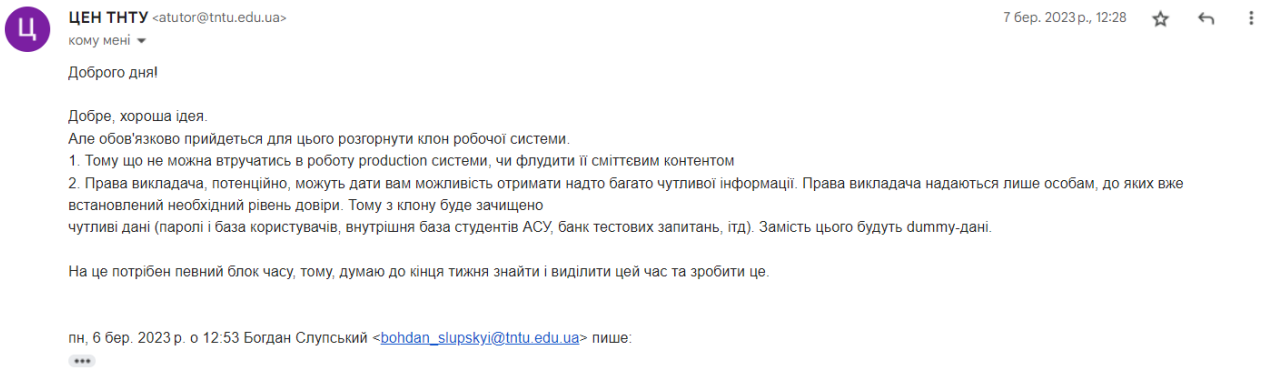


Рисунок 1.4 – Повідомлення адміністратора

Після отримання необхідних дозволів та узгоджень, наступним кроком у процесі підготовки до сканування було зняття обмежень на кількість одночасних запитів до сервера. Це важливий крок, оскільки обмеження, встановлені для захисту системи від DoS-атак, можуть вплинути на ефективність та точність сканування вразливостей.

Сканери вразливостей, як Acunetix, функціонують шляхом виконання великої кількості запитів до цілі, в цьому випадку до системи Atutor. Це включає

в себе надсилання різних видів запитів та аналіз відповідей сервера для виявлення потенційних вразливостей. Якщо обмеження на кількість запитів залишаються, сканер може не мати можливості провести повний аналіз або, що навіть гірше, отримати неправильні результати.

Тому, в ході подальшої комунікації з адміністратором, я попросив зняти обмеження на кількість одночасних запитів до сервера на час проведення сканування. На рисунку 1.5 продемонстровано домовленість про зняття захисту. Це допомогло забезпечити, що процес сканування пройде без перешкод і допоможе виявити всі потенційні вразливості системи Atutor.

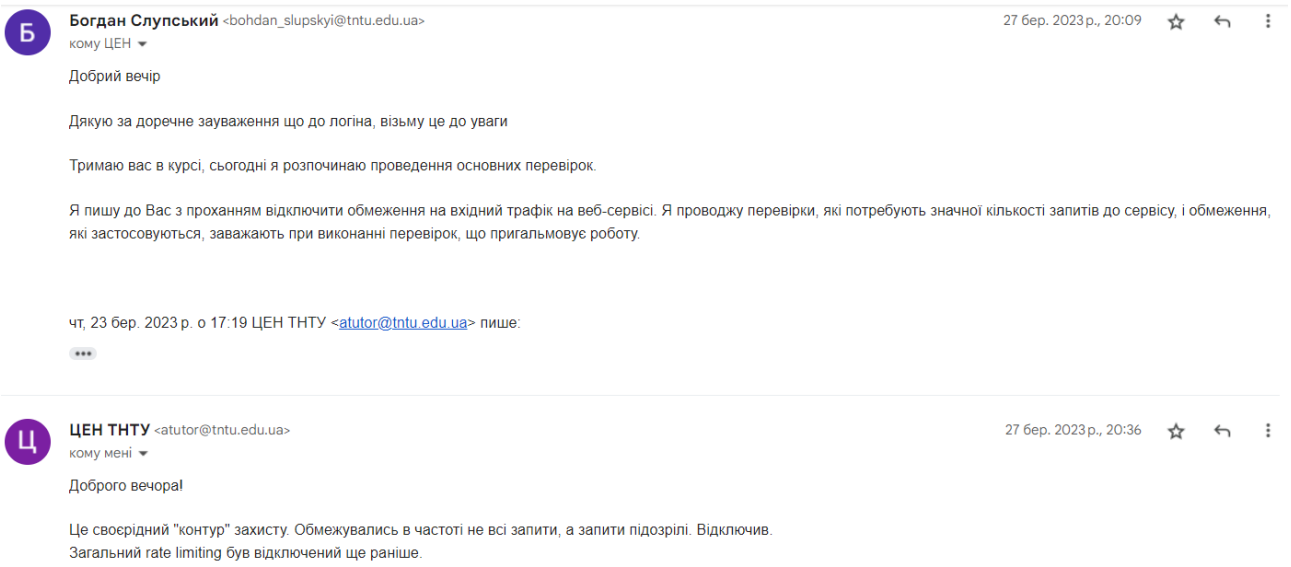


Рисунок 1.5 – Домовленість про зняття додаткового захисту

Продовжуючи підготовку до сканування, я отримав позитивну відповідь від адміністратора щодо моєї пропозиції зняти обмеження на кількість одночасних запитів до сервера. Це було критично важливим, оскільки ми можемо провести глибоке тестування без будь-яких перешкод.

Адміністратор також повідомив, що зняв інші механізми обмеження, які могли б блокувати підозрілі запити від нашого сканера вразливостей. Це було здійснено для того, щоб забезпечити максимально ефективне тестування та надійне виявлення вразливостей.

Таким чином, завдяки співпраці та підтримці адміністратора, ми змогли оптимізувати умови для проведення сканування. Наступним кроком буде безпосередньо сам процес сканування.

Після успішного погодження всіх необхідних деталей та успішного розгортання клону сервісу, я зміг перейти безпосередньо до проведення тестування безпеки. Оскільки ми працювали з клоном сервісу, мої дії не впливали на роботу основного сервісу та його користувачів. Це давало мені можливість виконувати сканування у зручний для мене час і досліджувати систему без обмежень, що в свою чергу забезпечувало глибокий аналіз та пошук потенційних вразливостей.

