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
“____” _____2021 року

# ДИПЛОМНА РОБОТА
# БАКАЛАВРА

на тему **Тестування безпеки та дослідження вразливостей інформаційно-аналітичної системи Львівського державного університету безпеки життєдіяльності**

Виконав:
здобувач IVкурсу, групи КБ-41
спеціальності (освітньої програми)
125 «Кібербезпека» (Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої програми))
Странатко Максим
(ім’я та прізвище)

Керівник Ростислав ТКАЧУК
(ім’я та прізвище)

Рецензент Наталя ЛИСА
(ім’я та прізвище)

Львів – 2021 року

# АНОТАЦІЯ

Странатко М. С. “Тестування безпеки та дослідження вразливостей інформаційно-аналітичної системи Львівського державного університету безпеки життєдіяльності”. Дипломна робота за спеціальністю 125 “Кібербезпека” складається з текстової частини, що містить 3 розділи, 50 сторінок, 1 таблицю, 17 рисунків, 30 літературних джерел.

Об’єкт – інформаційно – аналітична система Львівського державного університету безпеки життєдіяльності.

Мета роботи – провести тестування безпеки інформаційно – аналітичної системи Львівського державного університету безпеки життєдіяльності.

У практичній частині проведено тестування на проникнення у систему. Дане тестування враховує переваги існуючих методик тестування на проникнення у світі та містить перелік та опис інструментів для тестування.

У роботі також є аналіз поширених вразливостей у веб серверах, способи захисту від них, та оцінка вразливостей з використанням метрики CVSS.

Практичне значення роботи полягає у зниженні тривалості та обґрунтуванні вибору засобів та інструментів тестування на проникнення.

Результати здійснених у дипломній роботі досліджень можуть бути використані при тестуванні на проникнення веб-серверів.

Наукова новизна дослідження полягає у адаптації методів тестування на проникнення веб – додатків, та тестування лише на наявність вразливостей лише з критичним рівнем ризику.

Ключові слова: тестування на проникнення, веб – сервер, вразливість, методика, атаки, веб – додаток.

# ABSTRACT

Stranatko M. S. "Security testing and research of vulnerabilities of the information-analytical system of Lviv State University of Life Safety". Thesis in the specialty 125 "Cybersecurity" consists of a text part containing 3 sections, 50 pp., 1 tables, 17 pictures, 30 sources.

Object - information - analytical system of Lviv State University of Life Safety.

The purpose of the work is to test the security of the information - analytical system of Lviv State University of Life Safety.

In the practical part, penetration testing was performed. This testing takes into account the advantages of existing methods of testing for penetration into the world and contains a list and description of tools for testing.

There is also an analysis of common vulnerabilities in web servers, ways to protect against them, and vulnerability assessment using CVSS metrics.

The practical significance of the work is to reduce the duration and justify the choice of means and tools for penetration testing.

The results of research conducted in the thesis can be used in testing the penetration of web servers.

The scientific novelty of the research is the adaptation of testing methods for penetration of web applications, and testing only for the presence of vulnerabilities with only a critical level of risk.

Key words: penetration testing, web server, vulnerability, technique, attacks, web application.

# ЗМІСТ

# ЗАГАЛЬНІ ВИСНОВКИ

У дипломній роботі для тестування безпеки та дослідження вразливостей було використано сканери на пошук цих вразливостей, також за допомогою прямих атак на веб – додаток.

Сканери для перевірки та дослідження вразливостей ми обрали: Nmap, OWASP ZaP та W3af.

У першому розділі описано основні принципи функціонування веб – серверів та технологій їх побудування. Визначено що веб-сервери можуть також взаємодіяти з базами даних, якщо вони реалізовані таким чином, щоб отримувати інформацію з баз даних і надавати їх у певному форматі HTML. Враховуючи різноманітність технологій, що використовуються у компонентах веб – сервера, визначено, що виникає необхідність проведення аналізу існуючих мережевих атак на веб-сервер та способів захисту від них. Також розглянуто основні типи мережевих атак та приклади сценаріїв атак.

У другому розділі подано способи захисту веб серверу від атак а саме: від SQL-ін’єкцій, XSS-атак, CSRF – атаки, PHP – ін’єкцій, Brute force - атак, DoS і DDoS атак і захист від мережевої розвідки. Також надано кілька порад, для зменшення ймовірності взлому, чи успішної атаки на сайт і провведено порівняння тестових і продуктивних систем.

У третьому розділі визначено, що тестування необхідно проводити згідно з державними стандартами України і міжнародним стандартам. Проведено збір інформації про систему, завдяки утиліті nmap отримали інформацію які на веб сервері містяться можливі операційні системи. За допомогою сканера вразливостей OWASP ZaP було перевірено на захищеність від XSS-атак і виявлення такої вразливості. За результатами роботи сканеру W3af було виявлено CSRF-вразливість. Також за допомогою прямих атак на веб – сайт було виявлено, що присутня ще HTML-вразливість.

