

Державна служба України з надзвичайних ситуацій  
Львівський державний університет безпеки життєдіяльності  
Навчально-науковий інститут цивільного захисту  
Кафедра управління інформаційною безпекою

“Допущено до захисту”

Начальник кафедри управління  
інформаційною безпекою, д.т.н., доцент  
полковник служби цивільного захисту

Ростислав ТКАЧУК

“ \_\_\_\_\_ ” \_\_\_\_\_ 2022 року

**БАКАЛАВРСЬКА  
КВАЛІФІКАЦІЙНА РОБОТА**

на тему : **Аналіз загроз та розробка концепції захисту Web-додатків  
вивчення іноземної мови**

Виконав:

здобувач IV курсу, групи КБ-41  
спеціальності (освітньої-професійної програми)  
125 “Кібербезпека”

(Управління інформаційною безпекою)

(шифр і назва спеціальності (освітньої-професійної програми))

Тарас Шибунька

(ім'я та прізвище)

Керівник Марія Навитка

(ім'я та прізвище)

Рецензент \_\_\_\_\_

(ім'я та прізвище)

Львів – 2022 року

## АНОТАЦІЯ

Шибунька Тарас. «Аналіз загроз та розробка концепції захисту Web-додатків вивчення іноземної мови». Бакалаврська кваліфікаційна робота зі спеціальності 125 «Кібербезпека» складається з текстової (пояснювальної) частини, що містить 4 розділи, 59 сторінок. А також – графіка (презентація), що містить 11 слайдів.

Об'єкт дослідження – Web-додатки з вивченням іноземної мови.

Предмет дослідження – механізм безпеки Django та перевіряли за допомогою OWASP ZAP.

Мета – на прикладі створення веб-додатку для вивчення англійської мови представити концепції захисту Web-додатків. Веб-додаток реалізувати за допомогою Django. Розробити програму безпеки, використовуючи модель безпечної розробки whitelist та протестували все за допомогою OWASP ZAP.

Бакалаврська кваліфікаційна робота спрямована на розробку безпечних Web-додатків з вивченням іноземної мови.

Загальний обсяг роботи: 59 сторінок. Ключові слова: веб-додаток, іноземна мова, англійська мова, інформаційні технології, база даних, програмний продукт.

## **ABSTRACT**

Shibunka Taras. "Threat analysis and development of the concept of protection of Web-applications for learning a foreign language." The final work on the specialty 125 "Cybersecurity" consists of a text (explanatory) part containing 4 sections, 59 pages. And also - graphics (presentation) containing 11 slides.

Object of research - Web-applications with learning a foreign language.

The subject of the study was the Django security mechanism and was tested using OWASP ZAP.

Aim - The aim of this work is to create a web application for convenient and productive learning of English in higher education. The web application is implemented using Django. Developed a security program using the secure development model whitelist and tested everything with OWASP ZAP.

Bachelor's qualification work is aimed at developing secure Web-applications with foreign language learning.

Total volume of work: 59 pages. Keywords: web application, English language, information technologies, database, software product.

## ЗМІСТ

ВСТУП .....	6
1. АНАЛІЗ ПРОБЛЕМ ВИВЧЕННЯ ІНОЗЕМНОЇ МОВИ.....	9
1.1 Загальні відомості.....	9
1.2 Роль англійської мови у сучасному світі.....	10
1.3 Роль англійської мови у житті програміста.....	11
1.4 Способи вивчення англійської мови.....	12
1.5 Моделі додатків для вивчення англійської мови.....	14
1.6 Основні проблеми веб-додатків.....	15
2. ОСОБЛИВОСТІ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБ-РЕСУРСІВ.....	17
2.1 Аналіз вразливостей та загроз безпеки веб-ресурсів.....	17
2.2 Огляд існуючих методик тестування безпеки веб-ресурсів.....	22
2.3 Постановка задачі.....	26
3. ХАРАКТЕРИСТИКА ЕКСПЕРТНИХ СИСТЕМ ДЛЯ РОЗВ'ЯЗУВАННЯ ЗАДАЧ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	27
3.1 Основні компоненти експертної системи.....	27
3.2 Алгоритми функціонування експертної системи .....	31
4. Розробка і перевірка веб-застосунку з використанням моделі білого списку.....	37
4.1 Обґрунтування вибору веб-фреймворку і його можливості.....	37
4.2 Основні механізми безпеки Django.....	39
4.3 Процес розробки веб-додатку використовуючи модель безпечної розробки whitelist.....	41
4.4 Використані методи забезпечення відповідності до моделі.....	47
4.5 Використаний інструмент для перевірки.....	50
4.6 Тестування за допомогою OWASP ZAP.....	53
4.7 Результати тестування.....	55
ВИСНОВКИ.....	58
СПИСОК ЛІТЕРАТУРИ.....	57
ДОДАТКИ.....	58