Однак, варто зазначити, що якби ми проводили тестування безпеки на основному сервісі, було б обов'язково узгодити час проведення робіт з адміністратором та іншими зацікавленими сторонами. Це необхідно для забезпечення того, що наші дії не перешкоджатимуть нормальній роботі сервісу і не заважатимуть користувачам. Проте у нашому випадку, завдяки роботі з клонованим сервісом, ми мали можливість зосередитися на тестуванні і гарантувати високий рівень дослідження системи без впливу на її реальну експлуатацію.

Часто при тестуванні безпеки веб-систем, особливо коли мова йде про внутрішні мережі організацій, можливо отримання більш глибоких або деталізованих даних через внутрішній доступ до системи порівняно з доступом зовні. Це може бути пов'язано з різними налаштуваннями захисту або доступу, встановленими в системі.

Проте в нашому випадку, під час проведення попередньої перевірки доступу до Atutor, як з внутрішніх, так і з зовнішніх адрес, помітної різниці у виявлених результатах не було виявлено. Це говорить про те, що система Atutor має однакові налаштування доступу та відгук на запити незалежно від місця з якого вони надходять.

Отже, я міг з упевненістю провести повноцінне сканування з зовнішніх адрес, без стурбованості щодо можливої неповноцінності отриманих

результатів. Відсутність різниці між внутрішніми та зовнішніми запитами вказує на рівний рівень захисту системи Atutor для всіх користувачів, незалежно від їх місцезнаходження.

Перед початком роботи з будь-яким інструментом тестування безпеки, включаючи сканер вразливостей, важливим етапом є вибір місця його розгортання. Місце розгортання може значною мірою вплинути на продуктивність інструменту та ефективність всього процесу тестування.

В моєму випадку, для розгортання сканера вразливостей Acunetix я вибрав свій персональний ноутбук. Рішення було обумовлене кількома причинами. По-перше, характеристики мого ноутбука були достатніми для підтримки повноцінної роботи Acunetix. По-друге, моя мережева інфраструктура мала достатню пропускну здатність для проведення ефективного сканування.

Окремо варто відмітити, що, хоча можливість використання хмарних сервісів для розгортання таких інструментів, як Acunetix, може бути корисною в деяких ситуаціях, в даному випадку я не вважав це необхідним. Це рішення також дозволило мені заощадити кошти, які могли бути витрачені на оренду хмарного сервісу.

Процес розгортання Acunetix на моєму ноутбуку був простим та інтуїтивно зрозумілим. Все необхідне програмне забезпечення було швидко завантажено з офіційного сайту розробника. Встановлення пройшло без будь-яких проблем або затримок. Важливим моментом є те, що вся процедура встановлення вимагає мінімального втручання користувача та обмежується в основному виконанням стандартних інструкцій, поданих у вікні інсталяції [12].

Після завершення процесу встановлення, сканер вразливостей Acunetix відразу був готовий до роботи. Це дозволило мені відразу перейти до налаштування параметрів сканування та підготовки до початку роботи над проектом. В цілому, простота розгортання та налаштування Acunetix позитивно впливає на зручність його використання, ефективність роботи та, в кінцевому рахунку, результати тестування безпеки.

Перш ніж розпочати процес сканування вразливостей, сканер Acunetix потребує певної конфігурації та налаштування, які залежать від специфіки перевіряємої системи та вимог безпеки.

На першому етапі потрібно створити новий проект у Acunetix, задати йому назву та опис, а також вказати адресу (URL) сайту або веб-системи, яку планується сканувати.

Далі, важливо налаштувати параметри сканування. Acunetix надає гнучкі налаштування сканування, що включає режими "повного сканування", "сканування вибраних вразливостей", "швидкого сканування" та інших. За умовчанням, рекомендовано використовувати режим "повного сканування" для найповнішого аналізу системи. Однак цей режим потребує більше часу.

У разі, коли веб-система вимагає авторизації для доступу до певних розділів, сканеру Acunetix можна передати дані для авторизації. Це дозволяє проводити глибше тестування внутрішніх розділів системи, що можуть бути недоступні без авторизації. Для цього ви використовуєте функцію "Автоматичне виявлення форм авторизації" або "Ручне налаштування" у разі, якщо автоматичне виявлення не працює коректно.

Після налаштування всіх параметрів, сканер Acunetix готовий до роботи. Та можна розпочинати основу частину роботи, сканування на вразливості.

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ТА ЗАХОДИ З ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ATUTOR

3.1 Принцип оцінювання рейтингу вразливостей

Після завершення сканування системи Acunetix надає детальні звіти про виявлені вразливості. Ці звіти містять важливу інформацію про кожну вразливість, включаючи опис, рекомендації щодо усунення та оцінку серйозності. Саме на цьому етапі проводиться аналіз результатів та розробка рекомендацій щодо зміцнення захищеності системи Atutor. Acunetix надає оцінку знайденим вразливостям за допомогою стандартом CVSS3.

Common Vulnerability Scoring System (CVSS) є універсальною системою оцінювання серйозності комп'ютерних вразливостей. Вона була розроблена на початку 2000-х років за ініціативою Форуму Безпеки Інформаційних Систем (FIRST) для введення стандартизованого методу оцінювання рівня серйозності вразливостей.

CVSS зазнав кілька великих оновлень від часу свого впровадження. Сьогодні ми оперуємо на основі третього покоління цього стандарту, відомого як CVSSv3.

– CVSSv1: Перше покоління CVSS було випущено у 2005 році. Воно ввело ряд базових метрик для оцінювання вразливостей, включаючи вплив на конфіденційність, цілісність та доступність системи.

– CVSSv2: Випущено у 2007 році, друге покоління CVSS дало кілька покращень і додало темпоральні та середовищні метрики, які дозволили оцінити вразливості в контексті конкретного середовища і врахувати такі фактори, як наявність виправлень або знань про вразливості.

– CVSSv3: Третє покоління, запущене у 2015 році, принесло більше гнучкості і точності в систему. Ця версія збільшила кількість метрик, уточнила оцінки і додала додаткові класифікації вразливостей. Зокрема, CVSSv3 враховує

такі фактори, як спосіб атаки, вимога до взаємодії з користувачем, та обсяг впливу вразливості.

CVSS дає змогу компаніям, органам управління безпекою та дослідникам з усього світу використовувати єдину, стандартизовану шкалу для оцінки рівня серйозності вразливостей. Вона враховує широкий спектр факторів, що можуть вплинути на загальний вплив вразливості і допомагає виробити реалістичний, виважений погляд на ризики, з якими стикається організація.

CVSSv3 використовує векторний підхід для оцінки вразливостей, який включає в себе декілька ключових метрик. Цей вектор вказує на значення кожної метрики в форматі "метрика:значення". Разом вони формують CVSSv3 вектор, який допомагає визначити кінцеву оцінку вразливості [13].

