МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет прикладної математики та інформатики
(повне найменування назва факультету)

кібербезпеки
(повна назва кафедри)

Дипломна робота

Розробка проекту ідентифікації загроз інформаційній безпеці веб-ресурсів та оцінки їх ризиків

Виконав: студент групи ПМК-42с
спеціальності
125 «Кібербезпеки»
(шифр і назва спеціальності)

(підпис) Сорока О.О. (прізвище та ініціали)

Керівник (підпис) Вайганг Г.О. (прізвище та ініціали)

Рецензент (підпис) О.Є. Ілларіонов (прізвище та ініціали)

2023

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ФРАНКА

Факультет Прикладної математики та інформатики
Кафедра Кібербезпеки
Спеціальність: 125 «Кібербезпека»
«шифр і назва»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри _____

"31 "серпня 2022 року

ЗАВДАННЯ
на кваліфікаційну бакалаврську роботу студента
Сороки Олени
(прізвище, ім'я, по батькові)

1. **Тема роботи**: Розробка проекту ідентифікації загроз інформаційній безпеці веб-ресурсів та оцінки їх ризиків

   Керівник роботи доцент, к.т.н. Вайганг Г.О.
   затверджені наказом університету від «13» вересня 2021 року № 15
2. **Строк подання студентом роботи** «13» червня 2023 року
3. **Вихідні дані до роботи:**

4. **Зміст пояснювальної записки (перелік питань, які потрібно розробити)**
1. Огляд питання захисту веб-ресурсів
2. Дослідження рівня захищеності веб-ресурсів: загрози, вразливості, атаки
3. Архітектура веб-додатків та місце безпеки в ній
4. Дослідження захищеності веб-сайтів за допомогою експлуатації вразливостей

5. **Перелік графічного матеріалу:**

6. Консультанти розділів роботи

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

7. Дата видачі завдання **31 серпня 2022 р.**

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Уточнення постановки завдання	21.03.2023	
2	Аналіз літератури	28.03.2023	
3	Обґрунтування вибору рішення	31.03.2023	
4	Збір даних	07.04.2023	
5	Огляд питання захисту веб-ресурсів	18.04.2023	
6	Дослідження рівня захищеності	28.04.2023	
7	Архітектура веб-додатків та місце бекенду	12.05.2023	
8	Документування вразливості веб-сайтів	22.05.2023	
9	Оформлення та друк пояснювальної записки та додатків	06.06.2023	
10	Отримання рецензії	10.06.2023	
11	Подання роботи на кафедру	12.06.2023	
12	Захист в ЕК	16.06.2023	

Студент _____ Сорока О.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Вайганг Г.О.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Пояснювальна записка дипломного проекту складається зі вступу, чотирьох розділів, що містять 41 рисунків, висновків та списку використаних джерел з 38 найменувань. Загальний обсяг роботи становить 85 сторінок.

Об’єктом дослідження є безпека веб-сайту та його вразливості.

Метою роботи є дослідження загроз та вразливостей інформаційній безпеці веб-ресурсів та визначення рівня захищеності веб-сайтів шляхом експлуатації вразливостей.

У першому розділі розглядається загальний огляд питання захисту веб-ресурсів, який включає в себе визначення основних термінів і понять, пов'язаних з безпекою веб-додатків, а також огляд актуальних загроз та вразливостей, з якими стикаються веб-ресурси.

Другий розділ присвячений дослідженню рівня захищеності веб-ресурсів. У цьому розділі проводиться аналіз актуальних загроз та вразливостей, з якими стикаються веб-ресурси. Розглядаються різноманітні типи атак, включаючи SQL-ін'єкції, кросс-сайтовий скриптінг, аутентифікаційні атаки та інші. Описуються методи використання цих атак та можливі наслідки для безпеки веб-ресурсу.

Третій розділ присвячений архітектурі веб-додатків та ролі безпеки в цій архітектурі. Описуються загальні принципи безпеки веб-додатків, включаючи аутентифікацію, авторизацію, захист від вразливостей та шифрування даних.

У четвертому розділі розглядається дослідження захищеності веб-сайтів шляхом експлуатації вразливостей. Пояснюється, які типи вразливостей можуть бути використані для атаки на веб-сайт, і наводяться приклади реальних вразливостей та їх наслідків. Розглядаються також методи запобігання та виявлення вразливостей для підвищення рівня захищеності веб-сайтів.

Ключові слова: ЗАХИСТ ВЕБ-РЕСУРСІВ, БЕЗПЕКА, ЗАГРОЗИ, ВРАЗЛИВОСТІ, АТАКИ, SQL-ІН'ЄКЦІЇ, ТЕСТУВАННЯ.

ABSTRACT

The explanatory note of the diploma project consists of an introduction, four chapters containing 41 figures, conclusions and a list of 38 references. The total volume of the work is 85 pages.

The **object** of study is website security and its vulnerabilities.

The **purpose** of the study is to investigate threats and vulnerabilities to the information security of web resources and to determine the level of security of websites by exploiting vulnerabilities.

The first section provides a general overview of the issue of web resource protection, which includes the definition of basic terms and concepts related to web application security, as well as an overview of current threats and vulnerabilities faced by web resources.

The second section is devoted to the study of the level of security of web resources. This section analyzes the current threats and vulnerabilities faced by web resources. Various types of attacks are considered, including SQL injection, cross-site scripting, authentication attacks, and others. Methods of using these attacks and possible consequences for the security of a web resource are described.

