УДК 681.04 DOI: 10.26565/2519-2310-2022-2-05

ПОРІВНЯННЯ КОМЕРЦІЙНИХ СКАНЕРІВ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ ТА СКАНЕРІВ З ВІДКРИТИМ КОДОМ

Лахтін Іван, Дмитро Михайленко, Олексій Нарєжній

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
lakhtin.ivan@gmail.com, xa12850318@student.karazin.ua, o.nariezhnii@karazin.ua

Надійшла: жовтень 2022. Прийнята: листопад 2022.

Анотація: *У роботі порівнюється вісім сканерів вразливостей на основі двох, навмисно вразливих додатків. Порівняння виконується за допомогою п'яти критеріїв: точність, відкликання, розрахунок індекса Юдена, веб-бенчмарк від WASSEC та OWASP. У якості додатків, що тестувалися обрані: OWASP WebGoat та Damn Vulnerable Web Application (DVWA). Серед досліджуваних сканерів є три комерційних сканера: Acunetix, HP WebInspect, AppScan, та п'ять сканерів з відкритим кодом такі, як: Arachni, IronWASP, Skipfish, OWASP ZAP, Vega. За результатами тестування зроблено висновок, що комерційні сканери є більш ефективними по ряду показників (в т.ч. переліку загроз). Деякі сканери з відкритим кодом (наприклад, ZAP та Skipfish) можна визначити, як початково таргетовані на певних видах загроз. Підкреслено, що не існує єдиного сканеру безпеки, який забезпечував би стабільно високі показники виявлення для всіх типів вразливостей. За результатами проведеного огляду стверджується, що існуючи відмінності в частоті хибнопозитивних вразливостей (для обох груп сканерів), обумовлені тим, що більшість комерційних рішень, мають автоматизовані сканери, які виявляються більш ефективнішими, ніж ручне налаштування з боку тестувальника. Вочевидь, що результати ручних налаштувань мають прямий зв'язок з фактичним рівнем компетенцій тестувальника, та в значній мірі обумовлюють кінцеві результати.*

Ключові слова: *веб-додаток; вразливість; атака, сканер; безпека; тестування.*

1. Вступ

Економічна важливість веб-додатків у багатьох сферах, включаючи банківську діяльність, транспорт, промисловість, бізнес та освіту, збільшила потребу в механізмах контролю та підвищення їх якості. Широке використання веб-додатків в усіх галузях сучасної економіки, нажаль, призвело до настільки ж різкого збільшення числа атак. Ці атаки, як правило, спрямовані на «слабкі місця» програмного коду додатків, їх недоліки та помилки, що обумовлює наявність передумов виникнення вразливостей в механізмах забезпечення конфіденційності, цілісності та доступності програмних рішень, що пропонуються [1]. За оцінками спеціалістів з питань інформаційної безпеки (ІБ), щодня атакується більше мільйона веб-сайтів, причому 75% з цих веб-сайтів містять не усунені вразливості [2]. Коли атаки досягають своєї мети, вони можуть призвести до компрометації критичних даних та/або програмно-апаратних ресурсів жертви, та мати інші серйозні наслідки, які можуть поширювати далеко за межи корпоративної інфраструктури компанії (наприклад, створення бот-мережі).

Розробники програмного забезпечення (ПЗ) використовують сканери вразливостей для автоматизації процесу перевірки стану ІБ «своїх» веб-додатків та/або проведення масштабних тестувань поточного стану безпеки багатьох інших відомих веб-додатків [3]. Широке поширення сканерів вразливостей і існуючи відмінності в їх функціональності, щодо виявлення вразливостей, підвищують інтерес відносно оцінки (*тестування*) ефективності їх роботи. Основними цілями подібних тестувань, є оцінка та порівняння продуктивності комерційних сканерів та рішень з відкритим кодом, що дозволяє дослідити реальні показники їх можливостей, стосовно виявлення відомих загроз ІБ. У цій роботі представлені результати порівняльної оцінки деяких функцій безпеки та продуктивності для восьми існуючих інструментів виявлення вразливостей.

