Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Інструменти автоматизованого тестування на проникнення та їх ефективність"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Слупський Богдан Васильович
підпис (прізвище та ініціали)

Керівник Козак Р.О.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Приймак М.В
підпис (прізвище та ініціали)

м. Тернопіль – 2024

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)
«__» _____ 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Слупському Богдану Васильовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Інструменти автоматизованого тестування на проникнення та їх ефективність

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

Затверджені наказом ректора від «20» 11 2024 року № 4/7-1112

2. Термін подання студентом завершеної роботи 16.12.2024

3. Вихідні дані до роботи Автоматизовані інструменти тестування на проникнення та їх ефективність

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ, 1. Теоретичні основи автоматизованого тестування на проникнення, 1.1. Поняття та сутність тестування на проникнення, 1.2. Класифікація методів тестування на проникнення та їх застосування, 1.3. Автоматизація процесу тестування: переваги, обмеження та тенденції розвитку, 1.4. Огляд поширених інструментів автоматизованого тестування на проникнення, 2. Аналіз та порівняння автоматизованих інструментів тестування, 2.1. Критерії вибору інструментів для автоматизованого тестування, 2.2. Аналіз функціональних можливостей та архітектури інструментів, 2.3. Порівняльний аналіз точності та повноти виявлення вразливостей, 2.4. Переваги та недоліки автоматизованих інструментів у практичному застосуванні, 3. Практичне провадження та оцінка ефективності автоматизованих інструментів, 3.1. Вибір цільового середовища та підготовка до тестування, 3.2. Запуск автоматизованих сканерів на обраних цілях та збір результатів, 3.3. Аналіз точності, корисності та практичної цінності виявлених вразливостей, 3.4. Формування рекомендацій для підвищення безпеки та оптимізації вибору інструментів, 4. Охорона праці та безпека в надзвичайних ситуаціях, 4.1 Охорона праці, 4.2 Фактори ризику та можливі порушення

здоров’я користувачів комп’ютерної мережі, Висновок

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
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням кваліфікаційнрї роботи	23.09-25.09	Виконано
2.	Пошук і підбір наукових джерел за темою роботи	26.09-01.10	Виконано
3.	Опрацювання наукових джерел про проблематику	02.10-08.10	Виконано
	ефективності автоматизованих інструментів тестування		
	на проникнення		
4.	Огляд інструментів автоматизованого тестування	09.10-20.10	Виконано
5.	Оформлення розділу «Теоретичні основи	21.10-30.10	Виконано
	автоматизованого тестування на проникнення»		
6.	Розробка алгоритму дослідження	31.10-10.11	Виконано
7.	Налаштування тестових середовищ	11.11-14.11	Виконано
8.	Оформлення розділу «Аналіз та порівняння	15.11-20.11	Виконано
	автоматизованих інструментів тестування»		
9.	Виконня тестувань на тестовому середовище обраними	21.10-01.12	Виконано
	інструментами тестування		
10.	Оформлення розділу «Практичне провадження та оцінка	02.12-11.12	Виконано
	ефективності автоматизованих інструменті»		
11.	Виконання завдання до підрозділу «Охорона праці та	12.12-15.12	Виконано
	безпека в надзвичайних ситуаціях»		
12.	Нормоконтроль		
13.	Перевірка на плагіат		
14	Пеопередній захист кваліфікаційної роботи		
15.	Захист кваліфікаційної роботи		

Студент _____ Слупський Б. В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козак Р. О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Інструменти автоматизованого тестування на проникнення та їх ефективність // ОР «Магістр» // Слупський Богдан Васильович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // С. 67, рис. – 9, табл. – 10 , кресл. – 15 , додат. – 1.

Ключові слова: АВТОМАТИЗОВАНЕ ТЕСТУВАННЯ НА ПРОНИКНЕНЯ, СКАНЕРИ ВРАЗЛИВОСТЕЙ, OWASP JUICE SHOP, ACUNETIX, BURP SUITE, NESSUS, OWASP ZAP

У роботі досліджено ефективність автоматизованих інструментів тестування на проникнення, таких як OWASP ZAP, Acunetix, Burp Suite та Nessus, у контексті безпеки веб-додатків. Тестування проводилося у середовищі OWASP Juice Shop, розгорнутому на віртуальній машині Kali Linux. Послідовний підхід до сканування забезпечив точність результатів та унеможливив перенавантаження середовища.

Результати показали, що Acunetix є найбільш продуктивним інструментом для автоматизованого тестування, тоді як OWASP ZAP — найкращий вибір для малих організацій завдяки його безкоштовності. Burp Suite виявився ефективним у ручному аналізі вразливостей, а Nessus доцільно використовувати для перевірки мережевої інфраструктури.

Рекомендації щодо вибору інструментів залежать від потреб та ресурсів організації: OWASP ZAP оптимальний для базового аналізу, Acunetix — для глибокого тестування, Burp Suite — для ручного пошуку вразливостей, а Nessus — для мережевих перевірок. Такий підхід сприяє комплексному підвищенню рівня кібербезпеки.

ABSTRACT

Automated penetration testing tools and their effectiveness // Thesis of educational level "Master"// Bohdan Slupskyi // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group SBm-61 // Ternopil, 2024 // P. 67, figs. 9, tables 10, drawings – 15, added. – 1.

Keywords: AUTOMATED PENETRATION TESTING, VULNERABILITY SCANNERS, OWASP JUICE SHOP, ACUNETIX, BURP SUITE, NESSUS, OWASP ZAP

This study explores the effectiveness of automated penetration testing tools, including OWASP ZAP, Acunetix, Burp Suite, and Nessus, in the context of web application security. Testing was conducted in the OWASP Juice Shop environment deployed on a Kali Linux virtual machine. A sequential scanning approach ensured result accuracy and prevented environment overload.

The results showed that Acunetix is the most productive tool for automated testing, while OWASP ZAP is the best choice for small organizations due to its free availability. Burp Suite proved effective for manual vulnerability analysis, and Nessus is more suitable for network infrastructure assessments.

Recommendations for tool selection depend on organizational needs and resources: OWASP ZAP is optimal for basic analysis, Acunetix for in-depth testing, Burp Suite for manual vulnerability exploration, and Nessus for network audits. This approach enables a comprehensive enhancement of cybersecurity levels.

ЗМІСТ

ВСТУП

Сучасні інформаційні системи та веб-додатки є ключовими елементами бізнесу, державних установ і громадських організацій. Зі збільшенням кількості кіберзагроз та ускладненням програмного забезпечення питання забезпечення кібербезпеки стає критично важливим. Одним із ефективних підходів до виявлення вразливостей і мінімізації ризиків є тестування на проникнення. Однак традиційні ручні методи аналізу є трудомісткими та ресурсозатратними, що обмежує їх застосування в умовах швидко змінюваних середовищ. Автоматизовані інструменти тестування на проникнення надають можливість значно скоротити час і витрати, підвищити точність та забезпечити безперервний моніторинг безпеки.

Актуальність теми обумовлена необхідністю підвищення ефективності тестування інформаційних систем у контексті зростання складності атак і обмежених ресурсів організацій. Використання автоматизованих інструментів, таких як OWASP ZAP, Burp Suite та Nessus, дозволяє адаптувати процеси тестування до сучасних викликів та забезпечити високу якість виявлення вразливостей.

Мета роботи — оцінка ефективності автоматизованих інструментів тестування на проникнення та розробка рекомендацій щодо їх вибору й впровадження для забезпечення кібербезпеки.

Завдання дослідження:

1. Проаналізувати сучасні підходи до тестування на проникнення, з акцентом на автоматизовані методи.
2. Оцінити функціональні можливості популярних інструментів тестування, таких як OWASP ZAP, Burp Suite, Nessus.
3. Провести практичне тестування у середовищі OWASP Juice Shop із використанням обраних інструментів.
4. Порівняти результати тестування за критеріями точності, продуктивності та частоти хибних спрацювань.

5. Розробити рекомендації для організацій щодо впровадження автоматизованих інструментів залежно від їхніх потреб і ресурсів.

Об’єкт дослідження — процес автоматизованого тестування на проникнення.

Предмет дослідження — функціональні можливості інструментів та методів автоматизованого тестування.

Методи дослідження включають порівняльний аналіз функцій та засобів інструментарію, а також моделювання та випробування середовищ автоматизованого тестування.

Наукова новизна роботи полягає у розробці підходу та критеріїв для оцінки автоматизованих інструментів тестування, аналізі їхньої ефективності в умовах організацій різних масштабів.

Практична значимість роботи полягає у можливості застосування отриманих результатів для оптимізації процесів тестування інформаційних систем у реальних умовах. Це особливо актуально для організацій із обмеженими ресурсами, які прагнуть підвищити рівень своєї кібербезпеки.

Структура роботи. Робота складається з трьох розділів. У першому розділі розглянуто теоретичні аспекти тестування на проникнення та автоматизації процесів. Другий розділ присвячений аналізу функціональних можливостей і точності популярних інструментів. У третьому розділі проведено практичне тестування, описано результати й розроблено рекомендації щодо впровадження інструментів.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: XII науково-технічній конференції «Інформаційні моделі, системи та технології.

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

1.1. Поняття та сутність тестування на проникнення

Тестування на проникнення (англ. penetration testing) — це цілеспрямована оцінка безпеки інформаційних систем або додатків, яка проводиться шляхом симуляції кіберзагроз з метою виявлення та аналізу вразливостей. Цей процес дозволяє проактивно оцінити здатність системи протидіяти реальним атакам, забезпечуючи ефективність заходів кібербезпеки.

Основна концепція пентесту полягає у використанні методів та інструментів, які імітують дії зловмисників. Метою є визначення слабких місць у системах, таких як помилки конфігурації, дефекти програмного забезпечення або недостатній рівень захисту мережевої інфраструктури. Тестування на проникнення є важливим елементом управління ризиками в організаціях, оскільки воно сприяє виявленню можливих загроз до того, як вони можуть бути використані.

Термін "penetration testing" є широким і охоплює різноманітні техніки та підходи. Зазвичай, до пентесту належать етапи збору інформації, аналізу цільової системи, експлуатації вразливостей, а також звітування про виявлені ризики. Методології, що застосовуються для тестування, базуються на міжнародних стандартах, таких як NIST SP 800-115 [1], OWASP Testing Guide [2] або OSSTMM, які регламентують процеси оцінювання інформаційної безпеки.

Тестування на проникнення є надзвичайно важливим для підвищення рівня захищеності інформаційних систем у сучасному світі, де кількість кібератак постійно зростає. Завдяки цьому підходу організації можуть не лише виявляти існуючі ризики, але й формувати ефективні стратегії для їх усунення.

Основними цілями тестування на проникнення є виявлення слабких місць у захисті інформаційних систем, аналіз рівня їхньої захищеності та формування рекомендацій для усунення вразливостей. Це комплексний процес, спрямований на

ідентифікацію можливих шляхів несанкціонованого доступу до даних чи ресурсів організації, а також оцінку ефективності впроваджених заходів кібербезпеки.

1. Виявлення вразливостей. Це можуть бути помилки конфігурації, невиправлені програмні дефекти або слабкі паролі. Виявлення таких проблем дозволяє організаціям передбачити дії потенційних зловмисників і завчасно усунути можливі ризики.
2. Оцінка захищеності системи. Під час тестування аналізуються технічні та організаційні аспекти безпеки, включаючи процеси управління доступом, регулярність оновлення програмного забезпечення та відповідність встановлених механізмів захисту сучасним вимогам.
3. Надання рекомендацій для покращення захисту. Результати тестування оформлюються у вигляді звіту, що містить детальний опис знайдених проблем, їхній рівень критичності, а також запропоновані кроки для їх усунення.
4. Підвищення готовності до кіберзагроз. Тестування дозволяє відпрацьовувати реакцію на реальні атаки, що підвищує готовність персоналу до надзвичайних ситуацій.

Таким чином, цілі тестування на проникнення охоплюють як технічні, так і організаційні аспекти безпеки, забезпечуючи всебічний підхід до захисту інформаційних систем.

Тестування на проникнення широко використовується в різних сценаріях для оцінки захищеності інформаційних систем та додатків. Типові сфери його застосування включають веб-додатки, корпоративні мережі, системи управління даними, а також спеціалізовані галузі, такі як IoT та промислові системи.

1. Тестування веб-додатків. Фокусується на виявленні вразливостей, таких як SQL-ін’єкції, XSS або CSRF. Це забезпечує відповідність веб-додатків сучасним стандартам безпеки, наприклад OWASP Top 10.
2. Мережеве тестування. Оцінює безпеку корпоративних мереж, включаючи сканування відкритих портів, виявлення некоректно налаштованих сервісів і тестування захищеності протоколів передачі даних.

3. Оцінка систем управління (SCADA, IoT). Тестування допомагає виявити критичні вразливості у фізичних або програмних інтерфейсах, характерних для складних систем.
4. Безпека мобільних додатків. Аналізує загрози, пов’язані з передачею даних між пристроями та можливі витоки через небезпечні API.
5. Відповідність регуляторним вимогам. Перевірка відповідності стандартам, таким як PCI DSS або ISO 27001, для підтвердження рівня безпеки систем.

Таким чином, типові сценарії тестування на проникнення охоплюють широкий спектр завдань, що дозволяє адаптувати процес до конкретних потреб організації, забезпечуючи захищеність її інформаційних ресурсів та відповідність стандартам.

1.2. Класифікація методів тестування на проникнення та їх застосування

Ручне та автоматизоване тестування на проникнення є основними підходами до виявлення вразливостей інформаційних систем, кожен із яких має свої переваги, недоліки та сферу застосування. Їхнє порівняння дозволяє обґрунтовано обрати оптимальний підхід для конкретного завдання.

Ручне тестування передбачає виконання дій фахівцем, який безпосередньо аналізує систему, виявляє вразливості та імітує дії зловмисників. Цей підхід надає гнучкість та дозволяє враховувати контекст і специфіку системи. Особливістю ручного тестування є здатність виявляти складні вразливості, які важко ідентифікувати автоматизованими інструментами, наприклад, логічні помилки у бізнес-процесах або неочевидні конфігураційні недоліки. Проте ручний підхід є ресурсоємним і вимагає високої кваліфікації тестувальника, що підвищує його вартість.

Автоматизоване тестування, у свою чергу, базується на використанні спеціалізованих програмних засобів, таких як сканери вразливостей чи пентест-фреймворки. Перевагами автоматизації є висока швидкість, повторюваність і масштабованість. Інструменти можуть швидко сканувати великі системи, перевіряючи їх на відповідність відомим уразливостям. Проте автоматизовані

рішення схильні до генерації фальшивих спрацювань (false positives) і не завжди здатні врахувати специфіку аналізованої системи.

Ідеальним підходом є комбіноване використання ручного та автоматизованого тестування. Автоматизовані інструменти забезпечують базове покриття, виявляючи типові вразливості, тоді як ручний підхід дозволяє виявити більш складні та унікальні загрози. Такий синергічний підхід дозволяє досягти високого рівня надійності у забезпеченні безпеки інформаційних систем.