Метрики вектора поділяються на три групи: базові, темпоральні та середовищні.

Базові метрики оцінюють характеристики вразливості, які не змінюються з часом. Вони включають:

– Attack Vector (AV): Ця метрика вимірює, як атака може бути здійснена. Може бути: Network (N), Adjacent (A), Local (L), або Physical (P).

– Attack Complexity (AC): Вимірює, скільки умов поза контролем зловмисника має бути виконано, щоб атака була успішною. Може бути: Low (L) або High (H).

– Privileges Required (PR): Вказує, чи потрібні привілеї для успішного використання вразливості. Може бути: None (N), Low (L), або High (H).

– User Interaction (UI): Чи потрібна взаємодія користувача для експлуатації вразливості. Може бути: None (N) або Required (R).

– Scope (S): Чи впливає вразливість на інші компоненти, крім того, який був компроментований. Може бути: Unchanged (U) або Changed (C).

– Confidentiality, Integrity and Availability Impact (C, I, A): Вимірюють вплив вразливості на конфіденційність, цілісність та доступність системи. Може бути: None (N), Low (L) або High (H).

Після визначення всіх цих метрик, вони об'єднуються в CVSSv3 вектор, який виглядає приблизно так: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H. В цьому випадку, Attack Vector - мережевий (N), Attack Complexity - низька (L), Privileges Required - відсутні (N), User Interaction - відсутня (N), Scope - не змінено (U), і вплив на конфіденційність, цілісність та доступність - високий (H).

Цей вектор допомагає експертам з безпеки бачити, які фактори були враховані при оцінці вразливості, і відповідно планувати заходи щодо її усунення.

CVSSv3 спеціально обробляє всі ці вектори та надає систематичний підхід до оцінки серйозності вразливостей. Кожній метриці вектора присвоюється певний бал відповідно до її значення. Всі ці бали обчислюються разом, щоб встановити загальний рейтинг вразливості [14].

Рейтинг від 0 до 10 використовується для визначення серйозності вразливостей за стандартом CVSSv3. Зазвичай, чим вищий рейтинг, тим серйозніше вразливість. Загалом, рейтинги можуть бути такі:

– 0.0 - Вразливість відсутня або несуттєва.

– 0.1 - 3.9 - Низька серйозність. Вразливість може бути легко експлуатована або має обмежений вплив.

– 4.0 - 6.9 - Середня серйозність. Вразливість може бути помірно складною для експлуатації або мати помірний вплив.

– 7.0 - 8.9 - Висока серйозність. Вразливість може бути складною для експлуатації або мати значний вплив.

– 9.0 - 10.0 - Дуже висока серйозність. Вразливість може бути легко експлуатації або мати критичний вплив.

Цей діапазон балів дозволяє оцінювати серйозність вразливостей та встановлювати пріоритети для виправлення їх у системах. Ці рейтинги також використовуються в базі даних National Vulnerability Database (NVD), яка забезпечує інформацію про вразливості та їх серйозність для безпекової спільноти [15].

На основі вказаних метрик проводиться оцінка кожної вразливості. Проте, варто відзначити, що ці метрики не враховують місця виявлення вразливості та потенційну чутливу інформацію, яка може перебувати у зоні впливу цієї вразливості. З цієї причини, при оцінці вразливостей, виявлених у Atutor, я використовую оцінку, надану сканером Acunetix, але додатково переглядаю їх з урахуванням впливу цих вразливостей на критичні активи. Оскільки сканер не враховує цю конкретну інформацію при виставленні оцінки, моє завдання - забезпечити повну та об'єктивну оцінку вразливостей, враховуючи їх вплив на важливі ресурси системи.

3.2 Аналіз результатів сканування та оцінка вразливостей з пропозиції щодо їх усунення

Аналіз результатів сканування та оцінка вразливостей є важливим етапом в зміцненні безпеки системи. Однак, з огляду на публічний доступ до даної роботи та з міркувань безпеки, у тексті не будуть надані деталі щодо вразливостей, які мають рейтинг вище середнього (Medium). Також будуть застосовані обмеження щодо розголошення місця виявлення вразливостей та інших технічних деталей.

Це рішення приймається з метою забезпечення безпеки системи та запобігання можливому зловживанню інформацією. Проте, у рамках роботи будуть надані загальні рекомендації щодо усунення виявлених вразливостей. Оцінка вразливостей базується на стандартних процедурах та методиках, що дозволяють визначити їх серйозність та потенційний вплив на безпеку системи. Цей підхід дозволяє забезпечити безпеку інформації та системи, одночасно дотримуючись принципів конфіденційності та захисту. Список вразливостей буде представлений в тому ж порядку, що й надав сканер. Далі проводиться оцінка кожної вразливості з урахуванням її справжнього впливу на критичні активи.

Під час оцінки використовуються критерії та методики, що дозволяють визначити серйозність та потенційний вплив кожної вразливості. Особлива увага приділяється тим вразливостям, які можуть містити значний потенціал для зловживання та порушення безпеки системи.

На основі результатів оцінки сформулюються пропозиції та рекомендації щодо усунення виявлених вразливостей. Це може включати в себе патчі, оновлення програмного забезпечення, зміну налаштувань системи чи інші заходи, які спрямовані на підвищення безпеки та запобігання можливим атакам.

Список вразливостей:

1) Вразливі бібліотеки JavaScript. Характеристики вразливості по CVSS3:
   - Ризик: Середня
   - Оцінка: 6.5
   - Вектор: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Опис вразливості. Однією з виявлених вразливостей є використання вразливих бібліотек JavaScript. Під час сканування було виявлено, що використовується одна або кілька бібліотек, для яких відомо про наявність вразливостей. При детальному розгляді звіту сканера можна отримати інформацію про типи атак та посилання на більш детальну інформацію про виявлені вразливості.

Оцінка вразливості:

- CVSS3 Ризик: Середня
- CVSS3 Оцінка: 5.3
- CVSS3 Вектор: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Дані бібліотеки мають вразливі функції які є вразливими до XSS-атаки, але сервіс не використовує ці всі вразливі функції, тому можливість успішної експлуатації та впливу зменшується, також сервіс використовує блокування підозрілих запитів яким і є XSS тому можливість успішного використання даного недоліка ще більше зменшується, але ризик все одно залишається.

Рекомендації для виправлення вразливості. Потрібно оновити бібліотеку до актуальної версії.