На даний час існує достатньо проектів, які спрямовані на вивчення можливостей сканерів вразливостей веб-додатків, це можуть бути інтернет-блоги в сфері IT, або офіційні сайти якогось з інструментів безпеки. Але в цих випадках порівняння сканерів зводиться до пере-

ліку переваг і їх недоліків, короткого опису сканерів та порівняння ціни. Крім того існують більш серйозні - детальні тематичні дослідження, наприклад робота Alsaleh, M. та ін. *«Performance-Based Comparative Assessment of Open Source Web Vulnerability Scanners»* [3], в межах якої автори досліджують 4 сканери безпеки з відкритим кодом, аналізуючи відповідні показники виявлення загроз ІБ. У проекті Chen, S. *«WAVSEP 2017/2018 - Evaluating DAST against PT/SDL Challenges. Security Tools Benchmarking»* [4], розглядається близько двадцяти сканерів вразливостей, серед яких є як комерційні, так сканери з відкритим кодом. Вивчення результатів цих досліджень показує, що більшість з них зосереджені лише на впровадженні SQL та міжсайтовому сценарії атак.

2. Основна частина

2.1 Сканери в дослідженні

Архітектура сканерів вразливостей зазвичай поєднує чотири модулі: механізм сканування, базу даних (БД) сканування, модуль звітів та інтерфейс користувача. Механізм сканування виявляє вразливості безпеки щодо встановлених плагінів і порівнює результат із відомими сигнатурами. У БД сканування зберігається детальна інформація про відомі вразливості. Модуль звіту надає результати сканування з рекомендованими рішеннями для розробників та адміністраторів ІБ. Інтерфейс користувача забезпечує візуалізацію взаємодії користувачів зі сканерами. В межах проведеного оглядового дослідження сканерів розглянуто комбінацію з 8 програмних рішень (*як комерційні, так і з відкритим кодом*), що мають графічний інтерфейс користувача і працюють під управлінням ОС Windows:

1. *Acunetix* – комерційне рішення безпеки, що сканує веб-програми на наявність міжсайтових сценаріїв, ін'єкцій SQL та інших типів вразливостей. Використовує мультіпотоковий скан для безперервного обходу ряду веб-сторінок та створює різні форми відповідності вимогам і технічних звітів [5];
2. *WebInspect* – це комерційний інструмент тестування, який виявляє відомі і невідомі вразливості, включаючи міжсайтові сценарії і обхід каталогів у веб-додатках [6];
3. *AppScan* – це комерційна мережа, яка детектує та виправляє відомі вразливості [7];
4. *ZAP* – сканер з відкритим кодом та зручним інтерфейсом користувача, яке використовується для тестування на проникнення [8];
5. *Skipfish* – засіб з відкритим кодом, що надає інтерактивну мапу сайту для цільового сайту, виконуючи рекурсивний обхід та пошук словника. Створена мапа доповнюється результатами наступних тестувань. Підсумковий звіт, може слугувати основою для професійної оцінки стану безпеки веб-додатків [9];
6. *Arachni* – зручний сканер з відкритим кодом, забезпечує швидке сканування та пропонує різні варіанти інтерфейсу користувача, включаючи вихідні дані які представлені у HTML [10];
7. *Iron WASP* (*Iron Web Application Advanced Security Testing Platform*) – платформа тестування безпеки веб-додатків з відкритим кодом, яка постачається в різних комплектаціях «зовнішніх бібліотек», *IronPython, IronRuby* тощо [11];
8. *Vega* – автоматизований сканер з відкритим кодом для виявлення SQL ін’єкції та інших різновидів вразливостей безпеки [12].

В межах проведеного оглядового дослідження розглянути найбільш поширені сканери з відкритим кодом та комерційні сканери, відповідно до критеріїв консорціуму безпеки вебдодатків (*WASC*). Всі сканери перевірені на 2-х свідомо вразливих проектах *WebGoat* та

DVWA. Результати виявлення та продуктивність порівнювалися з використанням цільових показників (*точність, відкликання, Індекс Юдена, WBE і WASSEC*).

2.2 Показники продуктивності

2.2.1 Точність. OWASP визначає точність [13], як відсоток правильно виявлених вразливостей, як часку всіх зареєстрованих вразливостей (включаючи ті, що невірно позначені). Вираз для цієї метрики наведено нижче (1):

$$P = \frac{TP}{TP+FP} \quad , \tag{1}$$

де: - *TP* (*True Positive*), вірно виявлена вразливість; - *FP* (*False Positive*), хибно класифіковані вразливості.

Значення високої точності вказують на високу точність виявлення реальних вразливостей.

2.2.2 Відкликання. Відкликання – це кількість правильно детектованих вразливостей (R у виразі (2)), представлених, як частка всіх відомих вразливостей (*включаючи ті, що не були виявлені*),

$$R = \frac{TP}{TP+FN} \quad , \tag{2}$$

де: - *FN* (*False Negative*), це невизначена вразливість, яка насправді присутня, але сканер її не «помітив» (не виявив).

