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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Технічна оцінка захищеності вебсайту Великоберезовицької територіальної громади*

Виконав(ла): студент(ка) 4 курсу, групи СБ-41
спеціальності *125 «Кібербезпека»*
(шифр і назва спеціальності)

	(підпис)	*Бурмістрова Н.А.* (прізвище та ініціали)
Керівник	(підпис)	*Козак Р.О.* (прізвище та ініціали)
Нормоконтроль	(підпис)	(прізвище та ініціали)
Завідувач кафедри	(підпис)	*Загородна Н.В.* (прізвище та ініціали)
Рецензент	(підпис)	(прізвище та ініціали)

Тернопіль
2023

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

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

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
« » 20___ р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Бурмістровій Наталії Андріївній
(прізвище, ім'я, по батькові)

1. Тема роботи Технічна оцінка захищеності вебсайту Великоберезовицької територіальної громади

Керівник роботи Козак Руслан Орестович к.т.н,, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*03*» *04* 2023 року № *4/7-349*

2. Термін подання студентом завершеної роботи 17.06.2023

3. Вихідні дані до роботи вимоги до проведення оцінювання захищеності веб-ресурсу

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз вимог до оцінки веб-ресурсу на наявність вразливостей, аналіз можливих рішень поставленого завдання, проблеми безпеки сайтів на Joomla: Аналіз та заходи захисту, порівняння та аналіз сканерів вразливостей, аналіз та оцінка результатів сканування, ключові налаштування та конфігурація сканера Nessus, аналіз результатів сканування. оцінка знайдених вразливостей, розробка плану виправлення вразливостей

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

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	*Виконано*
2.	Аналіз вимог до системи захисту інформації	20.02 – 25.02	*Виконано*
3.	Аналіз можливих рішень поставленого завдання	26.02 – 14.03	*Виконано*
4.	Проблеми безпеки сайтів на Joomla: Аналіз та заходи захисту	15.03 – 16.03	*Виконано*
5.	Порівняння та аналіз сканерів вразливостей	16.03-27.04	*Виконано*
6.	Ключові налаштування та конфігурація сканера Nessus	27.03 – 15.04	*Виконано*
7.	Аналіз результатів сканування	16.04 – 29.04	*Виконано*
8.	Оцінка знайдених вразливостей	30.04 – 13.05	*Виконано*
9.	Розробка плану виправлення вразливостей	14.05 – 21.05	*Виконано*
10.	Виконання розділу «Безпека життєдіяльності, основи охорони праці»	22.05 – 05.06	*Виконано*
11.	Оформлення кваліфікаційної роботи	06.06 – 12.06	*Виконано*
12.	Нормоконтроль	10.06 – 15.06	*Виконано*
13.	Перевірка на плагіат	16.06 – 18.06	*Виконано*
14.	Попередній захист кваліфікаційної роботи	19.06 – 20.06	*Виконано*
15	Захист кваліфікаційної роботи	20.06.2023	

Студент _____ _____
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Технічна оцінка захищеності вебсайту Великоберезовицької територіальної громади // Кваліфікаційна робота ОР «Бакалавр» // Бурмістрова Наталія Андріївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // С. __ , рис. – __, табл. – __ , кресл. – , додат. – ___.

Ключові слова: ЗАХИЩЕНІСТЬ, ТЕХНІЧНА ОЦІНКА, ВЕБ-БЕЗПЕКА, ВРАЗЛИВОСТІ, АТАКИ, СКАНУВАННЯ.

Кваліфікаційна робота присвячена технічній оцінці захищеності вебсайту Великоберезовицької територіальної громади. В роботі проаналізовано вимоги до технічного завдання, вибір оптимального рішення поставленого завдання. Обґрунтовано вибір інструменту для сканування веб-сайту на наявність вразливостей. На основі аналізу вимог до технічного завдання налаштовано конфігурацію обраного сканера для проведення тестування безпеки. Розроблено рекомендації усунення знайдених вразливостей.

В першому розділі описано об'єкт тестування безпеки, визначено вимоги до проведення сканування та проаналізовано рішення поставленого завдання. В другому розділі описано найпоширеніші типи вразливостей на проаналізовано сканери для тестування безпеки. В третьому розділі висвітлено результати сканування та розроблено план усунення вразливостей.

ANNOTATION

Technical security assessment of the Velyka Berezovytsia Territorial Community website // Thesis of educational level "Bachelor" // Burmistrova Nataliia Andriivna // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, СБ-41 group // Ternopil, 2023 // P. ___ , fig. -____, table. - __ , chair. - ___ , added. -___.

Keywords: SECURITY, TECHNICAL ASSESSMENT, , WEB SECURITY, VULNERABILITIES, ATTACKS, SCANNING.

Qualification thesis is dedicated to the technical assessment of the security of the website of the Velyka Berezovytsia Territorial Community. The work analyzed the requirements for the technical task, the choice of the optimal solution to the given task. The choice of a tool for scanning a website for vulnerabilities is justified. Based on the analysis of the requirements for the technical task, the configuration of the selected scanner is configured for security testing. Recommendations for eliminating the vulnerabilities found have been developed.

The first section describes the the object of security testing is described, the requirements for scanning are defined, and the solution to the task is analyzed. The second section describes the most common types of vulnerabilities analyzed by scanners for security testing. The third section highlights the results of the scan and develops a plan to eliminate vulnerabilities.

ЗМІСТ

ВСТУП

Тестування безпеки сайту може допомогти попередити можливі кібератаки, особливо з урахуванням того, що в 2022 році було зареєстровано кіберінцидентів у 2.8 разів більше ніж у 2021 році.

Звіти про кібератаки в Україні за 2022 рік підтверджують високий рівень загроз, з якими стикаються власники сайтів.

Згідно зі статистичний звітом за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 року [1] було отримано такі дані:

- опрацьовано 58 млрд подій, отриманих за допомогою засобів моніторингу, аналізу та передання телеметричної інформації про кіберінциденти та кібератаки;
- детектовано 181 млн підозрілих подій ІБ при первинному аналізі;
- опрацьовано 179 тис. критичних подій ІБ, що є потенційними кіберінцидентами, які виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу;
- зареєстровано 415 кіберінцидентів критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки.

Ці дані підкреслюють важливість та актуальність даної роботи. Проведення тестування безпеки допоможе виявити потенційні проблеми в безпеці та захисті сайту, а також допоможе вдосконалити систему захисту та зменшити ймовірність кібератак на сайт.

Метою даної роботи є проведення технічної оцінки захищеності веб-сайту Великоберезовицької територіальної громади та розробка звіту, який включає рекомендації усунення знайдених вразливостей.

Об’єктом дослідження кваліфікаційної роботи є веб-ресурс, створений на платформі Joomla. Предметом дослідження є проведення сканування веб-сайту на наявність вразливостей. Робота включає аналіз веб-ресурсу, типів вразливостей та вибір інструменту сканування на основі попереднього аналізу.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести аналіз веб-ресурсу та вимог до технічної оцінки;
- проаналізувати можливі рішення поставленого завдання та обрати найбільш оптимальне;
- проаналізувати типи вразливостей веб-додатків та обрати інструмент для проведення сканування;
- провести сканування веб-сайту на наявність вразливостей;
- за результатами проведеної роботи проаналізувати знайдену інформацію та розробити рекомендації щодо усунення виявлених вразливостей.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Аналіз вимог до оцінки веб-ресурсу на наявність вразливостей

Сайт Великоберезовицької територіальної громади (https://vbsr.gov.ua) є об'єктом тестування безпеки з метою виявлення потенційних вразливостей та ризиків, пов'язаних з цим веб-порталом.

Даний сайт є офіційним веб-порталом, який надає інформацію про Великоберезовицьку громаду в Україні. Цей сайт призначений для мешканців та інших зацікавлених осіб, які шукають інформацію про послуги, події та новини, пов'язані з громадою. На веб-порталі можна знайти різноманітну інформацію, таку як контактні дані та графіки роботи адміністративних органів, новини та оголошення, програми та проекти громадського розвитку, а також інформацію про культурні та спортивні події в громаді.

У рамках дослідження сайту було розроблено блок-схему сторінок сайту, що відображає структуру та зв'язки між різними сторінками. Ця блок-схема надасть візуальне уявлення про організацію і навігацію по сайту.

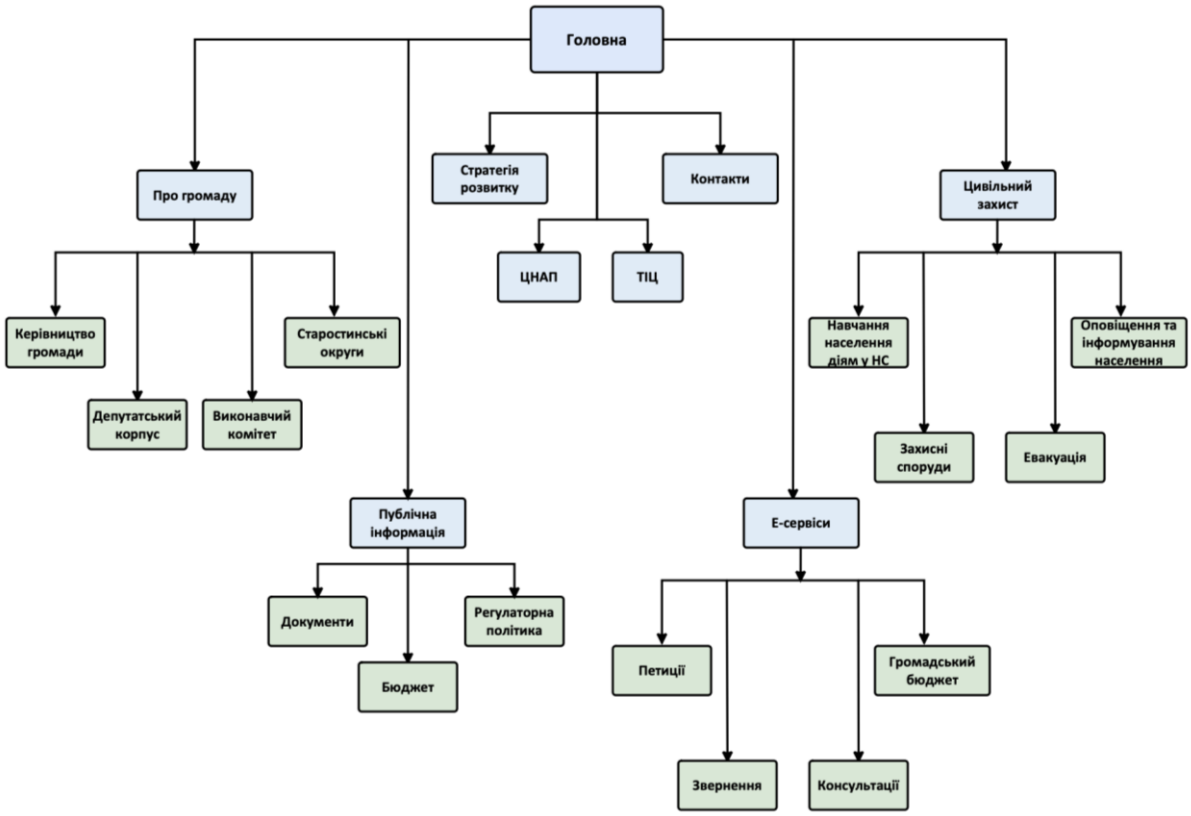

Рисунок 1.1 – Блок-схема структури сайту

Даний сайт розроблений з використанням платформи Joomla. Joomla є однією з популярних систем управління контентом (CMS), яка надає зручні інструменти для створення, оновлення та керування веб-сайтами. Це дозволяє ефективно організувати структуру та навігацію сайту, керувати його вмістом та розширювати функціональні можливості за допомогою різноманітних додатків і плагінів.
Вона підтримує розширення власними компонентами, модулями та плагінами, що дозволяє налаштовувати сайт під конкретні потреби. Крім того, Joomla має активну спільноту розробників, яка постійно працює над покращенням безпеки, виправленням помилок та розширенням функціональності платформи. Це забезпечує стабільну роботу сайту і захищає його від потенційних загроз.

