ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо виявлення вразливостей Web-додатків на основі Acunetix»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Іван КОНДРАТЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
КОНДРАТЕНКО Іван
(прізвище, ім'я)

Керівник д. ф., доцент МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
"___" _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кондратенко Іван Сергійовичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розроблення рекомендацій щодо виявлення вразливостей Web-додатків на основі Acunetix»

керівник кваліфікаційної роботи Марченко Віталій, д. ф., доцент
(прізвище, ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2024 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Acunetix;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми захисту кінцевих точок організації.
2. Аналіз методів та засобів виявлення вразливостей Web-додатків на основі Acunetix
3. Розроблення рекомендацій щодо застосування системи виявлення вразливостей Web-додатків на основі Acunetix.
4. Рекомендації щодо застосування методів та програмного забезпечення для

аналізу під час використання технології Acunetix.

5. Перелік графічного матеріалу

Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту Web-додатків	15.04.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.		
3.	Аналіз основних можливостей Acunetix.		
4.	Налаштування сканування Web-додатків на базі Acunetix.		
5.	Розроблення рекомендацій щодо виявлення вразливостей Web-додатків на основі Acunetix.		
6.	Оформлення результатів дослідження.		
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Іван Кондратенко
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу здобувача КОНДРАТЕНКО Івана

На тему: «Дослідження шляхів та розробка рекомендацій щодо щодо виявлення вразливостей Web-додатків на основі Acunetix»

Актуальність: Забезпечення безпеки Web-додатків організацій є ключовим для запобігання несанкціонованому доступу, витоку та втраті даних. Системи виявлення вразливостей Web-додатків, що дозволяє організаціям мати повну видимість стану безпеки та оперативно реагувати на нові загрози.

Кібератаки, які порушують роботу кінцевих пристроїв організації або ставлять їх під загрозу, можуть призвести до простоїв, що впливає на продуктивність і безперервність бізнесу. Тому тема кваліфікованої роботи актуальна і своєчасна.

Позитивні сторони:

1. На основі аналізу в статті визначається зміст проблеми, виявлення вразливостей Web-додатків, визначаються мета і призначення цього типу програмного забезпечення, а також його компоненти.
2. Досліджено методи та засоби виявлення вразливостей Web-додатків на основі Acunetix.
3. Запропоновано варіант виявлення вразливостей Web-додатків на основі Acunetix та рекомендації щодо їх виправлення застосування.
4. Текст представлений дуже грамотно і зв'язно. Був зроблений чіткий і змістовний висновок. Графічний матеріал розроблений з високою якістю. Перелік науково-технічної літератури свідчить про вміння використовувати матеріали по темі кваліфікованої роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз виявлення вразливостей Web-додатків конкретної організації.
2. Запропонований порядок застосування методів та засобів виявлення вразливостей Web-додатків бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“відмінно”**, а здобувач(ка) **Кондратенко Іван** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач КОНДРАТЕНКО Іван до захисту кваліфікаційної роботи

(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо виявлення вразливостей Web-додатків на основі Acunetix».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***КОНДРАТЕНКО Іван*** обрав тему роботи, метою якої було вивчити шляхи та засоби виявлення вразливостей Web-додатків та розробити рекомендації щодо їх реалізації. Список використовуваних ресурсів демонструє здатність заявника розуміти наукові проблеми та застосовувати їх у дослідженнях Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***КОНДРАТЕНКО Іван*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***КОНДРАТЕНКО ІВАНА*** на оцінку **"відмінно"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Віталій МАРЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **КОНДРАТЕНКО Іван** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 58 сторінки, рисунків 2, джерел 10.

Об'єкт дослідження – вразливостей Web-додатків.

Предмет дослідження – методи та засоби виявлення вразливостей Web-додатків на основі Acunetix.

Мета роботи розробити варіант системи на базі рішення Acunetix та рекомендації щодо застосування методів та засобів виявлення вразливостей Web-додатків.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Виявлення вразливостей веб-додатків – це програмні засоби, які допомагають організаціям виявляти та усувати вразливості у веб-додатках. Проводити глибоке сканування веб-додатків, виявляючи такі вразливості, як SQL-ін'єкції, XSS, CSRF та інші поширені загрози. Acunetix збирає та аналізує дані про безпеку веб-додатків, допомагаючи виявляти та виправляти проблеми до того, як вони вплинуть на роботу організації. Acunetix також забезпечує звітування та оповіщення про критичні вразливості, що дозволяє підтримувати високу безпеку веб-додатків.

У роботі досліджено проблему виявлення вразливостей веб-додатків організації, визначено мету та завдання тестування безпеки. Проведено аналіз існуючих методів та засобів виявлення вразливостей веб-додатків. Досліджено методи та засоби виявлення вразливостей веб-додатків на базі Acunetix. Визначено призначення, основні функції та склад рішення Acunetix.

На основі досліджень, проведених у роботі, запропоновано варіант системи виявлення вразливостей на базі Acunetix. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів захисту веб-додатків організації.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, WEB-ДОДАТКИ, ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ, МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

CSRF – Cross-Site Request Forgery

CSP – Content Security Policy

DMZ – Demilitarized Zone

DNS – Domain Name System

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

NGFW – Next-Generation Firewall

OWASP – Open Web Application Security Project

RFI – Remote File Inclusion

SaaS – Software as a Service

SLA – Service Level Agreement

SIEM – Security Information and Event Management

SQLi – SQL Injection

SSL – Secure Sockets Layer

WAF – Web Application Firewall

XSS – Cross-Site Scripting

CI/CD – Continuous Integration/Continuous Delivery

ВСТУП

Веб-додатки відіграють дедалі важливішу роль у сучасному цифровому світі, надаючи широкий спектр функціональних можливостей для користувачів і організацій. Їх застосування охоплює різні сфери діяльності, включаючи банківські послуги, соціальні мережі, освітні ресурси та багато іншого. Зі зростанням популярності та складності веб- додатків збільшується кількість загроз, які можуть бути використані зловмисниками для отримання несанкціонованого доступу, крадіжки конфіденційної інформації або порушення нормальної роботи. У зв'язку з цим забезпечення безпеки веб-додатків стає найважливішим завданням для розробників, адміністраторів і всіх, хто бере участь у їхній експлуатації.

Забезпечення безпеки веб-додатків охоплює різні аспекти, такі як конфіденційність, цілісність, доступність, аутентифікація, авторизація та аудит. Важливо розуміти, що загрози безпеці можуть бути як зовнішніми, так і внутрішніми. До зовнішніх загроз належать атаки хакерів, шкідливе ПЗ та інші форми кіберзлочинності, а внутрішні загрози можуть виникати через людські помилки, недбалість або навмисні дії співробітників. Таким чином, комплексний підхід до забезпечення безпеки веб-додатків повинен включати в себе технічні, організаційні та процедурні заходи.