The third section is devoted to the architecture of web applications and the role of security in this architecture. It describes the general principles of web application security, including authentication, authorization, vulnerability protection, and data encryption.

The fourth chapter discusses the study of website security through vulnerability exploitation. It explains what types of vulnerabilities can be used to attack a website and provides examples of real-world vulnerabilities and their consequences. It also discusses methods of preventing and detecting vulnerabilities to improve website security.

Keywords: WEB RESOURCE PROTECTION, SECURITY, THREATS, VULNERABILITIES, ATTACKS, SQL INJECTIONS, TESTING.

Зміст

ВСТУП

Актуальність. Діяльність будь-якої організації так чи інакше пов'язана із веб-технологіями. Широкого поширення набули веб-портали різних послуг (у тому числі державних), інтернет-магазини, торгові майданчики, різноманітні бізнес-додатки, системи дистанційного банківського обслуговування. Неможливо уявити собі сучасну організацію, чи то велика корпорація, чи невелика приватна фірма, яка не мала б свого офіційного сайту чи сторінки на якомусь публічному веб-ресурсі. Корпоративні програми, для яких необхідно встановлювати клієнтське програмне забезпечення та регулярно його оновлювати, йдуть у минуле. Веб-технології дозволяють спростити бізнес-процеси.

Щоб максимально використовувати переваги веб-технологій, необхідно забезпечити доступність ресурсів для цільової аудиторії, наприклад з Інтернету. Але доступу, отже, можуть отримати і зловмисники. Це і недобросовісні конкуренти, та інші категорії порушників, які керуються злочинними намірами, наприклад, з метою розкрадання коштів, порушення доступності ресурсу або отримання чутливої інформації. Компрометація додатків може призвести як до репутаційних втрат, так і до фінансових, у тому числі у вигляді втраченого прибутку (наприклад, якщо буде втрачено важливого клієнта або зірветься угода).

Веб-ресурси стали невід'ємною частиною сучасного світу, відкриваючи безліч можливостей для комунікації, обміну інформацією та здійснення різноманітних операцій. Однак, разом зі зростанням ролі веб-технологій у нашому житті з'являються нові виклики і загрози, пов'язані з інформаційною безпекою веб-ресурсів [1].

Забезпечення безпеки веб-ресурсів є однією з найбільш актуальних та важливих проблем у сучасному цифровому світі. З поширенням Інтернету та зростанням кількості веб-додатків і онлайн-сервісів з'являються нові загрози для інформаційної безпеки.

Ідентифікація загроз інформаційній безпеці веб-ресурсів та оцінка ризиків стали невід'ємною частиною стратегічного планування та управління безпекою в організаціях. Цей процес дозволяє виявити потенційні загрози, визначити вразливості та оцінити ризики, пов'язані з використанням веб-ресурсів.

Ідентифікація загроз полягає у визначенні потенційних небезпек, які можуть призвести до порушення конфіденційності, цілісності та доступності інформації на веб-ресурсах. Це можуть бути хакерські атаки, витоки даних, зловживання прав доступу, соціальний інжиніринг та інші загрози, які можуть негативно вплинути на діяльність організації та спричинити значні втрати [2].

Захист веб-ресурсів є надзвичайно важливою задачею в сучасному інтернет-середовищі. З ростом кількості веб-додатків та залежності суспільства від онлайн-сервісів, зловмисники стають все більш витонченими і винахідливими у своїх атаках. Веб-ресурси стають об'єктом постійних загроз і атак, таких як SQL-ін'єкції, кросс-сайтові скрипти, витік інформації, злам паролів та багато інших.

Для забезпечення надійної захисту веб-ресурсів необхідно провести оцінку їхньої захищеності. Цей процес включає в себе аналіз потенційних загроз і вразливостей, виявлення слабких місць у системі та розробку ефективних заходів безпеки. Оцінка захищеності веб-ресурсів є комплексним завданням, яке вимагає знань з різних областей, таких як безпека програмного забезпечення, мережева безпека, захист даних та інші.

Оцінка ризиків дозволяє визначити й ієрархію загроз та розмірковувати над визначенням стратегій захисту та прийняття відповідних заходів безпеки. Цей процес включає аналіз наслідків можливих загроз, імовірності їх виникнення та важливості для організації. Результатом оцінки ризиків є визначення пріоритетів у впровадженні заходів безпеки, що дозволяє ефективно використовувати ресурси та забезпечити найвищий рівень захищеності веб-ресурсів.

У даній роботі **метою** є дослідження загроз та вразливостей інформаційній безпеці веб-ресурсів та визначення рівня захищеності веб-сайтів шляхом експлуатації вразливостей.

Тому у дослідження передбачається детальний аналіз потенційних загроз, визначення вразливостей веб-додатків та систем, а також встановлення механізмів захисту, які дозволять зменшити ризики та забезпечити безпеку веб-ресурсів організації.

Для вирішення поставленої мети були сформовані наступні завдання:

1. розглянути питання захисту веб-ресурсів: основних принципів безпеки веб-додатків, загальних загроз та вразливостей;
2. проаналізувати актуальні загрози, з якими стикаються веб-ресурси, та охарактеризувати методи виявлення вразливостей, які можуть бути експлуатовані зловмисниками;
3. дослідити типи атак на веб-ресурси та їх наслідки;
4. провести практичне дослідження методів експлуатація вразливостей для оцінки рівня захищеності веб-ресурсів.

Об’єктом дослідження є безпека веб-сайту та його вразливості.