Наступним важливим моментом є дослідження домену сайту. Домен є ідентифікаційною назвою Інтернет-ресурсу та частиною URL-адреси (Uniform Resource Locator), що вказує на місцезнаходження веб-сайту в мережі Інтернет.

Домен gov.ua є доменом другого рівня, який використовується для українських урядових та державних організацій. З метою забезпечення безпеки домену gov.ua можуть бути використані різні системи та заходи захисту. Вони можуть варіюватись в залежності від урядових організацій та їхніх внутрішніх

політик безпеки. Хостинг провайдером для веб-сайту є компанія "Kyivstar PJSC". Компанія забезпечує надійне розміщення веб-сайту на своїх серверах, що розташовані в захищених дата-центрах. Вони забезпечують неперервний доступ до сайту, стабільну пропускну здатність та захист від потенційних загроз, таких як DDoS-атаки або несанкціонований доступ. Також вони забезпечують резервне копіювання даних, що дозволяє відновлювати сайт у разі втрати або пошкодження даних.

Щоб отримати інформацію про ціль, була організована зустріч із замовником. Клієнт не надав жодної інформації щодо веб-ресурсу, архітектури або потенційних вразливостей. Це означало, що у мене наявні обмежені вихідні дані та знання про цільову систему. Тому було зосереджено увагу на зовнішньому скануванні та аналізі поведінки системи, використовуючи публічно доступну інформацію та загальноприйняті методи тестування безпеки. Використовуючи цей підхід, було поставлено ціллю зрозуміти, як система взаємодіє зі своєму оточенням, виявити потенційні слабкі місця, аналізувати відповіді на запити, перевіряти застосування безпекових механізмів та реагування на атаки. Враховуючи все вище перелічене, було оголошені наступні вимоги щодо тестування безпеки веб ресурсу:

1) Провести пошук хостів, портів та сервісів, які розміщені на веб-ресурсі.

Даний етап включає в себе:

- пінгування методами TCP, UDP, ICMP та ARP;
- сканування хостів Novell Netware та пристроїв операційної технології;
- пошук локальних портів SSH, WMI та SNMP;
- пошук служб SSL, TLS та DTLS.

2) Проведення оцінки веб-ресурсу на стан захищеності.

До даного етапу належить:

- сканування веб застосунку;
- сканування динамічно створених сторінок;
- при скануванні перевірити всі доступні HTTP-методи;
- включити спроби HTTP-перегруження параметрів;
- виконати сканування вбудованих веб-серверів;

- провести пошук smb користувачів методами реєстр SAM, ADSI та WMI запитами;
- включити метод перебору різних комбінацій RID;
- включити опцію "Use detected SIDs".

1.2 Аналіз можливих рішень поставленого завдання

Існує декілька варіантів рішення для проведення тестування безпеки веб-сайту. Основними є:

1. Мануальний метод;
2. Тестування безпеки за допомогою запитань та анкет;
3. Проведення сканування веб-сайту на наявність вразливостей.

Мануальний метод тестування дозволяє зосередитися на конкретних аспектах безпеки. Він включає в себе ручне виконання різних тестових сценаріїв та перевірку різних аспектів безпеки веб-сайту. Основною ідеєю мануального тестування є виявлення потенційних вразливостей, які можуть бути пропущені автоматизованими сканерами або іншими засобами.

Тестування за допомогою анкет є методом самооцінювання, де анкети розробляються з питаннями та сценаріями, що стосуються безпеки веб-сайту. Ці анкети потім надсилаються створювачам веб-ресурсу або іншим особам, пов'язаним з його розробкою. Відповіді та коментарі аналізуються з метою виявлення потенційних проблем безпеки та написання рекомендацій щодо вдосконалення безпеки веб-додатку.

Метод сканування включає в себе використання спеціалізованих інструментів та програм для автоматичного перевірки веб-додатку на наявність потенційних вразливостей і потенційних проблем з безпекою.

Під час сканування веб-додатку, інструменти виконують різні види аналізу, такі як сканування портів, сканування вразливостей, перевірку безпеки конфігурації

сервера. Вони також можуть проводити перехоплення трафіку, аналізувати HTTP запити та відповіді, перевіряти валідність введених даних та виконувати інші техніки для виявлення вразливостей.

Після завершення сканування, інструменти звітуватимуть про знайдені вразливості, слабкості та рекомендації щодо виправлення проблем безпеки.

Для проведення тестування було обрано метод сканування веб-сайту на вразливості, оскільки це забезпечує швидку й ефективну перевірку можливих проблем безпеки. Проаналізувавши та перевіривши кожну вразливість, яку знайшов сканер, буде складено звіт із відповідними заходами щодо виправлення. Опираючись на даний метод тестування, було розроблено наступний план:

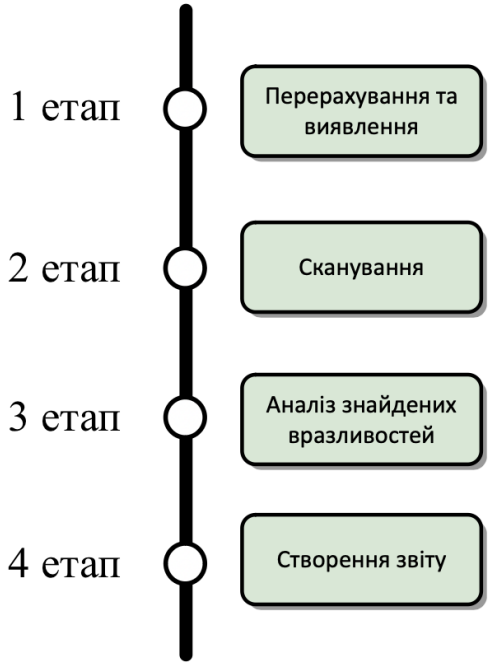

Рисунок 1.2 – План тестування методом сканування

На етапі перерахування та виявлення проводиться проводиться пошук хостів, портів та сервісів з метою виявлення всіх доступних систем та пов'язаних з ними служб. Даний момент важливий за для того щоб в подальшому здійснити ретельне сканування та дослідження з метою точного визначення запущених служб, включаючи ті, що можуть бути «замасковані» або «приховані», їх версій та можливих критичних точок вразливостей.

На стадії сканування проводиться сканування всіх знайдених напередодні портів та сервісів на наявність вразливостей, щоб мати можливість знайти якомога більше інформації, обмежуючи кількість помилкових спрацьовувань до мінімуму.

На наступному етапі здійснюється дослідження знайдених потенційних вразливостей, виявлених на попередніх етапах, щоб мати можливість перевірити їх достовірність та вплив на веб-ресурс.

Останній, проте дуже важливий етап, розробка звіту та рекомендацій усунення вразливостей. На цьому етапі всі виявлені проблеми безпеки збираються та класифікуються за рівнем критичності та можливим впливом на властивості веб-ресурс. Також на даному етапі розробляється план виправлення та усунення вразливостей.

2 АНАЛІЗ ТИПІВ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ ТА ВИБІР СКАНЕРА ВРАЗЛИВОСТЕЙ

2.1 Проблеми безпеки сайтів на Joomla. Аналіз та заходи захисту

Розуміння найпоширеніших вразливостей та атак на сайти Joomla допомагає провести повне та більш точне тестування безпеки. Завдяки цьому розробники сайту зможуть зберегти конфіденційність користувачів, запобігти втраті даних та зробити веб-сайт надійним та безпечним.

Vulnerability Trends Over Time - це аналіз та візуалізація змін у кількості та характері вразливостей протягом певного періоду часу. Цей аналіз надає можливість виявити тенденції та зробити висновки про розвиток безпеки в певній платформі. Нижче представлено графік з вразливостями на Joomla починаючи 2005 року [2]. Графік може показувати кількість вразливостей за роками, їх розподіл за категоріями, що дає уявлення про динаміку проблем безпеки.

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2005	4	1	1			1	1								
2006	51	3	19			2	4			2	3	1		17	
2007	59		41			18	9	1	1		3			22	
2008	89		75			73	2					1	1	2	2
2009	8						5				1		1		
2010	3						3								
2011	12		2			2	3				5				
2012	24		1			1	10				8	1			2
2013	11	1				1	4			3	3				2
2014	9	1	2			1	4			3					
2015	13		6			4	1	2			2		2		
2016	8		3			1						1			
2017	19		1			1	6			1	4		1		
2018	24		1			2	8				1		1	1	
2019	29		1			1	14	3		1			1		
2020	39					3	7	1		1	4		7		
2021	28					1	8	1		1	1		2		
2022	13					1	5	1							
2023	5						1						1		
Total	448	6	153			113	95	9	1	12	35	4	17	42	6
% Of All		1.3	34.2	0.0	0.0	25.2	21.2	2.0	0.2	2.7	7.8	0.9	3.8	9.4	

Рисунок 2.1 – Графік з вразливостями на платформі Joomla 2005-2023 років

Наступний графік показує загальну кількість вразливостей розділених за категоріями:

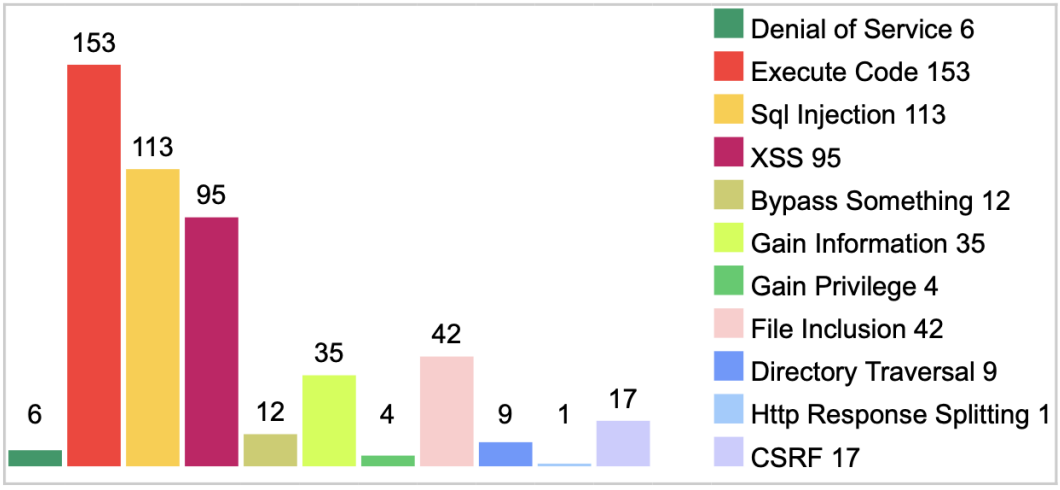

Рисунок 2.2 – Графік загальної кількості вразливостей на Joomla розділених по категоріях

Взявши до уваги кількість та критичність вразливостей, було виділено та проаналізовано більш детально наступні вразливості:

1) міжсайтовий скриптинг (Cross-Site Scripting або XSS);
2) SQL-ін'єкція (SQL Injection);
3) віддалене виконання коду (Remote Code Execution);
4) підроблення міжсайтових запитів (Cross-Site Request Imitation);

5) підвищення привілеїв (Privilege Escalation).

2.1.1 Міжсайтовий скриптинг (Cross-Site Scripting)

Міжсайтовий скриптинг Joomla - проблема безпеки, спричинена відсутністю фільтрації вхідних даних. Дана вразливість дозволяє зловмисникам обманом змусити жертв запустити шкідливий код JavaScript на сторінках Joomla. Зловмисник вставляє шкідливий скрипт, який буде використиним для крадіжки файлів cookie, фішингу тощо коли відвідувач виконає його у браузері. Це може бути JavaScript-код або інша форма виконуваного коду.

Дана атака може мати різноманітні наслідки, наприклад: крадіжка облікових записів, втрата конфіденційних даних, поширення шкідливих посилань чи інфекція користувачів шкідливим кодом.

Існують різні типи XSS-вразливостей:

1) stored XSS: скрипт зберігається на сервері і виконується при завантаженні сторінки користувачем;
2) reflected XSS: скрипт вбудовується у вихідні дані сервера та виконується при поверненні сервером відповіді;
3) DOM-based XSS: скрипт маніпулює DOM (Document Object Model) сторінки, в результаті чого виконується шкідливий код в браузері.

Дана проблема безпеки виявлена на платформі Joomla та отримала назву CVE-2019-12766.