У першому розділі цієї роботи буде детально розглянуто проблему безпеки веб-додатків, зокрема, основні концепції та теоретичні основи. Ми проаналізуємо основні вразливості, які можуть виникнути у веб-додатках, наприклад, **SQL-ін'єкції**, міжсайтовий скриптинг (**XSS**), підробка міжсайтових запитів (**CSRF**) та інші. Кожна з цих вразливостей має свої особливості та методи захисту, які необхідно знати та застосовувати на практиці. Крім того, буде представлено огляд різних типів веб-застосунків, зокрема статичних, динамічних, односторінкових (**SPA**) і багатосторінкових (**MPA**), та їхніх загальних вразливостей.

Другий розділ присвячено вивченню сучасних методів та інструментів для виявлення вразливостей у веб-додатках. Важливим аспектом є порівняння різних методів виявлення вразливостей, таких як ручне тестування, автоматичне

сканування та інтерактивні методи аналізу. Кожен із цих методів має свої переваги та недоліки, тому для досягнення максимального рівня безпеки доцільно використовувати їх у комбінації. Особливу увагу ми приділимо інструменту Acunetix, який є одним із провідних рішень для автоматичного сканування веб-додатків на наявність вразливостей. Ми проаналізуємо основні можливості цього інструменту, розглянемо його переваги та недоліки, а також продемонструємо використання Acunetix на практиці з аналізом отриманих даних.

У третьому розділі буде надано практичні рекомендації з виявлення вразливостей веб-додатків за допомогою Acunetix . Ми розглянемо процес налаштування цього інструменту для ефективного сканування, включно з параметрами конфігурації, вибором профілів сканування та іншими важливими аспектами. Крім того, буде розглянуто процес ідентифікації та класифікації виявлених вразливостей, що дасть нам змогу краще зрозуміти природу загроз і розробити ефективні заходи протидії. На основі отриманих результатів сканування ми запропонуємо рекомендації щодо оптимізації налаштування для підвищення ефективності виявлення вразливостей і поліпшення процесу аналізу результатів.

Мета цієї роботи - підвищити обізнаність про проблеми безпеки веб- додатків і дати практичні рекомендації щодо їх вирішення. Основні завдання роботи включають:

1. Вивчення та аналіз основних концепцій безпеки веб-додатків.
2. Виявлення типових вразливостей веб-додатків і методи їх виявлення.
3. Порівняння сучасних методів та інструментів для виявлення вразливостей.
4. Детальне дослідження можливостей інструменту Acunetix .
5. Розробка практичних рекомендацій для використання Acunetix для підвищення безпеки веб додатків.

Забезпечення безпеки веб- додатків є важливим завданням,що потребує постійної уваги та вдосконалення. Ця робота зробить внесок у розуміння проблеми, надасть цінні знання та рекомендації, які можуть бути використані розробниками та адміністраторами для підвищення безпеки своїх веб-додатків.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-ДОДАТКІВ

У сучасному світі інтернет-технологій проблема безпеки веб-додатків є однією з найактуальніших. Зі зростанням залежності від онлайн-сервісів і збільшенням обсягу цифрових транзакцій ризики кіберзлочинності постійно зростають. Універсальність і доступність веб-додатків призводить до зростання кількості атак, а відсутність належних заходів безпеки може мати серйозні наслідки для користувачів і організацій. Безпека веб-сайтів має бути пріоритетом для кожної організації. Сьогодні цей аспект корпоративної безпеки, яким нехтують найчастіше. Веб-додатки - інтернет-магазини, веб-форми, сторінки входу в систему, сторінки з динамічним контентом тощо дедалі частіше стають ціллю хакерів.

Вразливі веб-додатки доступні з будь-яких точок світу 24 години на

добу, 7 днів на тиждень. Вони забезпечують легкий доступ до внутрішніх корпоративних баз даних, а також дають змогу хакерам здійснювати

шахрайські дії з використанням зламаних сайтів. Безпека веб-додатків має вирішальне значення для захисту конфіденційності, цілісності та доступності даних. Слабкі місця в захисті можуть призвести до витоку конфіденційної інформації, втрати даних або навіть злому систем з метою злочинної діяльності[1].

1.1 Аналіз проблеми та основні поняття безпеки Web-додатків

Сучасні веб-додатки відіграють ключову роль у різних сферах життя суспільства - від особистих блогів до складних корпоративних систем. Зі зростанням значущості веб-додатків зростає і важливість їхньої безпеки. Недостатня увага до безпеки веб-додатків може призвести до серйозних наслідків, включно з втратою даних, фінансовими збитками та шкодою репутації. У цьому розділі ми розглянемо безпеку веб- додатків і визначимо поняття, пов'язані з цією темою, з акцентом на використання інструменту Acunetix для виявлення та усунення вразливостей.

Основні проблеми безпеки веб-додатків можна розділити на кілька категорій:

1. Зовнішні атаки: Веб-додатки часто стають об'єктом зовнішніх атак з боку зловмисників, які намагаються вкрасти дані, порушити роботу системи або отримати несанкціонований доступ. Серед таких атак найпоширенішими є **SQL-ін'єкції**, міжсайтовий скриптинг (**XSS**), підробка міжсайтових запитів (**CSRF**), атаки на сесії. Інструмент Acunetix допомагає виявити ці вразливості автоматично, значно знижуючи ризик експлуатації вразливостей[2].

2. Внутрішні загрози: До внутрішніх загроз відносяться зловмисники, які мають законний доступ до системи, наприклад незадоволені співробітники або партнери, які мають доступ до конфіденційної інформації. Внутрішні загрози можуть бути особливо небезпечні через права доступу і знання системи. Використання Acunetix дає змогу регулярно перевіряти внутрішні застосунки на наявність вразливостей, мінімізуючи ризик внутрішніх атак.

3. Технічні вразливості: Технічні вразливості виникають через помилки в програмному забезпеченні, використання застарілих бібліотек, неправильну конфігурацію серверів та інших компонентів системи. Ці вразливості можуть бути використані зловмисниками для отримання несанкціонованого доступу або порушення роботи веб-додатка. Acunetix дає змогу автоматизувати процес виявлення таких вразливостей, забезпечуючи своєчасне оновлення та виправлення помилок.

4. Соціальна інженерія: Соціальна інженерія охоплює методи обману користувачів з метою отримання конфіденційної інформації, такої як паролі або інші дані для аутентифікації. Це може бути зроблено за допомогою фішингових атак, шахрайських електронних листів або телефонних дзвінків. Хоча Acunetix не може безпосередньо запобігти атакам соціальної інженерії, він забезпечує захист від технічних вразливостей, які можуть бути використані в таких атаках.