РОЗДІЛ 1.
ОГЛЯД ПИТАННЯ ЗАХИСТУ ВЕБ-РЕСУРСІВ

1.1 Актуальний стан захисту інформації у мережі

Сьогодні Інтернет – це основа роботи багатьох компаній, спосіб миттєво обмінюватися інформацією, вести переговори, купувати. Практично кожна людина щодня використовує мережу в особистих цілях або для роботи, залишає в ній свій слід і надсилає інформацію, яку хотів би залишити конфіденційною.

Захист інформації в Інтернеті – це один із основних турбот більшості підприємств. Адже дотриматися балансу між застосуванням ефективних методів та зручністю співробітником при роботі не завжди просто. Однак система необхідна, щоб уникнути фінансових та репутаційних втрат [3].

Заздалегідь точно передбачити, як постраждає конкретний користувач або ціла організація, яка не звернула належну увагу на систему захисту інформації в Інтернеті, практично неможливо. Існують сотні різних варіантів скоєння злочинів, в основі яких найчастіше лежить комбінація із незаконних дій.

Найбільш поширеними ризиками вважаються [3]:

- отримання доступу до закритої інформації без будь-яких санкцій;
- крадіжка важливих даних компанії чи конкретної людини (рис. 1.1);
- підміна або внесення змін до інформації під час її передачі або під час утримання у сховищі;
- видалення важливих даних як злого наміру;
- розголошення незаконно одержаних даних;
- шифрування інформації з метою подальшого шантажу та здирництва.

Оскільки витоки даних стають все більш поширеними у нашому взаємопов’язаному світі, наше розуміння сучасних кібератак повинно стати все більш поширеним.

Можна зазначити частини з останніх кіберінциденти, що відбулися у 2020-22 роках:

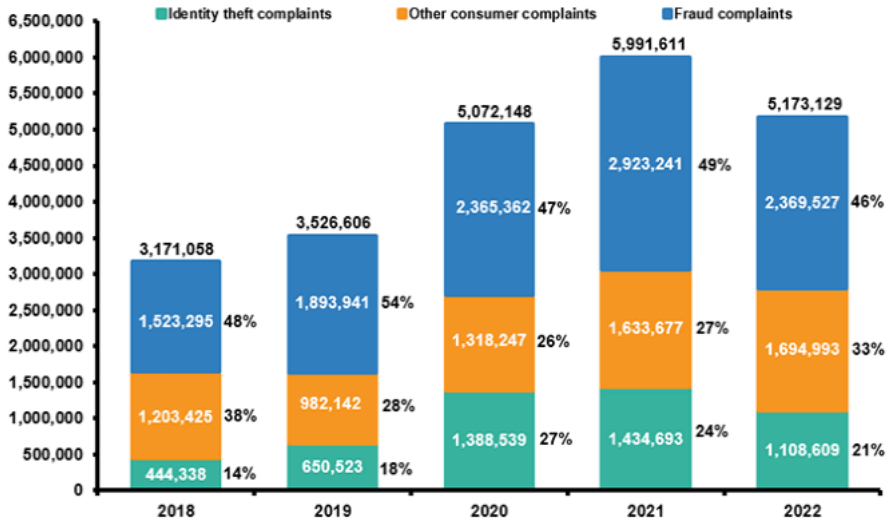

Рисунок 1.1 – Звіти про крадіжки особистих даних і шахрайство, 2018-2022

2022 – ботнет ZLoader, відповідальний за розповсюдження шкідливого програмного забезпечення ZLoader, було ліквідовано спільними зусиллями з Microsoft, ESET, Black Lotus Labs, Palo Alto Networks, HealthISAC і Financial Services-ISAC.

2021 рік – Kaseya зазнала атаки програм-вимагачів , яка підірвала до 1500 компаній із приголомшливою сумою викупу в 70 мільйонів доларів.

2021 – Saudi Aramco зазнала витоку даних, розкривши конфіденційні дані про співробітників і технічні характеристики організації. Група загроз ZeroX вимагає виплати 50 мільйонів доларів.

2021 рік – Порушення даних програми передачі файлів (FTA) Accellion вплинуло на понад 100 компаній, організацій, університетів і державних установ у всьому світі.

2021 – Pulse Secure VPN zero-day було використано, що призвело до злому кількох нерозкритих оборонних фірм і державних організацій у Сполучених Штатах і Європі.

2020 – Universal Health Services повідомляє про інцидент безпеки інформаційних технологій. Зловмисне програмне забезпечення, зокрема програмне забезпечення-вимагач Ryuk, націлене на 400 лікарень у США та

Великобританії. У UHS працює понад 90 000 співробітників, які щороку надають медичні послуги приблизно 3,5 мільйонам пацієнтів.

2020 рік – Університетська лікарня Дюссельдорфа заражена програмою-вимагачем, що призвело до першої смерті після атаки програми-вимагача.

2020 рік – компанія MGM Resorts зазнала масштабного витоку даних, що призвело до витоку 142 мільйонів особистих даних гостей готелю.

2020 – 500 000 викрадених паролів Zoom доступні для продажу на кримінальних форумах темної мережі.

2020 – Magellan Health постраждала від атаки програм-вимагачів і витоку даних, згідно з якими 365 000 пацієнтів постраждали від складної кібератаки.

2020 рік – добре скоординоване шахрайство, яке зловмисне у Twitter, змусило зловмисників виманити 121 000 доларів у біткойнах за допомогою майже 300 транзакцій.

Це перелік є дуже великим, тому що діяльність компаній та організаці перейшла у площину цифровізації, а злодії та шахраї постійно шукають джерела здирництва та фінансового зиску [4].