2.2.3 Індекс Юдена. Використовується для оцінки ефективності діагностичних тестів (3). Відображає значення в діапазоні [-1, 1], де: - значення «1» (*краще виявлення*) вказує на виявлення всіх вразливостей без помилкових спрацьовувань; - значення «-1» вказує лише на помилкові спрацьовування і відсутність справжніх спрацьовувань (*тобто, фактичні вразливості не виявлені*); - а індекс «0», означає, що отримано однаковий результат для веб-додатку з вразливостями, та для додатку без вразливостей (*тобто, неприпустимий результат*) [15].

$$J = \frac{TP}{TP+FN} + \frac{TN}{TN+FP} - 1 \quad , \tag{3}$$

де: - *TN* (*True Negative*), немає вразливостей, сканер підтверджує, що не виявив жодних.

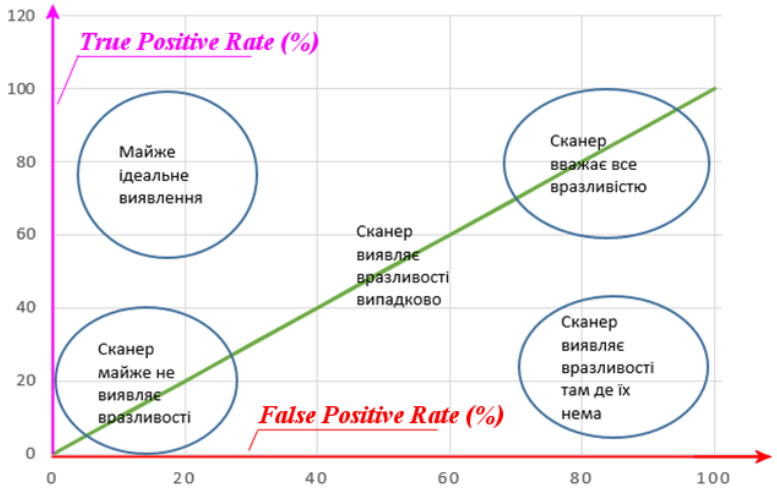


Рис. 1 – Приклад інфографіки представлення звіту WBE

2.2.4 Web Benchmark Evaluation (WBE). Проект *OWASP benchmark* запропонував систему оцінки ефективності інструментів статичного аналізу під назвою OWASP WBE, що являє собою візуальне уявлення ефективності виявлення на основі хибно-позитивних результатів та частоти відкликання.

Як слід із рис. 1, лінія, яка проходить через точки (0%, 0%) та (100%, 100%), є *«лінією вгадування»,* тобто продуктивність на цій лінії вказує на ту ж продуктивність, що і при випадковому виборі. Рис. 1 є прикладом того, наскільки коректно сканер, що тестується, визнає існуючи вразливості додатку [14].

2.2.5 Критерії оцінки сканера безпеки веб-додатків (WASSEC). Являють собою набір принципів для оцінки сканерів веб-додатків на предмет їх здатності ефективно тестувати веб-застосунки та виявляти вразливості безпеки. Основна мета WASSEC, це створення неза-

лежного від постачальників звіту, який допоможе фахівцям із ІБ, орієнтуватися під час оцінки параметрів сканерів веб-додатків. У цьому документі представлений повний перелік функцій, які слід враховувати при проведенні оцінки сканера безпеки веб-додатків. WASSEC поєднує такі можливості, як синтаксичний аналіз, обробку сеансів, тестування, звітність тощо [16], та складається з шести критеріїв оцінки (*див. Табл. 1*), які сприяють визначенню можливостей виявлення сканерів. В цілому, WASSEC надає користувачам можливості адаптивно (*вибірково*) використовувати наявний перелік функцій сканеру, та сфокусувати його на найбільш важливих для кожного користувача функціях, призначивши відповідну вагу для кожній функції [16].

Таблиця 1- Метрика WASSEC

КРИТЕРІЇ	ВРАЗЛИВОСТІ
1. Підтримка протоколу	*Get, Post, Cookie, Header, Secret, Pname, Custom, Proxy, Gzip, Eflate, Ssl.*
2. Автентифікація	*Basic, Digest, Ntlm, Ntlmv2, Kerberos, Form, Cert, Captcha*
3. Управління сеансами	*Custom Cookie, Custom, Header, Logout, Detection, Exclude, Log-Out, Exclude, Url, Exclude, Param*
4. Crawling	*Manual Crawl, Html Crawler, Ajax Crawler, Flash Crawler, Applet Crawler, Silverlight Crawler, Wsdl Crawler, Rest Crawler, Field Autofill, Smart Autofill, Anti Csrf Support, Viewstate Support*
5. Parsing	*Xml, Xmlatt, Xmltag, Json, Netenc, Amf, Javaser, Netser, Wcf, Wcf-Bin, Websock, Dwr, Url File*
6. Тестування	*Sqli, Bsqli, Ssjsi, Rxss, Pxss, Dxss, Jsonh, Lfi, Rfi, Cmdexec, Upload, Redirect, Crlfi, Ldapi, Xpaphi, Mxi, Ssi, Formati, Codei, Xmli, Eli, Buffero, Integero, Codedisc, Backupf, Padding, Authb, Prive, Xxe, Session, Fixation, Csrf, Ados.*