Тестування на проникнення здійснюється з використанням різних підходів, залежно від обсягу доступної інформації про цільову систему. Найбільш поширеними є методи White-box (тест «білого ящика»), Black-box (тест «чорного ящика») та Gray-box (тест «сірого ящика»). Кожен із цих методів має свої переваги, обмеження та специфіку застосування. [3]

White-box тестування передбачає повний доступ до інформації про цільову систему, включаючи вихідний код, конфігурації, структуру мережі та облікові дані. Цей підхід дозволяє максимально глибоко дослідити безпеку, оцінити рівень захищеності всіх компонентів та ідентифікувати складні вразливості, які можуть бути недоступними для інших методів. Однак його реалізація вимагає значних ресурсів і часу.

Black-box тестування, навпаки, проводиться без будь-якої попередньої інформації про систему. Тестер імітує дії зловмисника, використовуючи лише загальнодоступні методи збору даних. Це дозволяє перевірити захищеність системи від зовнішніх атак. Основним обмеженням є неможливість виявлення вразливостей, які приховані від загального доступу.

Gray-box тестування є компромісом між двома попередніми підходами. Тестеру надається часткова інформація про систему, наприклад доступ до облікових записів із певним рівнем привілеїв або документації. Цей підхід дозволяє оцінити як зовнішню, так і внутрішню безпеку, забезпечуючи баланс між глибиною аналізу та витратами на тестування.

Вибір методу залежить від завдань тестування, доступних ресурсів та необхідного рівня деталізації. Наприклад, Black-box підхід доцільний для оцінки

ризиків зовнішніх атак, тоді як White-box метод використовується для поглибленого аудиту безпеки. Gray-box тестування найчастіше застосовується для виявлення вразливостей у системах із розмежованим доступом.

Сфери застосування тестування на проникнення охоплюють широкий спектр інформаційних систем, включаючи корпоративні мережі, веб-додатки, а також IoT-пристрої. Вибір сфери залежить від специфіки об'єкта, цілей аналізу та характеру потенційних загроз.

Мережеве тестування є одним із ключових напрямів пентесту. Воно охоплює аналіз як внутрішніх, так і зовнішніх мереж організації. Основними завданнями є виявлення відкритих портів, слабко захищених служб, неправильно налаштованих мережевих пристроїв і потенційних точок входу для атак. Тестування допомагає захистити організацію від атак типу DoS, MitM або несанкціонованого доступу до критичних ресурсів.

Тестування веб-додатків фокусується на пошуку вразливостей у програмному забезпеченні, таких як SQL-ін’єкції, XSS (міжсайтовий сценарій) чи CSRF (міжсайтовий підроблений запит). Веб-додатки є критичним елементом цифрової інфраструктури, а їх вразливості можуть призвести до компрометації даних або функціональності. OWASP Top 10 є загальновизнаним стандартом для проведення такого тестування.

IoT-пристрої представляють нову сферу для тестування на проникнення. Зростаюча кількість розумних пристроїв, які взаємодіють через мережі, робить їх привабливою мішенню для зловмисників. Тестування IoT включає аналіз захищеності прошивки, мережевих протоколів і взаємодії пристроїв із хмарними сервісами. Особливістю цієї сфери є різноманітність пристроїв і платформ, що ускладнює створення універсальних рішень для забезпечення безпеки.

Усі ці сфери мають спільну мету — виявлення та усунення вразливостей, але кожна з них вимагає специфічного підходу та методології. Комплексне охоплення всіх напрямків є важливим для забезпечення всебічного захисту інформаційних систем і зниження ризиків кіберзагроз.

1.3. Автоматизація процесу тестування: переваги, обмеження та тенденції розвитку

Сучасні виклики в галузі кібербезпеки, зокрема зростання кількості складних атак і швидкий розвиток технологій, вимагають нових підходів до тестування на проникнення. Одним із ключових рішень є автоматизація цього процесу, яка значно підвищує ефективність виявлення вразливостей і забезпечує низку важливих переваг.

Основною причиною потреби в автоматизації є зменшення затрат часу. У порівнянні з ручним тестуванням, автоматизовані інструменти дозволяють швидко сканувати великі системи, перевіряючи їх на наявність відомих вразливостей. Це особливо актуально для організацій із розгалуженою інфраструктурою, де час є критичним фактором. Автоматизація забезпечує виконання перевірок у стислі строки, що сприяє оперативному реагуванню на можливі загрози.

Ще одним важливим аспектом є скорочення впливу людського фактора. Ручне тестування, навіть виконуване кваліфікованими фахівцями, є схильним до помилок через втомлюваність або суб'єктивність аналізу. Автоматизовані інструменти працюють за заданими алгоритмами, що забезпечує стабільність і повторюваність результатів. Це дозволяє уникнути пропуску важливих вразливостей, які могли б залишитися непоміченими при ручному аналізі.

Крім того, автоматизація спрощує процес регулярного тестування, забезпечуючи постійний моніторинг безпеки. Інструменти можуть бути інтегровані в цикли розробки програмного забезпечення (CI/CD), що дозволяє виявляти та виправляти вразливості ще на етапі створення продукту.

Автоматизація процесів тестування на проникнення надає низку ключових переваг, які роблять цей підхід незамінним у сучасній практиці забезпечення кібербезпеки. Серед основних вигод виділяються масштабованість, повторюваність і швидкість виконання. [4]

Масштабованість є однією з головних переваг автоматизації. У великих організаціях, де кількість інформаційних систем може обчислюватися сотнями,

ручне тестування стає практично неможливим через значний обсяг роботи. Автоматизовані інструменти дозволяють одночасно виконувати перевірки на багатьох об'єктах, забезпечуючи ефективне використання ресурсів та максимальне покриття.

Повторюваність тестів забезпечує їхню якість і консистентність. Автоматизовані сканери виконують однакові операції без відхилень, що дозволяє уникнути впливу людського фактора. Це особливо важливо при регулярному моніторингу, коли порівнянність результатів у часі є критичною для оцінки змін у безпеці системи.

Швидкість виконання — ще одна важлива перевага. Автоматизовані засоби значно швидше аналізують системи, перевіряючи їх на наявність тисяч вразливостей за короткий час. Це дає змогу швидко виявляти потенційні загрози та оперативно реагувати на них. У сучасних умовах, коли нові вразливості можуть використовуватися зловмисниками вже через кілька годин після їхнього виявлення, швидкість тестування має вирішальне значення.

Незважаючи на значні переваги автоматизації тестування на проникнення, цей підхід має низку обмежень, які необхідно враховувати при його впровадженні. Основними проблемами є високий рівень фальшивих спрацювань та недостатнє розуміння контексту системи автоматизованими інструментами.

Фальшиві спрацювання (false positives) є однією з ключових проблем автоматизованого тестування. Багато інструментів можуть визначати потенційні вразливості, які в реальності не становлять загрози. Це призводить до марнування часу фахівців, які змушені вручну перевіряти такі результати. Водночас, інструменти можуть пропустити специфічні загрози, що стає причиною недооцінки ризиків.

Недостатнє розуміння контексту системи. Автоматизовані інструменти працюють за заданими алгоритмами та шаблонами, що обмежує їх здатність аналізувати складні бізнес-логіки або специфічні конфігурації. Наприклад, унікальні процеси обробки даних чи користувацькі сценарії можуть залишитися поза увагою сканера.

Обмежену адаптивність до нових загроз. Хоча більшість сучасних рішень регулярно оновлюються, виникнення нових, ще не задокументованих вразливостей може залишитися поза межами їхнього виявлення.

Автоматизація тестування на проникнення продовжує еволюціонувати, і сучасні тенденції в цій сфері зосереджені на інтеграції з процесами безперервної розробки, вдосконаленні через впровадження штучного інтелекту (ШІ) та адаптації до нових підходів у кібербезпеці, таких як DevSecOps.

Однією з головних тенденцій є інтеграція автоматизованих інструментів у процеси CI/CD (Continuous Integration/Continuous Deployment). Ця інтеграція дозволяє проводити перевірки безпеки на кожному етапі розробки програмного забезпечення, що знижує ризики появи вразливостей у готових продуктах. Інструменти, такі як OWASP ZAP чи Burp Suite, вже підтримують автоматичні сканування в рамках CI/CD, забезпечуючи швидке виявлення загроз без уповільнення циклу розробки.

Ще однією важливою тенденцією є розвиток підходу DevSecOps, який передбачає інтеграцію безпеки як невід'ємної частини процесу розробки. У цьому контексті автоматизовані інструменти тестування на проникнення відіграють роль засобів забезпечення проактивної безпеки, дозволяючи розробникам своєчасно реагувати на виявлені загрози.

Застосування штучного інтелекту (ШІ) у тестуванні на проникнення відкриває нові горизонти. Завдяки використанню машинного навчання, інструменти стають здатними прогнозувати потенційні атаки, адаптуватися до нових загроз і знижувати рівень фальшивих спрацювань. Наприклад, ШІ допомагає автоматизувати складний аналіз логів або розпізнавати складні патерни атак, які можуть залишитися поза увагою традиційних сканерів.

У цілому, сучасні тенденції автоматизації орієнтовані на глибшу інтеграцію з розробкою, покращення точності та розширення функціональності інструментів. Ці підходи не лише підвищують ефективність тестування, але й дозволяють організаціям оперативніше реагувати на нові загрози, забезпечуючи високий рівень кібербезпеки у динамічних умовах сучасного середовища.

1.4. Огляд поширених інструментів автоматизованого тестування на проникнення

Вибір інструментів для автоматизованого тестування на проникнення є критично важливим етапом, що впливає на якість і ефективність процесу виявлення вразливостей. Основними критеріями вибору є функціональність, точність та сумісність із цільовим середовищем.

Функціональність інструмента є першочерговим критерієм, оскільки вона визначає можливості сканера або пентест-фреймворка. Сучасні інструменти повинні підтримувати широкий спектр тестів, включаючи пошук вразливостей у веб-додатках (SQLi, XSS, CSRF), аналіз конфігурацій мережі, сканування відкритих портів тощо. Важливо також враховувати наявність додаткових функцій, таких як генерація звітів, інтеграція з CI/CD чи підтримка багатокористувацького доступу.

Точність інструмента є не менш важливим аспектом. Це включає як здатність виявляти реальні вразливості (true positives), так і мінімізацію фальшивих спрацювань (false positives). Інструмент має надавати чіткі та релевантні результати, які можуть бути легко інтерпретовані спеціалістами безпеки.

Сумісність із цільовим середовищем є ще одним ключовим фактором. Інструмент повинен підтримувати різні операційні системи, платформи та програмні стекові технології, які використовуються у середовищі тестування. Наприклад, інструмент для тестування веб-додатків повинен бути сумісним із популярними фреймворками (Django, Laravel, React тощо) і хмарними сервісами.

При виборі інструменту слід також враховувати вартість ліцензування, доступність технічної підтримки та регулярність оновлень бази вразливостей. Сукупність цих критеріїв дозволяє обрати інструмент, який найкраще відповідає потребам організації та забезпечує ефективний рівень кібербезпеки.

Серед найбільш відомих інструментів для автоматизованого тестування на проникнення виділяються Acunetix, Nessus, OWASP ZAP і Burp Suite. Кожен із них має унікальні функціональні можливості, що робить їх придатними для різних завдань кібербезпеки. [5]

Acunetix — це комерційний інструмент, спеціалізований на тестуванні веб-додатків. Його перевагами є підтримка широкого спектра тестів, таких як SQL-ін’єкції, XSS і CSRF. Acunetix інтегрується з CI/CD конвеєрами та забезпечує високу швидкість сканування, що робить його зручним для використання в масштабних проєктах. [6]

Nessus — сканер вразливостей загального призначення, який використовується для аналізу мережевої безпеки. Його функціонал включає виявлення конфігураційних помилок, сканування портів і перевірку на наявність відомих уразливостей. Nessus має потужну базу плагінів і зручний інтерфейс для аналізу результатів. [7]

OWASP ZAP — це безкоштовний інструмент із відкритим кодом, орієнтований на тестування веб-додатків. Він підтримує як активне сканування, так і ручне тестування за допомогою проксі-сервера. ZAP ідеально підходить для початківців завдяки простоті використання та активній підтримці спільноти. [8]

Burp Suite — один із найпотужніших інструментів для тестування веб-додатків. Його перевагами є розширені можливості конфігурації, інтеграція з іншими інструментами та підтримка додаткових модулів для виявлення складних уразливостей. Комерційна версія Burp Suite забезпечує автоматизоване сканування, тоді як безкоштовна дає змогу проводити ручні перевірки. [9]

Ці інструменти покривають широкий спектр потреб у тестуванні на проникнення, що дозволяє організаціям обирати найбільш відповідні рішення залежно від завдань, масштабу та бюджету. Їх ефективне використання є важливим кроком до забезпечення надійного рівня кібербезпеки.

Ринок інструментів для автоматизованого тестування на проникнення поділяється на два основних сегменти: комерційні рішення та Open Source інструменти. Кожен із цих підходів має свої переваги та недоліки, які впливають на вибір залежно від потреб організації.

Комерційні рішення, такі як Acunetix, Nessus чи Burp Suite Pro, пропонують високу якість підтримки, регулярні оновлення бази вразливостей та широкий набір функцій. Їх основною перевагою є готовність до інтеграції у складні корпоративні

середовища, зокрема у CI/CD процеси. Вони мають зручний інтерфейс і забезпечують детальні звіти, що спрощує аналіз результатів. Однак, недоліком таких інструментів є висока вартість ліцензій, що може стати перешкодою для малих організацій або стартапів із обмеженим бюджетом.

Open Source інструменти, наприклад, OWASP ZAP чи Wapiti, забезпечують гнучкість і доступність. Їх головною перевагою є відсутність вартості ліцензії та можливість модифікації коду відповідно до потреб користувача. Вони активно підтримуються спільнотою, що дозволяє швидко реагувати на нові виклики у сфері безпеки. Проте, Open Source інструменти можуть вимагати більше часу на налаштування та не завжди забезпечують такий самий рівень функціональності, як комерційні аналоги. Крім того, підтримка з боку розробників іноді є обмеженою.

Комбінація комерційних і Open Source інструментів може бути ефективним рішенням. Наприклад, Open Source інструменти можуть використовуватися для початкового сканування, тоді як комерційні — для глибшого аналізу та інтеграції у робочі процеси. Такий підхід дозволяє організаціям оптимізувати витрати та забезпечити необхідний рівень кібербезпеки залежно від конкретних потреб.