CVE-2019-12766 - це ідентифікатор вразливості, яка відзначена в системі збору, розповсюдження та опису вразливостей - Common Vulnerabilities and Exposures (CVE). Дана вразливість впливає на версії Joomla 3.0.0 до 3.9.6. Вона стосується недостатньої перевірки доступу та можливості виконання коду через скомпрометований маршрутизатор API. Як наслідок зловмисники, які використовують цю вразливість, можуть вплинути на сайт, виконуючи шкідливий код або отримуючи несанкціонований доступ до конфіденційних даних [3].

Вразливість була виправлена в оновленні Joomla 3.9.7. Це основна причина чому потрібно оновлювати до останньої версії, адже це усунить цю вразливість та забезпечить безпеку веб-сайту.

Також рекомендується виконувати наступні заходи:

1) Проводити фільтрацію та екранування даних: вхідні дані, що надходять від користувачів, фільтрувати та проводити екранування щоб усунути потенційно небезпечні скрипти.
2) Налаштувати Content Security Policy (CSP): рекомендується встановити політику безпеки контенту, яка обмежує виконання JavaScript-коду тільки з надійних джерел та доменів.
3) Проводити аудит безпеки: регулярна перевірка сайту на наявність вразливостей XSS допоможе вчасно виявити дану вразливість.

2.1.2 SQL-ін'єкції (SQL Injection)

Наступною не менш небезпечною вразливістю на платформі Joomla є SQL-ін’єкції. Які є схожими на XSS. Обидві вразливості спрацьовують через відсутність належних системних процедур фільтрації вхідних даних. SQL-ін'єкція виникає через некоректну фільтрацію та перевірку вхідних даних, які вводяться користувачами на веб-сайті., пароль або інша чутлива інформація. Зловмисники можуть використовувати SQL для повного контролю компонентів джерела даних, що передбачає стирання таблиць, перевірку таблиць адміністратора, а також керування ними.

Така вразливість була виявлена в Joomla 3.5.0 до 3.8.5, яка називалася CVE-2018-8045. Її спричинила відсутність приведення змінної в Customer Notes Detail Sight. Також вона з’являється в результаті неправильної практики кодування. Як приклад у наслідок цього така вразливість була виявлена в розширені Joomla ARI Quiz 3.7.4 [4].

Заходи для запобігання SQL-ін'єкцій та забезпечення безпеки Joomla-сайту:

1) Використання параметризованих запитів: замість конкатенації значень в запиті варто використовувати параметризовані запити чи підготовлені заявки. Це дозволяє базі даних правильно обробляти дані та уникнути вразливостей.
2) Фільтрування та перевірка вхідних даних: перевірка та фільтрування вхідних даних, що надходять від користувачів, перед використанням у SQL-запитах допоможе усунути потенційно шкідливих символів.

3) Періодичне оновлення Joomla: регулярне оновлення та використання розширень останніх версій, зробить сайт більш захищеним, оскільки вони містять виправлення вразливостей та покращення безпеки.
4) Використання безпечних паролів: потрібно перевірити щоб всі користувачі мали сильні та унікальні паролі. Рекомендується використання комбінацій великих і малих літер, цифр і спеціальних символів.
5) Встановлення обмеження доступу до бази даних: варто налаштувати обмеження доступу до бази даних Joomla. Надання мінімальних прав доступу для користувачів допоможе обмежити вплив SQL-ін'єкції в разі успішного проникнення.

2.1.3 Віддалене виконання коду (Remote Code Execution)

Віддалене виконання коду Joomla - це проблема безпеки, яка виникає, коли зловмисник вводить команду в рядок або документ, а також виконує її мовний аналізатор. Це дозволяє віддалено виконувати власний шкідливий код на веб-сайті, отримуючи повний контроль над виконавчим середовищем.

Така вразливість зазвичай виникає через некоректну обробку вхідних даних або недостатню перевірку даних, що передаються на сервер. Через це у зловмисників з’являється можливість скомпрометувати веб-сайт, виконуючи власний код, отримувати несанкціонований доступ до сервера або змінювати функціонал сайту на свій розсуд. Схильність до віддаленого виконання коду містилася у версіях Joomla, перелічених нижче 3.8.13 і також названих CVE-2018-17856. Вразливість виникла через дефектний компонент оновлення Joomla під назвою com_joomlaupdate. Також, якщо взяти до уваги розширення Joomla, то таких схильних розширень зустрічається дуже багато. Як приклад, розширення vBizz 1.0.7 Joomla також було вразливе до віддаленого виконання коду [5].

Наслідки RCE досить серйозні. Вони можуть включати втрату контролю над веб-сайтом, крадіжку даних, поширення шкідливого програмного забезпечення чи повне компрометування сервера.

Для запобігання даної вразливості на веб-сайтах Joomla рекомендується вживати наступні заходи безпеки:

1) Вчасне оновлення Joomla та використання розширень останніх версій : регулярне оновлення захистить сайт, оскільки оновлення містять виправлення вразливостей та покращення безпеки.
2) Вимкнення дебаг-режиму: рекомендується вимкнути дебаг-режим на сервері, оскільки він може розкрити потенційно важливу інформацію та надати зловмисникам додаткові можливості для виконання коду.
3) Обмеження прав доступу: налаштування обмеження прав доступу до файлів та каталогів на сервері допоможе обмежити можливість виконання шкідливого коду в разі успішного проникнення.
4) Використання валідації та санітизації даних: завдяки виконанні перевірки даних, що вводяться користувачами, перед використанням, можна усунути потенційно шкідливі символи або код, які можуть бути виконані на сервері.

2.1.4 Підроблення міжсайтових запитів (Cross-Site Request Imitation)

Підроблення міжсайтових запитів дозволяє зловмиснику виконувати небажані дії на сайті, наприклад видаляти матеріали сторінки. Дана атака використовується зловмисниками щоб змусити автентифікованого користувача виконати небажані дії без їхньої належної згоди чи підтвердження. Наприклад, зловмисник може створити спеціальний HTML-код, що містить посилання чи форму, яка буде відображатись на сторінці, яку потенційна жертва відвідає. Коли користувач взаємодіє з цим посиланням чи формою, запит відправляється на сервер з довіреністю жертви, і небажана дія виконується без її згоди, така як зміна паролю, видалення даних або виконання фінансових операцій. Враховуючи те, що у зловмисника немає нагоди побачити зворотний зв’язок із запитом, він може видалити облікові записи, перенести компоненти з одного облікового запису в інший.

До підроблення міжсайтових запитів вразливі версії Joomla до 3.9.5, які входять до CVE-2019-10945. До цього ідентифікатора вразливості також входить помилка обходу сайту каталогу, якою можна маніпулювати для виконання CSRF. Обхід сайту каталогу дозволяє зловмисникам переглядати файли за межами сайту каталогу www [6].

Щоб запобігти атакам підроблення міжсайтових запитів на веб-сайтах Joomla рекомендуються наступні заходи безпеки:

1) Використання токенів захисту форми: рекомендується додавати унікальні токени захисту до форм та посилань. Ці токени можуть бути перевірені на валідність перед виконанням дій, що потребують авторизації, що дозволяє виявляти атаки підроблення міжсайтових запитів.
2) Встановлення правильних заголовків HTTP: встановлення заголовків HTTP, таких як "SameSite" та "Content Security Policy", допоможе обмежити можливість атак. Дані заголовки дозволяють контролювати, як браузер повинен поводитися при взаємодії зі сторонніми джерелами.
3) Підтвердження дій: додавання підтвердження для важливих дій, таких як видалення облікових записів чи зміна конфіденційної інформації допоможе захистити веб-сайт.
4) Вимкнення автозаповнення форм: рекомендується вимкнути автоматичне заповнення форм браузером для форм, що виконують небезпечні дії. Це зменшить ймовірність виконання небажаної дії без відповідної перевірки користувача.

2.1.5 Підвищення привілеїв (Privilege Escalation)

Останньою, проте не менш небезпечною вразливість є підвищення привілеїв Joomla. Ця вразливість дозволяє зловмисникам отримати вищі рівні привілеї, ніж мають звичайні користувачі. Наприклад, зловмисник, який був звичайним зареєстрованим користувачем на сайті, може збільшити привілеї для виконання команд як адміністратор сайту. Таким чином він отримає несанкціонований доступ до обмежених ресурсів та функціональності.

Дана вразливість переважно виникає через вразливості в коді. Якщо в ньому наявні помилки, то це може призвести до привілейової ескалації. Також вразливість виникає якщо адміністратор використовує слабкий пароль або пароль, який може бути легко зламаний. Недостатній контроль доступу, неправильне налаштування ролей і дозволів, а також відсутність механізмів моніторингу та виявлення несправедливої активності також можуть утворити простір для привілейової ескалації.

Для Joomla дана вразливість має назву CVE-2016-8869. До підвищення привілеїв вразливим файлом був controllers/user.php. Метод register даного файлу, який належав до класу UsersModelRegistration, відповідав за підвищення привілеїв. Використовуючи цей файл зловмисники могли ввести невідфільтровані дані для підвищення привілеїв під час реєстрації на сайті Joomla [7]. Дана вразливість є досить небезпечно й поширенішою, оскільки з’явився доступний модуль в Metasploit для експлотації вразливості.

Задля запобігання привілейової ескалації на веб-сайтах Joomla, рекомендуються заходи безпеки, які було перелічено раніше. А саме:

1) Забезпечення сильних та надійних паролів: використання складних паролів для всіх адміністративних облікових записів. Паролі повинні бути довгими, містити різні типи символів і бути унікальними для кожного облікового запису.
2) Використання принцип найменших привілеїв: рекомендується надавати користувачам лише ті привілеї, які вони потребують для своїх робочих обов'язків. Обов’язково потрібно обмежити доступ до критичних функцій та ресурсів тільки для облікових записів, які дійсно потребують такого доступу.
3) Оновлення програмного забезпечення.
4) Моніторинг та аудит безпеки: встановлення механізмів моніторингу та аудиту безпеки допоможе виявити незвичайну чи підозрілу активність на сайті. А це вже допоможе вчасно виявити спроби привілейової ескалації та вжити відповідних заходів.

Отже у цьому підрозділі було представлено найпоширеніші атаки на веб-сайти, побудовані на платформі Joomla. А також було надано аналіз та рекомендації щодо захисту. Розуміння особливостей та наслідків даних атак важливе для визначення стратегії тестування безпеки.

2.2 Порівняння та аналіз сканерів вразливостей

В даному підрозділі виконано порівняння трьох найпопулярніших сканерів, а саме OpenVAS, Invicti та Nessus.

Критерії початкового порівняння:

1) ключові особливості;
2) переваги технології;
3) недоліки технології;
4) ціна.

2.2.1 OpenVAS

OpenVAS (Open Vulnerability Assessment Scanner) – один із найпопулярніших сканерів вразливостей з відкритим кодом.

У 2006 році компанія Greenbone Networks почала фінансувати створення цієї технології. Сканер разом з іншими модулями з відкритим вихідним кодом становить Greenbone Community Edition, яка належить до сімейства комерційних продуктів управління вразливістю під назвою Greenbone Enterprise Appliance.

Його функції включають як неавтентифіковані, так і автентифіковані тестування, різноманітність високо та низькорівневих промислових та інтернет-протоколів, налаштування для здійснення діагностики та моніторингу мережевих комп'ютерів, завдяки чому стає можливо виявити проблеми у системі безпеки, а також оцінити та усунити вразливості.

Незважаючи на те, що дана технологія була розроблена як сканер Unix/Linux, її можна використовувати для сканування ширший діапазонів вразливостей, включаючи вразливості ОС Windows [8].

1) Ключові особливості:
   - сканування системи на відомі вразливості та відсутність виправлень безпеки;
   - можливість встановлення на будь-яку локальну або хмарну машину;
   - інтегрована веб-консоль керування;
   - надає повний перелік інформації про вразливість включно з рішеннями безпеки.

2) Переваги технології:
   - сканер безкоштовний;
   - велика спільнота для підтримки та нетворкінгу;
   - вихідний код доступний для перегляду;
   - оновлення виходять періодично.