2.3 Результати перевірки вразливих додатків

На рис. 2 представлені *TP* (*True Positive*) оцінки сканерів для 7 вразливостей у DVWA та відповідно, 9 вразливостей у WebGoat. Для випадку DVWA, хоча всі сканери і виявили вразливості CmdExec, XSS, XSS та SQLi, однак їх пошукова продуктивність значно відрізнялася. При цьому, відмінності в показниках виявлення DVWA можна пояснити тим, що окремі сканери розроблялися для пошуку конкретних типів вразливостей, причому правила ліцензування, опосередковано, впливають на кінцевий результат: наприклад, безкоштовна версія *Acunetix*, виявляє тільки XSS-уразливості. Крім того, можливості виявлення сканерів

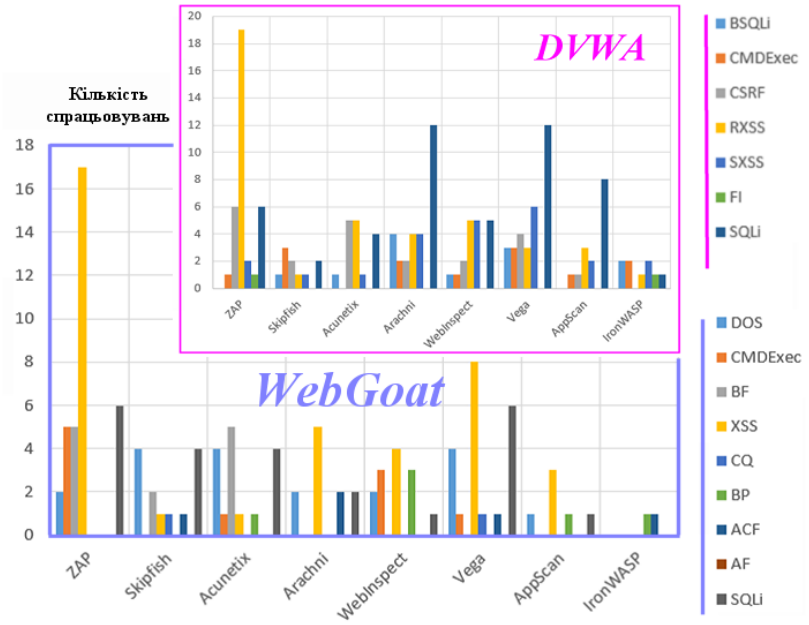


Рис. 2 – *TP*- співвідношення спрацьовувань для DVWA та WebGoat

помітно різняться в залежності від веб-додатків.

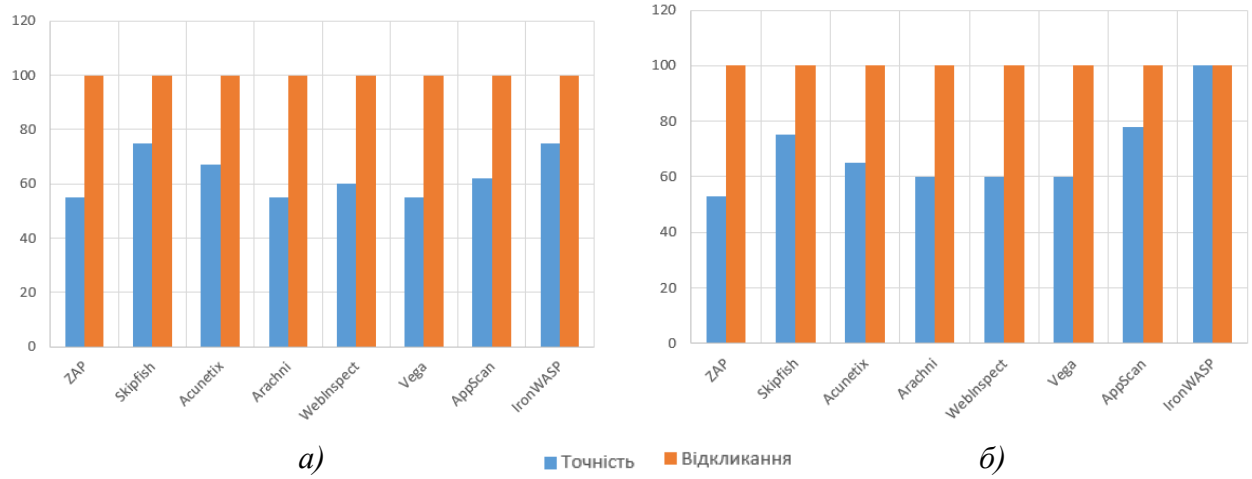
Для випадку WebGoat, всі рішення, за винятком IronWASP (*знайшов лише 2 вразливості*), виявили по кілька вразливостей, причому найбільш вдалого детекту зазнали XSS та SQLi. І хоча жоден сканер не зміг детектувати весь набор WebGoat, їх відмінності є чітким свідченням того, що ці рішення впроваджують різни стратегії їх побудови. В цілому, отримані результати дають наочне уявлення про загальні збіги та взаємодоповнюючі риси сканерів безпеки, що тестувались.