Сучасний розвиток інструментів для автоматизованого тестування на проникнення орієнтований на розширення функціональних можливостей, підвищення точності та адаптивності. Ключовими тенденціями є впровадження модульності та інтеграція технологій машинного навчання (Machine Learning, ML). 10

Модульність є важливою характеристикою сучасних інструментів, що дозволяє користувачам адаптувати функціонал під специфічні потреби. Завдяки модульній архітектурі користувачі можуть додавати або оновлювати окремі компоненти, такі як сканери вразливостей, генератори звітів чи аналітичні модулі. Це забезпечує гнучкість у використанні інструментів у різних середовищах, від малих локальних систем до масштабних корпоративних мереж.

Інтеграція Machine Learning відкриває нові можливості для автоматизації аналізу загроз. Завдяки ML інструменти можуть навчатися на основі історичних даних, розпізнавати складні патерни атак та прогнозувати потенційні ризики.

Наприклад, технології ML допомагають знижувати кількість фальшивих спрацювань, аналізувати логи великих обсягів даних і автоматично корелювати вразливості для створення комплексного аналізу загроз.

Ще однією перспективною тенденцією є інтеграція інструментів тестування на проникнення з платформами DevSecOps. Це дозволяє проводити безперервний моніторинг безпеки у межах CI/CD конвеєрів, забезпечуючи оперативне виявлення та усунення вразливостей.

Важливим напрямом розвитку є підвищення інтерактивності та зручності використання інструментів. Розробники прагнуть створювати інтерфейси, які дозволяють не лише тестувальникам, але й менеджерам з інформаційної безпеки легко отримувати доступ до результатів та рекомендацій.

Отже, сучасні тенденції у розробленні інструментів для тестування на проникнення орієнтовані на підвищення їхньої ефективності, адаптивності та інтеграції з іншими процесами. Вони дозволяють організаціям проактивно реагувати на загрози, оптимізуючи процеси забезпечення кібербезпеки.

РОЗДІЛ 2 АНАЛІЗ ТА ПОРІВНЯННЯ АВТОМАТИЗОВАНИХ ІНСТРУМЕНТІВ ТЕСТУВАННЯ

2.1. Критерії вибору інструментів для автоматизованого тестування

Критерії оцінки інструментів автоматизованого тестування на проникнення є ключовими для визначення їхньої ефективності та придатності для використання в конкретному середовищі. Основними параметрами є точність, продуктивність, юзабіліті (зручність використання) та інтеграція з іншими системами.

Точність визначає здатність інструменту виявляти реальні вразливості без значної кількості хибнопозитивних чи хибнонегативних результатів. Чим вища точність, тим ефективніше організація може виявляти та усувати загрози. Для оцінки точності використовуються стандартизовані тести, наприклад, OWASP Benchmark. [11]

Продуктивність відображає швидкість виконання тестів та здатність інструменту обробляти великі обсяги даних. Цей параметр є важливим для організацій із масштабною інфраструктурою, де час тестування може впливати на критичні бізнес-процеси.

Юзабіліті визначає, наскільки легко інструмент можна використовувати без необхідності глибоких технічних знань. Інтерфейс повинен бути інтуїтивно зрозумілим, а функціонал — доступним навіть для некваліфікованих користувачів. Наявність якісної документації та підтримки також є важливим фактором.

Інтеграція з іншими системами, такими як CI/CD платформи, SIEM-системи або платформи DevSecOps, дозволяє забезпечити безперервний процес тестування та швидке реагування на знайдені вразливості. Інструменти, що підтримують API, забезпечують гнучкість і можливість автоматизації.

Визначення базових критеріїв дозволяє об’єктивно оцінити інструменти автоматизованого тестування та обрати оптимальне рішення для конкретних завдань. Ці критерії слугують основою для подальшого аналізу їхньої ефективності.

Вибір інструментів для автоматизованого тестування на проникнення повинен враховувати специфіку середовища тестування, оскільки цей аспект визначає, наскільки ефективним буде тестування. Основними факторами є тип цільової системи та масштаб проєкту.

Тип цільової системи впливає на вимоги до функціональності інструмента. Для тестування веб-додатків інструменти повинні підтримувати виявлення таких вразливостей, як SQL-ін’єкції, XSS або CSRF. У випадку мережевого тестування необхідно забезпечити аналіз відкритих портів, конфігурацій мережевих пристроїв і протоколів. Для IoT-систем важлива підтримка аналізу взаємодії між пристроями та перевірки специфічних протоколів.

Масштаб проєкту визначає, які вимоги висуваються до продуктивності та масштабованості інструмента. У невеликих проєктах може бути достатньо базових можливостей сканера, тоді як у великих корпоративних мережах потрібна підтримка одночасного тестування багатьох систем. Крім того, масштаб проєкту впливає на обсяг звітності: для масштабних систем важливі автоматизація та структурування результатів.

Додатково слід враховувати динамічність середовища, наприклад, у хмарних або віртуалізованих середовищах. Інструмент має бути сумісним із такими платформами та підтримувати регулярне оновлення, щоб відповідати актуальним загрозам.

Врахування специфіки середовища тестування дозволяє обрати інструменти, які найкраще відповідають цілям та умовам проєкту. Це забезпечує оптимальне співвідношення між витратами та ефективністю, підвищуючи рівень кібербезпеки.

Оцінка економічних факторів є невід'ємною частиною вибору інструментів для автоматизованого тестування на проникнення, оскільки вона впливає на доступність та ефективність їхнього впровадження. Основними аспектами є вартість ліцензії, витрати на супровід та можливість довгострокового використання інструмента.

Ліцензійні витрати можуть варіюватися залежно від типу інструмента. Комерційні рішення, такі як Acunetix або Nessus, зазвичай вимагають значних

початкових інвестицій та щорічних платежів за підтримку. У той же час, Open Source інструменти, наприклад OWASP ZAP, надають базові можливості безкоштовно, що робить їх привабливими для малих організацій з обмеженим бюджетом. Проте, у випадку Open Source, додаткові витрати можуть виникати через потребу у налаштуванні та навчанні персоналу.

Вартість супроводу також є важливим фактором. Інструменти вимагають регулярного оновлення баз вразливостей для забезпечення актуальності. Комерційні рішення забезпечують цю функцію автоматично, що спрощує експлуатацію, тоді як для Open Source рішень може бути потрібна ручна підтримка.

Економічна ефективність визначається здатністю інструмента вирішувати завдання з мінімальними витратами. Наприклад, інструменти, які інтегруються в існуючу інфраструктуру, можуть знизити витрати на адаптацію. Крім того, важливим є забезпечення співвідношення між вартістю інструмента та його функціональністю: деякі дорогі рішення можуть надавати надлишкові можливості, які не використовуються.

Урахування економічних факторів дозволяє організаціям вибирати інструменти, що відповідають їхнім потребам, забезпечуючи оптимальне співвідношення вартості та ефективності. Це особливо актуально для малих організацій, де бюджетні обмеження відіграють вирішальну роль у прийнятті рішень.

2.2. Аналіз функціональних можливостей та архітектури інструментів

Автоматизовані інструменти тестування на проникнення базуються на багаторівневій архітектурі, що забезпечує їхню ефективність, масштабованість і гнучкість у застосуванні. Основні компоненти включають скануючі ядра, модулі аналізу та механізми звітування, які працюють у взаємодії для виявлення вразливостей.

Скануючі ядра є основою роботи будь-якого інструмента. Вони виконують основні функції сканування, аналізуючи цільову систему на наявність

вразливостей. Сканери використовують бази даних відомих уразливостей, наприклад CVE (Common Vulnerabilities and Exposures) [12], та вбудовані алгоритми для ідентифікації можливих загроз. Наприклад, ядра інструментів Nessus і Acunetix побудовані на технологіях, які забезпечують високу швидкість сканування з мінімальною кількістю хибних спрацювань.

Модулі аналізу розширюють можливості скануючого ядра, додаючи функції для специфічних типів тестування, таких як SQL-ін'єкції, міжсайтовий сценарій (XSS) або перевірка налаштувань мережі. Ця модульність дозволяє користувачам адаптувати інструмент до конкретних завдань. Наприклад, у Burp Suite модулі Spider і Intruder дозволяють виконувати глибокий аналіз структури веб-додатків і автоматизоване тестування.

Механізми звітування відповідають за представлення результатів тестування у зрозумілому форматі. Звіти часто містять список виявлених вразливостей із деталізацією рівня ризику, рекомендаціями щодо усунення та оцінкою впливу на систему. Багато інструментів, таких як OWASP ZAP, підтримують різні формати звітів, що дозволяє легко інтегрувати їх у процеси управління кібербезпекою.

Злагоджена робота цих компонентів забезпечує ефективне виявлення вразливостей, дозволяючи організаціям адаптувати інструменти до своїх потреб і підвищувати рівень захищеності інформаційних систем.

Ефективність інструментів автоматизованого тестування на проникнення значною мірою залежить від їхньої здатності виявляти різноманітні типи вразливостей. Серед них можна виділити серверні, клієнтські, архітектурні та мережеві вразливості, кожна з яких має свої особливості та вимоги до аналізу.

Серверні вразливості пов'язані з налаштуваннями серверів та їхньою взаємодією із програмним забезпеченням. Прикладами є SQL-ін'єкції, помилки автентифікації та відсутність належної перевірки даних. Інструменти, такі як Nessus і Acunetix, забезпечують сканування конфігурацій серверів та їхньої безпеки, виявляючи помилки у налаштуваннях і дефекти у взаємодії між компонентами.

Клієнтські вразливості стосуються проблем на стороні користувача, зокрема веб-браузерів або мобільних додатків. Найпоширенішими є XSS-атаки та помилки у обробці клієнтських запитів. OWASP ZAP і Burp Suite спеціалізуються на виявленні таких загроз, аналізуючи веб-додатки на наявність некоректної роботи із введенням даних.

Архітектурні вразливості виникають через недоліки у проектуванні системи. До них належать проблеми у логіці доступу, недостатня ізоляція між модулями або вразливі API. Виявлення таких дефектів потребує комплексного підходу, що поєднує автоматизацію з ручним аналізом, який можуть забезпечити інструменти на зразок Burp Suite з його модулем для перевірки бізнес-логіки.

Мережеві вразливості включають відкриті порти, використання застарілих протоколів чи помилки в конфігураціях маршрутизаторів і брандмауерів. Nessus і OpenVAS надають можливості для детального аналізу мережевої інфраструктури, включаючи перевірку відповідності стандартам безпеки.

Комплексна підтримка цих типів вразливостей забезпечує багатогранний аналіз безпеки системи. Інструменти, які здатні охоплювати різні категорії загроз, дозволяють організаціям формувати цілісний підхід до забезпечення кібербезпеки.

Одна з ключових характеристик сучасних інструментів автоматизованого тестування на проникнення — це наявність ефективного репортингу та підтримка інтеграції з CI/CD конвеєрами. Ці можливості забезпечують підвищення зручності аналізу результатів тестування та спрощують інтеграцію кібербезпеки у процеси розробки програмного забезпечення.

Репортинг є важливим елементом автоматизованих інструментів. Інструменти повинні генерувати зрозумілі та структуровані звіти, що містять деталі про виявлені вразливості, їх рівень критичності, а також рекомендації щодо усунення. Наприклад, такі інструменти, як Nessus і Acunetix, надають можливість експорту звітів у різних форматах (PDF, HTML, CSV), що полегшує їхню передачу та аналіз. OWASP ZAP забезпечує функцію кастомізації звітів для адаптації до специфічних вимог організації.

Інтеграція з CI/CD дозволяє включити тестування на проникнення у безперервний цикл розробки програмного забезпечення. Інструменти, такі як OWASP ZAP та Burp Suite, підтримують автоматичне сканування вразливостей під час етапів розробки, збірки та розгортання. Це дозволяє виявляти потенційні загрози ще до того, як продукт потрапить до кінцевого користувача. Інтеграція через API чи плагіни для популярних платформ CI/CD, таких як Jenkins чи GitLab, робить цей процес простим і ефективним.

Ефективний репортинг і підтримка CI/CD значно підвищують оперативність та зручність впровадження безпекових практик. Ці функції дозволяють забезпечити не лише якісне виявлення вразливостей, але й швидке реагування на них, сприяючи підвищенню рівня кібербезпеки організації.

2.3. Порівняльний аналіз точності та повноти виявлення вразливостей

Для оцінки ефективності інструментів автоматизованого тестування на проникнення важливо розробити методику порівняльних тестів, що дозволить об'єктивно визначити їх точність, продуктивність та здатність виявляти різноманітні вразливості. Основою такої методики є використання набору вразливих веб-додатків, які імітують реальні сценарії атак.

Підбір тестового середовища включає створення або використання вже існуючих наборів вразливих веб-додатків, таких як OWASP Juice Shop, Damn Vulnerable Web Application (DVWA) або Mutillidae. Ці середовища розроблені для навчання та тестування, тому включають широкий спектр типових вразливостей: SQL-ін’єкції, XSS, CSRF, некоректну автентифікацію тощо.

Етапи тестування включають налаштування інструментів, виконання сканування та аналіз отриманих результатів. Для кожного інструмента виконується кілька тестів, які охоплюють усі можливі вразливості, доступні у вибраних середовищах. Це дозволяє оцінити, наскільки добре інструмент справляється із завданням, і визначити його сильні та слабкі сторони.

Критерії оцінки результатів включають кількість виявлених вразливостей, співвідношення хибнопозитивних і хибнонегативних спрацювань, а також час, необхідний для завершення тестування. Такі метрики дозволяють не лише порівняти інструменти між собою, але й оцінити їх придатність для конкретних завдань.

Ретельно спланована методика порівняльних тестів забезпечує об'єктивність оцінки та дозволяє визначити, які інструменти є найефективнішими у виявленні вразливостей у різних сценаріях. Це стає основою для подальшого аналізу точності та повноти їхньої роботи.

Для об’єктивної оцінки ефективності автоматизованих інструментів тестування на проникнення важливо порівняти результати, отримані в процесі тестування, за кількісними та якісними показниками. Основними метриками для аналізу є загальна кількість виявлених вразливостей, їхній тип та рівень критичності.

Кількість виявлених вразливостей є базовим показником, що дозволяє оцінити масштаб роботи інструмента. Наприклад, інструменти з розширеними базами даних, такі як Nessus або Acunetix, зазвичай виявляють більше вразливостей завдяки їхній здатності аналізувати широкий спектр компонентів системи. Водночас інструменти, які генерують велику кількість хибнопозитивних результатів, можуть спотворювати ці дані, що потребує додаткової перевірки.

Типи виявлених вразливостей дозволяють оцінити спеціалізацію інструмента. Наприклад, OWASP ZAP ефективний у виявленні проблем веб-додатків, таких як XSS чи SQL-ін’єкції, тоді як Nessus фокусується на мережевих вразливостях, таких як відкриті порти чи помилки конфігурації серверів.

Рівень критичності є ключовим параметром для оцінки практичної цінності тестування. Інструменти мають не лише ідентифікувати вразливості, але й класифікувати їх за рівнем ризику: критичні, високі, середні та низькі. Наприклад, критичні вразливості, такі як відкриті паролі адміністратора чи некоректні права доступу, потребують негайного усунення. Системи, які пропонують чітке

ранжування виявлених ризиків, значно спрощують процес управління кібербезпекою.