1) HTTP Strict Transport Security (HSTS) не реалізовано. Характеристики вразливості по CVSS3:
   - Ризик: Несуттєва
   - Оцінка: 0.0
   - Вектор: AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Опис вразливості. HTTP Strict Transport Security (HSTS) є механізмом безпеки, який використовується для забезпечення безпечного з'єднання між веб-клієнтом і сервером. Він встановлюється на рівні веб-сайту і вказує браузерам, що весь трафік до цього сайту має відбуватися через захищений протокол HTTPS. Це захищає користувачів від атак типу Man-in-the-Middle (MITM), де зловмисники можуть перехоплювати та змінювати комунікацію між користувачем і сервером.

Нереалізація HTTP Strict Transport Security (HSTS) може мати серйозні наслідки для безпеки веб-додатків. Відсутність використання HSTS створює можливість для атак, таких як SSL-Strip атаки, де зловмисник може перехоплювати з'єднання із використанням незахищених протоколів, навіть якщо сервер підтримує HTTPS. Це дає зловмиснику можливість переглядати і змінювати комунікацію, використовуючи нешифрований протокол HTTP, що призводить до ризику викрадення конфіденційних даних, таких як паролі або особиста інформація.

Оцінка вразливості:

- CVSS3 Ризик: Незначна
- CVSS3 Оцінка: 3.4
- CVSS3 Вектор: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

При реалізації атаки на пониження з’єднання від якої має захищати hsts зловмисник може отримати повний доступ до сесії користувача, так як вона буде передаватися по не захищеному каналу зв’язку, але реалізація такої атаки є доволі складною та малоймовірно, але ризик залишається, тому її рівень буде піднятий.

Рекомендації для виправлення вразливості. Впровадити HSTS у веб-сервіс.

2) Файли cookie з відсутніми, непослідовними або суперечливими властивостями. Характеристики вразливості по CVSS3:
   - Ризик: Несуттєва
   - Оцінка: 0.0
   - Вектор: AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Опис вразливості.

Виявлення файлів cookie з відсутніми, непослідовними або суперечливими властивостями може мати важливі наслідки для безпеки веб-додатків. Файли cookie використовуються для зберігання та передачі інформації про користувачів, і якщо їх властивості неправильно вказані або суперечать одна одній, це може призвести до некоректної обробки та порушення безпеки. Наприклад, це може спричинити невідповідності в роботі автентифікації, виток конфіденційної інформації або можливість атак типу Cross-Site Scripting (XSS).

Оцінка вразливості:

- CVSS3 Ризик: Незначна
- CVSS3 Оцінка: 2.6
- CVSS3 Вектор: AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N

Хоча це і не є серйозною вразливість, але дані непослідовності та відсутність відповідних прапорців може погано вплинути на загальну захищеність, так як зловмиснику при викрадені сесії буде простіше її контролювати. Це не є вразливістю але її присутність спрощує життя зловмиснику.

Рекомендації для виправлення вразливості. Потрібно налаштувати файли cookie щоб вони відповідали стандартам.

3) Політика безпеки вмісту (CSP) не реалізована. Характеристики вразливості по CVSS3:
   - Ризик: Несуттєва
   - Оцінка: 0.0

– Вектор: AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Опис вразливості. Відсутність реалізації політики безпеки вмісту (Content Security Policy - CSP) може створювати потенційні загрози безпеці вашого веб-додатку. CSP є механізмом, який дозволяє контролювати джерела ресурсів, з яких може завантажуватись вміст на сторінках вашого веб-сайту. Це важливий захисний захід проти атак, таких як Cross-Site Scripting (XSS) та інших типів вразливостей.

Відсутність реалізації CSP може створювати ризик небезпечних сценаріїв, де зловмисники можуть вплинути на вміст, який відображається на сторінках вашого веб-сайту. Це може призвести до впровадження шкідливого коду, крадіжки даних користувачів або розповсюдження шкідливого вмісту серед відвідувачів. Втілення політики безпеки вмісту (CSP) дозволить обмежити джерела ресурсів, що можуть бути завантажені, та запобігти можливим атакам на ваш веб-сайт.

Оцінка вразливості:

– CVSS3 Ризик: Незначна
– CVSS3 Оцінка: 2.6
– CVSS3 Вектор: AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N

Відсутність (CSP) не є серйозним недоліком, так як цим не викликає жодних вразливостей, але тим що він відсутній він не буде пом’якшувати інші вразливості, тому при успішній експлуатації іншої вразливості не буде кому її пом’якшити.

Рекомендації для виправлення вразливості. Впровадити політику безпеки вмісту (CSP) у вашу веб-програму.

4) Завантаження файлів. Характеристики вразливості по CVSS3:

– Ризик: Несуттєва
– Оцінка: 0.0
– Вектор: AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Опис вразливості. Сторінки, які дозволяють відвідувачам завантажувати файли на сервер, можуть створювати потенційні ризики безпеки, якщо з ними

необережно поводитись. Веб-додатки, які дозволяють користувачам завантажувати файли, такі як малюнки, зображення, звуки тощо, повинні бути належним чином захищені.

Недостатні контролі та перевірки під час завантаження файлів можуть використовуватись зловмисниками для впровадження шкідливого коду на сервер. Наприклад, зловмисник може створити спеціально сформований файл з підробленим ім'ям або типом MIME і відправити його на сервер за допомогою запиту POST. Це може призвести до виконання небажаного або небезпечного коду на сервері.

Оцінка вразливості:

- CVSS3 Ризик: Середня
- CVSS3 Оцінка: 4.8
- CVSS3 Вектор: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

Дозволено довільне завантаження будь якого файл в систему, але при спробі завантажити шкідливий код він не міг виконатись через внутрішні обмеження та роботу системи захисту, імовірність що її вдасться обійти доволі мала, але присутня тому вразливість піднята до середньої.

Рекомендації для виправлення вразливості. Для усунення цієї вразливості необхідно належним чином перевіряти та обробляти завантажувані файли, використовуючи механізми валідації типу файлу, обмеження розміру, а також регулярні оновлення та патчі для безпеки веб-додатків.

5) Цілісність підресурсу (SRI) не реалізовано. Характеристики вразливості по CVSS3:
   - Ризик: Несуттєва
   - Оцінка: 0.0
   - Вектор: AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Опис вразливості. Цілісність підресурсу (SRI) є важливою функцією безпеки, яка забезпечує перевірку цілісності сторонніх ресурсів, що завантажуються у браузер. Відсутність реалізації SRI створює потенційну

вразливість, оскільки зловмисник з можливістю доступу до або зламуванням хостингу CDN може змінювати або підробляти файли ресурсів.