Отримані результати сканувань доцільно використати для покращення роботи просканованого веб-сайту, так як він уже містять опис причин вразлвостей та шляхи боротьби з ними. Усунення знайдених вразливостей неодмінно підвищить рівень безпеки веб – сайту Львівського державного університету безпеки життєдіяльності.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IP-спуфинг [Електронний ресурс]. – Режим доступу: http://um.co.ua/11/11-3/11-30168.html

2. XSS-атаки [Електронний ресурс]. – Режим доступу: http://www.univd.edu.ua/science-issue/issue/3345

3. А.Кичма, О.Полотай Загрози безпеки Wi-Fi мереж та основні протоколи захисту. "Інформаційна безпека та інформаційні технології": Збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів учених, студентів і курсантів. – Львів, 2021. – С. 49-51.

4. Анализ існуючих інформаційних атак на веб-ресурси та методів І засобів захисту від них [Електронний ресурс]. – Режим доступу: http://refua.in.ua/analiz-isnuyuchih-informacijnih-atak-na-veb-resursi-ta-metodiv.html

5. Аналіз сучасних Web-вразливостей [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/pdf/255343.pdf

6. Балацька В.С., Шабатура М.М. Дослідження комп’ютерної мережі сканером вразливості Nessus. Вісник Львівського державного університету безпеки життєдіяльності. 2019. Вип. 20. С. 6-11.

7. Балацька В.С., Шабатура М.М. Сканери вразливості комп’ютерної мережі. Захист інформації в інформаційно-комунікаційних системах: матеріали ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 28 листопада 2019 р. / ЛДУ БЖД. Львів, 2019.С. 34-36

8. Безпека і переповнення буфера [ Електронний ресурс]. – Режим доступу: http://pautina34.ru/p=167/

9. Безпека комп'ютерних мереж [ Електронний ресурс]. – Режим доступу: https://svitppt.com.ua/informatika/bezpeka-kompyuternih-merezh.html

10. Брутфорс [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/web-application-attacks-2018/

11. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і

курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124).

12. Використання інформаційно-комунікаційних технологій у професійній діяльності освітян [Електронний ресурс]. – Режим доступу: https://repository.kristti.com.ua/wp-content/uploads/2017/07/Tkach-Vordpres.pdf

13. Войтович В.С., Гриник Р.О. Необхідність створення комплексної системи захисту інформації. Зб. тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (м. Львів, 24 листопада 2017 р.). Львів: ЛДУ БЖД, 2017. С. 10–11.

14. Електронний журнал «Хакер» //Лучшие инструменты пен-тестера: брутфорс паролей [Електронний ресурс]. – Режим доступу: https://xakep.ru/2009/08/13/49191

15. Захист баз даних [Електронний ресурс]. – Режим доступу: http://ua.waykun.com/articles/zahist-baz-danih-2-stattja-storinka-7.php

16. Класифікація мережевих атак [ Електронний ресурс]. – Режим доступу: https://asyan.org/potre/%D0%9A%D0%BB%D0%B0%D1%81%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F+%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D1%85+%D0%B0%D1%82%D0%B0%D0%BAe/main.html

17. Мережеві атаки, можливості та недоліки мережевих екранів [Електронний ресурс]. –Режим доступу: World Wide Web. – URL: https://ukrbukva.net/page,2,91957-Setevye-ataki-vozmozhnosti-i-nedostatki-setevyhekranov.html

18. Мережеві атаки, можливості та недоліки мережевих екранів [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://ukrbukva.net/page,6,91957-Setevye-ataki-vozmozhnosti-i-nedostatki-setevyhekranov.html

19. Мережеві атаки, можливості та недоліки мережевих екранів[ Електронний ресурс]. – Режим доступу: https://ukrbukva.net/page,5,91957-Setevyeataki-vozmozhnosti-i-nedostatki-setevyh-ekranov.html

20. Об'єкти захисту інформації та технічні канали її витоку [Електронний ресурс]. –Режим доступу: World Wide Web. – URL: https://infopedia.su/1x978f.html

21. Оцінка стійкості роботи комп'ютерної інформаційної системи в умовах дії загрозливих чинників НС [Електронний ресурс]. – Режим доступу: https://studwood.ru/2388680/informatika/otsinka_stiykosti_roboti_kompyuternoyi_inform atsiynoyi_sistemi_umovah_zagrozlivih_chinnikiv

22. Система керування вмістом [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC98%D0%B0_%D0%BA%D0%B5%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B2%D0%BC%D1%96%D1%81%D1%82%D0%BE%D0%BC

23. Типи мережевих атак, їх опису, засоби боротьби [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://moluch.ru/conf/tech/archive/5/1115/

24. Усунення небезпеки XPath-впровадження [Електронний ресурс]. – Режим доступу: http://easy-code.com.ua/2012/09/usunennya-nebezpeki-xpathvprovadzhennya-isxodniki-rizne-programuvannya-statti/

25. Усунення небезпеки XPath-впровадження [Електронний ресурс]. – Режим доступу: http://easy-code.com.ua/2012/09/usunennya-nebezpeki-xpath-vprovadzhennyaisxodniki-rizne-programuvannya-statti/

26. Як захистити веб-додатки: основні поради, інструменти, корисні посилання [Електронний ресурс]. – Режим доступу: https://echo.lviv.ua/dev/6231

27. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

28. 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.

29. 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.

30. 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.