## ВИСНОВКИ

Дана робота присвячена виявленню вразливостей в додатках, що виникли через недоліки забезпечення безпеки. Рішення даної проблеми можливо з тестуванням безпеки web-дodatка за допомогою методології OWASP testing guide. Чим складніше сайт, тим більше часу потрібно на його перевірку і налагодження. На жаль, існує безліч прикладів, коли розробники і замовники втрачають етап тестування сайту, що практично завжди призводить до великих фінансових і тимчасових витрат в подальшому, невдоволення користувачів ресурсу і в результаті, необхідність доопрацювання (або навіть повторної розробки) ресурсу. Хоч провівши повний цикл тестування безпеки, не можна бути на 100% впевненим, що система по-справжньому безпечна. Але можна бути впевненим в тому, що відсоток несанкціонованих проникнень, крадіжок інформації і втрат даних буде в рази менше, ніж у тих, хто не проводить тестування безпеки.

В результаті роботи над кваліфікаційною бакалаврською роботою одержано наступні результати:

1. Описана концепція методики розробки безпечних веб-застосунків з використанням загальної моделі білого списку.
2. Розроблено прототип веб-застосуноку з використанням методики розробки та описаній в даній роботі, Також подано способи, за допомогою яких реалізовувано відповідність поведінки веб-застосунку до моделі білого списку.
3. У кваліфікаційній бакалаврській роботі отримано в цілому задовільний результат застосування розробленої методики.

## СПИСОК ЛІТЕРАТУРИ

1. Балацька В.С., Ящук В.І., Полотай О.І. Вразливість комп'ютерної мережі як проблема закладів вищої освіти. Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи: збірник тез доповідей VI Міжнародній науково-практичній конференції (м. Київ - м. Львів, 4-5 листопада 2021 р.). Львів: ЛДУ БЖД, 2021. С. 66–68.

2. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю. Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

3. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю. Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

4. Кленик О., Ткачук Р. Особливості побудови захищеної мережі підприємства. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 52–54.

5. Колядич І., Ткачук Р. Системи автоматичного керування програмним забезпеченням. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 55–57.

6. Купріков М. Методи тестування системи на проникнення для забезпечення кібернетичної безпеки / Н. Купріков, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80-83).

7. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 84–85.

8. Н.Думич, О.Полотай Особливості захисту Проху-сервера, як один із способів забезпечення безпеки розподілених інформаційних систем. Захист інформації в інформаційно-комунікаційних системах: збірник тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів. – Львів: ЛДУ БЖД, 2017. – С. 18-19.

9. НД ТЗІ 1.1–003–99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу - 1999.

10. Смик Д. Управління інформаційною безпекою ІТ – проєктів з використанням методики DevSecOps / Д.Смик, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.83-86).

11. Шахуб С. М., Ткачук Р. Л. Дослідження методів і засобів при запровадженні концепції BYOD на підприємстві. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 149–150.

12. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

13. Django documentation [Електронний ресурс] // Django Software Foundation. – 2016. – Режим доступу до ресурсу: <https://docs.djangoproject.com/en/2.2/>.

14. Django [електронний ресурс] - <https://uk.wikipedia.org/wiki/Django>

15. Information technology — Vocabulary, 2015. – (ISO/IEC 2382:2015)
16. ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure / 2018
17. O.Polotai, O. Belej, N. Nestor. Developing a local positioning algorithm based on the identification of objects in a wireless Wi-Fi network of the mall. IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.
18. O.Polotai, O. Belej., N. Nestor, S. Panchak Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.
19. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115.
20. Open Source Security Testing Methodology Manual (OSSTMM) : Режим доступа: <https://www.isc2.org/> .
21. OWASP TOP TEN [Электроний ресурс] / Andrew van der Stock, Brian Glas, Neil Smithline, Torsten Gigler - 2017— Режим доступа: <https://owasp.org/www-project-top-ten/>
22. OWASP ZAP [электронный ресурс] - <https://owasp.org/www-project-zap/>
23. WASC Threat Classification. WASC [Электроний ресурс] / Robert Auger - 2012 — Режим доступа: <http://projects.webappsec.org/w/page/13246978/Threat%20Classification>
24. Whitelist [электронный ресурс] - <https://help.eset.com/glossary/uk-UA/whitelist.html>