Основні поняття безпеки веб-додатків

Щоб забезпечити безпеку веб-додатків, необхідно розуміти основні поняття і принципи, що лежать в основі захисту інформаційних систем. До них належать:

1. Конфіденційність: Конфіденційність означає, що інформація доступна тільки тим користувачам, які мають відповідні права доступу. Для забезпечення конфіденційності використовуються методи шифрування даних, контроль доступу та інші заходи безпеки. Acunetix допоможе вам перевірити вразливості, які можуть призвести до витоку даних.

2. Цілісність: Цілісність означає, що дані не можуть бути змінені або видалені неавторизованими користувачами. Для забезпечення цілісності використовуються методи аутентифікації, контроль версій та інші засоби. Acunetix дає змогу виявити вразливості, які можуть вплинути на цілісність даних, наприклад, сеансові атаки та SQL-ін'єкції.

3. Доступність: Доступність означає, що інформаційні системи та дані доступні користувачам у будь-який час, коли вони необхідні. Для забезпечення доступності використовуються методи резервного копіювання, відновлення після збоїв, захисту від DDoS-атак та інші засоби. Acunetix може допомогти виявити вразливості, які можуть бути використані для порушення доступності веб-додатків.

4. Аутентифікація: Аутентифікація - це процес перевірки особи користувача для підтвердження його права на доступ до системи. Для аутентифікації використовуються паролі, біометричні дані, токени та інші методи. Acunetix підтримує перевірку безпека механізмів аутентифікації, що допомагають забезпечити надійний доступ до системи.

5. Авторизація: Авторизація - це процес надання користувачеві прав доступу до певних ресурсів або функцій системи після успішної аутентифікації. Авторизація забезпечує розмежування прав доступу і дає змогу контролювати дії користувачів у системі. Acunetix дає змогу перевірити правильність налаштувань авторизації та виявити потенційні вразливості.

6. Реєстрація та моніторинг: Ведення журналу та моніторинг мають на увазі запис і аналіз дій користувачів і системи для виявлення можливих загроз і реагування на них. Ведення журналу дає змогу відстежувати системні події, виявляти підозрілу активність і проводити аудит безпеки. Acunetix можна інтегрувати з іншими системами реєстрації та моніторингу для забезпечення комплексного підходу до безпеки.

7. Контроль доступу: Контроль доступу включає в себе методи і засоби, що обмежують доступ користувачів до певних ресурсів або функцій системи. Контроль доступу може бути реалізований за допомогою різних механізмів, таких як списки контролю доступу (ACL), модель доступу на основі ролей (RBAC) тощо. Acunetix допомагає виявити помилки в налаштуваннях управління доступом, забезпечуючи відповідний рівень захисту.

8. Криптографія: Криптографія охоплює методи шифрування та дешифрування даних для забезпечення їхньої конфіденційності та цілісності. Основні криптографічні методи охоплюють симетричне й асиметричне шифрування, хешування та цифрові підписи. Використання перевірок Acunetix криптографічні методи для виявлення потенційних вразливостей у шифруванні даних.

Важливість безпеки веб-додатків

Безпека веб-додатків дуже важлива з кількох причин:

1. Захист конфіденційної інформації: Веб-додатки часто працюють із конфіденційною інформацією, такою як особисті дані користувачів, фінансові дані та інша конфіденційна інформація. Безпека веб-додатків дає змогу захистити ці дані від несанкціонованого доступу та витоку. Acunetix допомагає забезпечити такий захист шляхом виявлення та усунення вразливостей.

2. Захист репутації: Інциденти безпеки можуть негативно вплинути на репутацію організації та призвести до втрати довіри користувачів. Захист веб-додатків допомагає запобігти подібним інцидентам і зберегти репутацію компанії. Acunetix дає змогу оперативно виявляти вразливості та запобігати можливим загрозам.

3. Відповідність вимогам законодавства: У багатьох країнах існують закони і нормативні акти, що вимагають забезпечення безпеки персональних даних та інших конфіденційних відомостей. Забезпечення безпеки веб-додатків допомагає організаціям відповідати цим вимогам і уникати штрафів. Використання Acunetix дає змогу виконувати ці вимоги шляхом регулярного сканування та складання звітів про стан безпеки.

4. Фінансові наслідки: Інциденти безпеки можуть призвести до значних фінансових втрат, включно з витратами на відновлення системи, штрафи, компенсація постраждалим користувачам та інші витрати. Захист веб-додатків допомагає знизити ризик фінансових втрат. Acunetix допомагає знизити ці ризики, виявляючи та усуваючи вразливості на ранніх стадіях.

Підходи до забезпечення безпеки веб-додатків

Для забезпечення безпеки веб-додатків використовують різні підходи і методи:

1. Безпечне розроблення: включає в себе використання методів безпечного програмування на етапі розроблення веб-додатків. Це охоплює використання найкращих практик програмування, регулярні перевірки коду і використання інструментів статичного аналізу коду. Acunetix можна використовувати як частину циклу безпечного розроблення для автоматизації перевірок безпеки.

2. Тестування безпеки: включає в себе регулярне тестування веб-додатків на наявність вразливостей за допомогою різних методів, таких як тестування на проникнення, сканування вразливостей та інші методи. Acunetix – це потужний інструмент автоматизованого тестування безпеки, який дає змогу виявляти широкий спектр вразливостей.

3. Моніторинг і реагування: включає в себе постійний моніторинг веб-додатків і реагування на інциденти безпеки в режимі реального часу. Це допомагає виявляти і запобігати атакам на ранній стадії. Acunetix може бути інтегрований із системами моніторингу для забезпечення комплексного підходу до безпеки.

4. Навчання та підвищення обізнаності: охоплює навчання розробників, адміністраторів і користувачів основам безпеки веб-додатків і передовим методам забезпечення інформаційної безпеки. Acunetix пропонує ресурси та документацію для навчання користувачів, що дає змогу підвищити рівень обізнаності про безпеку.

5. Використання сучасних інструментів і технологій: Включає в себе використання сучасних інструментів для забезпечення безпеки веб-додатків, таких як веб-брандмауери, системи виявлення вторгнень, засоби шифрування та інші технології. Acunetix - один із провідних інструментів у цій галузі, що забезпечує комплексний підхід до виявлення та усунення вразливостей.