Порівняння за цими показниками дозволяє визначити інструменти, які найкраще підходять для конкретних завдань. Виявлення сильних та слабких сторін кожного інструмента формує основу для вибору оптимального рішення в умовах реальних кіберзагроз.

Для визначення точності інструментів автоматизованого тестування на проникнення важливо оцінити частоту та вплив фальшивих позитивів (false positives) і фальшивих негативів (false negatives). Ці показники відображають, наскільки інструмент надає релевантні результати, і впливають на якість подальшого аналізу безпеки.

Фальшиві позитиви виникають, коли інструмент позначає безпечні елементи як уразливості. Це може створювати додаткове навантаження на команду безпеки, яка змушена вручну перевіряти некоректні результати. Наприклад, інструменти з високим рівнем фальшивих позитивів, як-от деякі Open Source рішення, потребують налаштування для зменшення таких спрацювань. Наявність функцій фільтрації або ранжування результатів, що реалізована у таких інструментах, як Acunetix чи Burp Suite, значно полегшує цей процес.

Фальшиві негативи є більш критичним недоліком, оскільки вразливості залишаються непоміченими, що створює потенційні ризики для безпеки системи. Наприклад, недостатня підтримка специфічних типів атак, як-от бізнес-логічні помилки, може стати причиною пропуску загроз. Інструменти, які інтегрують штучний інтелект або алгоритми машинного навчання, здатні зменшувати кількість фальшивих негативів, адаптуючись до нових видів атак.

Для об’єктивної оцінки інструментів важливо використовувати стандартизовані середовища, як-от OWASP Benchmark, які дозволяють порівнювати рівень фальшивих позитивів і негативів серед різних рішень. Комбінація цих показників допомагає визначити інструменти, які надають найбільш достовірні результати, мінімізуючи ризики для організації.

Таким чином, оцінка фальшивих позитивів і негативів є ключовим етапом у визначенні надійності автоматизованих інструментів тестування. Вона дозволяє вибирати рішення, які найкраще відповідають вимогам організації та забезпечують ефективне управління кібербезпекою.

2.4. Переваги та недоліки автоматизованих інструментів у практичному застосуванні

Автоматизовані інструменти тестування на проникнення мають ряд сильних сторін, які роблять їх незамінними у процесах забезпечення кібербезпеки. До ключових переваг належать висока швидкість виконання тестів, повторюваність результатів і масштабованість у різних середовищах.

Швидкість тестування є однією з головних переваг автоматизованих рішень. Інструменти, такі як Nessus чи Acunetix, здатні одночасно перевіряти тисячі компонентів, що дозволяє виявляти вразливості значно швидше, ніж це можливо при ручному тестуванні. Це особливо важливо у випадках, коли потрібно виконати перевірку великих систем або провести оперативний аудит після змін у конфігурації.

Повторюваність забезпечує консистентність результатів незалежно від кількості запусків. Завдяки алгоритмічному підходу, автоматизовані інструменти гарантують однакові результати при повторних тестах, що дозволяє точно відстежувати динаміку безпеки системи. Це також мінімізує вплив людського фактора, що є характерним для ручного тестування.

Масштабованість дозволяє використовувати автоматизовані інструменти у середовищах будь-якого масштабу — від невеликих стартапів до великих корпоративних мереж. Інструменти можуть виконувати перевірку одночасно на багатьох об'єктах, підтримуючи багаторівневі архітектури та інтеграцію з хмарними платформами.

Ці сильні сторони роблять автоматизовані інструменти тестування ефективним вибором для організацій, які прагнуть оперативно виявляти вразливості,

забезпечувати стабільність безпеки та адаптуватися до зростаючих потреб у масштабах своєї інфраструктури. Вони є невід'ємною частиною сучасного підходу до управління кібербезпекою.

Незважаючи на численні переваги, автоматизовані інструменти тестування на проникнення мають свої обмеження. Серед типових проблем виділяються необхідність ручної перевірки результатів і обмежена глибина аналізу в окремих сценаріях.

Необхідність ручної перевірки є важливим аспектом використання автоматизованих інструментів. Хоча інструменти здатні виявляти більшість відомих вразливостей, вони нерідко генерують хибнопозитивні результати, що потребує додаткової перевірки вручну. Наприклад, OWASP ZAP або Nessus можуть позначати елементи як потенційно небезпечні, хоча насправді вони не становлять загрози. Це створює додаткове навантаження на команду безпеки, яка повинна фільтрувати некоректні спрацювання.

Обмежена глибина аналізу стосується складних або специфічних загроз, таких як логічні помилки у бізнес-процесах чи вразливості, пов’язані із взаємодією унікальних компонентів системи. Автоматизовані інструменти часто базуються на відомих шаблонах атак і не здатні аналізувати сценарії, які потребують інтуїтивного підходу або детального розуміння контексту. Наприклад, автоматичне тестування може не враховувати специфіку взаємодії у багатокористувацьких середовищах або в розподілених системах.

Ці обмеження підкреслюють важливість комбінування автоматизованого і ручного тестування. Використання автоматизованих інструментів для первинного аналізу та ручної перевірки для детального вивчення складних випадків дозволяє досягти балансу між ефективністю та точністю, що є критично важливим для забезпечення кібербезпеки.

Ефективність використання автоматизованих інструментів тестування на проникнення значною мірою залежить від досвіду та кваліфікації оператора, який виконує тестування. Навіть найбільш функціональні інструменти можуть бути

неефективними за відсутності належного рівня розуміння методології та практичних аспектів кібербезпеки.

Роль експерта у налаштуванні інструментів. Перед запуском тестування оператору необхідно налаштувати параметри інструмента відповідно до специфіки цільової системи. Наприклад, для коректної роботи Nessus або Acunetix важливо визначити обсяги сканування, виключення, специфічні для системи, та налаштувати відповідні політики. Невірне налаштування може призвести до неповного аналізу або великої кількості хибнопозитивних результатів.

Аналіз отриманих результатів також потребує глибоких знань. Інструменти автоматизованого тестування можуть надавати великі обсяги даних, які потребують правильної інтерпретації. Експерт повинен відрізняти реальні вразливості від хибнопозитивних спрацювань і розставляти пріоритети для їхнього усунення залежно від рівня критичності загроз.

Комбінація з ручним тестуванням. Висококваліфікований оператор здатний доповнювати автоматизоване тестування ручним аналізом, особливо у випадках складних логічних або бізнес-логічних вразливостей, які часто залишаються поза увагою автоматизованих інструментів. Це дозволяє досягти глибшого розуміння та підвищити ефективність тестування.

Досвідченість оператора є ключовим фактором у забезпеченні якісного тестування на проникнення. Високий рівень експертних знань дозволяє оптимально використовувати можливості автоматизованих інструментів, підвищуючи загальну ефективність процесу забезпечення кібербезпеки.

Використання автоматизованих інструментів тестування на проникнення у малих організаціях з обмеженими ресурсами має свої особливості, які визначають підхід до їхнього впровадження. Основними викликами для таких організацій є фінансові обмеження, недостатність технічних знань персоналу та відсутність виділених команд кібербезпеки.

Фінансові обмеження є одним із ключових факторів, що впливають на вибір інструментів. У малих організаціях перевага часто надається безкоштовним або недорогим Open Source рішенням, таким як OWASP ZAP чи Wapiti. Ці інструменти

дозволяють виконувати базове тестування без значних інвестицій у програмне забезпечення. Проте, організації повинні бути готовими до додаткових витрат на налаштування та підтримку таких інструментів.

Недостатність технічних знань може створювати труднощі у використанні навіть базових функцій автоматизованих інструментів. Для вирішення цієї проблеми важливим є проведення навчання персоналу або залучення зовнішніх експертів. Також варто віддавати перевагу інструментам із простим і зрозумілим інтерфейсом та якісною документацією, як-от Nessus.

Відсутність виділених команд кібербезпеки підкреслює необхідність використання автоматизованих інструментів, які можуть виконувати перевірки з мінімальним втручанням з боку користувача. Інтеграція таких інструментів у бізнес-процеси дозволяє регулярно проводити тестування без суттєвого навантаження на співробітників.

Таким чином, впровадження автоматизованих інструментів у малих організаціях вимагає адаптації до їхніх ресурсних обмежень. Правильний вибір інструментів та раціональний підхід до їхнього використання дозволяють підвищити рівень кібербезпеки навіть у межах обмеженого бюджету.

РОЗДІЛ 3 ПРАКТИЧНЕ ВПРОВАДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ АВТОМАТИЗОВАНИХ ІНСТРУМЕНТІВ

3.1. Вибір цільового середовища та підготовка до тестування

Для практичного тестування автоматизованих інструментів на проникнення важливо забезпечити використання репрезентативного середовища, яке відображає реальні сценарії кіберзагроз. Вибір тестових веб-додатків або їх емуляції залежить від цілей дослідження, рівня складності аналізованих систем та доступних ресурсів.

Тестові веб-додатки слугують ідеальним середовищем для оцінки можливостей інструментів. Вони містять заздалегідь інтегровані вразливості, які дозволяють оцінити здатність інструмента ідентифікувати різні типи загроз. Популярні платформи, такі як OWASP Juice Shop, Damn Vulnerable Web Application (DVWA) або Mutillidae, широко використовуються у навчальних і дослідницьких цілях. Ці додатки охоплюють широкий спектр уразливостей, від SQL-ін’єкцій до міжсайтового сценарію (XSS), що дозволяє комплексно оцінити функціональність інструментів. [13]

Емуляція середовища є доцільною, якщо дослідження потребує моделювання специфічних архітектур або бізнес-логіки, які не завжди доступні в стандартних тестових додатках. Використання інструментів для створення емуляцій, таких як Docker чи Kubernetes, дозволяє створювати динамічні середовища з кастомізованими налаштуваннями.

Обґрунтований вибір середовища тестування має базуватися на специфіці досліджуваних інструментів. Наприклад, для перевірки веб-сканерів, таких як OWASP ZAP чи Burp Suite, доцільно використовувати додатки з інтегрованими вразливостями, тоді як для аналізу мережевих сканерів, таких як Nessus, необхідна імітація складних мережевих топологій.

Для цілей цього дослідження розглядаються найбільш популярні середовища тестування, які зарекомендували себе у сфері кібербезпеки. Зокрема, середовища OWASP Juice Shop, Damn Vulnerable Web Application (DVWA), Mutillidae, bWAPP та WebGoat є визнаними платформами для аналізу вразливостей. Їх вибір обумовлений широким спектром підтримуваних загроз, високим рівнем документації та підтримки спільноти. Популярність цих середовищ підтверджується їхньою активною експлуатацією в освітніх і дослідницьких проєктах, а також їхньою здатністю імітувати реальні загрози для інформаційних систем. Такий підхід забезпечує репрезентативність результатів дослідження та дозволяє провести комплексний аналіз автоматизованих інструментів тестування на проникнення.

Таблиця 3.1 – Список продуктів для проведення перевірок

Середовище тестування	Широкий спектр вразливостей	Простота налаштування	Гнучкість адаптації	Відповідність реальним сценаріям	Документація та підтримка
OWASP Juice Shop	SQLi, XSS, CSRF, баги автентифікації	Висока	Обмежена вбудованими функціями	Середня	Велика спільнота та активне оновлення
Damn Vulnerable Web Application (DVWA)	SQLi, XSS, CSRF, некоректні конфігурації	Висока	Обмежена вбудованими функціями	Середня	Велика спільнота
Mutillidae	SQLi, XSS, слабкі паролі	Середня	Обмежена вбудованими функціями	Середня	Менш популярна
Docker з кастомними додатками	Будь-які вразливості, налаштовані користувачем	Залежить від досвіду	Повна	Висока	Залежить від налаштувань користувача
bWAPP (Buggy Web Application)	SQLi, XSS, слабкі паролі, проблеми з автентифікацією	Середня	Обмежена вбудованими функціями	Середня	Добре документоване

Продовження таблиці 3.1

WebGoat	SQLi, XSS, логічні помилки у бізнес-процесах	Середня	Обмежена вбудованими функціями	Середня	Активно підтримується OWASP

Найкращим вибором для поставленої задачі є OWASP Juice Shop. Це середовище надає широкий спектр вразливостей, а також дозволяє тестувати сценарії аутентифікації. Простота налаштування та велика підтримка спільноти роблять його доступним навіть для користувачів із базовими знаннями. Активна підтримка проекту та актуалізація вразливостей гарантують, що результати тестування будуть максимально відповідати реальним загрозам. Крім того, OWASP Juice Shop має високу якість документації та орієнтований на навчання, що дозволяє дослідникам і тестувальникам ефективно працювати з ним. Варто зазначити що середовище побудоване не на вузькоспеціалізованих чи специфічних технологія а використовує поширені в сьогоденні рішення що дозволяє йому бути більш репрезентативним в цьому плані (див. рисунок 3.1).

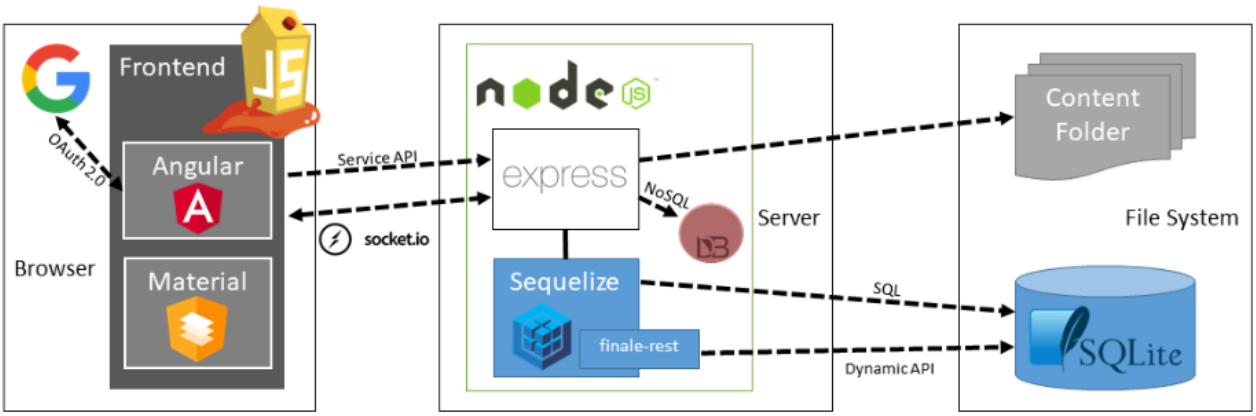

Рисунок 3.1 – Аріхтектура тестового сереодовища

Для проведення тестування на проникнення середовище OWASP Juice Shop, встановлено у Docker-контейнері на віртуальній машині з операційною системою Kali Linux. Це забезпечує ізоляцію тестового середовища та створює реалістичні умови для аналізу вразливостей за допомогою автоматизованих інструментів.