За останні 10 років зросла кількість атак нульового дня (рис. 1.2)

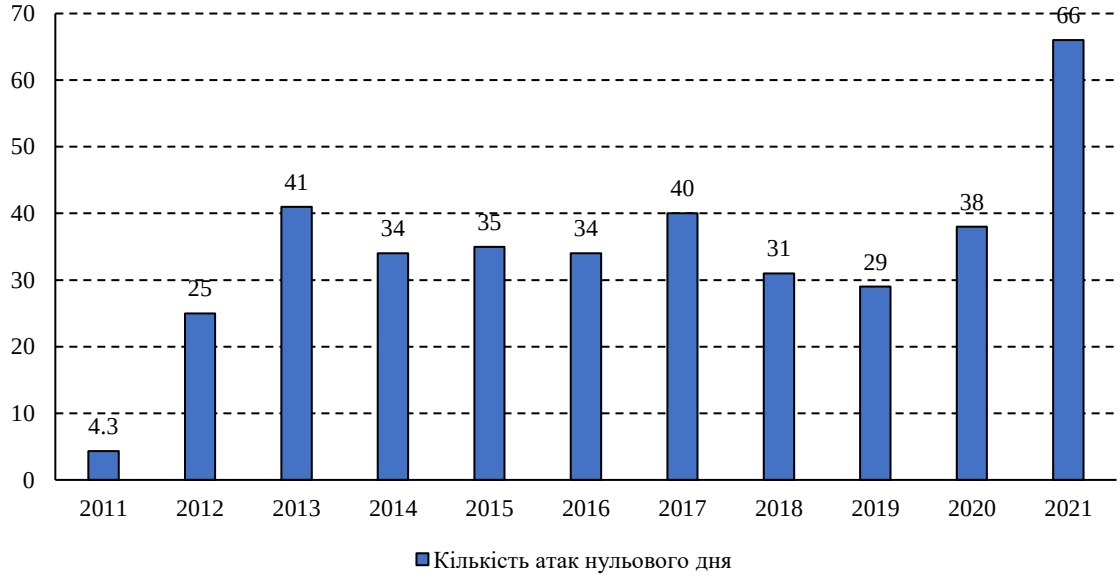

Рисунок 1.2 – Динаміка кількості атак нульового дня за 2011-2021 рр.

Зловмисне програмне забезпечення нульового дня зросло до 67,2% у третьому кварталі 2021 року, що на 3% більше, ніж у попередньому кварталі.

користувача, пароль та набір одноразових паролів для проведення транзакцій), вихідний код деяких файлів або функцій тощо.

Принцип "білої скриньки" (white-box). Цей принцип має на увазі передачу виконавцю всього додатка з його подальшим розгортанням на майданчику консультанта, який виконує роботу з його аналізу, або організацію аналогічної копії додатку у власній інформаційній системі з наданням виконавцю повного доступу до цього ресурсу. У цьому випадку є можливість відстежити, яким чином додаток реагує на будь-який запит. Це найбільш продуктивний метод проведення аналізу захищеності Web-додатків, що дозволяє виявити найбільшу кількість вразливостей. Однак варто зауважити, що цей метод позбавлений можливості поглянути на додаток з позиції атакуючого.

Висновок до розділу 1

Актуальний стан захисту інформації у мережі є надзвичайно важливою темою у сучасному цифровому світі. Інтернет став неодмінною складовою нашого повсякденного життя, але разом з його перевагами постають і ризики, пов'язані з безпекою і конфіденційністю інформації.

Поняття інформаційної безпеки охоплює комплекс заходів і політик, спрямованих на захист інформації від незаконного доступу, втрати, зміни або розголошення. Це включає захист конфіденційності, цілісності та доступності інформації.

РОЗДІЛ 2.
ДОСЛІДЖЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ВЕБ-РЕСУРСІВ: ЗАГРОЗИ, ВРАЗЛИВОСТІ, АТАКИ

2.1 Аналіз вразливостей та загроз безпеки веб-застосунків

Приблизно 95% веб-сайтів працюють на JavaScript і HTML5 — мовах, які можна легко перехопити, переглянути та зламати. Це робить веб-додатки та API вразливими для атак на стороні клієнта, особливо якщо покладатися лише на традиційні інструменти безпеки периметра, такі як WAF. За даними Symantec, понад 4800 веб-сайтів щомісяця скомпрометовані через formjacking. Атаки вилучення даних на стороні клієнта є лише одним із векторів загроз, з якими стикаються веб-додатки, тому багаторівневий підхід до безпеки є настільки важливим.

Топ-10 OWASP — це стандартний документ для розробників і безпеки веб-додатків. Він представляє широкий консенсус щодо найбільш критичних ризиків для безпеки веб-додатків [26].

OWASP Foundation працює над підвищенням безпеки програмного забезпечення за допомогою своїх проектів програмного забезпечення з відкритим кодом під керівництвом спільноти, сотень відділень по всьому світу, десятків тисяч членів і проведення локальних і глобальних конференцій.

Є три нові категорії, чотири категорії зі змінами в назві та охопленні, а також деяка консолідація в Топ-10 на 2021 рік (рис. 2.1).