Отже, аналіз проблем та основні поняття Безпека веб-додатків – важлива складова забезпечення надійності та стабільності інформаційних систем. Розуміння основних загроз, вразливостей і методів захисту дає змогу розробникам, адміністраторам і користувачам ефективно боротися з кіберзагрозами та забезпечувати безпеку веб-застосунків на всіх етапах їхнього життєвого циклу. Інтеграція безпеки в розробку, тестування, моніторинг та експлуатацію веб-додатків - ключ до успіху в сучасному цифровому середовищі. Використання інструменту Acunetix значно спрощує й автоматизує процес гарантування безпеки, даючи вам змогу зосередитися на розробці й удосконаленні веб-додатків, не забуваючи про їхню безпеку.

1.2 Аналіз вразливостей та види Web-додатків

Вразливості у веб-додатках можуть виникати з різних причин, включно з недостатньою перевіркою даних, неправильною обробкою відповідей сервера, недостатнім контролем доступу і відсутністю ефективного моніторингу атак. У міру зростання популярності та різноманітності веб-додатків збільшується і кількість потенційних вразливостей, які можуть бути використані зловмисниками для різних типів атак.

Захист веб-застосунків - одне з ключових завдань кібербезпеки, що вимагає глибокого розуміння як типів застосунків, так і типів вразливостей, які вони містять.

Види вразливостей веб-додатків:

SQL Ін'єкції:

SQL-ін'єкції - одна з найпоширеніших і найнебезпечніших вразливостей веб-додатків. Атака полягає у впровадженні шкідливого SQL-коду в поля введення даних, що обробляються додатком. У разі успіху атаки зловмисник може отримати несанкціонований доступ до бази даних і видаляти, змінювати або вставляти нові дані[3].

Основні причини SQL-ін'єкцій включають:

1. Недостатнє екранування введених даних.

2. Використання динамічних SQL-запитів без підготовлених виразів (prepared statements).

3. Невикористання параметризованих запитів.

Методи захисту від SQL-ін'єкцій включають:

1. Використання підготовлених виразів і параметризованих запитів.

2. Екранування введених даних.

3. Використання ORM (Object-Relational Mapping) інструментів, які автоматично обробляють введені дані.

Міжсайтовий скриптинг (XSS):

Міжсайтовий скриптинг (**XSS**) дає змогу зловмисникам впровадити у веб сторінку шкідливий скрипт, який потім виконується в браузері користувача. Це може призвести до крадіжки ідентифікаторів сеансів, виконання небажаних дій від імені користувача та інших шкідливих наслідків)[4].

Існує кілька видів XSS-атак:

1. Відображуваний (Reflected) XSS: Шкідливий код вбудовується в запит та відображається на сторінці.

2. Збережений (Stored) XSS: Шкідливий код зберігається на сервері і відображається всім користувачам.

3. DOM-based XSS: Шкідливий код вводиться та виконується у клієнтському скрипті, не взаємодіючи з сервером.

Методи захисту від XSS включають:

1. Екранування введених даних і вмісту HTML.

2. Використання Content Security Policy (CSP).

3. Перевіркаі очищення введених даних.

Підробка міжсайтових запитів (CSRF)

Підробка міжсайтових запитів (**CSRF**) дає змогу зловмиснику змусити користувача виконати небажану дію у веб-додатку, на якому він аутентифікований. Це може призвести до зміни пароля, фінансових операцій та інших небажаних дій.

Основні методи захисту від CSRF включають:

1. Використання унікальних токенів CSRF у формах.

2. Перевірка реферера або джерела запиту.

3. Використання методів аутентифікації, таких як подвійна аутентифікація.

Безпека сесій та автентифікації:

Недостатній захист сеансів і аутентифікації може призвести до крадіжки сесійних ідентифікаторів, що дасть змогу зловмиснику виконувати дії від імені легітимного користувача. Основні вразливості включають:

Основні вразливості включають:

1. Використання слабких паролів.

2. Недостатнє захищення сесійних файлів cookie.

3. Відсутність тайм-ауту сесій.

Методи захисту включають:

1. Використання сильних паролів та 2FA.

2. Захист файлів cookie (за допомогою прапорів HttpOnly та Secure).

3. Встановлення обмеження часу життя сесії.

Неправильне управління доступом:

Неправильний доступ до управління може дати змогу зловмисникам виконувати дії, на які у них немає прав. Це відбувається через:

1. Неправильну конфігурацію контролю доступу.

2. Відсутність належної валідації прав доступу на стороні сервера.

Методи захисту включають:

1. Використання централізованої системи управління доступом.

2. Регулярний аудит та перевірка прав доступу.

3. Обмеження доступу за принципом найменших привілеїв.

Ін’єкція команд (Command Injection):

Зловмисник може виконувати шкідливі команди на сервері, використовуючи веб-додаток як посередника. Це стає можливим через недостатню перевірку введених даних.

Методи захисту включають:

1. Перевірка та очищення введених даних.

2. Використання безпечних API.

3. Відокремлення прав користувача додатку від системних прав.

Вразливості, пов'язані з завантаженням файлів:

Недостатня перевірка файлів, що завантажуються, може дозволити зловмисникам завантажити на сервер шкідливий код або інші небезпечні файли.

Методи захисту включають:

1. Перевірка типу файлів перед завантаженням.

2. Обмеження прав доступу до завантажуваних файлів.

3. Використання антивірусного ПЗ для сканування завантажених файлів.

Види веб-додатків:

Статичні веб-додатки:

Статичні веб-додатки складаються з фіксованого набору сторінок, які відображаються користувачеві без змін. Вони зазвичай містять HTML, CSS і JavaScript і використовуються для простих веб-сайтів, блогів або лендінгу. Через

свою простоту вони менш сприйнятливі до складних атак, але все ж можуть бути вразливі для XSS та інших базових загроз.

Характеристики статичних веб-додатків:

1. Простота розробки та підтримки.
2. Висока швидкість завантаження сторінок.
3. Відсутність серверної обробки даних.

Недоліки статичних веб-додатків:

1. Обмеженість функціональних можливостей.
2. Відсутність інтерактивного та динамічного контенту.

Динамічні веб-додатки:

Динамічні веб-додатки генерують та доповнюють сторінки у реальному часі, базуючись на даних з бази даних або інших джерел. Вони широко використовуються для соціальних мереж, інтернет-магазинів, форумів і т.п. Динамічні веб-додатки частіше піддаються складним атакам, таким як SQL-ін'єкції, CSRF та інші.

Характеристики динамічних веб-додатків:

1. Генерація контенту на основі запитів користувача.
2. Використання серверних мов програмування, таких як PHP, ASP.NET.
3. Інтерактивність і багатофункціональність.

Недоліки динамічних веб-додатків:

1. Складніша розробка та підтримкиа.
2. Збільшене навантаження на сервер.
3. Підвищені вимоги до безпеки.