Віртуальна машина Kali Linux розгорнута за допомогою платформи VMware Workstation. Мережеві налаштування встановлені у режимі "Host-Only", що забезпечує обмежений доступ до зовнішніх мережевих ресурсів та підвищує безпеку під час тестування [14]. Kali Linux обрана через її передвстановлені інструменти для аналізу безпеки та сумісність із Docker [15].

Docker встановлений із офіційного репозиторію, що гарантує актуальність програмного забезпечення. OWASP Juice Shop розгорнуто за допомогою стандартної Docker-команди docker run, що дозволяє швидко створити середовище з базовими налаштуваннями. Контейнер надає всі необхідні компоненти для проведення тестування, включаючи доступ до вбудованих уразливостей.

Використання режиму "Host-Only" у VMware Workstation дозволяє ізолювати тестове середовище від зовнішніх мереж, зберігаючи доступність для локальних інструментів тестування. Це підходить для забезпечення конфіденційності даних тестування та запобігання потенційним впливам на інші системи.

Одним із ключових етапів підготовки до тестування є перевірка коректності та репрезентативності обраних тестових цілей. У контексті даного дослідження таким середовищем є OWASP Juice Shop.

Перед початком тестування було виконано базові тести для підтвердження коректної роботи середовища. Це включало запуск контейнера, доступ до веб-інтерфейсу Juice Shop через локальну мережу та перевірку функціональності вбудованих уразливостей. Наприклад, було перевірено, чи доступні для тестування типові сценарії SQL-ін’єкцій та міжсайтового сценарію (XSS). Усі перевірки підтвердили стабільну роботу середовища та його готовність до подальшого використання.

OWASP Juice Shop обраний через його здатність імітувати реальні сценарії атак на веб-додатки. Середовище включає широкий спектр вразливостей, що дозволяє перевірити функціонал автоматизованих інструментів тестування на різних рівнях: від базового аналізу до виявлення складних загроз. Крім того, активна підтримка проекту та відповідність сучасним стандартам безпеки (OWASP Top 10) забезпечують актуальність тестових сценаріїв.

3.2. Запуск автоматизованих сканерів на обраних цілях та збір результатів

Для ефективного проведення тестування автоматизованих інструментів на проникнення було розгорнуто тестове середовище на віртуальній машині Kali Linux, яка забезпечує необхідну ізоляцію та безпеку для аналізу. Обрані сканери, зокрема OWASP ZAP, Acunetix , Nessus та Burp Suite версії яких можна побачити на таблиці нижче.

Таблиця 3.2 – Список версій використаних сканерів

Назва	Версія	Дата релізу
Acunetix	24.10.24	2024-10-07
Burp Suite Professional	2024.11.2	2024-12-19
Nessus Professional	10.8.3	2024-09-11
OWASP ZAP	2.15.0	2024-05-07

Результати сканерів автоматизованого тестування на проникнення.

OWASP ZAP, інструмент виявив кілька серйозних вразливостей, серед яких SQL-ін’єкції, відсутність заголовків CSP (Content Security Policy), міждоменні неправильні конфігурації та розголошення приватних IP-адрес. OWASP ZAP показав високий рівень деталізації результатів, надавши чіткі рекомендації щодо усунення знайдених загроз. Незважаючи на кілька хибнопозитивних спрацювань, таких як виявлення метаданих хмари, загальна продуктивність і точність були на високому рівні.

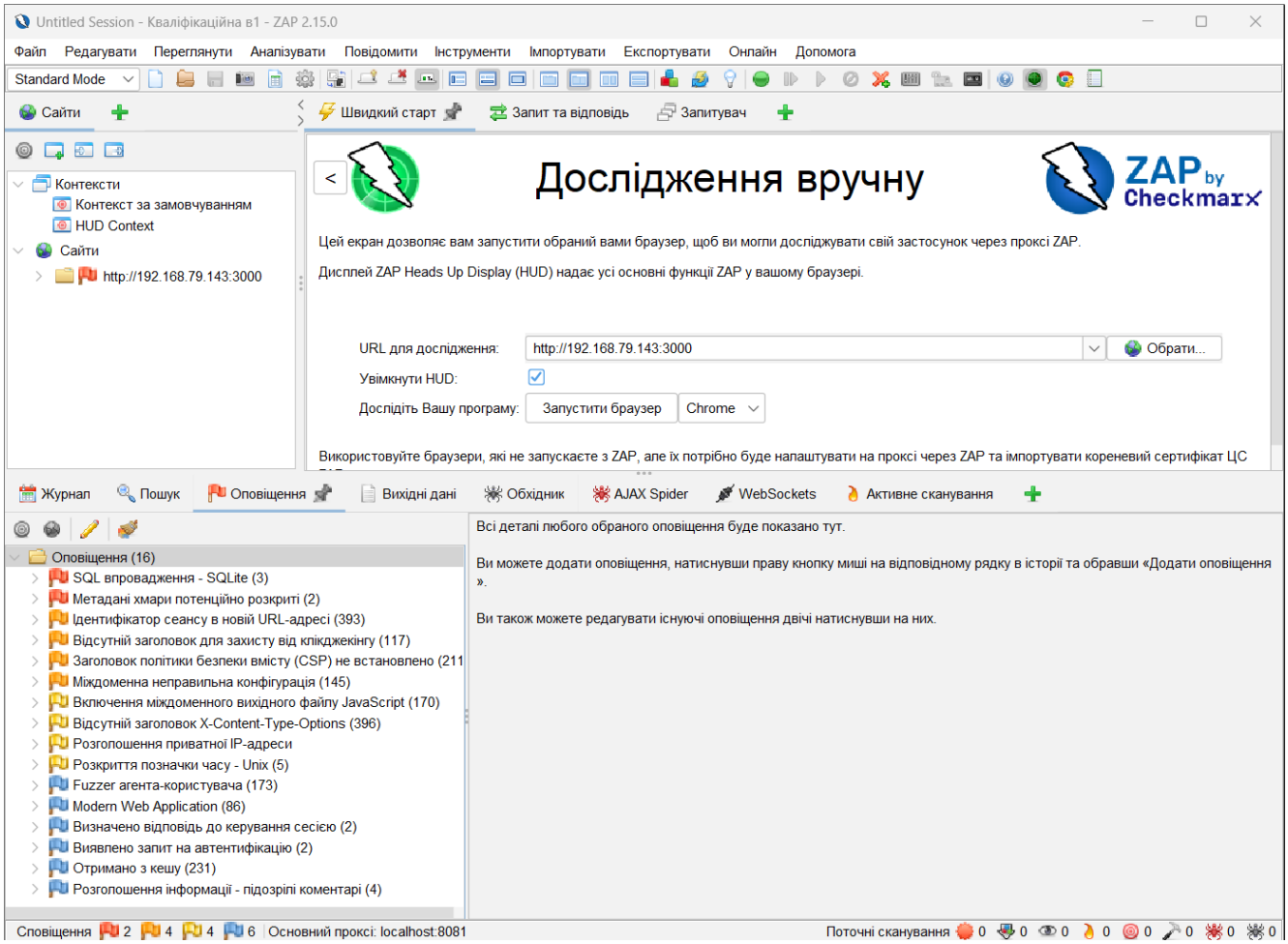

Рисунок 3.2 – Скріншот результату сканування OWASP ZAP 2.15.0

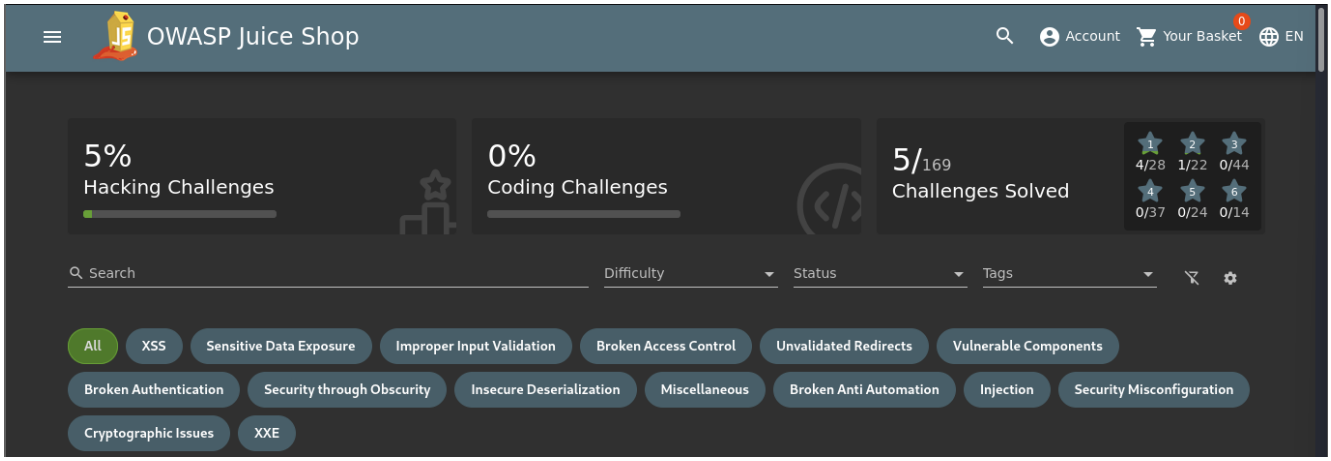

Рисунок 3.3 – Автоматичне виявлення знайдених вразливостей OWASP ZAP

Таблиця 3.3 – Список знайдених вразливостей OWASP ZAP 2.15.0

№	Severity	Vulnerability	Validity
1	High	SQL впровадження - SQLite	Valid

Продовження таблиці 3.3

2	High	Метадані хмари потенційно розкриті	False positives
3	Medium	Ідентифікатор сеансу в новій URL-адресі	Valid
4	Medium	Відсутній заголовок для захисту від клікджекінгу	Valid
5	Medium	Заголовок політики безпеки вмісту (CSP) не встановлено	Valid
6	Medium	Міждоменна неправильна конфігурація	Valid
7	Low	Включення міждоменного вихідного файлу JavaScript	Valid
8	Low	Відсутній заголовок X-Content-Type-Options	Valid
9	Low	Розголошення приватної IP-адреси	False positives
10	Low	Розкриття позначки часу - Unix	Valid
11	Info	Fuzzer агента-користувача	Valid
12	Info	Modern Web Application	Valid
13	Info	Визначено відповідь до керування сесією	Valid
14	Info	Виявлено запит на автентифікацію	Valid
15	Info	Отримано з кешу	Valid
16	Info	Розголошення інформації - підозрілі коментарі	Valid

Nessus, основний акцент зробив на мережевих вразливостях, таких як дозволені методи HTTP, відсутність або слабкі CSP-заголовки, а також ідентифікація відкритих служб. Інструмент надав детальну карту мережевих компонентів і їхніх характеристик, забезпечуючи широке охоплення. Виявлені вразливості переважно мали інформаційний характер, однак Nessus відзначився точністю та стабільністю результатів.

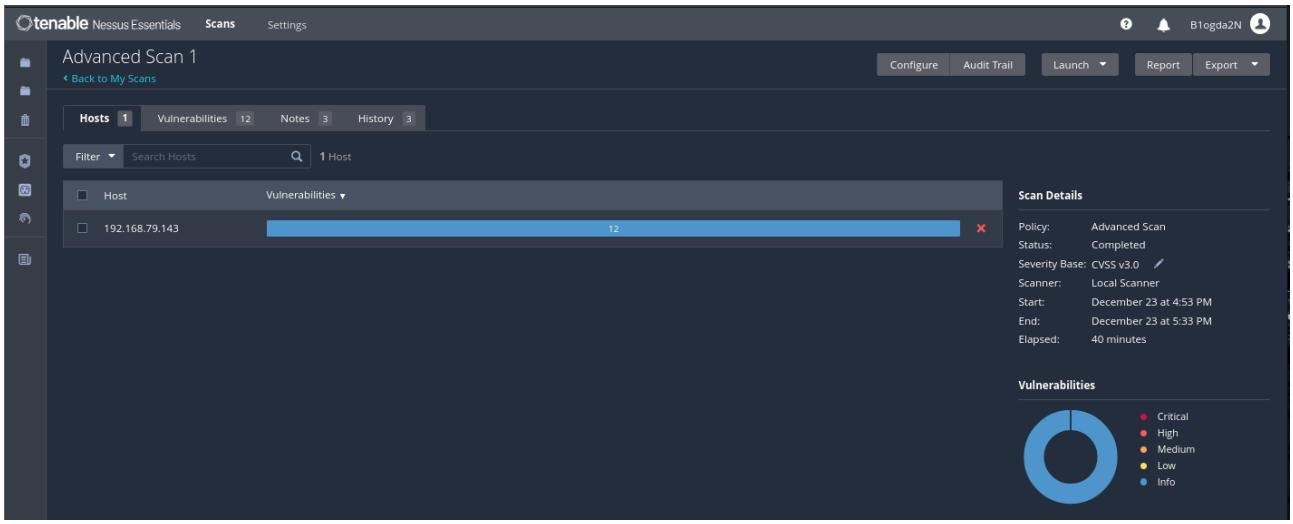

Рисунок 3.4 – Скріншот результату сканування Nessus Professional 10.8.3

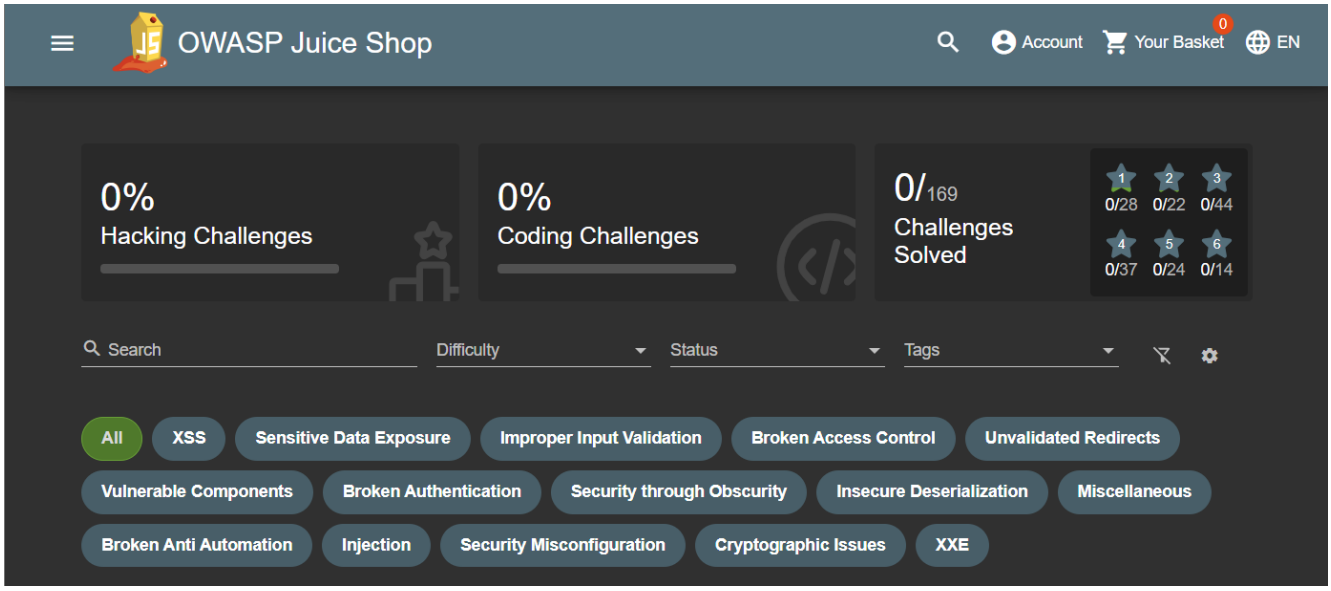

Рисунок 3.5 – Автоматичне виявлення знайдених вразливостей Nessus

Таблиця 3.4 – Список знайдених вразливостей Nessus Professional 10.8.3

№	Severity	Vulnerability	Validity
1	Info	Common Platform Enumeration (CPE)	Valid
2	Info	Device Type	Valid
3	Info	External URLs	Valid
4	Info	HTTP Methods Allowed (per directory)	Valid
5	Info	HyperText Transfer Protocol (HTTP) Information	Valid
6	Info	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	Valid
7	Info	Nessus TCP scanner	Valid
8	Info	OS Identification	Valid
9	Info	Service Detection	Valid
10	Info	Web Application Sitemap	Valid
11	Info	Web Server No 404 Error Code Check	Valid
12	Info	Web Server robots.txt Information Disclosure	Valid

Acunetix, сканер виявив критичні SQL-ін’єкції, проблеми з безпекою API, а також численні XSS-загрози. Особливу увагу Acunetix приділив вразливим JavaScript-бібліотекам та неправильній конфігурації TLS/SSL. Надані результати містили глибокий аналіз знайдених загроз і рекомендації щодо їх усунення. Acunetix також виділявся високою швидкістю сканування.