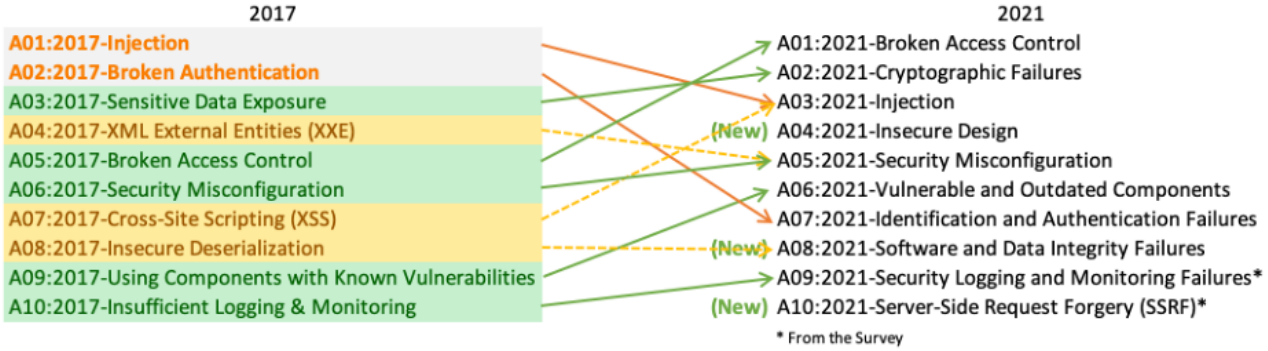

Рисунок 2.1 – Топ-10 OWASP найпоширеніших загроз та ризиків

Наступний варіант, самий класичний, - LOIC HTTP. А тут взагалі нема чого ловити. Принцип у нього простий: GET '/' так швидко, як ми тільки зможемо, та ще й заголовки невалидность. З точки зору захисту, такі запити до вашого бекенд доходити в принципі не повинні, якщо ваше додаток правильно побудовано.

Ось ще такий цікавий інструментарій Anonymous - OWASP / SLOWPOST. Відкриваємо з'єднання і шолом дані з затримкою так довго, як тільки можна, щоб зайняти ресурси Воркер на стороні сервера. Атака стара - нічого нового тут немає.

Є ще відносно новий інструментарій HOIC (High Orbit Ion Cannon) с кумедними апгрейдами. Атаки в цьому інструменті можна скріптовать, можна додавати список юзер-агентів і реферерів, які буде проставляти гармата, щоб збити захищає сторону з пантелику і не дати побудувати стратегію по паттернам. Користувачеві навіть пропонується зробити список URL, які потім гармата вибере випадковим чином. Втім, відбитися все одно не так складно.

На щастя, зловмисників, які використовують LOIC, досить легко виявити; його не можна використовувати через проксі-сервер, тому IP-адреси зловмисників видно цілі. Багато країн вжили законних заходів проти зловмисників, що використовують LOIC, включаючи США, Великобританію, Іспанію та Туреччину.

Висновок до розділу 2

Важливо провести детальний аналіз останніх атак, що відбулися на веб-ресурси. Це допоможе зрозуміти оновлені методики та загрози, з якими стикаються веб-додатки. Наприклад, атаки на вразливості, такі як XSS (Cross-Site Scripting), SQL injection, CSRF (Cross-Site Request Forgery), можуть бути особливо поширеними і вимагають уваги при аналізі веб-застосунків.

Для ефективного виявлення вразливостей веб-додатків, варто дослідити різноманітні існуючі продукти та інструменти для сканування та аналізу безпеки. Наприклад, OWASP ZAP (Open Web Application Security Project Zed

Attack Proxy), Burp Suite, Nessus, Acunetix тощо. Важливо вибрати той, який відповідає потребам вашої організації і надає найкращі результати при аналізі вразливостей.

Під час аналізу вразливостей веб-застосунків, важливо дотримуватись встановленої методології, такої як OWASP Testing Guide або PTES (Penetration Testing Execution Standard). Вони надають рамки та керівництво для виконання збалансованого та систематичного аналізу, що допомагає забезпечити повноту та точність оцінки безпеки.

Безпека веб-додатків є постійним процесом, і важливо постійно оновлювати знання та навички в області аналізу вразливостей. Також потрібно забезпечувати регулярну підтримку та оновлення веб-додатків, включаючи усунення виявлених вразливостей та застосування патчів безпеки.

РОЗДІЛ 3.
АРХІТЕКТУРА ВЕБ-ДОДАТКІВ ТА МІСЦЕ БЕЗПЕКИ В НІЙ

3.1 Огляд архітектури веб-додатків та алгорит захисту

Архітектура веб-програми представляє макет із усіма компонентами програмного забезпечення (такими як бази даних , програми та проміжне програмне забезпечення) і те, як вони взаємодіють один з одним. Він визначає, як дані доставляються через HTTP, і гарантує, що сервер на стороні клієнта та внутрішній сервер можуть їх зрозуміти. Крім того, він також забезпечує наявність дійсних даних у всіх запитах користувачів. Він створює та керує записами, забезпечуючи доступ і автентифікацію на основі дозволів. Вибір правильного дизайну визначає зростання вашої компанії, надійність і сумісність, а також майбутні IT-потреби. Таким чином, важливо розуміти компоненти, що складають архітектуру веб-програм.

Архітектура веб-програми описує макет усіх компонентів веб-програми, а також висвітлює взаємодію між різними компонентами програми, системами проміжного програмного забезпечення сторонніх виробників, веб-службами та базами даних. Це забезпечує моментальний знімок взаємодії між кількома додатками, які одночасно працюють разом, щоб надавати послуги кінцевим користувачам (рисю 3.1).