Односторінкові додатки (SPA):

Односторінкові додатки (SPA) завантажують одну HTML-сторінку і динамічно оновлюють її вміст за допомогою JavaScript. Це забезпечує швидку взаємодію з користувачем і підвищує зручність роботи. Однак такі додатки можуть бути вразливими до XSS, CSRF і вразливостей API.

Характеристики SPA:

1. Динамічне оновлення контенту.

2. Використання фреймворків, таких як Angular, React, Vue.js.

3. Зниження навантаження на сервер завдяки клієнтській обробці даних.

Недоліки SPA:

1. Потреба в належному управлінні станом додатку.

2. Підвищені вимоги до безпеки клієнтської частини.

3. Можливі проблеми з SEO (пошуковою оптимізацією).

Багатосторінкові додатки (MPA):

Багатосторінкові додатки (MPA) складаються з декількох сторінок, кожна з яких завантажується окремо з сервера. Вони підходять для великих проєктів з багатою функціональністю. Такі додатки можуть бути вразливі для багатьох типів атак, оскільки кожна сторінка може мати свої власні вразливості.

Характеристики MPA:

1. Функціональність розподілу між кількома сторінками

2. Кожна сторінка виконує окремий запит до сервера.

3. Легкість в управлінні великими проектами.

Недоліки MPA:

1. Більше часу на завантаження сторінок порівняно з SPA.

2. Підвищене навантаження на сервер.

3. Ускладнена навігація для користувача.

Мобільні веб-додатки:

Мобільні веб-додатки оптимізовані для роботи на мобільних пристроях і доступні через браузери на смартфонах і планшетах. Вони можуть бути вразливі до атак на мобільні платформи, таких вразливості API.

Характеристики мобільних веб-додатків:

1. Оптимізація інтерфейсу для мобільних пристроїв.

2. Використання адаптивного дизайну.

3. Підтримка різних мобільних браузерів.

Недоліки мобільних веб-додатків:

1. Обмеженість у використанні ресурсів порівняно з нативними додатками.
2. Можливі проблеми з продуктивністю на старих пристроях.
3. Підвищені вимоги до безпеки через можливість зловживань API.

Прогресивні веб-додатки (PWA):

Прогресивні веб-додатки (PWA) поєднують у собі найкращі риси веб-додатків і мобільних додатків, забезпечуючи високу продуктивність, автономний доступ і функціональність пристроїв. Вони можуть бути вразливі для різних типів атак, включно з XSS, CSRF та іншими.

Характеристики PWA:

1. Підтримка автономного режиму з використанням Service Workers.
2. Швидке завантаження та висока продуктивність.
3. API для доступу до функцій пристрою, таких як камера та геолокація

Недоліки PWA:

1. Підвищені вимоги до знань і навичок розробників.
2. Не всі функції нативних додатків доступні у PWA.
3. Можливі проблеми при підтримці старих браузерів.

Таким чином, аналіз вразливостей веб-додатків показує, що кожен тип додатків має свої специфічні ризики та загрози. Основне завдання розробників і адміністраторів - виявити ці вразливості та реалізувати ефективні заходи захисту. Це охоплює регулярне сканування застосунків на предмет використання вразливостей сучасних інструменти безпеки, як-от Acunetix, і дотримання найкращих практик розроблення безпечного коду. Розуміння типових вразливостей та особливостей різних типів веб- застосунків дасть вам змогу краще захистити інформаційні системи від потенційних загроз і забезпечити надійну роботу веб-застосунків[5]. Важливо пам'ятати, що забезпечення безпеки веб-застосунків - це безперервний процес, який потребує постійної уваги, моніторингу та вдосконалення.

1.3 Визначення ролі і місця сканерів виявлення вразливостей для безпеки веб-додатків

У сучасному цифровому світі веб-додатки стають невід'ємною частиною бізнесу, соціального життя і державного управління. Зі зростанням їхньої значущості зростає і кількість кіберзагроз, спрямованих на них. Забезпечення безпеки веб-додатків є пріоритетним завданням для забезпечення конфіденційності, цілісності та доступності інформації. Одним із ключових інструментів у цій боротьбі є сканери вразливостей. У цьому розділі розглянемо роль і місце сканерів вразливостей в забезпеченні безпеки веб-додатків.

Роль сканерів вразливостей

Сканери вразливостей - це автоматизовані інструменти, що аналізують веб-додатки на предмет наявності вразливостей і потенційних загроз. Їхню роль у забезпеченні безпеки веб-додатків важко заперечувати з кількох причин:

1. Автоматизація процесу виявлення: Сканери дають змогу автоматизувати процес виявлення вразливостей, що значно скорочує час і ресурси, необхідні для ручного тестування. Наприклад, Acunetix забезпечує автоматизоване сканування веб-додатків, що охоплює широкий спектр вразливостей, включно з SQL-ін'єкціями, XSS, CSRF та іншими.

2. Систематичний підхід: Сканери вразливостей забезпечують систематичний підхід до виявлення загроз, охоплюючи широкий спектр потенційних вразливостей. Сканери вразливостей використовують бази даних відомих вразливостей і методи евристичного аналізу для виявлення нових загроз. Acunetix наприклад, використовує передові алгоритми для ідентифікації складних вразливостей, таких як логічні помилки та проблеми з авторизацією.

3. Безперервний моніторинг: Багато сканерів вразливостей підтримують безперервний моніторинг веб-додатків, що дає змогу виявляти нові вразливості в режимі реального часу і швидко реагувати на них. Acunetix забезпечує безперервний моніторинг і автоматичне повідомлення про нові вразливості, що допомагає підтримувати високий рівень безпеки.

4. Документування і звітність: Сканери вразливостей генерують детальні звіти про знайдені вразливості, включаючи рекомендації щодо їх усунення. Acunetix створює зрозумілі звіти, які містять не тільки перелік вразливостей, але й конкретні поради щодо їх усунення, а також приклади коду для розробників.

Місце сканерів вразливостей у системі безпеки

Сканери вразливостей є невід'ємною частиною безпеки веб-додатків. Вони взаємодіють з іншими безпеки, забезпечуючи комплексний захист:

1. Інтеграція з процесом розробки: Сканери можуть бути інтегровані у процес розробки (DevSecOps), що дає змогу виявляти й усувати вразливості на ранніх етапах життєвого циклу веб-додатків. Acunetix підтримує інтеграцію з популярними CI/CD системами, як-от Jenkins і GitLab, що дає змогу автоматизувати процес сканування на кожному етапі розроблення.