2.3.1 Час сканування. Ефективність сканерів оцінювалась, в т.ч., за параметром часу (в секундах), що потрібен для завершення виявлення вразливостей: - для DVWA, від 30 до 360 сек; - для WebGoat, від 30 до 900 сек (*див. табл. 2*). Відмінності в часі виявлення окремих сканерів, також, можуть бути пов'язані з внутрішніми компонентами безпеки додатків. Так наприклад, якщо для сканеру ZAP, у WebGoat, знадобилося лише 60 сек, то в випадку DVWA, він працював вже 360 сек.

Таблиця 2 – Час сканування вразливих додатків

Тип Сканеру	**Час сканування** *(сек)*	
	DVWA	**Web Goat**
ZAP	*360*	*60*
Skipfish	*120*	*120*
Acunetix	*122*	*120*
Arachni	*60*	*900*
WebInspect	*180*	*181*
Vega	*60*	*60*
AppScan	*62*	*70*
Iron WASP	*60*	*30*
	CPU Intel Core i5-6200U; 2.3 ГГц; 8 Gb RAM; OS Win 10 Home	

2.3.2 Аналіз точності та «відкликання» сканерів. Ці параметри оцінювалися в діапазоні 0÷100%, де: - ефективний інструмент (*без хибно-негативних або хибно-позитивних результатів*), має значення 100%, як для точності, так і для оцінки його «відклику». На рис. 3 наведені значення (в %) для DVWA та WebGoat відповідно.



а) *б)*

Рис. 3 – Точність та відклик для DVWA *(а)* та WebGoat *(б)*

Хоча всі сканери і досягли 100%-го показника відкликання (*що підтверджує їх здатність виявляти реальні вразливості*), однак існують значні відмінності в їх показниках точності, що скоріш за все, можна пояснити «унікальністю» конструктивної реалізації кожного сканеру. Таким чином, показники, котрі менше 100% відображають той факт, що сканери

безпеки маркували «*як уразливості*» певні проблеми, які насправді не були такими (*тобто, це приклад помилкових спрацьовувань*).

2.3.3 OWASP WBE. Довідник з тлумачення результатів OWASP WBE забезпечує графічну візуалізацію ефективності інструментів тестування, зіставляючи його *TP* результат із частотою хибно-позитивних (*FP*) результатів (*див. рис. 4*). В ході тестування, у відповідності з виразами (4) і (5), визначається загальна частота TP_t та FP_t результатів, як загальне число, для DVWA та WebGoat:

$$TP_t = TP_D + TP_W\,, \tag{4}$$

$$FP_t = FP_D + FP_W\,, \tag{5}$$

де: - TP_t та FP_t, це загальні показники істинних і хибно-позитивних результатів;

- TP_D та FP_D, це показники істинних і хибно-позитивних результатів для випадку DVWA;
- TP_W і FP_W, це показники істинних і хибно-позитивних результатів для випадку WebGoat.