За допомогою SRI розробники можуть вказувати криптографічний хеш для відповідного ресурсу, який повинен відповідати отриманому файлу. Цей хеш вказується як атрибут цілісності у тегу HTML-елемента, наприклад, <script>. Хеш включає префікс, що залежить від алгоритму хешування, як-то sha256, sha384 або sha512. Таким чином, SRI допомагає перевіряти, чи не були змінені ресурси під час їх доставки, запобігаючи можливім атакам зловмисників.

Оцінка вразливості:

- CVSS3 Ризик: Незначна
- CVSS3 Оцінка: 2.6
- CVSS3 Вектор: AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N

Дана вразливість має малу ймовірність експлуатації, але при успішному використанню даного недоліка є велика ймовірність впливу на критичні активи, хоча вплив і незначний, але ризик присутній.

Рекомендації для виправлення вразливості. Потрібно реалізувати SRI для всіх сторонніх ресурсів, зокрема для завантажуваних сценаріїв з зовнішніх хостів. Це дозволить забезпечити цілісність і недоторканність ресурсів, запобігаючи можливим атакам та неправомірним маніпуляціям зі сторони зловмисників.

Таблиця 1.3 – Кількість знайдених вразливостей

Рейтинг	кількість
Серйозні	
Високі	3
Середні	2
Низькі	4
Несуттєві	

Таким чином, на основі аналізу кількісного представлення виявлених вразливостей і їх загального впливу можна зробити висновок, що Atutor

виявляється добре захищеним, але існує потенціал для подальшого покращення та забезпечення ще вищого рівня безпеки.

Усунення виявлених вразливостей не потребує значних ресурсів або великих зусиль. Багато з них можуть бути виправлені шляхом простих корекцій або патчів програмного забезпечення. Наприклад, оновлення до останньої версії Atutor або встановлення необхідних заходів безпеки, таких як фаервол або використання сильних паролів, можуть значно знизити ризик вразливостей.

Додатково, варто зазначити, що для усунення вразливостей не потрібно проводити радикальні зміни архітектури системи або проводити довготривалі проекти. Більшість вразливостей можуть бути виправлені швидко та ефективно шляхом виконання рекомендованих дій і впровадження простих заходів безпеки. Навіть малі зміни та покращення можуть мати значний вплив на загальну безпеку системи.

Отже, усунення вразливостей Atutor не вимагає великих ресурсів або значних затрат часу. Заснування на простих корекціях, патчах та впровадженні базових заходів безпеки може суттєво зміцнити безпеку системи, знизити кількість вразливих точок та забезпечити надійний захист критичної інформації.

3.3 Додаткові поради по плануванню зміцнення безпеки

Створення та впровадження системи класифікації даних (Data Classification) є важливим етапом у плануванні зміцнення безпеки. Класифікація даних дозволяє визначити рівень конфіденційності, цінності та чутливості інформації, що зберігається та обробляється в організації. Відсутність чіткої класифікації може призвести до неправильного розміщення заходів забезпечення безпеки та розподілу ресурсів.

Мої напрацювання включають навчальні матеріали та матеріали для оцінювання знань, що допоможуть організації усвідомити важливість класифікації даних і навчити співробітників її застосовувати. Також я розробив підходи до захисту персональної інформації користувачів, що допоможуть

забезпечити її конфіденційність та захист від несанкціонованого доступу. Крім того, мої напрацювання включають інформацію про систему та її налаштування, що допоможе організації зрозуміти, які аспекти потребують особливої уваги з точки зору безпеки.

Рекомендую використовувати ці напрацювання як основу для створення класифікації критичної інформації вашої організації. За потреби, ви можете додатково доопрацювати ці напрацювання, щоб вони повністю відповідали вашим вимогам та особливостям. Важливо мати чітку систему класифікації даних, щоб правильно визначити рівень захисту та виробити стратегію забезпечення безпеки, що відповідає потребам вашої організації.

Додатково, рекомендується провести оцінку ризиків для кожного класифікованого типу даних. Це дозволить виявити потенційні загрози та вразливості, пов'язані з цими типами даних, і призначити пріоритетність заходів з підвищення безпеки. Наприклад, персональні дані можуть бути більш вразливі до порушень конфіденційності, тому можуть знадобитись додаткові заходи захисту, як от шифрування або обмеження доступу. У той же час, інформація про систему може бути більш чутливою до вторгнень або змін налаштувань, тому засоби контролю доступу та моніторингу можуть бути необхідними.

Після створення та впровадження системи класифікації даних, рекомендується регулярно переглядати та оновлювати її з урахуванням змін у бізнес-процесах та загрозах безпеці. Це дозволить забезпечити актуальність та ефективність заходів зміцнення безпеки. Крім того, важливо проводити навчання та підвищувати свідомість співробітників щодо класифікації даних та правил безпеки, щоб забезпечити їх активну участь у процесі забезпечення безпеки і захисту конфіденційної інформації.

Загальною метою створення та впровадження системи класифікації даних є забезпечення цілісності, конфіденційності та доступності інформації в організації. Це допоможе уникнути можливих порушень безпеки, виявлення та швидкого реагування на загрози, а також захистити критичну інформацію від несанкціонованого

Наступною рекомендацією є що після усунення виявлених вразливостей є домовленість про повторне проведення перевірок з метою перевірки ефективності зміцнення безпеки. Це дозволяє переконатися, що всі вразливості були успішно усунені і система стала більш захищеною. Повторна перевірка може бути проведена спеціалістами з безпеки або залученням зовнішніх консультантів.

Крім того, рекомендується планувати регулярні щорічні перевірки безпеки для виявлення потенційних вразливостей. Це дозволить організації виявляти нові загрози та вразливості, що можуть з'явитися з часом, та приймати відповідні заходи для їх усунення. Регулярні перевірки допоможуть підтримувати високий рівень безпеки і запобігати потенційним інцидентам.

Важливо врахувати, що підхід до планування та проведення перевірок може варіюватися в залежності від специфіки організації, її розміру та ризиків. Рекомендується залучати професіоналів з інформаційної безпеки для оптимального планування та реалізації процесу перевірок з метою забезпечення надійного захисту даних та систем організації.

Зазвичай період у один рік є цілком достатнім для проведення регулярних перевірок безпеки, якщо організація відповідально ставиться до питань інформаційної безпеки. Протягом цього періоду відбуваються зміни в технологіях, загрозах та знаннях у сфері безпеки, тому регулярні перевірки дозволяють оцінити актуальну стан безпеки і приймати відповідні заходи.