3) Недоліки технології:

- інтерфейс не такий зручний, порівняно з інтерфейсом комерційних інструментів;
- велика кількість одночасних сканувань може привести до збою сканера;
- функціонал дуже технічний, тому більше підходить для людей з відповідним досвідом.

4) Ціна:

- OpenVAS доступний безкоштовно.

2.2.2 Invicti

Invicti - інструмент сканування вразливостей веб-сайтів і програм. Незважаючи на те, що інструменти сканування вразливостей веб-сайтів і програм пов’язані з мережевими, хмарними та іншими інструментами сканування вразливостей IT-інфраструктури, вони застосовують спеціалізовані алгоритми для пошуку вразливостей програмування. Invicti, раніше відомий як Netsparker, є популярним сканером уразливостей додатків, призначеним для корпоративного масштабу та автоматизації [9].

Ключові особливості:

- автоматичне та безперервне сканування для оновлення інвентаризації веб-сайту, програми та API;
- уникає черг сканування, дозволяючи кілька одночасних сканувань і сканерів, які надходять у централізоване сховище для звітів;
- розгортається локально, у хмарі, в образах Docker або як гібридне рішення. Хмарні агенти запускаються для сканування, а потім самостійно видаляються, коли сканування завершується;
- динамічне та автоматизоване сканування динамічного тестування безпеки додатків (DAST), інтерактивного тестування безпеки додатків (IAST) і аналізу складу програмного забезпечення (SCA);
- асинхронне тестування вразливостей;
- датчики IAST часто можуть надати назву файлу та номер рядка програмування для вразливостей;

- сканує сторінки, автентифіковані шляхом надсилання форми, OAuth2, NTLM/Kerberos;
- сканує складні шляхи та багаторівневі форми, захищені паролем області, сайти з великою кількістю скриптів (JavaScript або HTML5), односторінкові програми (SPA), незв’язані сторінки;

Переваги технології:

- сканує приховані файли;
- виявляє неправильно налаштовані файли конфігурації;
- найкраще в галузі виявлення хибнопозитивних результатів тестування;
- буде відстежувати стан безпеки програм з часом і виявляти тенденції вразливості;
- активно зменшує помилкові спрацьовування та може перевіряти вразливості та надавати докази використання;
- інтеграція з конвеєрними інструментами та засобами відстеження проблем, такими як Jenkins, Jira та GitHub, для інтеграції робочого процесу розробника.

Недоліки технології:

- неефективне тестування багатофакторної автентифікації;
- повільне сканування великих веб-додатків;
- доступно лише з установкою програмного забезпечення Windows;

Ціна:

Invicti не публікує ні інформацію про ціни, ні рівні ліцензій на своєму веб-сайті. Існує три плани:

- стандартний локальний настільний сканер;
- командний сканер;
- сканер для підприємств:

2.2.3 Tenable Nessus Vulnerability Scanner

Tenable Nessus Vulnerability Scanner - це найбільш популярний сканер для автоматичного пошуку вразливостей, виявлення застарілих та вразливих конфігурацій сервісів і мережевих пристроїв всієї IT-інфраструктури компанії.

Також даний сканер надає можливість сканування пристроїв без використання облікових даних, які використовуються на ньому [10].

Ключові особливості:

- широкий вибір шаблонів для різних видів сканування;
- автоматично виконується повне сканування, щойно додаються нові плагіни вразливостей;
- шаблони звітів надають швидкі знімки;
- наявна можливість створювати персональні звіти;
- автоматизовані сповіщення про вразливість і неправильну конфігурацію для управління інцидентами безпеки та подіями.

Переваги технології:

- місце за найпростішим у використанні програмним забезпеченням сканера вразливостей на G2;
- керівні інформаційні панелі та потужна фільтрація для опрацювання знайдених вразливостей;
- може оцінити сучасну інфраструктуру як код (IaC);
- безагентне сканування;

Недоліки технології:

- деколи знаходить помилкові вразливості, які не наявні в системі;
- деякі користувачі скаржаться на обмежену інтеграцію API.

Ціна:

1) Nessus Professional:
   - необмежена кількість сканувань та конфігурацій;
   - 3,390 доларів на рік із можливістю розширеної підтримки та навчання.
2) Nessus Expert:
   - сканування хмарної інфраструктури;
   - 500 попередньо створених політик сканування;
   - можливість додавання доменів;
   - 7490 доларів на рік із можливістю розширеної підтримки та навчання;

3) Nessus Essentials:
   - безкоштовна версія, проте обмежені можливості;
   - одне сканування обмежується до 16 IP-адрес;
   - жодних перевірок відповідності чи аудиту вмісту;
   - немає технічної підтримки.

Далі було проведено детальніше порівняння сканерів для визначення їх технічних характеристик.

Використану словесну шкалу оцінки, що вказує на рівень відповідності критерію: "низька", "середня", "висока".

Таблиця 2.1 – Порівняння технічних характеристик сканерів

Критерії	**Nessus Essentials**	**OpenVAS**	**Invicti**
Широкий спектр сканування	середня	висока	висока
Точність виявлення	висока	середня	висока
Швидкість сканування	середня	висока	висока
Зручний інтерфейс користувача	висока	низька	висока
Підтримка зовнішніх інтеграцій	середня	висока	висока

Продовження таблиці 2.1

Підтримка зовнішніх інтеграцій	середня	висока	висока
Підтримка актуальних вразливостей і баз даних	висока	висока	висока
Зручність у налаштуванні сканування	висока	середня	висока
Візуалізація результатів	висока	середня	висока
Підтримка автоматизованих звітів	висока	висока	висока
Масштабованість	висока	середня	висока
Підтримка розподіленого сканування	низька	висока	висока
Підтримка хмарних сервісів	висока	висока	висока

Для проведення сканування безпеки веб-сервісу в нашому випадку ключовими критеріями є широкий функціонал, висока точність виявлення, підтримка актуальних вразливостей і баз даних, візуалізація результатів та підтримка автоматизованих звітів.

Опираючись на дані, представлені вище, для проведення тестування безпеки було обрано сканер вразливостей Nessus. Оскільки дана система включає всі необхідні функції для проведення тестування, а також є надійним інструментом для виявлення та управління вразливостями.

3 АНАЛІЗ ТА ОЦІНКА РЕЗУЛЬТАТІВ СКАНУВАННЯ

3.1 Ключові налаштування конфігурації сканера Nessus

Конфігурація Nessus – одна з найважливіших частин використання даного сканера вразливостей. Вона визначає параметри сканування, поведінку та результати, які буде отримано під час виконання сканування веб-сайту.

У цьому підрозділі було детально розглянуто та обгрунтовано налаштування конфігурації Nessus. А також надано пояснення впливу кожного пункту конфігурації на процес сканування та результати. Розглянуто наступні ключові аспекти: Пошук (Discovery) та Оцінка (Assessment).

3.1.1 Пошук

Налаштування пошуку включає в себе пошук хостів, портів та сервісів. Основна функція пошуку хостів- пінгування віддалених хостів (Remote Host Ping) Завдяки даному налаштуванні буде виконуватися пінгування віддалених хостів

перед перевіркою їх на вразливості. Це дозволяє встановити доступність цих хостів та зменшити кількість фальшивих позитивних результатів [5].

Налаштування пінгування включає в себе кілька різних методів, які дозволяють встановити доступність віддалених хостів:

- TCP Ping;
- UDP Ping;
- ICMP Ping;
- ARP Ping.

У виборі ICMP Ping є додаткові налаштування, а саме включення опції "Assume ICMP unreachable from the gateway means the host is down" (Припустити, що недоступність хосту через ICMP недоступна від шлюзу означає, що хост недоступний) та "Maximum number of retries" (Максимальна кількість повторних спроб).

Не було включено функцію "Assume ICMP unreachable from the gateway means the host is down", оскільки вона потенційно могла вплинути на точність результатів сканування.

Ось кілька причин, чому не рекомендовано включати дану функцію:

- Мережевий пристрій, що виконує функцію шлюзу, не завжди може відправляти ICMP-повідомлення про недоступність хосту. Такий розвиток подій може бути у випадку неправильної конфігурації, блокування ICMP на шлюзі або через певні його особливості. У такому разі, якщо ввімкнена даної функції, сканер помилково визначить хост як недоступний.
- Потенційні фальшиві негативні результати: Якщо мережевий пристрій надсилає ICMP-повідомлення про недоступність коли насправді хост активний, можливі ситуації, коли сканер пропустить такі хости під час сканування, вважаючи їх недоступними. Це може призвести до пропуску виявлення вразливостей або пропуску активних систем у вашій мережі.
- Вплив на точність сканування: Включення даної опції може вплинути на точність результатів сканування, зменшуючи його надійність. Nessus вважатиме хост недоступним, навіть якщо він справді активний, якщо отримає ICMP-повідомлення про недоступність від шлюзу. Це може

призвести до неправильної інтерпретації стану хостів та недостовірних результатів сканування.

Зважаючи на вище перелічені моменти було вирішено не включати дану функцію до сканування щоб отримати максимально точні результати сканування.

Наступним етапом налаштування конфігурації пошуку хостів є "Fragile Devices" (Крихкі пристрої). До них належать:

- сканування мережевих принтерів;
- сканування хостів Novell Netware;
- сканування пристроїв операційної технології.

Під час налаштування конфігурації не було включено опцію "Сканування мережевих принтерів", оскільки було відомо про їх відсутність. Отже, включати цей параметр було не доцільно, оскільки це б лише повпливало на тривалість сканування.

До налаштувань було включено параметр «Сканування хостів Novell NetWare». Він використовується для сканування хостів під керуванням операційних систем Novell NetWare на наявність уразливостей. Novell NetWare - це мережева операційна система, яка широко використовується в корпоративних середовищах і має унікальний набір вразливостей. Хоча це доволі стара операційна система, проте була вірогідність, що її використовують. А отже, сканування Novell NetWare є важливою частиною підтримки загальної безпеки мережі.

Також було включено параметр "Scan Operational Technology (OT) Devices". Він використовується для сканування пристроїв, які використовуються в промислових системах керування (ICS) або системах диспетчерського керування та збору даних (SCADA).

Сканування пристроїв OT є важливим для підтримки безпеки середовищ критичної інфраструктури, оскільки ці пристрої можуть бути вразливими до кібератак, які можуть мати серйозні наслідки. Однак варто зазначити, що сканування пристроїв OT може бути складним і вимагає спеціальних знань та інструментів, тому важливо, щоб кваліфікований персонал виконував ці сканування, щоб переконатися, що вони виконуються безпечно та ефективно.

Далі було налаштовано пошук портів. В першу чергу було змінено діапазон сканування портів. За замовчування стоїть параметр "default", що включає в себе

сканування лиш популярних портів. Тому його було змінено на параметр "all", який включає сканування всіх портів.

Наступним параметром є перелічення локальних портів, яке включає в себе:

- SSH (netstat);
- WMI (netstat);
- SNMP;
- перевірка відкритих портів TCP, знайдених локальними нумераторами портів.

Наявність сканування локальних портів дозволяє виявити потенційні вразливості і незахищені сервіси, які можуть бути доступні з мережевих пристроїв. Це дає можливість виявити порти, які можуть бути відкритими неправильно або порти, які повинні бути закритими, але залишилися відкритими через помилки в налаштуванні [11].

Також було налаштовано сканери мережевих портів. Основна суть роботи сканерів мережевих портів полягає в тому, що вони відправляють мережеві пакети на певні порти і чекають на відповіді від пристроїв у мережі. За результатами цього сканування можна визначити, які порти відкриті, а які закриті чи фільтруються мережевими пристроями.

Щоб зробити налаштування більш точним та просканувати більшу кількість портів, було налаштовано SYN-сканування. Сканер мережевих портів надсилає TCP-пакети з встановленим флагом SYN на певний порт пристрою, на який він хоче перевірити доступність. Якщо порт відкритий, то цей пристрій відправить відповідь у вигляді TCP-пакета з флагом SYN/ACK. Сканер отримує цю відповідь і визначає, що порт відкритий.

У разі, якщо порт закритий чи фільтрується мережевим пристроєм, сканер отримає відповідь з флагом RST (Reset), що сигналізує про те, що порт закритий і не готовий для з'єднання. За рахунок того, що SYN-сканування не повністю встановлює з'єднання TCP, воно воно певні фільтри та правила, які можуть бути налаштовані для блокування чи обмеження сканування портів. Це допомагає зробити більш точну оцінку стану портів.