Зазвичай архітектура веб-додатків складається з 3 основних компонентів:

1) Веб-браузер: браузер або компонент на стороні клієнта або компонент інтерфейсу є ключовим компонентом, який взаємодіє з користувачем, отримує вхідні дані та керує логікою презентації, одночасно контролюючи взаємодію користувача з програмою. За потреби також перевіряються введені користувачем дані.

2) Веб-сервер: веб-сервер, також відомий як серверний компонент або серверний компонент, керує бізнес-логікою та обробляє запити користувачів, направляючи запити до потрібного компонента та керуючи всіма операціями

Висновок до розділу 3

Архітектура веб-додатків є ключовим елементом у забезпеченні ефективної та безпечної роботи веб-ресурсів. Дослідження архітектури та місця захисту в ній, а також алгоритмів захисту дозволяє зрозуміти, яким чином веб-додатки будуються та як можна забезпечити їхню безпеку.

Вивчення архітектури веб-додатків дозволяє ознайомитись зі структурою та компонентами системи. Розуміння рівнів сучасної архітектури, таких як клієнтський рівень, серверний рівень та рівень бази даних, допомагає визначити місця потенційних загроз та вразливостей.

Вивчення алгоритмів захисту дозволяє розробити систему захисту інформації веб-ресурсу. Це можуть бути заходи безпеки на рівні мережі, застосунків, бази даних, шифрування даних, контроль доступу, моніторинг та логування подій тощо. Важливо підібрати відповідні алгоритми захисту, які враховують специфіку веб-додатку та потенційні загрози.

Враховуючи виявлені вразливості та загрози, можна розробити алгоритм для системи захисту інформації веб-ресурсу. Це включає в себе використання різних технологій та інструментів, реалізацію контрмірних заходів, валідацію вхідних даних, впровадження захисту від вразливостей, контроль доступу та моніторинг безпеки.

РОЗДІЛ 4.
ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ВЕБ-САЙТІВ ЗА ДОПОМОГОЮ ЕКСПЛУАТАЦІЇ ВРАЗЛИВОСТЕЙ

4.1 Загальні етапи оцінки захищеності веб-ресурсів

Забезпечення безпеки веб-додатків є важливим завданням в сучасному інформаційному середовищі. Однією з найбільш поширених загроз для безпеки веб-додатків є SQL-ін'єкції. Ці атаки полягають у використанні шкідливого SQL-коду для отримання несанкціонованого доступу до бази даних веб-додатка.

Розглянемо етапи оцінки захищеності веб-ресурсів від SQL-ін'єкцій.

Аналіз додатку .Перший етап оцінки захищеності веб-ресурсів від SQL-ін'єкцій - це аналіз самого додатку. Необхідно визначити, як додаток взаємодіє з базою даних та які SQL-запити використовуються. Аналізуючи додаток, можна виявити потенційні вразливості, які можуть бути використані для впровадження SQL-ін'єкцій.

Валідація та фільтрація вхідних даних. Другий етап оцінки захищеності полягає у валідації та фільтрації вхідних даних, що передаються до бази даних. Важливо перевірити, чи введені дані відповідають очікуваним форматам і чи не містять вони шкідливого коду. Це можна зробити шляхом використання параметризованих запитів та попередньої валідації даних на стороні сервера. Такі заходи допоможуть запобігти виконанню шкідливого SQL-коду, переданого через вхідні дані.

Використання підготовлених запитів. Третій етап оцінки захищеності веб-ресурсів - використання підготовлених запитів. Підготовлені запити дозволяють відокремити SQL-код від вхідних даних та передавати його окремо, що ускладнює впровадження SQL-ін'єкцій. Цей підхід дозволяє використовувати параметри для передачі даних, замість включення їх безпосередньо в SQL-запити.

Захист від потенційних вразливостей. Останній етап оцінки полягає у застосуванні заходів для запобігання потенційним вразливостям, пов'язаним з SQL-ін'єкціями. Це може включати встановлення відповідних політик безпеки, застосування оновлень програмного забезпечення, регулярну перевірку на наявність вразливостей та моніторинг активності веб-додатків [37].

Оцінка захищеності веб-ресурсів від SQL-ін'єкцій є важливим етапом у забезпеченні безпеки веб-додатків. Аналіз додатку, валідація та фільтрація вхідних даних, використання підготовлених запитів та захист від потенційних вразливостей допомагають запобігти SQL-ін'єкціям та забезпечити безпеку бази даних. Важливо постійно оновлювати та перевіряти безпеку веб-додатків, оскільки загрози постійно змінюються, а заходи захисту повинні відповідати сучасним стандартам та найкращим практикам [38].

При перевірці захищеності веб-сайти можна виконати кроки, які наведені на рис. 4.1.