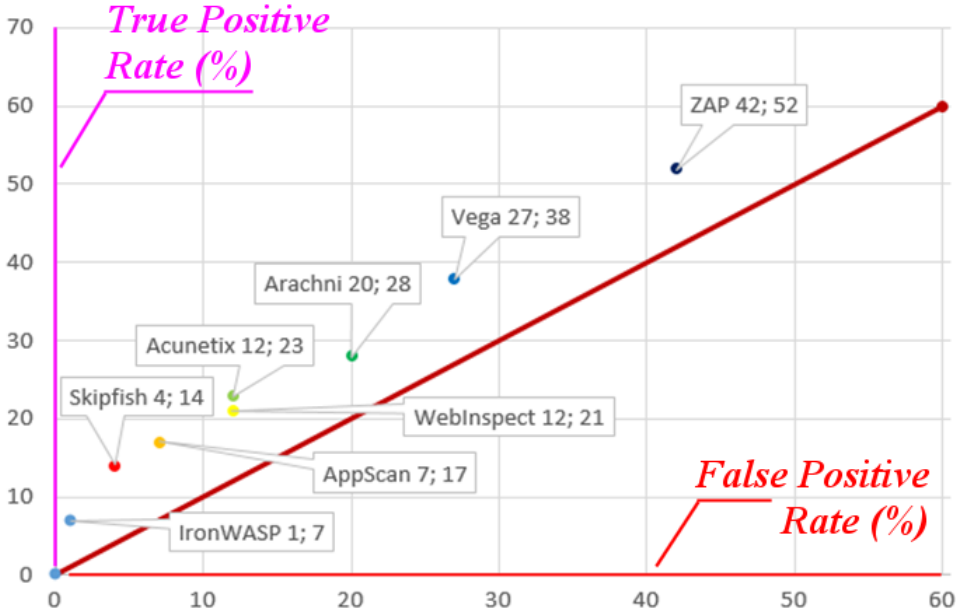


Рис. 4 – Інтерпретації WBE для досліджуваних сканерів

Як тлумачиться в посібнику WBE (розділ 4.4) [14], ефективність детектування вразливостей для того чи іншого сканеру, визначається його положенням на даної інфографіки. Так, наприклад, позиція IronWasp відповідає категорії «ніщо не вразливе» (*де істинні і хибно-позитивні показники невеликі*). Продуктивність цього сканеру можна обґрунтувати тим, що це рішення було розроблено для певного типу виявлення вразливостей.

Щодо позиції ZAP, у верхньому правому куті, то цей сканер виявляє та повідомляє, що *«все вразливе»* (справжні та хибно-позитивні показники, високі). Решта сканерів, згідно із пропонованою інтерпретацією результатів, потрапили до категорії *«інструмент повідомляє, що ніщо не вразливе»*, за винятком Arachni - (20;28), що є надто близький до категорії *«інструмент повідомляє про вразливість випадковим чином»*.

2.3.4 Індекс Юдена. На рис. 5 представлений Індекс Юдена для досліджуваних сканерів безпеки. Згідно з представленими даними, IronWASP має найвищий індекс (0,83), що вказує на його високу ефективність у виявленні відомих вразливостей, з невеликою кількістю помилкових спрацьовувань або взагалі без них.

Наступними сканерами з найкращими індексами є, Skipfish, Appscan, Webinspect і Acunetix (0,45, 0,31, 0.23 і 0,21 бали). Крім того, результати свідчать, що кілька сканерів з відкритим кодом, можуть функціонувати так само ефективно, як і деякі комерційні рішення.

Тобто, сам факт ліцензування не є аргументованим показником для оцінки ефективності інструментів тестування вразливостей.

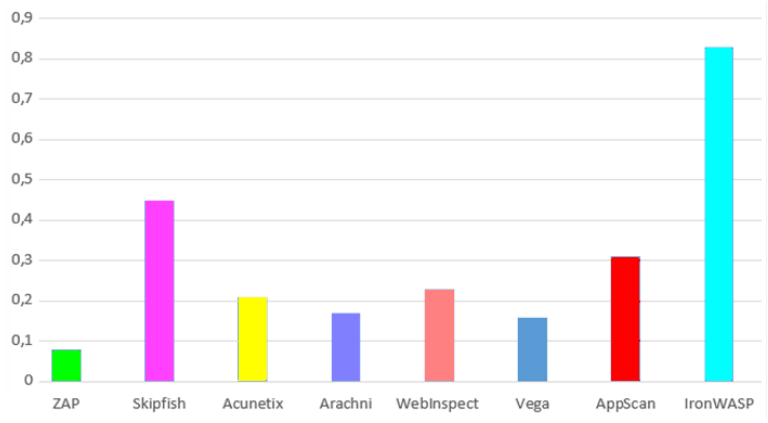


Рис. 5 – Індекс Юдена

Наступними сканерами з найкращими індексами є, Skipfish, Appscan, Webinspect і Acunetix (*0,45, 0,31, 0.23 і 0,21 бали*). Крім того, результати свідчать, що кілька сканерів з відкритим кодом, можуть функціонувати так само ефективно, як і деякі комерційні рішення. Тобто, сам факт ліцензування не є аргументованим показником для оцінки ефективності інструментів тестування вразливостей.