В налаштуваннях пошуку сервісів першим важливим пунктом налаштування є "Probe all ports to find services". Даний параметр зіставляє кожен відкритий порт

зі службою чи додатком, які відповідають на цьому порту. Цей параметр корисний для отримання максимально повного звіту про наявні служби та прослуховуючі порти. Він дозволяє виявити служби, які можуть працювати на нестандартних портах або служби, які не є стандартними для певного типу пристрою. Також це дозволяє виявити потенційні служби, які можуть бути вразливими до атак чи потребують оновлення.

Наступним пунктом налаштування конфігурацію було Пошук служб SSL/TLS/DTLS ("Search for SSL/TLS/DTLS services"). Даний параметр дозволяє сканеру шукати та виявляти пристрої або служби, що використовують протоколи для захищеної передачі даних по мережі, а саме:

- SSL (Secure Sockets Layer);
- TLS (Transport Layer Security);
- DTLS (Datagram Transport Layer Security).

Цей параметр виконує спеціальні запити та перевірки на портах, де можуть функціонувати ці протоколи, і аналізує отримані відповіді для виявлення наявних служб. Він дозволяє знайти пристрої або служби, які можуть використовувати SSL/TLS/DTLS протоколи, навіть якщо вони працюють на нестандартних портах. Це допомагає забезпечити повність сканування та виявлення всіх потенційних служб, які використовують ці протоколи для забезпечення безпеки комунікацій.

Наступними пунктами налаштування були:

- пошук SSL/TLS на всіх TCP портах;
- пошук DTLS на всіх UDP портах.

Вказування параметра "All TCP ports" в налаштуваннях "Search for SSL/TLS" означає, що Nessus буде шукати служби, які використовують протоколи SSL/TLS на всіх доступних TCP-портах цільового пристрою.

TLS та SSL - це протоколи, які забезпечують захищену передачу даних по мережі. Вони найчастіше використовуються на TCP-портах. Тому було додано параметр "all tcp ports" щоб сканер знайшов служби, які використовують ці протоколи, навіть якщо вони працюють на нестандартних портах.

По такій же логіці було вибрано параметр "All UDP ports" в налаштуваннях "Search for DTLS".

DTLS є варіантом протоколу TLS (Transport Layer Security), який працює з дейтаграмами UDP (User Datagram Protocol). Він досить часто використовується в мережевих пристроях. Оскільки цей параметр було добавлено до конфігурації, то сканер шукав DTLS на всіх портах UDP, навіть на нестандартних портах, де можуть функціонувати такі служби.

Також до конфігурації було додано параметр "Identify certificates expiring within x days" (Виявлення сертифікатів, які закінчуються протягом x днів). Даний параметр дозволяє сканеру перевіряти сертифікати SSL/TLS на цільових пристроях та ідентифікувати ті, які закінчуються протягом певного періоду часу. Було залишено значення по замовчуванню, а саме 60 днів.

Застарілі сертифікати можуть призвести до недоступності веб-сайтів, проблем з шифруванням даних та порушень безпеки. Завчасне виявлення закінчуючихся сертифікатів дозволяє операторам мережі своєчасно оновлювати та замінювати сертифікати перед їхньою експірацією, запобігаючи можливим проблемам.

Даний параметр допомагає забезпечити вчасну зміну та оновлення сертифікатів, підтримуючи безпеку мережі та уникнення проблем, пов'язаних із застарілими сертифікатами.

3.1.2 Оцінка

В першу чергу було виконано загальні налаштування. Головним параметром в даному пункті конфігурації є точність. До нього відносяться наступні налаштування:

- перевизначення нормальної точності ("Override normal accuracy");
- проведення ретельного тесту ("Perform thorough tests").

Перевизначення нормальної точності відноситься до налаштувань алгоритму або системи, які впливають на його здатність розпізнавати та класифікувати дані з високою точністю. Це налаштування дозволяє перевизначити стандартну точність алгоритму і збільшити або зменшити його чутливість до різних типів даних чи паттернів [12].

Данний параметр має додаткові налаштування:

- уникнення можливих помилкових сигналів ("Avoid potential false alarm");
- показати можливі помилкові сигнали ("Show potential false alarms").

Оскільки в налаштувані конфігурації було надано пріоритет зменшенню кількості помилкових класифікацій, то було обрано додаткове налаштування уникнення можливих помилкових сигналів ("Avoid potential false alarm");

Параметр проведення ретельного тесту не було додано до конфігурації, оскільки він негативно впливає на продуктивність та завантаженість мережі. Даний вид сканування може значно збільшити навантаження на мережу. Це може призвести до падіння швидкості передачі даних або навіть до перебоїв у роботі мережі. Також сканування може призвести до вимкнення деяких служб або впровадження змін.

У пункті "Веб-застосунок" ("Web Application") першим важливим параметром є налаштування сканування веб застосунків. До нього входить налаштування значення заголовку User-Agent під час взаємодії з веб-сервером.

User-Agent - це рядок, який відправляється веб-клієнтом до сервера для ідентифікації типу клієнта, його версії та інших характеристик.

Під час налаштування було залишено дефолтне значення "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)", що вказує на веб-клієнт, який симулює браузер Internet Explorer 8, що працює під операційною системою Windows NT 5.1. Даний User-Agent використовується для підтримки сумісності зі старими веб-сайтами, які можуть вимагати певних версій Internet Explorer або функціональності, що була присутня у старих версіях браузера.

Наступним пунктом є налаштування параметрів поведінки Веб-сканера ("Web Crawler"); Веб-сканер автоматично перебирає веб-сторінки та витягує з них інформацію для індексації або аналізу. Важливим параметром налаштування є правила переходу за веб-сканер буде переходити з однієї сторінки на іншу. Це включає обмеження на глибину переходу, іншими словами максимальну кількість сторінок, які веб-сканер може відвідати під час сканування. В нашому випадку значення параметра дорівнює 6. Це означає, що веб-сканер буде переходити на нові сторінки до глибини 6 посилань від початкової сторінки. Це значення було обрано таким чином, щоб воно задовольняло потреби у зборі інформації, при цьому не перевантажуючи веб-сервер і не затримуючи процес сканування.

Наступним важливим налаштуванням є "Maximum pages to crawl", що встановлює максимальну кількість сторінок, які сканер може сканувати чи індексувати під час процесу сканування веб-сайту. Для цього було обрано значення 1000. Як тільки ця максимальна кількість буде досягнута, процес сканування припиниться. Це значення оптмальне для контролю обсягу збереженої інформації або обмеження впливу сканування на продуктивність веб-сервера.

Також до конфігурації було додано параметр "Follow dynamically generated pages" (Слідувати за динамічно створеними сторінками). Це вказує сканеру на те, чи слідувати за сторінками, які динамічно формуються на сервері, наприклад, на основі запитів користувачів або параметрів URL. Даний параметр корисний щоб зібрати більше інформації про різні варіації сторінок, які генеруються динамічно.

Одним із найважливіших пунктів налаштування "Application Test Settings". До нього було включено наступні налаштування:

- налаштування тестів веб-додатків ("Enable generic web application tests"): цей параметр було ввімкнуто для виконання загальних тестів безпеки веб-додатків. Це включає перевірку на вразливості, такі як SQL-ін'єкція, міжсайтовий скриптінг (XSS) та інші.
- спроби всіх HTTP-методів ("Try all HTTP methods"): даний параметр вказує сканеру спробувати всі доступні HTTP-методи (GET, POST, PUT, DELETE тощо) при взаємодії з веб-додатком. Це дозволяє виявити потенційні проблеми безпеки, які можуть відрізнятися залежно від використаного методу.
- спроби HTTP-перегруження параметрів ("Attempt HTTP Parameter Pollution"): цей параметр вказує сканеру виконати спроби використання HTTP-перегруження параметрів для пошуку вразливостей. Це означає, що він може спробувати внести зміни в значення параметрів запиту для перевірки, чи призводить це до некоректної поведінки або вразливостей.
- тестування вбудованих веб-серверів ("Test embedded web servers"): даний параметр дозволяє сканеру тестувати веб-додатки, які запускаються на вбудованих веб-серверах, таких як Tomcat чи Jetty.

Також було додано додаткові налаштування такі як: "Тестування більше одного параметра за раз на форму" та "Не зупинятися після знаходження першої

вразливості на одній веб-сторінці". Ці налаштування допомагають виявити вразливості, які можуть виникнути при взаємодії кількох параметрів одночасно, а також дозволяє виявити більше потенційних проблем безпеки на сторінці і збільшити шанси на повну ідентифікацію проблем.

Далі було виконано налаштування Віндовс. Першим важливим налаштуванням є запит на пошук інформації про SMB домен (Server Message Block). Це дозволяє отримати детальну інформацію про конфігурацію та безпеку SMB домену. На основі зібраної інформації сканер проводить оцінку безпеки SMB домену та виявляє потенційні вразливості. Це можуть бути налаштування, які піддають мережу ризику, недостатні заходи безпеки або наявність вразливих версій протоколу SMB.

Наступним кроком було налаштовано методи визначення користувачів (User Enumeration Methods). Дані налаштування дозволяють виявити та зібрати інформацію про користувачів, які існують в мережі чи домені. Завдяки цьому можна отримати більш повне розуміння структури користувачів та їх привілеїв.

Основні методи визначення користувачів:

- Реєстр SAM ("SAM Registry"): даний метод використовує доступ до реєстру системи Windows, який називається реєстр SAM. Він містить інформацію про локальних користувачів, їх хеші паролів та інші дані.
- Запит ADSI ("ADSI Query"): метод використовує технологію ADSI (Active Directory Service Interfaces) для запиту до служби каталогів Active Directory. За допомогою даного методу ми можемо отримувати інформацію про користувачів, групи, організаційні одиниці та інші об'єкти в структурі Active Directory.
- Запит WMI (WMI Query): останній, проте не менш важливий метод використовує інтерфейс WMI (Windows Management Instrumentation). Цей інтерфейс управління надає доступ до різноманітних інформаційних ресурсів та функцій. Сканер використовує запити WMI для отримання інформації про користувачів, їхні групи, привілеї та інші атрибути.

До конфігурацію було включено параметр "RID Brute Forcing". Завдяки цьому сканер може виявити потенційні вразливості, пов'язані із атаками на ідентифікатори об'єктів безпеки (RID), використовуючи метод перебору різних

комбінацій RID. Сканер буде автоматично перебирати ідентифікатори об'єктів безпеки, аналізувати їх використання та виявляти можливі проблеми безпеки. Завдяки включенню даної опції можна виявити:

1. Використання непідтверджених або слабких RID.
2. Незахищені облікові записи.
3. Недостатні заходи безпеки.

Також було налаштовано перелік локальних та користувачів домену. Дана опція дозволяє сканеру отримати інформацію про користувачів, які мають облікові записи в домені та локальних користувачів на окремих комп'ютерах або серверах в мережі Windows.

Перерахування користувачів може допомогти виявити потенційні проблеми, такі як:

1. Наявність неактивних облікових записів: завдяки переліку користувачів можна ідентифікувати облікові записи, які були створені, але більше не використовуються. Це можуть бути облікові записи колишніх співробітників або осіб, які вже не мають доступу до мережі.
2. Виявлення слабких паролів: дані налаштування дають можливість виявити облікові записи зі слабкими паролями. Це може бути ознакою недостатньої політики паролів або недбалості користувачів при виборі паролів.
3. Виявлення несанкціонованого доступу: роблячи перелік користувачів можна перевірити, чи є серед них облікові записи, які мають доступ до певних ресурсів чи систем в мережі, до яких не мають дозвуолц. Це може вказувати на можливі проблеми з управлінням доступом або незадокументовані облікові записи, які можуть представляти потенційну загрозу безпеці.