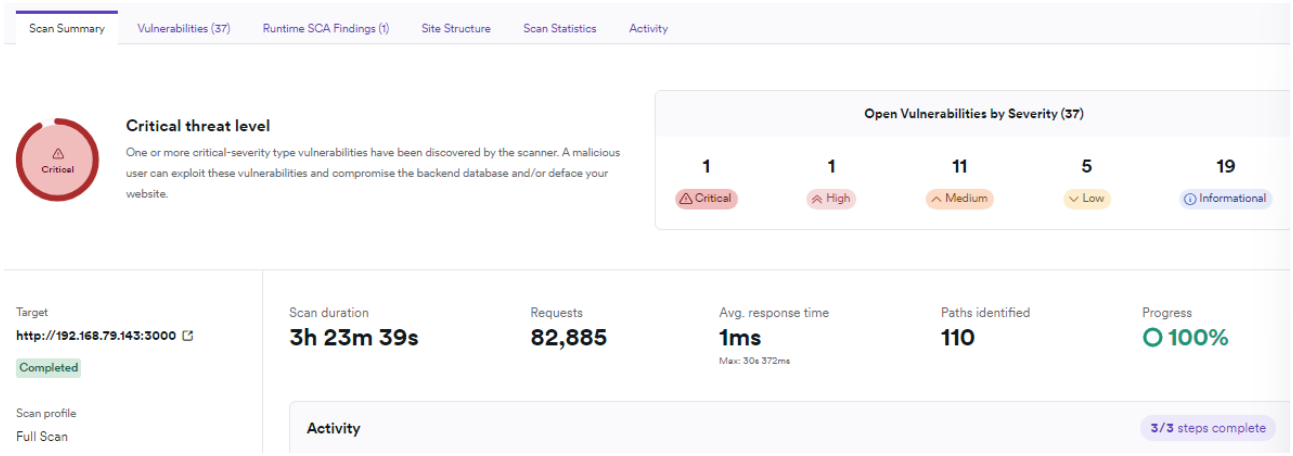

Рисунок. 3.6 – Скріншот результату сканування Acunetix 24.10.24

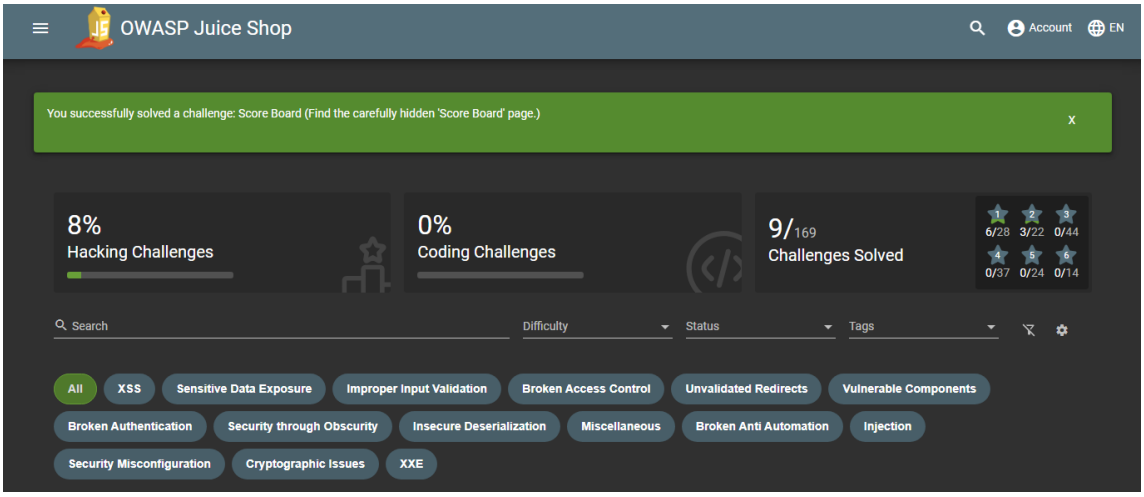

Рисунок 3.7 – Автоматичне виявлення знайдених вразливостей Acunetix

Таблиця 3.5 – Список знайдених вразливостей Acunetix 24.10.24

№	Severity	Vulnerability	Validity
1	Critical	SQL Injection	Valid
2	High	API Sensitive Info(PII) accessible without authentication	Valid
3	Medium	Insecure HTTP Usage	Valid
4	Medium	jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability	Valid
5	Medium	jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability	Valid

Продовження таблиці 3.5

6	Medium	jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability	Valid
7	Medium	jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability	Valid
8	Medium	jQuery Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability	Valid
9	Medium	Password found in server response	Valid
10	Medium	SSL/TLS Not Implemented	Valid
11	Medium	URL redirection (Web Server)	Valid
12	Medium	Vulnerable JavaScript libraries	Valid
13	Medium	Vulnerable JavaScript libraries	Valid
14	Low	[Possible] Internal IP Address Disclosure	False positives
15	Low	Clickjacking: CSP frame-ancestors missing	Valid
16	Low	Cookies Not Marked as HttpOnly	Valid
17	Low	Cookies with missing, inconsistent or contradictory properties	Valid
18	Low	Unrestricted access to Prometheus Metrics	Valid
19	Info	(Possible) Cross site scripting	Valid
20	Info	(Possible) Cross site scripting	Valid
21	Info	(Possible) Cross site scripting	Valid
22	Info	(Possible) Cross site scripting	Valid
23	Info	(Possible) Cross site scripting	Valid
24	Info	(Possible) Cross site scripting	Valid
25	Info	(Possible) Cross site scripting	Valid
26	Info	(Possible) Cross site scripting	Valid
27	Info	(Possible) Cross site scripting	Valid

Продовження таблиці 3.5

28	Info	(Possible) Cross site scripting	Valid
29	Info	(Possible) Cross site scripting	Valid
30	Info	Access-Control-Allow-Origin header with wildcard (*) value	Valid
31	Info	An Unsafe Content Security Policy (CSP) Directive in Use	Valid
32	Info	Content Security Policy (CSP) Not Implemented	Valid
33	Info	File Upload Functionality Detected	Valid
34	Info	Generic Email Address Disclosure	Valid
35	Info	Missing object-src in CSP Declaration	Valid
36	Info	Permissions-Policy header not implemented	Valid
37	Info	Subresource Integrity (SRI) Not Implemented	Valid

Burp Suite, інструмент виявив низькорівневі вразливості, такі як незашифровані комунікації, небезпечні JavaScript-залежності та відсутність безпечних налаштувань CORS. Burp Suite продемонстрував високу точність у виявленні проблем, пов’язаних із клієнтською стороною, та виділявся зручністю інтерфейсу для ручного дослідження додаткових аспектів безпеки.

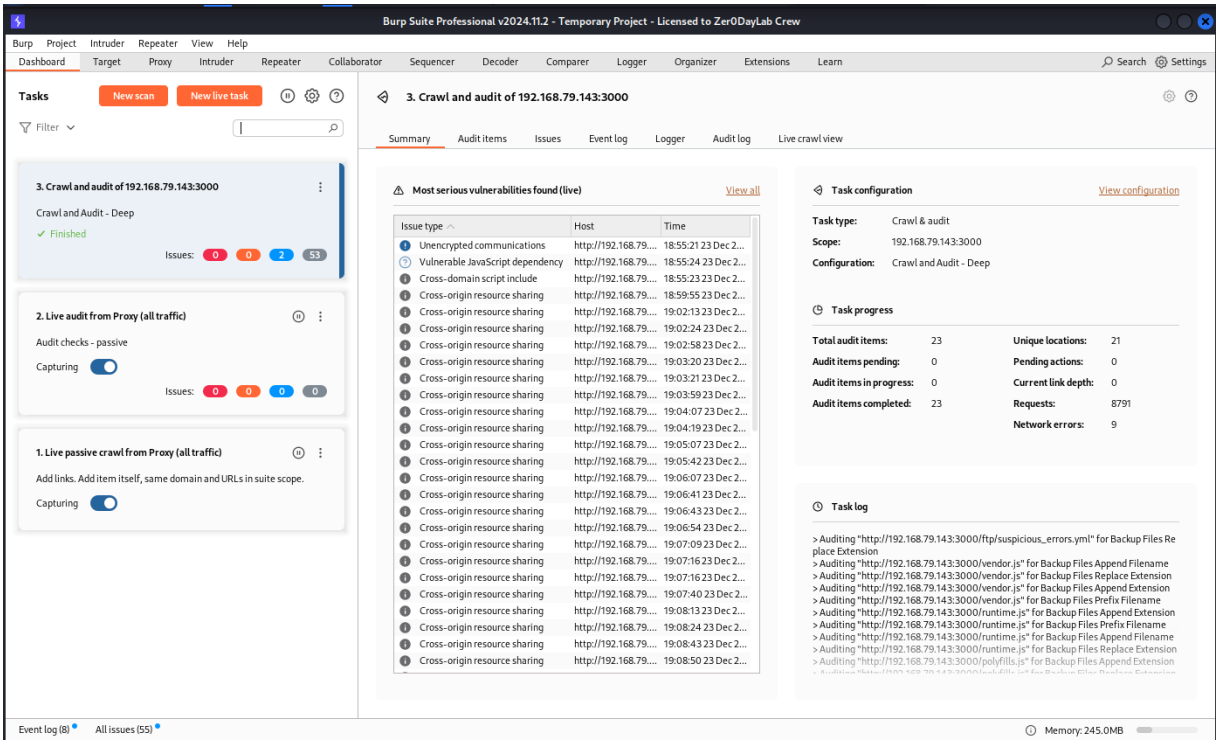

Рисунок 3.8 – Скріншот результату сканування Burp Suite Professional 2024.11.2

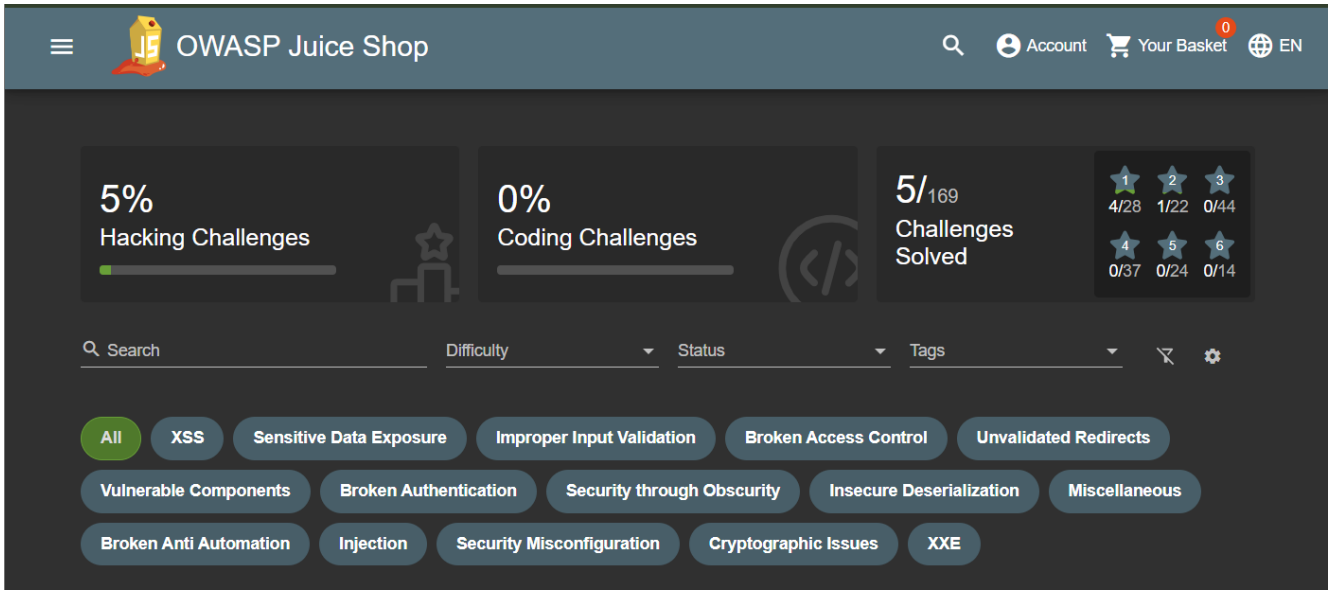

Рисунок 3.9 – Автоматичне виявлення знайдених вразливостей Burp Suite

Таблиця 3.6 – Список знайдених вразливостей Burp Suite Professional 2024.11.2

№	Severity	Vulnerability	Validity
1	Low	Unencrypted communications	Valid

Продовження таблиці 3.6

2	Low	Vulnerable JavaScript dependency	Valid
3	Info	Cross-origin resource sharing	False positives
4	Info	Cross-origin resource sharing: arbitrary origin trusted	Valid
5	Info	Input returned in response (reflected)	Valid
6	Info	Cross-domain script include	Valid
7	Info	Robots.txt file	Valid
8	Info	OpenAPI definition found (active scan check)	Valid
9	Info	Path-relative style sheet import	Valid

Для підтвердження надійності результатів сканування та забезпечення відтворюваності експерименту кожен сканер було запущено двічі. Це дозволило перевірити, чи результати залишаються стабільними за однакових умов тестування.