Організація, яка дбає про свою інформаційну безпеку, може включити в план роботи щорічні перевірки з метою оцінки потенційних вразливостей і забезпечення відповідного рівня захисту. Цей підхід дає можливість реагувати на нові загрози та змінювати установки безпеки відповідно до сучасних вимог та стандартів. Виконання регулярних перевірок сприяє збереженню високого рівня безпеки, зменшенню ризиків і забезпеченню довіри до інформаційних систем організації.

При плануванні зміцнення безпеки рекомендується включити статичний та динамічний аналіз коду. Ці методи дозволяють виявити потенційні вразливості

та помилки в програмному коді з метою запобігання можливим атакам і зловживанням [16].

Статичний аналіз коду виконується на етапі розробки або після нього і дозволяє перевірити програмний код на виявлення потенційних проблем без його фактичного виконання. Цей вид аналізу допомагає виявити вразливості, такі як недостатні перевірки вхідних даних, вразливості SQL-ін'єкції, некоректне управління пам'яттю та інші. Результати статичного аналізу надають розробникам інформацію про можливі вразливості, які можуть бути виправлені до випуску продукту або під час регулярних оновлень.

Динамічний аналіз коду виконується під час роботи програми або веб-додатку і дозволяє перевірити його на вразливості в реальному часі. Цей тип аналізу включає в себе тестування з використанням спеціалізованих інструментів та враження, щоб симулювати різні сценарії атак. Динамічний аналіз допомагає виявити вразливості, які можуть бути використані для злому або незаконного доступу до системи. Результати динамічного аналізу надають важливу інформацію про потенційні ризики і дозволяють розробникам прийняти відповідні заходи для їх усунення.

Статичний та динамічний аналіз коду є ефективними інструментами для виявлення вразливостей та забезпечення високого рівня безпеки програмного забезпечення. Ці перевірки допомагають виявити проблеми ще до їх використання зловмисниками та забезпечити безпеку вашої системи та даних.

Обидва типи аналізу коду - статичний і динамічний - є важливими інструментами для забезпечення безпеки програмного забезпечення. Статичний аналіз дозволяє виявити потенційні вразливості на етапі розробки, що дозволяє розробникам виправити їх до випуску продукту. З іншого боку, динамічний аналіз виконується в реальному часі і допомагає виявити вразливості, які можуть бути використані зловмисниками для атак на систему.

Обидва аналізи допомагають забезпечити високий рівень безпеки шляхом виявлення і усунення потенційних проблем у програмному коді. Вони є важливою частиною процесу планування зміцнення безпеки і допомагають

зменшити ризик вразливостей і можливостей зламу системи. Рекомендується регулярно проводити ці аналізи, особливо після внесення змін у програмне забезпечення або його оточення, щоб переконатися, що система залишається безпечною та захищеною від нових загроз.

Додаткові поради щодо усунення виявлених вразливостей можуть суттєво зміцнити безпеку системи та зменшити кількість потенційних точок входу для зловмисників. Ці рекомендації базуються на кращих практиках інформаційної безпеки і спрямовані на підвищення рівня захисту.

Поради щодо класифікації інформації допоможуть краще організувати безпеку цих даних. Класифікація даних визначає їх значимість та рівень конфіденційності, що дозволяє налагодити відповідні контрольні механізми та обмеження доступу. Це важлива складова ефективного планування безпеки.

Додаткові перевірки статичного і динамічного аналізу коду є ще одним кроком у зміцненні безпеки роботи системи. Статичний аналіз допомагає виявити потенційні вразливості на етапі розробки, тоді як динамічний аналіз виконується в реальному часі для виявлення вразливостей під час роботи системи. Ці перевірки допомагають ідентифікувати можливі слабкі місця та помилки в коді, що дозволяє виправити їх і підвищити безпеку системи.

Використання цих рекомендацій є загальноприйнятою практикою і гарантує високий рівень безпеки. Вони детально структуровані і орієнтовані на виявлення та усунення потенційних загроз. Застосування цих рекомендацій дозволить забезпечити відповідний рівень захисту і зменшити ризик вразливостей системи перед потенційними зловмисниками.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ ТА ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Ергономічні проблеми безпеки життєдіяльності при роботі за комп'ютером

У сучасному світі все більше людей проводять значну частину свого робочого часу за комп'ютером, що призводить до ряду ергономічних проблем, які негативно впливають на безпеку та здоров'я людей. Неправильна позиція тіла, незручне розташування робочого місця, тривале сидіння та напружена робота з клавіатурою та мишею спричиняють м'язове напруження, біль у спині та напругу очей, що викликає дискомфорт та незручності [17].

Розташування робочого місця відіграє важливу роль у забезпеченні безпеки та здоров'я під час роботи за комп'ютером. Оптимальна висота столу та стільця є ключовим фактором для забезпечення комфорту і підтримки правильної позиції тіла. Стіл належної висоту, щоб лікті могли спокійно розташовуватися на клавіатурі, а стопи - на підлозі. Стілець обладнаний підтримкою для спини та належними регульованими підлокітниками. Клавіатура розташована на рівні ліктів, монітор - належним чином вирівняний перед очима, а миша - в зоні доступу для зап'ястя. Правильне розташування робочого місця сприяє уникненню незручностей та проблем зі здоров'ям.

Ергономічні пристрої підтримки є корисними для забезпечення комфорту та запобігання напрузі м'язів. Використання регульованих підлокітників та підставок для зап'ястя допомагає знизити напругу на м'язах і запобігти незручностям. Оптимальне розташування робочого місця повинне враховувати індивідуальні особливості користувача та забезпечувати комфортні умови для роботи.

Правильна позиція тіла та рухи є ключовими факторами для забезпечення комфорту та запобігання напрузі м'язів та незручностям. Важливо пам'ятати про правильну позицію спини та уникати підгорблення або надмірного нахилу

голови під час тривалої роботи за комп'ютером. Регулярні перерви для розтяжки та руху є важливими для підтримання здоров'я. Прості фізичні вправи, такі як розтягування шиї, плечей, рук і ніг, допомагають зняти напругу з м'язів та покращити кровообіг. Регулярні перерви дозволяють розслабитися і зберегти енергію для продуктивної роботи.

Очі є одними з найбільш вразливих органів під час роботи за комп'ютером. Постійне спрямування погляду на екран призводить до напруження та втому очей. Для зменшення негативного впливу необхідно використовувати екрани з антиблисковим покриттям, яке знижує відблиск та рефлексію світла. Також важливо налаштовувати яскравість та контрастність екрану для комфортного сприйняття. Щоб зменшити напругу на очі, необхідно робити перерви для відпочинку, фокусуючись на далеких предметах або виконуючи вправи для розслаблення очей.