Було залишено значення по умовчанню "Start UID 1000" і "End UID 1200 ". Дані значення означають діапазон ідентифікаторів користувачів (UID), які будуть використовуватись під час брутфорсу RID

"Start UID 1000" вказує на початковий ідентифікатор користувача, з якого розпочинається перебір, тим часом як "End UID 1200 " вказує на кінцевий ідентифікатор, до якого будуть перебирані ідентифікатори користувачів. Дані

значення оптимальні, оскільки використання обмеженого діапазону UID, такого як від 1000 до 1200, дозволяє скоротити кількість комбінацій RID, які будуть випробовуватись. Це зменшує навантаження на систему та сканер, а також зменшує час, необхідний для виконання сканування. А також це є заходом безпеки, оскільки дозволяє сконцентрувати пошук на певному діапазоні користувачів з вищими UID.

Враховуючи ці фактори, використання значень Start UID 1000 і End UID 1200 може бути оптимальним варіантом для брутфорсу RID при скануванні, забезпечуючи збалансований аналіз безпеки для звичайних користувачів у відповідних діапазонах UID.

Щоб сканування було повноцінним, було додано опцію "Use detected SIDs". Вона корисна для виявлення безпекових ідентифікаторів (SIDs) під час сканування системи Windows. Це може включати облікові записи, які можуть бути приховані або неявні, але виявлені під час сканування системи. До таких облікових засобів можуть належати облікові записи, які були спеціально створені для зловживання.

Також дана опція дозволяє сканеру з'ясувати, які облікові записи мають доступ до певних ресурсів або систем. Це допомагає ідентифікувати можливі проблеми з безпекою, такі як облікові записи з неправомірним доступом до конфіденційної інформації або облікові записи з надмірними привілеями.

Підсумовуючи, використання параметру "Use detected SIDs" дозволяє покращити ефективність та точність сканування і допомагає виявити потенційні проблеми безпеки, які пов'язані з обліковими записами та доступом.

3.2 Аналіз результатів сканування

Під час сканування сайту за допомогою Nessus було виявлено служби та вразливості, що можуть мати вплив на безпеку та конфіденційність системи. Далі буде розглянуто кожен з цих результатів:

Виявлено службу FTP (File Transfer Protocol). Це означає, що сайт підтримує можливість передачі файлів за допомогою даного протоколу. Під час сканування FTP-сервера не було виявлено жодної вразливості, що може вказувати на його безпеку. Це позитивний результат, який свідчить про те, що FTP-сервер має належну конфігурацію та захищений від відомих вразливостей. Однак, безпека FTP-сервера не обмежується виявленням вразливостей під час даного сканування.

Рекомендується встановити належні політики безпеки, використовувати сильні паролі, шифрувати передачу даних та регулярно оновлювати програмне забезпечення для забезпечення максимальної безпеки FTP-сервера.

Наступною виявленою службою є DNS (Domain Name System), що використовується для розрізнення та перетворення доменних імен на IP-адреси. Також було виявлено BIND (Berkeley Internet Name Domain) - відкритий програмним продукт для реалізації DNS-сервера. Він є стандартом для DNS-серверів і забезпечує трансляцію доменних імен на відповідні IP-адреси, дозволяючи користувачам знайти ресурси в мережі за допомогою зрозумілих доменних імен. Було розкрито версію BIND, а саме "9.11.4-P2". Зловмисник, отримавши цю інформацію, потенційно міг би використати відомі вразливості для атаки на сервер DNS. Проте таких вразливостей на даний момент не існує і сервер цілком захищений.

Виявлення служби POP (Post Office Protocol) означає, що сайт підтримує протокол POP для отримання електронної пошти. Під час сканування сайту не було виявлено жодної вразливості. Це свідчить про те, що служба POP на сайті не має відомих вразливостей, які можуть бути використані для несанкціонованого доступу або витоку даних. Однак, безпека POP-сервера також залежить від належної конфігурації та застосування належних заходів безпеки. Використання безпечних паролів, встановлення обмежень на доступ до поштових скриньок та моніторинг активності на сервері можуть покращити безпеку служби POP.

Наступним виявленим протоколом є ICMP (Internet Control Message Protocol). Це свідчить про наявність мережевої служби, яка використовує цей протокол для обміну повідомленнями. У результаті сканування було виявлено розкриття інформації про дату на сервері. Це не несе прямої загрози, проте рекомендовано вжити заходів для усунення цієї вразливості.

Останньою виявленою службою є SNMP (Simple Network Management Protocol). Це свідчить про те, що на сайті встановлено SNMP-агент для моніторингу

та керування мережевими пристроями. Під час сканування було виявлено вразливість "SMTP Server Non-standard Port Detection".

Вразливість "SMTP Server Non-standard Port Detection" (виявлення нестандартного порту SMTP-сервера) відноситься до сфери безпеки мережевих протоколів і зокрема до протоколу Simple Mail Transfer Protocol (SMTP).

Стандартними портами для SMTP є порти: 25, 465, 587 і 2525. Проте веб-сайт використовує 26 порт, що може призвести до певних проблем з безпекою. Зловмисник може використати спеціальні інструменти або програми для виявлення SMTP-серверів, які працюють на нестандартних портах. Потім він може використати цю інформацію для проведення подальших атак, таких як спам-розсилка, фішинг атаки, внедрення шкідливих кодів, або злам системи.

Потенційна шкода, яку може спричинити ця вразливість, полягає в тому, що атакуючий може зламати систему із застосуванням іншого порту, який не очікується адміністраторами. Це може призвести до незаконного доступу до електронної пошти, перехоплення комунікацій та поширення шкідливих впливів на мережу.

Під час дослідженні, Nessus спробував встановити зв'язок з SMTP сервером, відправивши певні запити. Як результат, він отримав відповідь у вигляді банера, який містить інформацію про сервер. Вивід банера, представлено на рисунку 3.1.

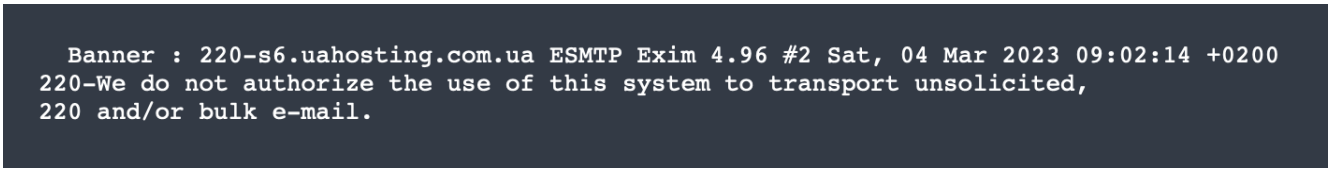

Рисунок 3.1 – Банер з виводом інформації про SMTP сервер

Даний банер містить певну корисну інформацію про сервер і його налаштування:

- "220" є кодом статусу, що позначає, що сервер готовий приймати команди;
- "s6.uahosting.com.ua" є ім'ям сервера;
- "ESMTP Exim 4.96" вказує на тип сервера та його версію;
- "Sat, 04 Mar 2023 09:02:14 +0200" є датою та часом відправки відповіді.

Порядок повідомлень вказує на те, що сервер відмовляється авторизувати використання системи для передачі небажаних або масових електронних листів (спаму). Це може бути обмеженням або політикою сервера, яка дотримується для забезпечення безпеки та зменшення спаму. Важливо зауважити, що це не означає, що SMTP сервер повністю захищений, але свідчить про те, що сервер має встановлені заходи для запобігання використанню системи для відправки спаму.

3.3 Оцінка знайдених вразливостей

Для оцінювання критичності та важкості потенційних вразливостей Nessus шкалу оцінювання CVSS Використання даної шкали дозволяє присвоювати кожній знайденій вразливості числове значення, що відображає її важкість і потенційний вплив на систему [13]. Це дає змогу класифікувати та порівнювати вразливості залежно від їх серйозності, а також допомагає зорієнтуватися у пріоритетах усунення вразливостей. Також такий метод оцінювання сприяє стандартизації процесу оцінювання вразливостей, що полегшує співпрацю та обмін інформацією між різними фахівцями з безпеки.

Загалом, використання шкали оцінювання CVSS в Nessus забезпечує об'єктивну оцінку рівня загрози і дозволяє приймати обґрунтовані рішення стосовно заходів безпеки для забезпечення високого рівня захищеності інформаційних систем.

Версія 2.0 шкали CVSS була створена з метою забезпечення більш точного і об'єктивного оцінювання вразливостей.

Оцінка CVSS складається з трьох наборів показників (базовий, розширений та очікуваний). На рисунку 3.2 наведено набори показників шкали оцінювання CVSS [14].

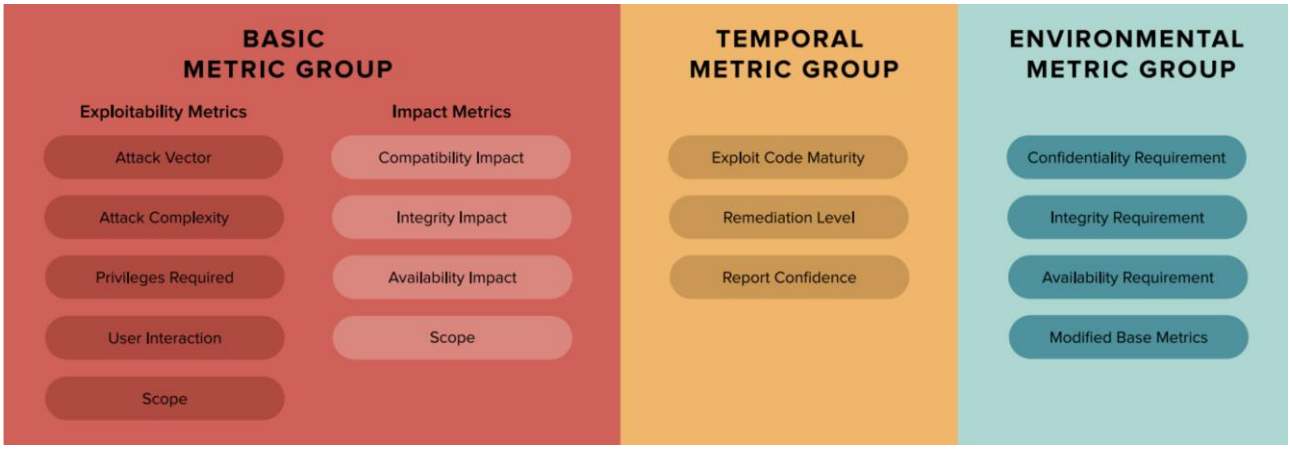

Рисунок 3.2 – Групи шкали оцінювання CVSS

Базова група (Basic Metric Group) визначає властивості самої вразливості, такі як рівень складності атаки, рівень доступу до системи та вплив на конфіденційність, цілісність та доступність даних.

Можливість використання вразливості – показники, які складаються з характеристик уразливого компонента, при цьому можливість використання складається з чотирьох додаткових підкомпонентів.

Вектор атаки – ця оцінка залежить від рівня доступу, необхідного для використання вразливості. Оцінка буде вищою для експлойтів, які можна виконати віддалено (тобто за межами мережі компанії), ніж для експлойтів, які вимагають фізичної присутності (тобто необхідно мати доступ до фізичного порту на пристрої або доступ до локальної мережі всередині приватних даних центр).

Складність атаки – ця оцінка змінюється залежно від факторів поза контролем зловмисника, необхідних для використання вразливості. Оцінка буде вищою для експлойтів, які вимагають додаткової роботи з боку зловмисника, як-от викрадення спільного секретного ключа або атаки «людина посередині», ніж для атаки, яка не потребує таких додаткових зусиль.

Необхідні привілеї – ця оцінка залежить від привілеїв, необхідних зловмиснику для здійснення експлойту. Уразливість, для використання якої потрібні адміністративні привілеї, матиме вищу оцінку, ніж уразливість, яка не потребує автентифікації або підвищених привілеїв з боку зловмисника.

Взаємодія користувача – ця оцінка залежить від того, чи повинен зловмисник залучити добровільного чи мимовільного учасника, щоб виконати своє завдання.

Оцінка буде вищою, якщо зловмисник зможе працювати автономно, без участі користувача.

Область застосування стосується того, чи може вразливість в одному компоненті поширюватися на інші компоненти. Оцінка обсягу вища, якщо можливе поширення.

Вплив – вплив зосереджується на фактичному результаті, якого може досягти атакуючий в результаті використання даної вразливості. Показники впливу складаються з трьох підметрик – конфіденційності, цілісності та доступності.