Всі інструменти — OWASP ZAP, Nessus, Acunetix та Burp Suite — працювали у контрольованому середовищі з незмінними параметрами конфігурації тестової платформи OWASP Juice Shop. Це забезпечило однакові вхідні дані для кожного циклу тестування.

Усі повторні запуски сканерів продемонстрували ті самі виявлені вразливості, що і під час первинного аналізу. OWASP ZAP знову виявив критичні SQL-ін’єкції та проблеми з CSP, Nessus підтвердив результати картографії мережі, Acunetix виявив XSS-загрози та вразливі JavaScript-бібліотеки, а Burp Suite зазначив низькорівневі загрози, такі як незашифровані комунікації та небезпечні залежності.

Стабільність результатів підтверджує надійність і точність використаних інструментів. Це також підвищує достовірність аналізу та дозволяє покладатися на отримані дані для подальшого дослідження та усунення виявлених вразливостей.

3.3. Аналіз точності, корисності та практичної цінності виявлених вразливостей

Під час тестування автоматизованих інструментів на проникнення важливим етапом є оцінка релевантності виявлених вразливостей. Для цього аналізувалися результати роботи кожного зі сканерів, включаючи OWASP ZAP, Nessus, Acunetix та Burp Suite, з особливим акцентом на хибнопозитиви (false positives).

Найбільшу кількість хибнопозитивів виявлено у результатах OWASP ZAP та Acunetix. Наприклад, OWASP ZAP помилково позначив як вразливість розкриття метаданих хмари, тоді як ця загроза не була актуальною для тестованого середовища. Acunetix також виявив внутрішні IP-адреси як потенційно небезпечні, хоча вони не становили реальної загрози у контрольованому середовищі.

Релевантність дійсних вразливостей. Усі інструменти ідентифікували критичні та високоризикові вразливості, такі як SQL-ін’єкції, міжсайтовий сценарій (XSS), проблеми зі слабкими налаштуваннями CSP та TLS/SSL. Вони підтверджені ручною перевіркою та визнані справжніми. Наприклад, Nessus коректно визначив відсутність захисних заголовків CSP, що може бути використано зловмисниками для атак типу clickjacking.

Для оцінки релевантності всі знайдені вразливості було проаналізовано вручну. Це включало перевірку їхньої експлуатаційності, актуальності для середовища OWASP Juice Shop та можливого впливу на безпеку системи. Ручний аналіз підтвердив більшість знайдених вразливостей, за винятком кількох хибнопозитивів.

Оцінка релевантності знайдених проблем показала, що автоматизовані інструменти здатні забезпечувати високу точність у виявленні реальних загроз. Проте наявність хибнопозитивів підкреслює необхідність ручного аналізу результатів, що є важливим для досягнення максимальної достовірності тестування. Цей підхід дозволяє не лише виключити помилкові вразливості, але й надати більш цілісний погляд на стан безпеки системи.

Таблиця 3.7 – Кількість знайдених вразливостей кожним із сканерів

Назва	Версія	Critical	High	Medium	Low	Info
Acunetix	24.10.24	1	1	11	5	19
Burp Suite Professional	2024.11.2				2	7
Nessus Professional	10.8.3					12
OWASP ZAP	2.15.0		2	4	4	5

Таблиця 3.8 – Відсоток False positives у кожному із сканерів

Назва	Кількість знахідок	Кількість False positives	False positives %
Acunetix	37	1	2.7%
Burp Suite Professional	9	1	11.1%
Nessus Professional	12	0	0%
OWASP ZAP	16	2	12.5%

Таблиця 3.9 – Відсоток виявлених вразливостей у середовищі.

Назва	Кількість знахідок	Виявлених підтверджених вразливостей%
Acunetix	9\169	5.32%
Burp Suite Professional	5\169	2.95%
Nessus Professional	0\169	0%
OWASP ZAP	5\169	2.95%

Отримані результати демонструють, що Acunetix виявився найбільш точним та продуктивним серед досліджуваних інструментів. Незважаючи на наявність одного хибнопозитиву, його рівень підтвердження вразливостей сервісом склав 5,32%, що

є найвищим серед сканерів. Acunetix знайшов найбільшу кількість критичних та високо-ризикових вразливостей, а також забезпечив детальні звіти щодо виявлених недоліків безпеки.

Хоча Nessus не мав жодного хибнопозитиву, його інформаційні сповіщення мали обмежену цінність для практичного аналізу. Більшість знайдених недоліків належали до низькорівневих або інформаційних категорій, що не завжди є критично важливими для забезпечення безпеки системи. Відсутність виявлених критичних вразливостей ставить під сумнів його ефективність у контексті досліджуваних сценаріїв.

Наступними за продуктивністю виявилися Burp Suite та OWASP ZAP, які виявили однакову кількість підтверджених вразливостей (2,95%). Проте OWASP ZAP надав більше сповіщень про можливі недоліки безпеки, що свідчить про його ширше охоплення аналізу. Водночас Burp Suite продемонстрував вищу точність, оскільки частка хибнопозитивів у нього склала 11,1%, у той час як в OWASP ZAP цей показник був значно вищим (12,5%).

Окремо варто зазначити, що кількість сповіщень сканера, яка перевищує кількість підтверджених сервісом вразливостей, не завжди свідчить про хибнопозитиви. Багато з таких сповіщень вказують на недостатню захищеність або потенційні ризики, які не можна ігнорувати.

Таким чином, Acunetix виявився лідером у виявленні вразливостей завдяки своїй точності та продуктивності. Nessus, незважаючи на відсутність хибнопозитивів, мав обмежену ефективність, а Burp Suite і OWASP ZAP забезпечили збалансований підхід до аналізу безпеки.

3.4. Формування рекомендацій для підвищення безпеки та оптимізації вибору інструментів

На основі отриманих результатів можна зробити висновок, що продуктивність і точність автоматизованих інструментів тестування на проникнення суттєво відрізняються залежно від їхньої спеціалізації та підходу до виявлення

вразливостей. У контексті дослідження було розглянуто чотири сканери: Acunetix, Burp Suite, Nessus та OWASP ZAP, кожен із яких продемонстрував свої сильні сторони та обмеження.

Acunetix підтвердив свою ефективність як один із найбільш продуктивних інструментів, з найвищим відсотком підтверджених сервісом вразливостей (5,32%). Сканер продемонстрував високу точність у виявленні критичних і високоризикових вразливостей, зокрема SQL-ін'єкцій та міжсайтових сценаріїв (XSS). Незначний рівень хибнопозитивів (2,7%) свідчить про його надійність у контексті автоматизованого тестування.

Burp Suite та OWASP ZAP показали себе як універсальні інструменти з різними акцентами. Burp Suite забезпечив точніші результати з меншим відсотком хибнопозитивів (11,1%), тоді як OWASP ZAP охопив ширший спектр вразливостей, але мав вищий відсоток хибнопозитивів (12,5%). Обидва інструменти добре впоралися з аналізом клієнтських і серверних вразливостей, але поступаються Acunetix за рівнем підтверджених сервісом загроз.

Nessus виявився найстабільнішим інструментом без хибнопозитивів, однак його основна увага була зосереджена на мережевих і інформаційних сповіщеннях. Це обмежує його ефективність для аналізу складних веб-додатків, де важливе виявлення бізнес-логічних вразливостей.

Загалом, точність та продуктивність інструментів залежать від їхньої орієнтації на певні типи загроз. У даному дослідженні найкращим вибором для тестування веб-додатків виявився Acunetix завдяки збалансованому підходу до точності, продуктивності та низькому рівню хибнопозитивів. Інші інструменти можуть використовуватися як доповнення для отримання більш цілісної картини безпеки.

Результати аналізу роботи автоматизованих інструментів тестування на проникнення дозволяють зробити висновки щодо їхньої відповідності специфіці поставлених завдань. Для цього оцінювалися такі аспекти, як здатність виявляти критичні вразливості, кількість хибнопозитивів та продуктивність під час тестування веб-додатків у середовищі OWASP Juice Shop.

Acunetix найкраще відповідає завданням тестування складних веб-додатків, демонструючи високий рівень підтверджених вразливостей (5,32%) і низький відсоток хибнопозитивів (2,7%). Його здатність ідентифікувати критичні загрози, зокрема SQL-ін’єкції та міжсайтові сценарії (XSS), підтверджує його ефективність у забезпеченні глибокого аналізу безпеки веб-додатків. Крім того, розширені звіти та рекомендації сприяють оперативному усуненню знайдених проблем.

Burp Suite і OWASP ZAP мають сильні сторони у виявленні клієнтських та серверних вразливостей, проте їх точність і продуктивність відрізняються. Burp Suite демонструє менший відсоток хибнопозитивів (11,1%), що робить його більш відповідним для завдань, де важлива точність. Натомість OWASP ZAP забезпечує ширше охоплення можливих загроз, але має вищий відсоток хибнопозитивів (12,5%). Ці інструменти ефективні для доповнення результатів Acunetix, особливо при перевірці специфічних аспектів безпеки.

Nessus, хоча й забезпечує стабільність і відсутність хибнопозитивів, обмежений у виявленні складних вразливостей веб-додатків. Його фокус на мережевих вразливостях та інформаційних сповіщеннях робить його менш придатним для вирішення поставлених завдань.

Acunetix є найкращим вибором для проведення всебічного тестування веб-додатків завдяки високій точності та здатності ідентифікувати критичні загрози. Burp Suite та OWASP ZAP доповнюють цей інструмент, дозволяючи забезпечити більш комплексний підхід до тестування, тоді як Nessus може бути корисним для мережевих перевірок. Такий комбінований підхід дозволяє максимально адаптувати тестування до специфіки завдань.

Результати аналізу роботи автоматизованих інструментів тестування на проникнення дозволяють зробити висновки щодо їхньої відповідності специфіці поставлених завдань. Для цього оцінювалися такі аспекти, як здатність виявляти критичні вразливості, кількість хибнопозитивів та продуктивність під час тестування веб-додатків у середовищі OWASP Juice Shop.

Acunetix найкраще відповідає завданням тестування складних веб-додатків, демонструючи високий рівень підтверджених вразливостей (5,32%) і низький

відсоток хибнопозитивів (2,7%). Його здатність ідентифікувати критичні загрози, зокрема SQL-ін’єкції та міжсайтові сценарії (XSS), підтверджує його ефективність у забезпеченні глибокого аналізу безпеки веб-додатків. Крім того, розширені звіти та рекомендації сприяють оперативному усуненню знайдених проблем.

Burp Suite і OWASP ZAP мають сильні сторони у виявленні клієнтських та серверних вразливостей, проте їх точність і продуктивність відрізняються. Burp Suite демонструє менший відсоток хибнопозитивів (11,1%), що робить його більш відповідним для завдань, де важлива точність. Натомість OWASP ZAP забезпечує ширше охоплення можливих загроз, але має вищий відсоток хибнопозитивів (12,5%). Ці інструменти ефективні для доповнення результатів Acunetix, особливо при перевірці специфічних аспектів безпеки.

Nessus, хоча й забезпечує стабільність і відсутність хибнопозитивів, обмежений у виявленні складних вразливостей веб-додатків. Його фокус на мережевих вразливостях та інформаційних сповіщеннях робить його менш придатним для вирішення поставлених завдань.

Таблиця 3.10 – Відсоток виявлених вразливостей у середовищі.

Назва	Кількість знахідок	False positives	Відсоток виявлення вразливостей	Ціна
Acunetix	37	2.7%	5.32%	Вартість 1-річної ліцензії становить $1000
Burp Suite Professional	9	11.1%	2.95%	$449 за одного користувача
Nessus Professional	12	0%	0%	Вартість 1-річної ліцензії становить $3,990

Продовження таблиці 3.10

OWASP ZAP	16	12.5%	2.95%	Безкоштовний

Загалом, Acunetix є найкращим вибором для проведення всебічного тестування веб-додатків завдяки високій точності та здатності ідентифікувати критичні загрози. Burp Suite та OWASP ZAP доповнюють цей інструмент, дозволяючи забезпечити більш комплексний підхід до тестування, тоді як Nessus може бути корисним для мережевих перевірок. Такий комбінований підхід дозволяє максимально адаптувати тестування до специфіки завдань.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Сучасний розвиток технологій і автоматизація виробничих процесів забезпечують підвищення ефективності роботи підприємств. Комп'ютерна техніка є невід'ємною складовою господарської діяльності, проте її масове використання висуває низку вимог до охорони праці. Законодавство України встановлює норми безпеки для працівників, які працюють із комп'ютерними пристроями, з метою забезпечення їхнього здоров'я та комфорту [16].

Згідно з нормативними актами України з охорони праці (НПАОП 0.00-7.15-18), на робочі місця працівників з електронними пристроями поширюються такі вимоги:

1. Площа робочого місця. На одне робоче місце має припадати не менше 6 кв. м, а об'єм приміщення повинен становити не менше 20 куб. м [17].
2. Ергономіка робочого місця. Конструкція має забезпечувати підтримання оптимальної пози працівника, знижуючи фізичне навантаження та перевтому.
3. Рівень випромінювання. Випромінювання від екранних пристроїв повинно бути зведене до гранично допустимих рівнів для мінімізації впливу на здоров'я [17].
4. Ергономічність організації простору. Усі елементи робочого місця мають відповідати антропологічним, психофізіологічним і ергономічним вимогам [18].
5. Освітлення. Освітлення робочого місця повинно забезпечувати належний контраст між екраном і навколишнім середовищем відповідно до вимог ДСанПіН.
6. Мікроклімат приміщень. Температурний режим, вологість і чистота повітря повинні відповідати вимогам ДСН 3.3.6.042-99, затвердженим головним державним санітарним лікарем [19].

Приміщення, в яких встановлюються комп’ютери, мають відповідати проектній документації, затвердженій державними органами. Враховуються:

1. Санітарні норми освітлення.
2. Параметри мікроклімату (температура, вологість).
3. Рівень шуму, вібрації та інших фізичних факторів.
4. Безпека щодо електромагнітних, ультрафіолетових і інфрачервоних полів.

Робочі місця не допускається облаштовувати у підвальних або цокольних приміщеннях. Заборонено використовувати матеріали, що виділяють шкідливі хімічні речовини [17].

Згідно з ДБН В.2.5-28:2018 "Природне і штучне освітлення", приміщення з постійним перебуванням людей мають бути забезпечені природним освітленням. Для штучного освітлення рекомендується використовувати енергоефективні джерела світла, такі як світлодіодні лампи.