2. Взаємодія з системами моніторингу та реагування: Сканери вразливостей можуть працювати спільно з системами моніторингу та реагування на інциденти (SIEM), забезпечуючи своєчасне виявлення і реагування на потенційні загрози. Acunetix можна інтегрувати з іншими системами безпеки, щоб забезпечити комплексний підхід до безпеки.

3. Підтримка політик безпеки: Використання сканерів вразливостей допомагає організаціям дотримуватися внутрішніх політик безпеки та відповідати законодавчим вимогам і стандартам (наприклад GDPR, PCI DSS). Acunetix генерує звіти, які можна використовувати для перевірки відповідності цим стандартам.

Функціональні можливості сканерів вразливостей

Сучасні сканери вразливостей, такі як Acunetix, мають широкий функціонал:

1. Автоматичне сканування: Сканери виконують автоматичне сканування веб-додатків, включно з перевіркою на наявність відомих вразливостей. Acunetix перевіряє понад 4 500 відомих вразливостей, використовуючи актуальні бази даних і передові алгоритми.

2. Евристичний аналіз: Деякі сканери використовують методи евристичного аналізу для виявлення нових, раніше невідомих вразливостей. Acunetix використовує машинне навчання та інші інноваційні технології для аналізу поведінки застосунків і виявлення потенційних загроз.

3. Аналіз конфігурації: Сканери перевіряють налаштування серверів і веб-додатків, виявляючи потенційно небезпечні конфігурації. Acunetix аналізує конфігурації веб-серверів, баз даних та інших компонентів інфраструктури з метою виявлення вразливостей.

4. Звіти та рекомендації: Генеруйте докладні звіти про знайдені вразливості, включно з рекомендаціями щодо усунення та прикладами коду для розробників. Acunetix створює інформативні звіти, які можна налаштувати відповідно до потреб організації, надаючи чіткі інструкції з усунення вразливості.

5. Інтеграція з інструментами розробки: Підтримка інтеграції з системами управління вихідним кодом (наприклад, Git) і конвеєрами CI/CD для автоматичного сканування в процесі розробки. Acunetix легко інтегрується з різними інструментами розробки, забезпечуючи безперервний контроль безпеки впродовж усього життєвого циклу застосунку.

6. Постійний моніторинг: Підтримка постійного моніторингу веб-додатків і повідомлень про нові вразливості в режимі реального часу. Acunetix забезпечує безперервний моніторинг безпеки, автоматично повідомляє про виявлені загрози.

Приклад використання Acunetix

Acunetix є одним з провідних інструментів для сканування вразливостей веб-додатків, що пропонує такі можливості:

1. Автоматизоване сканування: Acunetix виконує повне сканування веб-додатків, включаючи перевірку на понад 4500 відомих вразливостей, таких як SQL-ін'єкції, XSS, CSRF та інші. Це дозволяє виявляти як поширені, так і рідкісні вразливості.

2. Глибокий аналіз: Acunetix використовує передові алгоритми для глибокого аналізу веб-додатків, виявляючи складні вразливості, такі як логічні помилки, проблеми з авторизацією та конфігураційні помилки. Інструмент також

здатний виявляти вразливості у SPA (Single Page Applications) і підтримує сканування REST API.

3. Інтеграція з CI/CD: Acunetix підтримує інтеграцію з популярними CI/CD-системами, такими як Jenkins, GitLab, Azure DevOps, що дозволяє автоматизувати процес сканування на кожному етапі розробки. Це забезпечує безперервний контроль безпеки і допомагає виявляти вразливості на ранніх етапах розробки, знижуючи ризики і витрати на виправлення помилок.

4. Звіти та рекомендації: Acunetix генерує детальні звіти з описом знайдених вразливостей і рекомендаціями щодо їх усунення. Звіти можуть бути налаштовані відповідно до вимог користувача, включаючи інформацію, необхідну для різних аудиторій – від технічних фахівців до керівників.

5. Постійний моніторинг: Acunetix підтримує функції постійного моніторингу веб-додатків і надає повідомлення про нові вразливості в режимі реального часу. Це дозволяє організаціям своєчасно реагувати на нові загрози і підтримувати високий рівень безпеки.

6. Легкість використання: Інтерфейс Acunetix є зручним і інтуїтивно зрозумілим, що дозволяє швидко налаштувати і почати використовувати інструмент навіть користувачам з мінімальним досвідом у сфері безпеки. Acunetix також надає широкий спектр ресурсів для навчання, включаючи документацію, відео-уроки і технічну підтримку.

Отже, сканери вразливостей, такі як Acunetix, відіграють ключову роль у забезпеченні безпеки веб-додатків. Вони автоматизують процес виявлення та усунення вразливостей, забезпечують системний підхід до виявлення загроз, постійний моніторинг, документування та звітність. Інструменти, такі як Acunetix, пропонують широкий набір функцій для глибокого аналізу веб-додатків, інтеграції з процесом розробки та безперервного моніторингу. Використання сканерів вразливостей є невід'ємною частиною комплексної системи безпеки, яка допомагає організаціям гарантувати безпеку своїх веб-додатків та їхню відповідність законодавчим і нормативним вимогам.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЩОДО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ В ОРГАНІЗАЦІЯХ

2.1 Дослідження сучасних методів та засобів виявлення вразливостей і їх порівняння

У міру розвитку технологій веб-додатки стають дедалі складнішими та багатофункціональнішими, що робить їх привабливою мішенню для кіберзлочинців. Виявлення вразливостей веб-додатків є ключовим аспектом забезпечення їхньої безпеки. У цьому розділі ми розглянемоvсучасні методи та інструменти для виявлення вразливостей, а також порівняємо їх, щоб визначити найефективніші підходи до захисту веб-додатків. Особливу увагу буде приділено аналізу можливостей Acunetix, одного з провідних інструментів у цій галузі.

Методи виявлення вразливостей

Існує кілька основних методів виявлення вразливостей веб-додатків[6]:

1. Статичний аналіз коду (Static Analysis):

- Опис: Статичний аналіз коду виконується без запуску програми. Він аналізує вихідний або скомпільований код на наявність вразливостей.

- Переваги: Дає можливість виявити вразливості на ранніх стадіях розробки, що зменшує збитки та забезпечує глибокий аналіз коду.

- Недоліки: Не завжди може виявляти логічні помилки або вразливості, що проявляються тільки під час виконання програми.

2. Динамічний аналіз (Dynamic Analysis):

- Опис: Динамічний аналіз виконується під час роботи веб-додатка. Він імітує дії реальних користувачів і аналізує поведінку програми. Переваги: Виявляє вразливості, що проявляються тільки під час виконання програми. Може виявити логічні помилки і проблеми з конфігурацією.