Розширена група враховує часові аспекти вразливості, такі як наявність виправлення, доступність експлойтів або зміна у широкому поширенні вразливості.

Зрілість експлойт-коду – доки не існує методу використання вразливості, він є відносно безпечним. Як і у випадку з більшістю програмного забезпечення, код, доступний для здійснення експлойтів, може з часом розвиватися, ставати стабільнішим і доступнішим. Коли це станеться, оцінка цього підкомпонента збільшиться.

Рівень виправлення – коли вразливість виявляється вперше, можливо, не буде доступного виправлення чи іншого обхідного шляху. З часом стають доступними обхідні шляхи, тимчасові виправлення та, зрештою, офіційні латки, що знижує оцінку вразливості в міру вдосконалення виправлення.

Повідомлення про достовірність – достовірність вимірює рівень перевірки, який демонструє, що вразливість є реальною та її можна використовувати.

Очікувана група враховує контекстові фактори, пов'язані з вразливістю, такі як важливість системи, доступність заходів безпеки та можливість відновлення після атаки.

Вимоги безпеки характеризують критичність відповідного активу. Критично важливі дані або активи отримують вищу оцінку, ніж менш важливі активи. Наприклад, уразливість, виявлена в базі даних усіх клієнтів, отримає вищу оцінку, ніж уразливість, виявлена на робочій станції непривілейованого користувача.

Змінені базові показники – організація може змінити значення базових показників CVSS на основі заходів пом’якшення, які вона застосувала. Результатом є те, що базова метрика вектора атаки в цьому випадку зменшується.

Враховуючи вище перелічені фактори, виноситься формується оцінка числового значення. На рисунку 3.3 наведено відповідність числового значення до рівня критичності вразливості.

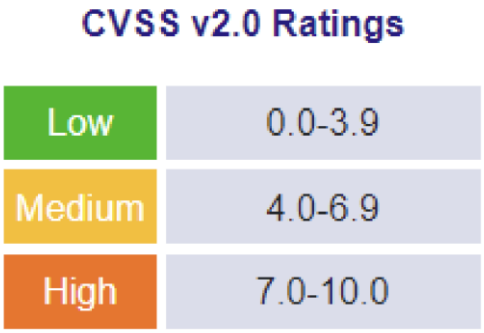

Рисунок 3.3 – Шкала оцінювання CVSS

Сканер оцінив вразливість "SMTP Server Non-standard Port Detection" наступним вектором: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N.

Щоб проаналізувати оцінку, вектор було розбито на метрики та розглянуто детальніше.

AV (Attack Vector) розшифровується як вектор атаки. В даному випадку вектором є мережа (Network). Тобто вразливість може бути використана з мережі, що означає, що для експлуатації вразливості атакуючий повинен мати доступ до мережі, в якій розташована цільова система.

Наступним метриком є AC (Access Complexity), що означає складність доступу. Вона оцінена низьким рівнем (Low). Експлуатація вразливості вимагає незначних знань або навичок з боку атакуючого, або потребує спеціальних умов або обмежень. Дана умова значно підвищує рівень критичності вразливості.

Au (Authentication) вказує на те, чи потрібна аутентифікація щоб проексплотувати вразливість. Значення N (None) означає, що зловмисник не потребує аутентифікації для експлуатації вразливості, тобто він може зламати систему без необхідності мати обліковий запис або пароль.

Значення C (Confidentiality Impact) вказує на те, чи має вразливість вплив на конфіденційність. В даному випадку значення N (None) показує, що вразливість не має прямого впливу на конфіденційність інформації.

I (Integrity Impact) визначає вплив на цілісність. Значення P (Partial) вказує на те, що експлуатація вразливості може призвести до часткового порушення цілісності інформації.

Останьою метрикою є A (Availability Impact), що показує вплив на доступність. Значення N (None) показує, що вразливість не має прямого впливу на доступність системи, тобто не викликає перебоїв в роботі системи або сервісів.

Підсумувавши результати оцінки кожного метрика видно, що дана вразливість має характеристики представлені в таблиці 3.1.

Таблиця 3.1 – Характеристики вразливості

Вектор атаки	Може бути виконана через мережу
Складність доступу	Низька
Аутентифікація	Не потрібна
Вплив на конфіденційність	Відсутній прямий вплив
Вплив на цілісність	Часткове порушення цілісності інформації
Вплив на доступність	Відсутній прямий вплив
Оцінка	5

Цей вектор допомагає зрозуміти характер вразливості та визначити її потенційні наслідки для системи. Якщо конвертувати вектор в числове значення, то отримаємо оцінку 5. Це означає, що вразливість має помірний рівень серйозності та може потенційно впливати на систему.

Також варто взяти до уваги, що багатьох випадках фаєрволи та брандмауери налаштовані для моніторингу та блокування трафіку, що протікає через стандартні порти. Проте, якщо SMTP-сервер використовує нестандартний порт, як в нашому випадку, порт 26, то цей трафік може пройти в обхід захисту, оскільки багато захисних механізмів спираються на стандартні порти. Це може бути використано зловмисниками для надання недостовірних даних або для виконання атаки на поштовий сервер.

Ця вразливість підкреслює важливість належної конфігурації та моніторингу поштових серверів, включаючи контроль за використанням нестандартних портів.

3.4 Розробка плану виправлення вразливостей

Для усунення вразливості, пов'язаної з використанням нестандартного порту SMTP сервера, було розроблено два плани дій.

Перший план передбачає зміну порту SMTP на стандартний. Цей підхід включає встановлення з'єднання з сервером, перевірку поточного порту, зміну налаштувань порту на стандартний, збереження змін у конфігураційному файлі сервера, перезапуск сервера для застосування змін та перевірку доступності сервера на новому стандартному порту.

Другий план спрямований на залишення нестандартного порту (порт 26) і передбачає налаштування додаткових захисних механізмів для забезпечення безпеки. Цей підхід включав встановлення з'єднання з сервером, перевірку поточного порту, налаштування файрволу або інших захисних механізмів для моніторингу трафіку на нестандартному порті, встановлення сильної аутентифікації для доступу до сервера через цей порт.

Обидва плани були розроблені з метою забезпечення безпеки сервера SMTP, проте різнилися у своїх підходах до усунення вразливості. Кінцевий вибір між цими двома планами залежить від контексту, вимог безпеки та впливу веб-сайт. План дій представлено на рисунку 3.4.

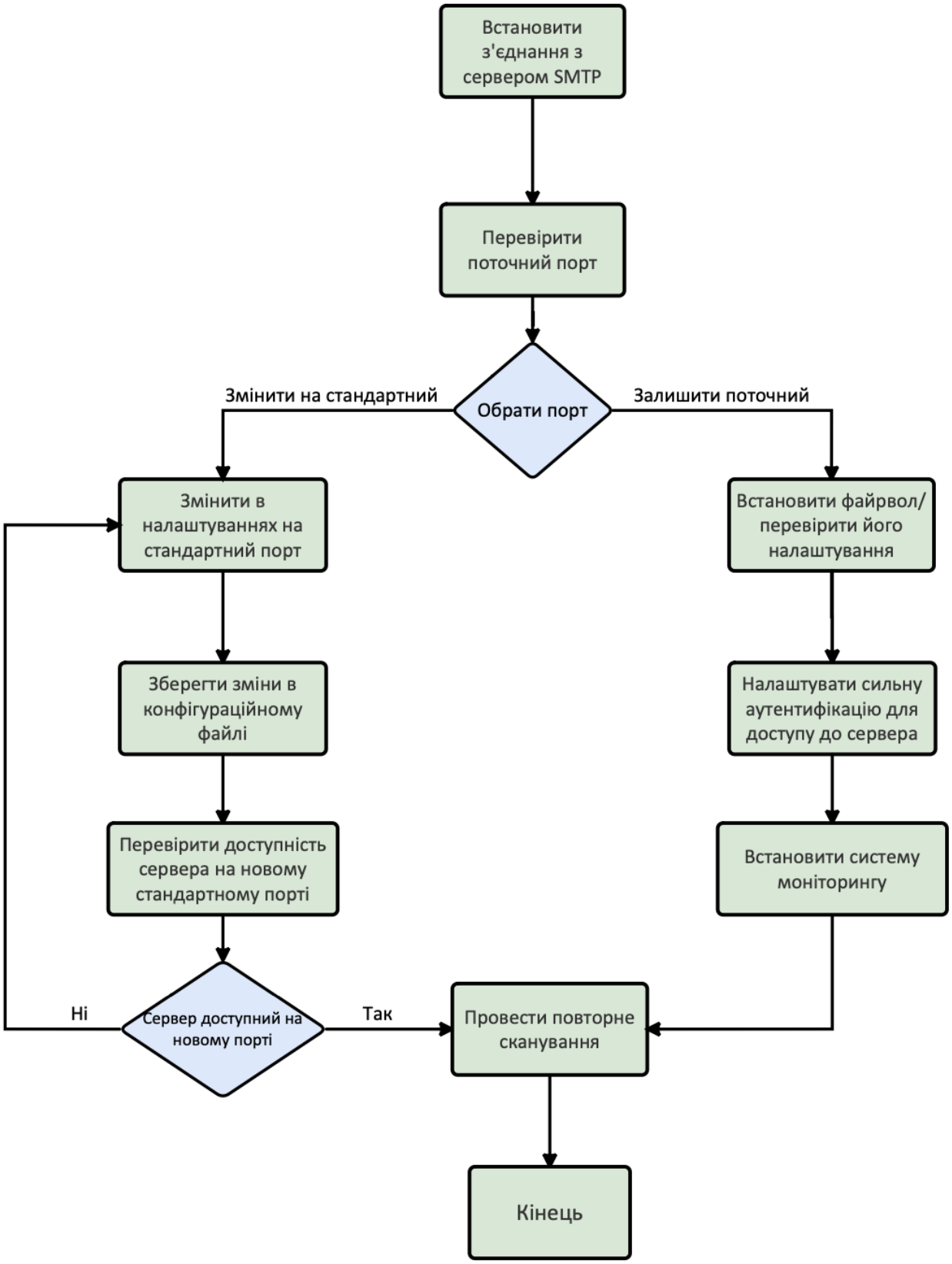

Рисунок 3.4 – План виправлення вразливостей

Для переведення сервера SMTP на стандартний порт наведено більш детальний план дій. Кроки можуть змінюватися в залежності від використовуваного серверного програмного забезпечення.

- Відкрити конфігураційний файл сервера SMTP. Зазвичай це файл з розширенням ".conf" або ".cfg". Шлях до файлу може залежати від використовуваного серверного програмного забезпечення.
- Знайти розділ або параметр, що відповідає за налаштування порту сервера SMTP. Цей параметр може мати назву "SMTP Port", "Port Number" або схожу.
- Змінити значення параметра на відповідний стандартний порт SMTP.
- Зберегти внесені зміни у конфігураційному файлі.
- Перезапустити сервер SMTP, щоб зміни набрали чинності.
- Після перезапуску перевірити, чи сервер SMTP тепер слухає на новому стандартному порті. Виконати тестове підключення до сервера SMTP за допомогою клієнта електронної пошти або інструментів, таких як Telnet, і перевірити, чи працює підключення через новий порт.

У випадку, якщо необхідно залишити SMTP сервер на нестандартному порті, рекомендується перевірити та налаштувати системи захисту, такі як: брандмауер, аутентифікація та система моніторингу. Це дозволить контролювати трафік, що надходить на цей порт і забезпечує виявлення та блокування небажаних або шкідливих дій.

Брандмауер - це програмне забезпечення, яке контролює вхідний та вихідний мережевий трафік і визначає, які з'єднання дозволено або блоковано.