Працівники зобов’язані проходити інструктажі з охорони праці, які включають навчання надання першої допомоги та дій у разі аварійних ситуацій. Інструктажі поділяються на такі види:

1. Вступний. Проводиться з усіма новими працівниками, а також із працівниками сторонніх організацій, які беруть участь у виробничому процесі.
2. Первинний. Здійснюється безпосередньо перед початком роботи на новому місці.
3. Повторний. Проводиться регулярно, з урахуванням умов праці (не рідше одного разу на 6 місяців).
4. Позаплановий. Організовується у разі змін у нормативно-правових актах, після аварій або порушень правил безпеки.
5. Цільовий. Проводиться перед виконанням робіт із підвищеною небезпекою або в умовах надзвичайних ситуацій.

Дотримання вимог охорони праці забезпечує не лише безпеку працівників, але й підвищує ефективність виробничих процесів.

4.2 Фактори ризику та можливі порушення здоров’я користувачів комп’ютерної мережі

Комп’ютерні мережі є невід’ємною частиною сучасного життя, забезпечуючи ефективність роботи у різних галузях. Однак, тривала взаємодія з інформаційно-комунікаційними технологіями (ІКТ) може негативно впливати на здоров’я користувачів. У цьому розділі розглянуто основні фактори ризику, пов’язані з використанням комп’ютерних мереж, їх можливі наслідки для здоров’я, а також надано рекомендації щодо зменшення таких ризиків.

Основні фактори ризику:

1. Фізіологічні фактори:
    1) Сидячий спосіб життя:
        - Тривале перебування у фіксованій позі викликає м’язову напругу, біль у спині, шиї та плечах. [20]
        - Порушення кровообігу, ризик варикозу та інших судинних патологій. [20]
    2) Напруження зору:
        - Постійна робота з моніторами спричиняє синдром комп’ютерного зору: сухість очей, порушення фокусування, головний біль. [21]
        - Неправильна освітленість робочого місця посилює навантаження на очі. [21]
    3) Шумове забруднення:
        - Постійний фоновий шум від комп’ютерного обладнання може викликати стрес і знижувати продуктивність.
2. Психоемоційні фактори:
    1) Психологічне перевантаження:
        - Надмірне використання комп’ютера спричиняє емоційне вигорання.

- Часті технічні проблеми підвищують рівень стресу.

2) Соціальна ізоляція:
    - Зниження міжособистісного спілкування через надмірне перебування онлайн.

3. Ергономічні фактори:
    1) Неправильне робоче місце:
        - Недостатня висота стільця, неправильний нахил монітора та відсутність підставки для ніг створюють додаткове навантаження на опорно-руховий апарат. [20]
    2) Погане освітлення:
        - Надмірно яскраве або тьмяне світло спричиняє перевтому зору. [21]

Можливі порушення здоров’я:

1. Порушення зору
    - Синдром сухого ока.
    - Прогресування міопії.
2. Захворювання опорно-рухового апарату
    - Остеохондроз.
    - Синдром карпального каналу (пов’язаний із тривалою роботою мишкою та клавіатурою).
3. Психологічні розлади
    - Хронічний стрес, тривожність.
    - Порушення сну, спричинені змінами добового ритму через роботу в нічний час.

Рекомендації щодо зменшення ризиків:

1. Організація робочого місця
    1) Використання ергономічних меблів. Обирайте стілець із регульованою висотою, підлокітниками та підтримкою попереку. Робочий стіл повинен бути достатньо широким, щоб розмістити всі необхідні пристрої, не створюючи незручностей. [22]

2) Налаштування монітора: Встановіть монітор так, щоб верхній край екрана був на рівні очей. Відстань між очима та екраном має становити 50-70 см. Використовуйте підставки для монітора за потреби.[22]
3) Освітлення: Забезпечте рівномірне освітлення робочого місця. Уникайте відблисків на екрані, використовуючи штори або антивідблискові фільтри.

2. Дотримання режиму роботи
   1) Перерви кожні 20-30 хвилин: Використовуйте правило 20-20-20: кожні 20 хвилин робіть перерву на 20 секунд, дивлячись на об'єкт на відстані 20 футів (приблизно 6 метрів). Це допомагає розслабити очі та зменшити навантаження. [22]
   2) Регулярна зміна пози: Уникайте тривалого перебування в одній позі. Час від часу вставайте, розминайтеся, щоб покращити кровообіг і знизити м'язову напругу.
3. Вправи для зору та тіла
   1) Гімнастика для очей: Робіть вправи для зняття напруги, наприклад, плавно рухайте очима вліво-вправо, вгору-вниз, а також виконуйте кругові рухи.
   2) Фізичні вправи: Виконуйте розминку для спини, шиї, рук і ніг. Наприклад, нахили голови, обертання плечима, розтяжка рук і ніг. Такі вправи допоможуть уникнути застійних явищ у м'язах і суглобах.
4. Контроль психоемоційного стану
   1) Техніки релаксації: Використовуйте методи, такі як глибоке дихання, медитація або прогресивна м'язова релаксація для зняття стресу.
   2) Планування робочого часу: Визначте чіткі межі між роботою та відпочинком, уникайте багатозадачності та перевантаження.
   3) Зменшення когнітивного навантаження: Організовуйте завдання за пріоритетністю, використовуйте спеціалізовані інструменти для управління часом, щоб уникнути хаосу в роботі.

Фактори ризику, пов’язані з використанням комп’ютерних мереж, суттєво впливають на здоров’я користувачів. Вони включають як фізіологічні, так і психоемоційні аспекти, що вимагають комплексного підходу до їх усунення. Для мінімізації негативних наслідків необхідно дотримуватися низки рекомендацій, які охоплюють організацію робочого місця, раціональний режим роботи, регулярну фізичну активність і підтримку психоемоційного балансу. Зокрема, ефективна ергономіка дозволяє знизити навантаження на опорно-руховий апарат, а перерви та вправи для очей зменшують втому і напруження зору. Крім того, важливо використовувати техніки релаксації для запобігання стресу і організовувати завдання за пріоритетами для уникнення когнітивного перевантаження. Такий інтегрований підхід не лише сприяє збереженню здоров’я користувачів комп’ютерних мереж, але й забезпечує підвищення їхньої продуктивності та загального благополуччя.

ВИСНОВКИ

Рекомендації щодо практичного використання. У рамках практичної реалізації рекомендовано використовувати OWASP ZAP як основний інструмент для виявлення критичних загроз, а Acunetix — для глибокого аналізу середніх за ризиком вразливостей. Burp Suite доцільно застосовувати для деталізації залежностей і конфігураційних проблем, тоді як Nessus буде корисним на початкових етапах картографії системи.

Значення дослідження. Отримані результати підтверджують, що автоматизовані інструменти є важливим елементом забезпечення кібербезпеки. Їх ефективне використання залежить від правильного вибору та налаштування відповідно до конкретних завдань і середовищ тестування. Поєднання кількох інструментів дозволяє досягти балансу між широтою аналізу та глибиною дослідження.

У підсумку, результати роботи є основою для подальших досліджень у сфері автоматизованого тестування на проникнення, а також для практичного впровадження таких інструментів у процеси забезпечення кібербезпеки.

Результати проведеного дослідження дозволяють зробити висновок про ефективність та доцільність використання автоматизованих інструментів тестування на проникнення в залежності від специфіки завдань, які стоять перед організацією, та доступних ресурсів.

OWASP ZAP підтвердив свою роль як найкращого безкоштовного рішення для малих організацій із обмеженим бюджетом. Інструмент надає широкий спектр можливостей для базового тестування, підтримується активною спільнотою та демонструє достатню ефективність у виявленні вразливостей. Незважаючи на вищий відсоток хибнопозитивів, OWASP ZAP є надійним вибором для початкового рівня тестування веб-додатків.

Acunetix показав найвищу продуктивність та точність серед досліджуваних інструментів. Завдяки високому відсотку підтверджених сервісом вразливостей (5,32%) та низькому рівню хибнопозитивів, Acunetix є оптимальним вибором для

організацій, які можуть дозволити собі інвестиції в комерційні інструменти. Це рішення забезпечує всебічний аналіз безпеки та є найбільш ефективним у контексті автоматизованого тестування.

Burp Suite зарекомендував себе як універсальний інструмент для ручного тестування, який особливо підходить для тестувальників на проникнення. Завдяки гнучкості та широкому набору функцій, цей інструмент може доповнювати автоматизовані рішення, такі як Acunetix, для глибшого аналізу складних або специфічних вразливостей.

Nessus, хоч і не продемонстрував високої ефективності у веб-додатках, може бути корисним для аналізу мережевої інфраструктури. Його спеціалізація на мережевих вразливостях робить його менш придатним для аналізу веб-додатків, проте цінним для забезпечення безпеки загальної IT-інфраструктури.

Таким чином, організаціям із обмеженим бюджетом доцільно використовувати OWASP ZAP як базовий інструмент тестування, доповнюючи його іншими рішеннями у разі необхідності. Для організацій із більшими фінансовими ресурсами Acunetix залишається найкращим вибором для забезпечення комплексного підходу до автоматизованого тестування, тоді як Burp Suite може використовуватися для ручного аналізу. Такий комбінований підхід дозволяє максимально ефективно використовувати наявні ресурси та адаптувати методи тестування до потреб кожної організації.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NIST. (n.d.). Technical Guide to Information Security Testing and Assessment (SP 800-115). Retrieved from https://csrc.nist.gov/pubs/sp/800/115/final
2. OWASP. (n.d.). Web Security Testing Guide. Retrieved from https://owasp.org/www-project-web-security-testing-guide/
3. ASMED. (n.d.). Black-Box, Grey-Box, White-Box Testing. Retrieved from https://asmed.com/black-box-grey-box-white-box-testing/
4. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
5. HackYourMom. (n.d.). Сканери для пошуку вразливостей у веб-серверах. Retrieved from https://hackyourmom.com/pryvatnist/skanery-dlya-poshuku-vrazlyvostej-u-veb-serverah/
6. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.
7. Tenable. (n.d.). Nessus. Retrieved from https://www.tenable.com/products/nessus
8. Yesin, V., Karpinski, M., Yesina, M., Vilihura, V., Kozak, R., & Shevchuk, R. (2023). Technique for Searching Data in a Cryptographically Protected SQL Database. Applied Sciences, 13(20), 11525.
9. PortSwigger. (n.d.). Burp Suite Professional. Retrieved from https://portswigger.net/burp
10. Skorenkyy, Y., Zolotyy, R., Fedak, S., Kramar, O., & Kozak, R. (2023, June). Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices. In CITI (pp. 12-23).
11. OWASP. (n.d.). OWASP Benchmark. Retrieved from https://owasp.org/www-project-benchmark/

12. Ревнюк, О. А., Загородна, Н. В., Козак, Р. О., Карпінський, М. П., & Флуд, Л. О. (2024). The improvement of web-application SDL process to prevent Insecure Design vulnerabilities. Прикладні аспекти інформаційних технологій, 7(2), 162-174.
13. Rafed. (n.d.). Vulnerable Applications for Practicing Pentesting. Retrieved from https://rafed.github.io/devra/posts/security/vulnerable-applications-for-practicing-pentesting/
14. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.
15. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.
16. Міністерство соціальної політики України. (2018). Наказ "Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями". Retrieved from https://zakon.rada.gov.ua/laws/show/z0508-18
17. Закон України "Про охорону праці". (1992). Retrieved from https://zakon.rada.gov.ua/laws/show/2694-12
18. Міністерство внутрішніх справ України. (2015). Наказ "Про затвердження Правил пожежної безпеки в Україні". Retrieved from https://zakon.rada.gov.ua/laws/show/z0252-15
19. Державний комітет ядерного регулювання України. (2008). Проект консультацій щодо підвищення безпеки джерел іонізуючого випромінювання в Україні. Київ.
20. ISO. (2010). ISO 9241-210:2010. Ergonomics of human-system interaction — Principles and requirements for designing ergonomic systems.
21. Сидоренко, Є. В. (2019). Основи ергономіки та безпеки життєдіяльності. Київ: Наукова думка.

22. World Health Organization. (2020). Working Safely with Display Screen Equipment. Retrieved from https://www.who.int

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ

2024

УДК 001

66

М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професо**р.**

Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.

Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.

Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень - завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.

Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

М34 Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 25-49-83.
E-mail: conffis2024@gmail.com

Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп'ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

УДК 004.056.53
Слупський Богдан, студент гр. СБм-61, Козак Руслан, к.т.н., доцент
(Тернопільський національний технічний університет імені Івана Пулюя)

ІНСТРУМЕНТИ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЇХ ЕФЕКТИВНІСТЬ

Slupskyi Bohdan, student of gr. СБм-61, Kozak Ruslan, Ph.D., Assoc. Prof.

AUTOMATED PENETRATION TESTING TOOLS AND THEIR EFFECTIVENESS

Автоматизоване тестування на проникнення є складовою комплексного підходу до забезпечення кібербезпеки [1]. Постійне зростання кількості кібератак, швидкий розвиток веб-додатків та динамічні зміни у їх архітектурі та функціоналі вимагають систематичного моніторингу й оперативного виявлення вразливостей. Веб-додатки часто стають ціллю зловмисників через відкритий доступ, розгалужену функціональність і велике коло користувачів. Використання автоматизованих інструментів дає змогу суттєво скоротити час на ідентифікацію вразливих місць, мінімізує вплив людського фактору та підвищує загальну ефективність тестування [2].

У дослідженні розглянуто інструменти автоматизованого тестування на проникнення з акцентом на їхнє застосування до веб-додатків. Проведено оцінку точності виявлення різноманітних типів вразливостей, швидкодії сканування та зручності взаємодії користувача з інструментами. Також проаналізовано можливості інтеграції інструментів у процеси розробки та супроводу програмних продуктів. Враховано потреби малих організацій, для яких питання оптимального вибору інструментів та зниження витрат на спеціалізованих фахівців є особливо актуальним [2], [3].

На основі отриманих даних сформовано практичні рекомендації щодо оптимального вибору засобів автоматизованого тестування відповідно до конкретних вимог та ресурсів організації. Зокрема, визначено, які інструменти здатні найкраще виявляти критичні вразливості веб-додатків, а які забезпечують більш широкий, але менш глибинне ооплення потенційних загроз.

Перспективним напрямом подальших досліджень є удосконалення методик оцінювання ефективності інструментів, застосування штучного інтелекту для інтелектуального аналізу результатів тестування та розробка адаптивних систем автоматизованого тестування, що динамічно адаптуються до особливостей цільових веб-додатків.

Література

1. Guo W., Jin G. Automated Penetration Testing: An Overview. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/325030351_Automated_Penetration_Testing_An_Overview
2. Aloul, F., Al-Azani, S. Adopting Automated Penetration Testing Tools: A Cost-Effective Approach to Enhancing Cybersecurity in Small Organizations. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/381847814_Adopting_Automated_Penetration_Testing_Tools_A_Cost-Effective_Approach_to_Enhancing_Cybersecurity_in_Small_Organizations
3. Shah, M.P. Automated Vulnerability Scanning and Testing. Master Thesis, National College of Ireland, 2019. [Електронний ресурс]. – Режим доступу: https://norma.ncirl.ie/4165/1/mandarprashantshah.pdf