- Недоліки: Для аналізу потрібен працюючий додаток, що може унеможливити процес тестування на ранніх стадіях розробки.

3. Аналіз на основі поведінки (Behavioral Analysis):

- Опис: Цей метод аналізує поведінку веб-додатка в різних умовах і порівнює її з нормальною поведінкою для виявлення аномалій.

- Переваги: Може виявляти нові та невідомі вразливості. Добре підходить для виявлення атак "нульового дня".

- Недоліки: Може давати помилкові спрацьовування, що ускладнює аналіз результатів. Потрібно багато часу на навчання і налаштування

4. Тестування на проникнення (Penetration Testing):

- Опис: Тестування на проникнення імітує реальні атаки на веб-додаток для виявлення його вразливостей.

- Переваги: Забезпечує реалістичне уявлення про стан безпеки. Виявляє вразливості, які можуть бути використані зловмисниками.

- Недоліки: Для проведення тестування потрібні висококваліфіковані фахівці. Це може бути дорогий і тривалий процес.

Засоби виявлення вразливостей

Сучасні засоби виявлення вразливостей веб-додатків включають різноманітні інструменти, кожен з яких має свої особливості, переваги та недоліки. Особливу увагу варто звернути на Acunetix – один із провідних інструментів у цій сфері.

1. Acunetix:

- Опис: Acunetix - це автоматизований інструмент для сканування веб-додатків на наявність вразливостей. Він є представником динамічного аналізу, що робить його потужним інструментом безпеки.

- Переваги: Підтримує велику кількість різних вразливостей, включаючи SQL-ін'єкції, XSS та CSRF. Інтегрується з CI/CD системами, забезпечуючи безперервний моніторинг. Генерує детальні звіти з рекомендаціями щодо усунення вразливостей. Acunetix також має функцію інтерактивного сканування, що дозволяє зменшити кількість хибних спрацювань.

- Недоліки: Може бути складним у налаштуванні для нових користувачів. Потребує регулярного оновлення бази даних вразливостей. Вартість ліцензії може бути високою для малих компаній.

2. Burp Suite:

- Опис: Burp Suite - це потужний інструмент для проведення тестування веб-додатків на проникнення тестування веб-додатків.

- Переваги: Включає широкий спектр інструментів для ручного й автоматизованого тестування. Підтримує модульність і розширюваність за допомогою плагінів.

- Недоліки: Вимагає високого рівня знань і досвіду для ефективного використання. Дорого для невеликих компаній.

3. OWASP ZAP (Zed Attack Proxy):

- Опис: OWASP ZAP є відкритим вихідним кодом інструментом для динамічного аналізу веб-додатків.

- Переваги: Безкоштовний, з відкритим вихідним кодом, активно підтримується спільнотою. Підходить як для новачків, так і для досвідчених фахівців.

- Недоліки: Може мати обмежений функціонал у порівнянні з комерційними рішеннями. Потребує додаткового налаштування для складних тестів.

4. Nessus:

- Опис: Nessus є інструментом для сканування вразливостей мережевих і веб-додатків.

- Переваги: Висока точність виявлення вразливостей. Широкий спектр підтримуваних платформ і вразливостей.

- Недоліки: Потребує ліцензії для повного функціоналу. Складним у налаштуванні для нових користувачів.

Порівняння засобів виявлення вразливостей

Для порівняння розглянутих засобів виявлення вразливостей використаємо кілька ключових критеріїв:

1. Точність виявлення:

- Acunetix: Висока точність завдяки регулярному оновленню бази даних вразливостей та інтерактивному скануванню.
- Burp Suite: Висока точність, особливо при ручному тестуванні.
- OWASP ZAP: Помірна точність, що залежить від налаштувань і знань користувача.
- Nessus: Висока точність для мережевих вразливостей, помірна для веб-додатків.

2. Легкість використання:

- Acunetix: Зручний інтерфейс, проте може бути складним у налаштуванні для нових користувачів.
- Burp Suite: Складний інтерфейс, потребує високого рівня знань.
- OWASP ZAP: Зручний для новачків, потребує налаштувань для складних тестів.
- Nessus: Зручний інтерфейс, проте потребує деякого часу на освоєння.

3. Інтеграція з CI/CD:

- Acunetix: Підтримує інтеграцію з популярними CI/CD системами, що дає змогу автоматизувати процес сканування.
- Burp Suite: Можлива інтеграція, але потребує додаткових налаштувань.
- OWASP ZAP: Підтримує інтеграцію з CI/CD через API.
- Nessus: Підтримує інтеграцію з CI/CD системами, проте здебільшого орієнтований на пошук мережевих вразливостей.

4. Вартість:

- Acunetix: Комерційне рішення з високою вартістю, проте пропонує широкий спектр можливостей та високу точність виявлення вразливостей.
- Burp Suite: Дороге комерційне рішення, яке виправдовує свою вартість широким спектром інструментів.

- OWASP ZAP: Безкоштовне з відкритим вихідним кодом, що робить його доступним для будь-якої організації.

- Nessus: Потребує ліцензії для повного функціоналу, що може бути дорогим для малих компаній.

Acunetix як провідний інструмент для виявлення вразливостей

Acunetix відрізняється від інших інструментів завдяки можливості поєднувати різні методи виявлення вразливостей. Він забезпечує не тільки автоматичне сканування, а й інтерактивне тестування, що значно підвищує точність і ефективність виявлення вразливостей.

Особливості Acunetix:

1. Регулярне оновлення бази даних вразливостей:

Acunetix постійно оновлює свою базу даних вразливостей, щоб виявляти нові загрози й атаки.

2. Інтеграція з CI/CD системами:

Підтримка інтеграції з популярними системами CI/CD дає змогу автоматизувати процес сканування і забезпечити безперервний моніторинг безпеки.

3. Детальні звіти та рекомендації:

Acunetix генерує докладні звіти з виявленими вразливостями і надає рекомендації щодо їх усунення.

Порівняння з іншими засобами

Якщо порівнювати Acunetix з іншими інструментами, такими як Burp Suite, OWASP ZAP і Nessus, то можна виділити кілька ключових аспектів:

1. Точність і ефективність:

- Acunetix демонструє високу точність під час інтерактивного сканування завдяки регулярному оновленню бази даних вразливостей. Інші інструменти, такі як Burp Suite, також забезпечують високу точність, але потребують більше ручної роботи та налаштувань.

2. Зручність використання:

- Acunetix має зручний інтерфейс і добре підходить для автоматичного сканування. OWASP ZAP зручний для новачків, але потребує налаштування для складних тестів. Burp Suite, незважаючи на свою міць, вимагає високого рівня знань для ефективного використання.