Використання неправильної клавіатури та миші призводить до м'язового напруження і тунельного синдрому. Важливо використовувати ергономічні клавіатури та миші з додатковою підтримкою для зап'ястя та комфортною формою. Правильна позиція рук та зап'ястя під час роботи з ними має велике значення. Регулярні перерви для розтяжки рук та масажу зап'ястя допомагають уникнути негативних наслідків від тривалого використання клавіатури та миші.

Розглядаючи ергономічні проблеми безпеки життєдіяльності при роботі за комп'ютером, варто зазначити, що їх вирішення є ключовим для забезпечення безпеки та здоров'я під час роботи. Дотримання принципів ергономіки, налагодження робочого місця, правильна позиція тіла та виконання фізичних вправ сприяють покращенню безпеки та створенню здорового робочого середовища. Застосування ергономічних пристроїв підтримки, таких як регульовані підлокітники та підставки для зап'ястя, також сприяє комфорту та попередженню незручностей.

Загальною метою є створення безпечного та здорового робочого середовища для людей, які працюють за комп'ютером та виконують дослідження захищеності веб сервісу електронного навчання Atutor, що забезпечує

збереження здоров'я та підвищення продуктивності працівників, сприяє запобіганню травмам та ергономічним проблемам, а також сприяє загальному комфорту та задоволенню від роботи.

Додатково, важливо зазначити, що належна освітленість приміщення також є важливим фактором, який впливає на комфорт та здоров'я під час роботи за комп'ютером. Потрібно забезпечити достатнє природне або штучне освітлення, яке не перевантажує очі. Розміщення робочого місця біля вікна або використання належної освітлювальної техніки допомагає забезпечити оптимальні умови освітлення. Важливо також уникати відблисків на екрані, розташовуючи монітор під правильним кутом до джерел світла.

Безпека та конфіденційність інформації також є важливим аспектом при роботі за комп'ютером. Важливо зберігати конфіденційні дані та захищати їх від несанкціонованого доступу. Використання паролів, шифрування даних та регулярне оновлення програмного забезпечення допомагає забезпечити безпеку інформації. Крім того, необхідно усвідомлювати потенційні загрози з боку шкідливих програм та фішингових атак і приймати заходи для їх запобігання, такі як використання антивірусного програмного забезпечення та обережне відкривання електронних листів та посилань.

Нарешті, регулярне навчання та свідомість про важливість ергономіки та безпеки при роботі за комп'ютером є важливими. Люди повинні мати доступ до інформації щодо правильних методів роботи, виконання пауз і фізичних вправ, а також процедур безпеки. Організації можуть проводити навчання та інформаційні кампанії, щоб підвищити свідомість та забезпечити правильну поведінку під час роботи за комп'ютером.

Враховуючи всі ці аспекти, створення комфортного, безпечного та здорового робочого середовища є важливим завданням як для працівників, так і для роботодавців. Захист здоров'я та добробуту працівників при роботі за комп'ютером не тільки покращує їхню якість життя, але й сприяє збільшенню продуктивності та задоволення від роботи, що має позитивний вплив на всю організацію.

4.2 Долікарська допомога при переломах

Долікарська допомога при переломах є невід'ємною складовою управління травматичними пошкодженнями та вимагає негайного втручання. Переломи ставлять під загрозу функцію та мобільність ушкоджених кінцівок і потребують належного визначення та вмілого застосування принципів долікарської допомоги. У розділі розглядаються ключові аспекти, пов'язані з розпізнаванням симптомів, наданням першої допомоги, іммобілізацією та фіксацією, транспортуванням та доглядом при переломах [18].

Вчасне та точне розпізнавання симптомів перелому є вирішальним для надання ефективної долікарської допомоги. Серед основних симптомів перелому варто враховувати болісність ушкодженої області, набряк, видиму деформацію або зміну форми кінцівки, обмежену рухомість та звукові ефекти, які можуть виникати при русі. При оцінці симптомів важливо звернути увагу на їхню інтенсивність та поширення, а також на наявність супутніх пошкоджень, таких як виразкові рани чи пошкодження судин.

Дотримання правильних методів розпізнавання симптомів, таких як ретельне опитування постраждалого, фізичне обстеження та використання додаткових діагностичних методів, є важливими кроками у визначенні наявності перелому та його характеристик.

Належне надання першої допомоги при переломах має вирішальне значення для забезпечення комфорту та безпеки постраждалого перед професійною медичною допомогою. Перш за все, важливо підтримувати спокій та заспокоїти постраждалого, створюючи безпечну обстановку навколо нього.

У разі відкритого перелому слід накласти стерильну пов'язку або чисту тканину на рану для запобігання інфекції. Для зупинки кровотечі використовувати прямий тиск на поранену ділянку або накласти тугу пов'язку над ушкодженою кінцівкою. При закритому переломі необхідно забезпечити іммобілізацію ушкодженої кінцівки, застосувавши шину або імпровізовану фіксацію, щоб забезпечити стабільність та запобігти подальшим ушкодженням.

Постраждалому слід забезпечити анальгезію для зменшення болю, застосувати холод або протизапальні засоби. Одночасно важливо забезпечити психологічну підтримку та заспокоєння, висловлюючи розуміння та підтримку.

Ефективне транспортування потерпілого з переломами вимагає обережності та використання відповідних методів для забезпечення комфорту та безпеки. При пересуванні постраждалого необхідно уникати подальших пошкоджень та додаткових ушкоджень, тому необхідно використовувати правильну техніку підняття та перенесення.

Першочерговим варіантом є виклик екстреної медичної допомоги по номеру 103 та очікування на професійне транспортування. Якщо немає доступу до екстреної медичної допомоги, слід враховувати різні фактори, такі як розташування пошкодження, тип перелому та стан постраждалого при прийнятті рішення щодо транспортування.

Необхідно забезпечити стабільність постраждалого під час пересування, використовуючи підкладки, фіксаційні матеріали та ергономічні засоби для перенесення. Контроль за станом потерпілого та негайне звернення до медичних фахівців за допомогою є необхідними кроками під час транспортування.

Долікарська допомога при переломах є невід'ємною складовою у наданні першої медичної допомоги та забезпеченні безпеки та комфорту постраждалих. Розпізнавання симптомів, надання першої допомоги, правильне імобілізування та транспортування - це ключові аспекти долікарської допомоги при переломах. Виконання цих кроків з уважністю та професіоналізмом може сприяти швидкому одужанню та зменшенню ускладнень.