Для моніторингу трафіку на порті 26 потрібно налаштувати правила, які дозволять переглядати і аналізувати вхідний трафік на цьому порті. Це може включати створення правил, що дозволяють записувати інформацію про підключення, аналізувати типи пакетів, встановлення обмежень на основі IP-адрес або використання вимог до безпеки, таких як вимагання аутентифікації або шифрування. Після налаштування, він почне моніторити трафік, який надходить на порт 26. Це дозволяє виявляти потенційно небезпечні або небажані з'єднання, спостерігати за підозрілими діями та вчасно реагувати на потенційні загрози. У разі виявлення небажаного або шкідливого трафіку він може блокувати або обмежувати доступ до цього порту. Це допомагає забезпечити, що лише легітимні або довірені джерела матимуть доступ до сервера на цьому порті, мінімізуючи ризик атак і зловживань.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Психологічні чинники небезпеки

У сучасному світі, де постійно зіштовхуються з різноманітними ризиками і небезпеками, важливо не тільки розуміти технічні аспекти безпеки, але й усвідомлювати вплив психологічних чинників на нашу поведінку та прийняття рішень. Ключовими психологічні аспектами, які можуть впливати на сприйняття небезпеки та нашої реакції на неї є:

- Страх і паніка.
- Соціальний вплив.
- Вплив стресу.
- Підсвідоме сприйняття.

Страх є природним реакцією на небезпеку і може бути корисним, якщо ми використовуємо його для активування захисних механізмів і уникнення ризикових ситуацій. Однак, коли страх перетворюється на паніку, це може призвести до неправильних рішень та нерозсудливої поведінки. Важливо вміти контролювати свої емоції і аналізувати ситуацію об'єктивно, щоб уникнути непотрібних ризиків.

Люди часто спираються на думки та поведінку інших людей у ситуаціях небезпеки. Це може бути корисно, коли інші люди мають досвід або експертизу в даній області. Однак, соціальний вплив також може призводити до масової паніки або безрозсудних дій, якщо всі просто копіюють поведінку одне одного. Важливо здійснювати самостійний аналіз ситуації і засновувати свої рішення на розумінні фактів і можливих наслідків.

Стресові ситуації можуть впливати на наше мислення та прийняття рішень. Під впливом стресу ми можемо стати менш уважними, розсіяними та схильними до помилок. При оцінці небезпеки важливо враховувати свої емоційні стани та вживати заходів для зменшення стресу, наприклад, використання релаксаційних технік чи звернення до підтримки від рідних та друзів.

Наші реакції на небезпеку часто базуються на підсвідомому сприйнятті і інтуїції. Наші мозки здатні сприймати сигнали ризику, навіть якщо ми не можемо пояснити їх об'єктивно. Варто довіряти своїм інтуїтивним відчуттям, проте також

важливо здійснювати об'єктивний аналіз ситуації та використовувати наявну інформацію для прийняття розумних рішень.

Психологічні чинники небезпеки становлять загрозу не лише людині, а також компанії, де вона працює. Одним з таких чинників є соціальна інженерія, яка використовується зловмисниками для маніпулювання людьми та отримання невірної інформації або доступу до конфіденційних даних. Вона ґрунтується на використанні психологічних механізмів, щоб переконати людей розкрити конфіденційну інформацію або виконати певні дії [15].

Це стає особливо важливим у сфері кібербезпеки, де соцінженери можуть використовувати психологічні прийоми для отримання доступу до паролів, конфіденційної інформації або навіть для впровадження шкідливих програм. Вони можуть використовувати фішингові електронні листи, смішні теми, соціальні медіа або інші методи, щоб залучити людей до своїх підступних схем.

Розуміння психологічних чинників є важливим для ефективного захисту від соціальної інженерії. Підприємства повинні проводити навчання та підвищувати свідомість персоналу щодо таких психологічних методів атаки. Також важливо розробляти політики безпеки, які враховують ці ризики та встановлюють процедури для перевірки та перевірки ідентичності, контролю доступу та обмеження прав[16].

Під час тестування безпеки також враховується можливість соціальної інженерії та психологічних атак. Тестери здійснюють аналіз поведінки користувачів, виявляють можливі точки вразливості і розробляють рекомендації щодо поліпшення безпеки. Вони можуть проводити фішингові тести, тестування соціальної інженерії та інші методи, щоб перевірити реакцію персоналу на підступи та виявити слабкі місця в системі безпеки.

Загальна мета полягає в тому, щоб підвищити усвідомленість щодо соціальної інженерії та психологічних атак серед персоналу. Це означає навчання співробітників розпізнавати ці види загроз і вживати заходів для їх захисту. Додатково, ця ініціатива спрямована на вдосконалення політик та процедур, щоб зменшити ризики, пов'язані зі співробітництвом зловмисників.

Розуміння соціальної інженерії та психологічних атак допомагає працівникам виявляти маніпуляції, фішингові атаки, вимагання розкриття

конфіденційної інформації та інші схеми обману. Навички розпізнавання таких загроз допомагають персоналу бути більш пильними та уважними у взаєминах з незнайомцями, в розмовах по телефону та в електронній комунікації. Розробка і впровадження політик та процедур, спрямованих на захист від соціальної інженерії, включає створення чітких правил для обміну конфіденційною інформацією, перевірку автентичності запитів та інструкцій, а також регулярні навчання і перевірки для персоналу.

Ці заходи мають на меті зменшити ризики, пов'язані зі співробітництвом зловмисників і забезпечити більш безпечне робоче середовище для всього персоналу компанії.

4.2 Естетичне оформлення робочого місця адміністратора веб-сайту

Робоче місце адміністратора є важливим елементом, який може значно впливати на настрій, комфорт та продуктивність працівника. Естетичне оформлення цього простору відіграє важливу роль у створенні зручного та приємного середовища для роботи.

Один з головних аспектів естетичного оформлення робочого місця адміністратора - це правильне розташування обладнання та аксесуарів. Зручний доступ до комп'ютера, монітора, клавіатури та миші допомагає забезпечити комфортну роботу без зайвих напружень і незручностей.

При розміщенні обладнання варто враховувати ергономіку робочого простору. Монітор повинен бути розташований на відстані, що не надто близька до очей, з правильною висотою і нахилом, щоб забезпечити оптимальне зорове сприйняття. Клавіатура та миша також повинні бути розташовані належним чином, забезпечуючи зручний доступ і натуральну позицію рук і зап'ястя.

Крім того, важливо правильно організувати кабелі. Чистота та порядок є не менш важливими аспектами естетичного оформлення. Проводи від комп'ютера, монітора, принтера та інших пристроїв слід прокладати таким чином, щоб уникнути їх непотрібного скупчення, плутанини та перешкод.

Все це сприяє не лише естетичному вигляду робочого місця, але й забезпечує комфорт, зручність та ефективність роботи адміністратора ПК.

Правильне розташування обладнання та організація кабелів створюють затишок, допомагають уникнути непотрібних перешкод та покращують робочий процес.

Нарешті, естетично оформлене робоче місце сприяє загальному задоволенню працівника виконувати свої обов'язки. Відчуття комфорту та гармонії в робочому середовищі позитивно впливає на мотивацію та задоволення від роботи.

Вибір правильного крісла та столу має велике значення для забезпечення комфорту під час тривалої роботи. Крісло повинно мати зручну спинку, належну підтримку для спини та плечей, а також регульовану висоту. Стіл повинен бути достатньо великим для розміщення всього необхідного обладнання та документів, а також мати плавні поверхні без гострих країв.

Колірна схема та освітлення також мають значення при естетичному оформленні робочого місця. Яскраві, насичені кольори можуть викликати втому та розсіювати увагу, тоді як природні та нейтральні відтінки сприяють спокою та зосередженості. Освітлення повинно бути рівномірним, не створювати блискіт та тіні на робочій поверхні, а також не викликати напруження очей.

Необхідними елементами естетичного оформлення робочого місця є також організація простору та особисті аксесуари. Правильно розташовані полиці, ящики та інші зручні елементи допоможуть підтримувати порядок та організованість. Особисті аксесуари, які відображають інтереси та особистість адміністратора, додають унікальності та комфорту до простору[17].

Наочне оформлення робочого місця адміністратора не лише створює приємну атмосферу, але й впливає на продуктивність та настрій працівника. Естетично приємне та комфортне робоче середовище сприяє покращенню зосередженості, стимулює творче мислення та зберігання енергії.

На першому етапі, естетичне оформлення робочого місця створює почуття затишку та комфорту, що впливає на загальну психологічну стабільність працівника. Чистота, організованість та естетика робочого простору створюють позитивний настрій та сприяють відчуттю злагоди.

Далі, естетичне оформлення робочого місця сприяє підвищенню концентрації та зосередженості. Правильно підібрані кольори, приємне освітлення

та ергономічні меблі допомагають уникнути відволікань та забезпечують оптимальні умови для роботи.

Крім того, естетичне оформлення робочого простору може сприяти підвищенню творчого потенціалу. Вибір стильного дизайну, розташування мотивуючих елементів та особисті аксесуари можуть стимулювати творчість та інноваційність у роботі.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи було проведено технічну оцінку захищеності веб-сайту Великоберезовицької територіальної громади. З метою забезпечення безпеки сайту було проведено аналіз веб-ресурсу та визначено основні типи вразливостей, до яких вразливі веб-сайти створені на платформі Joomla.

В результаті виконання кваліфікаційної роботи виконано наступні завдання:

- проведено аналіз веб-ресурсу та визначено вимоги до технічної оцінки;
- проаналізовано три рішення поставленого завдання та обрано найбільш відповідний;
- визначено та проаналізовано типи вразливостей веб-додатків розроблених на платформі Joomla та на основі цього обрано інструмент для проведення сканування;
- проведено сканування веб-сайту на наявність вразливостей;
- проаналізовано знайдену інформацію;
- розроблено рекомендації щодо усунення виявленої вразливостей.

У першому розділі було досліджено об’єкт тестування. Було розроблено блок-схему, що відображає структуру та зв'язки між сторінками веб-сайту. Також було проаналізовано вимоги технічного оцінювання. Виходячи з інформації, яка була доступна щодо веб-сайту, було поставлено завдання перевірити як система взаємодіє зі своєму оточенням, виявити потенційні слабкі місця, проаналізувати відповіді на запити, перевірити застосування механізмів безпеки та реагування на атаки.

У другому розділі було проведено аналіз типів вразливостей, їх рівень критичності та заходи захисту. Опираючись на ці дані, було обрано для аналізу сканери вразливостей. Проаналізувавши кожен, було обрано сканер для проведення технічної оцінки захищеності веб-сайту Великоберезовицької територіальної громади.

У третьому розділі було детально описано й обґрунтовано налаштування конфігурації для сканування. Проаналізовано та оцінено знайдену інформацію й потенційні вразливості. А також розроблено план виправлення виявленої вразливості.

У розділі "Безпека життєдіяльності, основи охорони праці" було визначено психологічні чинники небезпеки та проаналізовано вплив естетичного оформлення робочого місця адміністратора веб-сайту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Державний центр кіберзахисту державної служби спеціального зв’язку та захисту інформації України. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 року. URL: https://scpc.gov.ua/ua/articles/233

2. Joomla: Vulnerability Statistics. Vulnerability Trends Over Time. URL: https://www.cvedetails.com/vendor/3496/Joomla.html

3. Security Announcements [20190602] - Core - XSS in subform field. URL: https://developer.joomla.org/security-centre/784-20190602-core-xss-in-subform-field

4. CVE-2018-8045. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8045

5. CVE-2018-17856. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17856

6. CVE-2019-10945. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10945

7. CVE-2016-8869. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8869

8. Greenbone OpenVAS. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8869

9. Application security with zero noise. URL: https://www.invicti.com/product/

10. Tenable Nessus Vulnerability Scanner: Product overview. URL: https://www.techtarget.com/searchsecurity/feature/Tenable-Nessus-Vulnerability-Scanner-Product-overview

11. Discovery Scan Settings. URL: https://docs.tenable.com/nessus/Content/DiscoverySettings.htm

12. Assessment Scan Settings. URL: https://docs.tenable.com/nessus/Content/AssessmentSettings.htm#GNAccuracy

13. Common Vulnerability Scoring System SIG. URL: https://www.first.org/cvss/

14. What are CVSS Scores. CVSS Score Metrics URL: https://www.balbix.com/insights/understanding-cvss-scores/

15. Н.Є. Твердохлєбова. Психологічні аспекти безпеки праці. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/54b4e10c-7a11-416f-96e0-f2cd2f861d65/content

16. А. А. Мельниченко. Соціальна інженерія як фактор забезпечення стійкого розвитку соціальних систем. URL: http://visnyk-psp.kpi.ua/article/view/123398

17. Є. А. Самохіна. Ергономічне забезпечення робочого місця. URL: http://repo.snau.edu.ua/handle/123456789/9270