2.3.5 Критерії оцінки сканера безпеки веб-додатків (WASSEC). У таблиці 3 наведені результати виявлень за критеріями WASSEC [16] для тестованих сканерів. Згідно з ними сканер Acunetix має кращу підтримку протоколу, потім Appscan та Skipfish. Незважаючи на відмінності в продуктивності сканерів, є подібності в області обходу, автентифікації та тестування. На рис. 6 наведені середні результати WASSEC, що визначають пару лідерів з кращою продуктивністю, це Acunetix та AppScan (*0,81 та 0,65*). При цьому, сканери з відкритим кодом Skipfish та ZAP (*третє і четверте місце, з хорошими показниками та оцінками 0,43 і 0,40*), підтверджують високе реноме, як для не ліцензованих рішень.

Таблиця 3 – Результати виявлень WASSEC

Сканер	Підтримка протоколу	Управління сеансами	Тестування	Parsing	Автентифікація	Crawling
ZAP	*7*	*5*	*12*	*2*	*3*	*4*
Skipfish	*8*	*5*	*13*	*3*	*3*	*4*
Acunetix	*10*	*6*	*28*	*7*	*7*	*9*
Arachni	*6*	*5*	*12*	*2*	*3*	*3*
WebInspect	*7*	*6*	*4*	*0*	*7*	*1*
Vega	*6*	*5*	*10*	*2*	*3*	*3*
AppScan	*8*	*6*	*22*	*4*	*6*	*8*
IronWASP	*6*	*5*	*9*	*3*	*3*	*2*

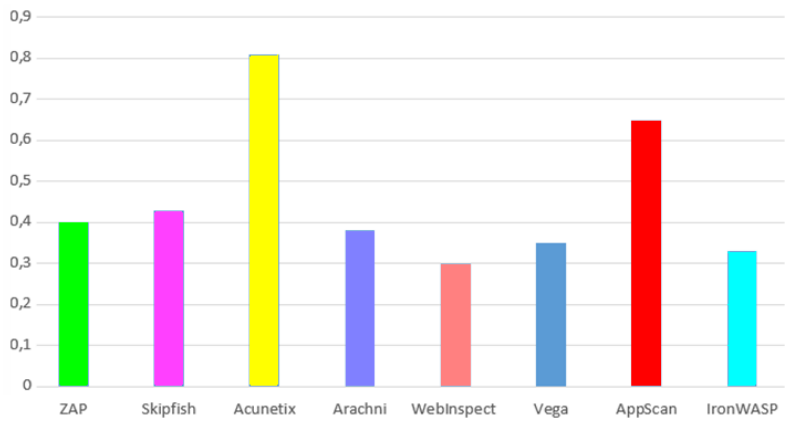


Рис. 6 – Середні значення WASSEC

7. Висновки

1. Сканери з відкритим кодом, як і їх комерційні рішення, є ефективним інструментом виявлення вразливостей у веб-додатках. Основні відмінності між цими двома групами сканерів полягають в різних показниках їх точності (*помилкових виявленнях*), що свідчить про необхідність оцінки ефективності використовуваних інструментів, на основі найменшої кількості хибно-позитивних результатів. При цьому слід враховувати, що різні сканери по різному виявляють різні вразливості (*тобто схильні для певного типу вразливостей*), наприклад: – Acunetix, проявив гарні здібності у виявленні XSS вразливостей, а OWASP ZAP, навпаки, у виявленні вразливостей типу CmdExec.

2. Результати проведеного огляду дають підстави стверджувати, що комерційні сканери Acunetix та Appscan, є більш ефективними при виявленні розглянутого складу вразливостей, але сканери з відкритим кодом (*наприклад, ZAP та Skipfish*), були однаково ефективними при виявленні деяких різновидів вразливостей, що розглядалися (тобто, є початково таргетовані на цих загрозах).

3. Не існує єдиного сканеру, який забезпечував би стабільно високі показники виявлення для всіх типів вразливостей. На прикладі проведеного огляду результатів тестування, можна стверджувати, що існуючи відмінності в частоті хибно-позитивних вразливостей (*для обох груп сканерів*), обумовлені тим, що більшість комерційних рішень, мають автоматизовані сканери і обхідники, котрі виявляються більш ефективнішими, ніж ручне налаштування та втручання тестувальника, яке необхідне у випадку використання сканерів з відкритим кодом і, що потребує певних додаткових компетенцій від персоналу.