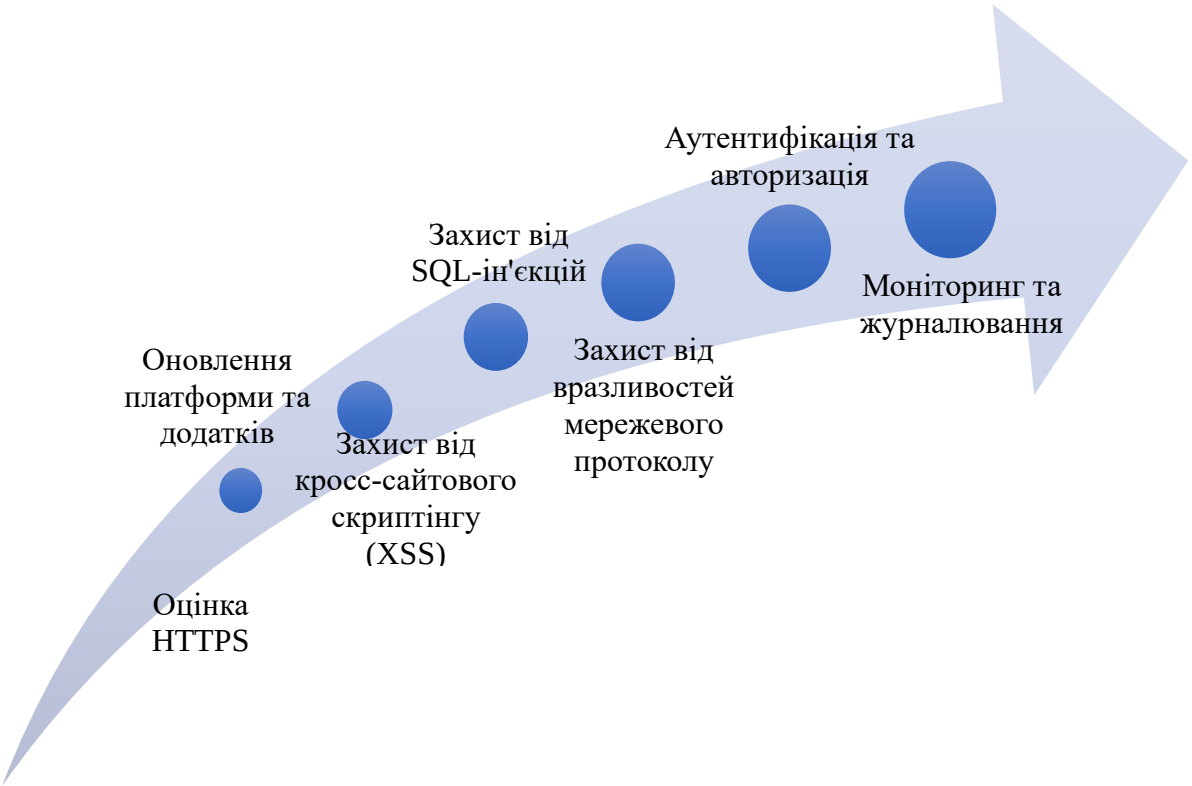

Рисунок 4.1 – Етапи перевірки захищеності веб-ресурсів

Для аналізу на початковому етапі необхідно перевірити, чи використовується протокол HTTPS для захищеної передачі даних між

15. Розробники веб-додатків повинні мати належний рівень знань у галузі інформаційної безпеки та безпечної розробки коду.
16. Необхідно використовувати захист веб-додатків (WAF).
17. Адміністратори сайту повинні переконатися, що веб-сервер правильно налаштований.

Загальні рекомендації щодо усунення вразливостей веб-сайтів можуть служити як основа для забезпечення безпеки вашого веб-проекту. Проте, слід пам'ятати, що безпека - постійний процес, і необхідно вдосконалювати свої знання та практики безпеки для ефективного захисту веб-сайту.

Висновки до розділу 4

У результаті проведеного дослідження захищеності веб-сайтів за допомогою експлуатації різних вразливостей, були розглянуті різноманітні аспекти безпеки, що стосуються цих ресурсів.

Визначено загальні етапи оцінки захищеності веб-ресурсів, які включають розвідку, аналіз вразливостей, експлуатацію та документування результатів.

Розглянуті конкретні вразливості, такі як Union SQL Injection, Blind SQL-ін'єкція та LFI. Для кожної з цих вразливостей було розкрито принцип роботи, потенційні наслідки та методи експлуатації.

Сформовано та визначено загальні рекомендації щодо усунення вразливостей веб-сайтів. Ці рекомендації включають встановлення оновлень програмного забезпечення, використання сильних паролів, перевірку даних вводу, застосування принципу найменшого доступу, захист веб-сервера та регулярні аудити безпеки.

ВИСНОВКИ

Актуальний стан захисту інформації у мережі є надзвичайно важливою темою у сучасному цифровому світі. Інтернет став неодмінною складовою нашого повсякденного життя, але разом з його перевагами постають і ризики, пов'язані з безпекою і конфіденційністю інформації.

Поняття інформаційної безпеки охоплює комплекс заходів і політик, спрямованих на захист інформації від незаконного доступу, втрати, зміни або розголошення. Це включає захист конфіденційності, цілісності та доступності інформації.

Інструменти та методи захисту інформації включають в себе широкий спектр технологій, процесів та практик. До них належать шифрування даних, автентифікація та авторизація, мережеві файерволи, системи виявлення і запобігання вторгненням (IDS/IPS), віртуальні приватні мережі (VPN), резервне копіювання та відновлення даних, системи моніторингу та аналізу безпеки, аудит безпеки, навчання та свідомість користувачів та багато іншого.

При впровадженні заходів захисту інформації важливо розробляти комплексний план, враховуючи специфічні потреби та загрози кожного веб-ресурсу чи організації. Крім технічних заходів, також важливо розробляти політики безпеки, навчати персонал з питань інформаційної безпеки та впроваджувати механізми постійного оновлення та оцінки ефективності заходів.

Забезпечення захисту інформації є постійним процесом, оскільки загрози і технології постійно змінюються. Тільки шляхом постійного оновлення, аналізу і вдосконалення заходів захисту можна забезпечити ефективний рівень безпеки в мережі.

Архітектура веб-додатків є ключовим елементом у забезпеченні ефективної та безпечної роботи веб-ресурсів. Дослідження архітектури та місця захисту в ній, а також алгоритмів захисту дозволяє зрозуміти, яким чином веб-додатки будуються та як можна забезпечити їхню безпеку.