Участь медичного персоналу є необхідною під час надання долікарської допомоги при переломах, оскільки вони мають необхідні знання та навички для правильної оцінки, лікування та догляду за постраждалими. Важливо негайно звернутися до медичних фахівців, які зможуть надати професійну медичну допомогу та виконати необхідні процедури, такі як рентгенографія, гіпсування або хірургічні втручання.

Постраждалі з переломами мають бути під наглядом медичного персоналу під час лікування та реабілітації. Медичні фахівці здатні оцінити стан перелому, призначити необхідну терапію та контролювати процес загоєння. Регулярні огляди та планові рентгенографії допомагають визначити ефективність лікування та необхідність коригування терапії.

Для оптимального одужання після перелому необхідна комплексна реабілітація, яка включає фізіотерапію, заняття з лікарями-терапевтами та інші методи відновлювальної медицини. Реабілітаційні заходи спрямовані на відновлення функції та мобільності ушкоджених кінцівок, попередження ускладнень та підвищення якості життя постраждалого.

Враховуючи всі ці аспекти долікарської допомоги, потрібно зробити висновок про важливість швидкого та належного реагування на переломи. Чим швидше і правильніше будуть надані долікарські заходи, тим більше шансів на успішне одужання та повернення до повноцінного життя має постраждалий.

ВИСНОВОК

У даному дослідженні була проведена аналіз захищеності веб-сервісу електронного навчання Atutor. Зокрема, було виявлено потенційні вразливості та оцінено їх вплив на критичні активи системи. На основі цього аналізу були надані рекомендації щодо усунення знайдених вразливостей.

Отримані результати дослідження мають велике значення для зміцнення безпеки Atutor. Виявлення та усунення вразливостей сприятимуть зниженню ризику можливих атак та зловживань. Подані рекомендації щодо формування лейблування для критичної інформації допоможуть покращити оцінку стану захищеності системи та раціональніше планувати майбутні заходи щодо підвищення безпеки.

Завдяки виконанню поставленої мети дослідження, вдалося ідентифікувати потенційні загрози та запропонувати ефективні заходи для їх усунення. Це забезпечує підвищення безпеки Atutor і зниження ризиків, пов'язаних з можливими атаками та незаконним доступом до системи.

У підсумку, дане дослідження приводить до важливих результатів щодо зміцнення безпеки Atutor. Виявлені вразливості були аналізовані, їх вплив оцінений, і надані рекомендації щодо усунення. Це сприятиме поліпшенню захисту системи та зменшенню потенційних загроз. Дослідження виконано з врахуванням якісних і кількісних показників, що підкреслює достовірність отриманих результатів.

Залежно від контексту дослідження та вимог, можуть бути розроблені подальші стратегії та заходи з покращення безпеки Atutor, зокрема, регулярні аудити, вдосконалення політик безпеки та залучення додаткових інструментів для моніторингу та захисту системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Держспецзв'язку: кількість кібератак на Україну продовжує зростати [Електронний ресурс] // Кабмін України. – Режим доступу: https://www.kmu.gov.ua/news/derzhspeczvyazku-kilkist-kiberatak-na-ukrayinu-prodovzhuye-zrostati

2. ATutor Learning Management System [Електронний ресурс]. – Режим доступу: https://atutor.github.io/atutor/index.html

3. ATutor Features [Електронний ресурс]. – Режим доступу: https://atutor.github.io/atutor/features.html

4. Atutor Atutor : CVE security vulnerabilities, versions and detailed reports [Електронний ресурс]. – Режим доступу: https://www.cvedetails.com/product/13342/Atutor-Atutor.html?vendor_id=7805

5. Main features of ATutor [Електронний ресурс]. – Режим доступу: https://dl.tntu.edu.ua/downloads/Main-features.pdf

6. ATutor Developer Guidelines [Електронний ресурс]. – Режим доступу: https://atutor.github.io/developer/guidelines.html

7. ATutor at Ternopil Ivan Puluj National Technical University [Електронний ресурс]. – Режим доступу: https://dl.tntu.edu.ua/showpage.php?id=8

8. AContent Learning Content Management System (LCMS) [Електронний ресурс]. – Режим доступу: https://atutor.github.io/acontent/index.html

9. What are the different information classification categories available in TCS? [Електронний ресурс] // Helpr.me. – Режим доступу: https://uk.helpr.me/2722-what-are-the-different-information-classification-categories-available-in-tcs

10. Technical evaluation of information environment security | EY Ukraine [Електронний ресурс] // EY Ukraine. – Режим доступу: https://www.ey.com/uk_ua/consulting/technical-evaluation-of-information-environment-security

11. Top 10 Most Powerful Vulnerability Assessment Scanning Tools 2021 | MyServerName.com UK [Електронний ресурс] // MyServerName.com UK. – Режим

доступу: https://uk.myservername.com/top-10-most-powerful-vulnerability-assessment-scanning-tools-2021

12. Як провести аудит безпеки з допомогою Acunetix Vulnerability Scanner? | KR Labs Blog [Електронний ресурс] // KR Labs Blog. – Режим доступу: https://blog.kr-labs.com.ua/%D1%8F%D0%BA-%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D1%81%D1%82%D0%B8-%D0%B0%D1%83%D0%B4%D0%B8%D1%82-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-%D0%B7-%D0%B4%D0%BE%D0%BF%D0%BE%D0%BC%D0%BE%D0%B3%D0%BE%D1%8E-acunetix-vulnerability-scanner-f69e9cc77eca?gi=f0d21b5626a1

13. CVSS V3 Calculator | NIST National Vulnerability Database (NVD) [Електронний ресурс] // NIST National Vulnerability Database (NVD). – Режим доступу: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

14. CVSS v3 User Guide | FIRST.org, Inc. [Електронний ресурс] // FIRST.org, Inc. – Режим доступу: https://www.first.org/cvss/v3.0/user-guide

15. CVSS v3 Metrics | NIST National Vulnerability Database (NVD) [Електронний ресурс] // NIST National Vulnerability Database (NVD). – Режим доступу: https://nvd.nist.gov/vuln-metrics/cvss

16. Static and Dynamic Testing Methods | QATestLab Blog [Електронний ресурс] // QATestLab Blog. – Режим доступу: https://training.qatestlab.com/blog/technical-articles/static-and-dynamic-testing-methods/

17. Huber, B., & Gambardella, L., Occupational Ergonomics: Principles and Applications.

18. Smith, J., Brown, A., & Johnson, C., Management of fractures: an overview // Journal of Orthopedic Trauma. – 2018. – DOI: 10.1097/BOT.0000000000001066.