Список літератури

[1] Amankwah, R., Chen, J., Kudjo, P. K., & Towey, D. (2020). An empirical comparison of commercial and open-source web vulnerability scanners. Software: Practice and Experience, 50(9), 1842–1857. https://doi.org/10.1002/spe.2870

[2] El, M., McMahon, E., Samtani, S., Patton, M., & Chen, H. (2017). Benchmarking vulnerability scanners: An experiment on SCADA devices and scientific instruments. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). https://doi.org/10.1109/isi.2017.8004879

[3] Alsaleh, M., Alomar, N., Alshreef, M., Alarifi, A., & Al-Salman, A. (2017). Performance-Based Comparative Assessment of Open Source Web Vulnerability Scanners. Security and Communication Networks, 2017, 1–14. https://doi.org/10.1155/2017/6158107

[4] Chen, S. (2017, November 10). WAVSEP 2017/2018 - Evaluating DAST against PT/SDL Challenges. Security Tools Benchmarking. https://sectooladdict.blogspot.com/.

[5] Acunetix | Web Application Security Scanner. (2022). Acunetix. https://www.acunetix.com/

[6] The leader in Web application security assessment. (2011). Retrieved November 4, 2022, from http://www.hp.com/hpinfo/newsroom/press_kits/2011/risk2011/HP_WebInspect_data_sheet.pdf

[7] HCL Software. (2021). Hcltechsw.com. https://www.hcltechsw.com/appscan

[8] OWASP ZAP Tutorial: Comprehensive Review Of OWASP ZAP Tool. (2022). Www.softwaretestinghelp.com. https://www.softwaretestinghelp.com/owasp-zap-tutorial/

[9] skipfish. (2017). Kali.tools. Retrieved November 4, 2022, from https://kali.tools/all/?tool=1256

[10] Arachni - Web Application Security Scanner Framework. (n.d.). Arachni - Web Application Security Scanner Framework. https://www.arachni-scanner.com/

[11] IronWASP - Инструменты Kali Linux. (n.d.). Retrieved November 4, 2022, from https://kali.tools/?p=1786

[12] Vega Vulnerability Scanner. (n.d.). Subgraph.com. https://subgraph.com/vega/

[13] OWASP. (n.d.). OWASP foundation, the open source foundation for application security. Owasp.org. https://owasp.org/

[14] OWASP Benchmark. (n.d.). Owasp.org. https://owasp.org/www-project-benchmark/

[15] Youden, W. J. (1950). Index for rating diagnostic tests. Cancer, 3(1), 32–35. https://doi.org/3.0.co;2-3">10.1002/1097-0142(1950)3:1<32::aid-cncr2820030106>3.0.co;2-3

[16] The Web Application Security Consortium / Web Application Security Scanner Evaluation Criteria. (2009). Projects.webappsec.org. http://surl.li/dtuti

Received: October 2022. Accepted: November 2022.

Authors:

Ivan Lakhtin, student Computer Science Department (magistrate), V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.

E-mail: lakhtin.ivan@gmail.com

Dmytro Mykhailenko, CSD Student (bachelor degree), V. N. Karazin Kharkiv National University, Kharkov, Ukraine.
E-mail: xa12850318@student.karazin.ua

Oleksii Nariezhnii, Ph.D., Associate Professor, V. N. Karazin Kharkiv National University, Kharkov, Ukraine.
ORCID ID https://orcid.org/0000-0003-4321-0510
E-mail: o.nariezhnii@karazin.ua

Comparison of commercial web application vulnerability scanners and open source scanners.

Abstract. The paper compares eight vulnerability scanners based on two intentionally vulnerable applications. The comparison is performed using five criteria: accuracy, recall, Juden index calculation, web benchmark from WASSEC and OWASP. OWASP WebGoat and Damn Vulnerable Web Application (DVWA) are selected as the tested applications. Among the tested scanners there are three commercial scanners: Acunetix, HP WebInspect, AppScan, and five open source scanners such as: Arachni, IronWASP, Skipfish, OWASP ZAP, Vega. According to the results, it was concluded that commercial scanners are more effective in a number of criteria (including the list of threats). Some open source scanners (such as ZAP and Skipfish) can be characterized as originally targeted at certain types of threats. It is emphasized that there is no single security scanner that provides consistently high detection rates for all types of vulnerabilities. Based on the results of the review, it is claimed that the existing differences in the frequency of false-positive vulnerabilities (for both groups of scanners) are due to the fact that most commercial solutions have automated scanners, which are more effective than manual settings by the tester. It is obvious that the results of manual settings have a direct relationship with the actual level of the tester's competence, and largely determine the final results.

Keywords: web application, vulnerability, attack, scanner, security, testing.