Вивчення архітектури веб-додатків дозволяє ознайомитись зі структурою та компонентами системи. Розуміння рівнів сучасної архітектури, таких як клієнтський рівень, серверний рівень та рівень бази даних, допомагає визначити місця потенційних загроз та вразливостей.

Під час дослідження вразливостей веб-сайтів було проведено тестування на проникнення та оцінку безпеки веб-сайтів. Тестування проводилося вручну і автоматично. Методологія тестування чорного ящика. Ця методика дозволяла тестувати веб-сайти з боку зловмисника. Під час тестування були використані наступні інструменти:

- Burp Suite Pro;
- Dirb;
- Gobuster;
- Google Dorks;
- SQLMap.

Були виявлені критичні вразливості, такі як:

- SQL-ін'єкція;
- LFI- ін'єкція;
- розкриття інформації.

Ці вразливості дозволили отримати конфіденційну інформацію. Всі вразливості були класифіковані відповідно до OWASP.

Наведено загальні рекомендації щодо усунення вразливостей. Всі знайдені вразливості були знайдені на різних платформах, це PHP і ASP.NET. Досліджувані ділянки мали різну структуру і технологію розробки, що дозволило комплексно розглянути аспект реалізації безпеки сайту.

Загальні рекомендації щодо усунення вразливостей веб-сайтів можуть служити важливим керівництвом для підвищення рівня безпеки веб-проектів. Проте, важливо пам'ятати, що безпека - постійний процес, і необхідно вдосконалювати свої знання та практики безпеки для ефективного захисту веб-сайтів і попередження можливих загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Defining Incident Management Processes for CSIRTs: A Work in Progress // CMU/SEI-2004-TR-015: ESC-TR-2004-015 Chris Alberts, Audrey Dorofee, Georgia Killcrece October 2004 Networked Systems Survivability Program.

2. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2011. – Вип. 2 (92). – С.53-56.

3. Bhavani A.B. Cross-site Scripting Attacks on Android WebView / A.B. Bhavani // International Journal of Computer Science and Network. — 2013. — Vol. 2, Issue 2. — 5 p. – Режим доступу: http://ijcsn.org/IJCSN-2013/2- 2/IJCSN-2013-2-2-03.pdf

4. Скакун, Р. Г. Дослідження методів забезпечення безпеки інформаційних систем від фішингових атак. 2019.

5. Грайворонський М. В. Сучасні підходи до забезпечення кібернетичної безпеки / Матеріали XVII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених “Теоретичні і прикладні проблеми фізики, математики та інформатики”, НТУУ “КПІ”, 2015 р. — С. 10–17.

6. Нечволод К.В. Аналіз безпеки даних в ЕММ системах / К.В. Нечволод, О.В. Сєвєрінов, А.В. Власов // Системи управління, навігації та зв’язку. – Полтава: ПНТУ. - 2019. – Вип. 3(55). – С. 131-134

7. The WASC Threat Classification v2.0 / The Web Application Security Consortium. [Електронний ресурс] – Режим доступу: http://projects.webappsec.org/w/page/13246978/Threat%20 Classification.

8. Chen, Jinyin, et al. DGEPN-GCEN2V: a new framework for mining GGI and its application in biomarker detection. Science China Information Sciences, 2019, 62: 1-3.

9. Nordbotten, Nils Agne. XML and web services security standards. IEEE Communications Surveys & Tutorials, 2009, 11.3: 4-21.

10. Mouli, Varsha R.; Jevitha, K. P. Web services attacks and security-a systematic literature review. Procedia Computer Science, 2016, 93: 870-877.

B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D0%B8-c-%D0%BF%D0%BE%D0%BC%D0%BE%D1%89%D1%8C%D1%8E-owasp-zap- a99183c32013

30. Riadi, Imam; Umar, Rusydi; Sukarno, Wasito. Vulnerability of injection attacks against the application security of framework based bebsites open web access security project (OWASP). J. Inform, 2018, 12.2: 53-57.

31. Idris, Muhammad; Syarif, Iwan; Winarno, Idris. Development of vulnerable web application based on owasp api security risks. In: 2021 International Electronics Symposium (IES). IEEE, 2021. p. 190-194.

32. Fröschl, Agnes. Semantic approaches to detect file system log events for analyzing data exfiltration. 2020. PhD Thesis. Wien.

33. Touseef, Pariwish, et al. Analysis of automated web application security vulnerabilities testing. In: Proceedings of the 3rd international conference on future networks and distributed systems. 2019. p. 1-8.

34. Sagar, Deepika, et al. Studying open source vulnerability scanners for vulnerabilities in web applications. IIOAB JOURNAL, 2018, 9.2: 43-49.

35. Zunnurhain, Kazi; Patel, Ankur J.; James, Mairura. Investigation of Vulnerabilities with Monitoring Tools. In: Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2018. p. 71-78.

36. Idris, Muhammad; SYARIF, Iwan; Winarno, Idris. Development of vulnerable web application based on owasp api security risks. In: 2021 International Electronics Symposium (IES). IEEE, 2021. p. 190-194.

37. Alghawazi, Maha; Alghazzawi, Daniyal; Alarifi, Suaad. Detection of sql injection attack using machine learning techniques: a systematic literature review. Journal of Cybersecurity and Privacy, 2022, 2.4: 764-777.

38. Tang, Peng, et al. Detection of SQL injection based on artificial neural network. Knowledge-Based Systems, 2020, 190: 105528.