3. Інтеграція з CI/CD:

- Acunetix пропонує просту інтеграцію з системами CI/CD, що дає змогу автоматизувати процес сканування. Це забезпечує безперервний моніторинг і виявлення вразливостей.

4. Вартість:

- Acunetix - це комерційне рішення з високою вартістю, яка може виявитися непідйомною для невеликих компаній. OWASP ZAP безкоштовний і доступний для будь-якої організації, але може мати обмежену функціональність порівняно з комерційними рішеннями.

Отже, дослідження сучасних методів і засобів виявлення вразливостей веб додатків показало, що Acunetix є одним із найефективніших інструментів у цій галузі. Його регулярне оновлення бази даних вразливостей, підтримка інтеграції з системами CI/CD роблять його потужним інструментом для вдосконалення безпеки веб-додатків. Незважаючи на високу вартість, Acunetix пропонує широкий спектр можливостей, що робить його гідним вкладенням коштів для організацій, які прагнуть забезпечити високий рівень безпеки своїх веб-додатків. Інші інструменти, як-от Burp Suite, OWASP ZAP і Nessus, також мають свої переваги і можуть бути ефективними в певних умовах. Вибір відповідного інструменту залежить від конкретних потреб організації, її розміру, рівня знань фахівців і бюджету. Використання декількох інструментів одночасно може забезпечити більш комплексний підхід до виявлення та усунення вразливостей веб-додатків, що допоможе підвищити загальну безпеку організації.

2.2 Аналіз основних можливостей Acunetix

Забезпечення захисту веб-додатків – важливе питання в сучасному світі кібербезпеки. Збільшення кількості та складності атак вимагає від організацій використання надійних та ефективних інструментів для виявлення та усунення вразливостей. Acunetix є одним із таких інструментів, який зарекомендував себе як потужний сканер вразливостей веб-додатків. У цьому розділі ми розглянемо основні можливості Acunetix, його переваги та роль у забезпеченні безпеки веб-додатків.

Основні можливості Acunetix

1. Автоматизоване сканування

Acunetix пропонує високий рівень автоматизації процесу сканування веб-додатків, що значно скорочує час, необхідний для виявлення вразливостей. Автоматизоване сканування виявляє широкий спектр вразливостей, такі як SQL-ін'єкції, міжсайтовий скриптинг (XSS), підробки міжсайтових запитів (CSRF), директиви безпеки вмісту (CSP) і багато інших. Завдяки цьому інструменту організації можуть швидко й ефективно виявляти й усувати вразливості, знижуючи ризик компрометації даних.

2. Підтримка різних платформ і технологій

Acunetix підтримує сканування веб-додатків, розроблених на різних платформах і з використанням різних технологій, включно з HTML5, JavaScript, AJAX, RESTful веб-сервіси і SOAP. Це дає змогу виявляти вразливості в сучасних веб-додатках незалежно від використовуваної технології. Підтримка таких різних платформ робить Acunetix універсальним засобом захисту для різних середовищ розробки.

3. Регулярне оновлення бази даних вразливостей

Acunetix постійно оновлює свою базу даних вразливостей, що дає змогу виявляти нові загрози та методи атаки. Оновлення забезпечують актуальність інструменту і його здатність виявляти новітні вразливості, що виникають у швидко

мінливому світі кібербезпеки. Це робить Acunetix надійним інструментом для безперервного моніторингу безпеки веб додатків.

4. Генерація звітів і рекомендацій

Acunetix генерує докладні звіти про виявлені вразливості, надаючи детальну інформацію про кожну з них, включно з описом, рівнем серйозності, потенційним впливом і рекомендаціями щодо усунення. Це значно спрощує процес виправлення вразливостей і дає змогу командам розробників оперативно реагувати на загрози. Звіти також можуть бути налаштовані для різних типів аудиторій, включно з технічними фахівцями, менеджерами та зовнішніми аудиторами.

5. Інтеграція з CI/CD

Acunetix підтримує інтеграцію з популярними системами CI/CD (Continuous Integration / Continuous Deployment), такими як Jenkins, GitLab, Bamboo та іншими. Це дає змогу автоматизувати процес сканування на кожному етапі розробки, забезпечуючи безперервний моніторинг безпеки та швидке виявлення вразливостей. Інтеграція з системами CI/CD критично важлива для сучасних процесів розробки, де швидкість і безпека є ключовими вимогами.

Переваги Acunetix

1. Висока точність виявлення

Acunetix демонструє високу точність виявлення вразливостей завдяки інтерактивному скануванню і регулярному оновленню бази даних. Це дає змогу організаціям своєчасно виявляти й усувати вразливості, запобігаючи потенційним атакам. Висока точність зменшує кількість помилкових спрацьовувань, що економить час і ресурси команди безпеки.

2. Широкий спектр підтримуваних вразливостей

Acunetix підтримує виявлення великої кількості різних вразливостей, включно з найпоширенішими та найнебезпечнішими. Це робить його універсальним інструментом для захисту різних типів веб-додатків.

Завдяки цьому організації можуть бути впевнені в комплексному підході до захисту своїх ресурсів.

3. Зручність використання

Інтерфейс Acunetix розроблено з урахуванням потреб як новачків, так і досвідчених фахівців з безпеки. Інтуїтивно зрозумілий дизайн дає змогу швидко налаштовувати сканування й отримувати результати без додаткових зусиль. Це скорочує час на навчання і дає змогу зосередитися на виявленні та усуненні вразливостей.

4. Масштабованість

Acunetix добре підходить для організацій будь-якого розміру, від малих підприємств до великих корпорацій. Його можливості масштабування дають змогу ефективно сканувати як окремі додатки, так і великі веб-ресурси з великою кількістю сторінок. Це робить Acunetix гнучким інструментом, який може адаптуватися до потреб будь-якої організації.

Недоліки Acunetix

1. Вартість

Acunetix - комерційний продукт, і його вартість може бути високою, особливо для невеликих компаній. Однак інвестиції в цей інструмент_виправдані його можливостями та ефективністю.

2. Складність налаштування для новачків

Незважаючи на зручний інтерфейс, деякі функції Acunetix можуть бути складними в налаштуванні для нових користувачів. Необхідність попереднього навчання може затримати початок ефективного використання інструменту. Це може вимагати додаткових ресурсів для навчання персоналу та адаптації до нового інструменту.

3. Потреба в регулярному оновленні

Для забезпечення актуальності і точності виявлення вразливостей Acunetix необхідно регулярно оновлювати. Це може вимагати додаткових зусиль з боку фахівців з безпеки. Однак регулярні оновлення необхідні для підтримки високої ефективності інструменту.

2.3 Застосування Acunetix та аналіз отриманих даних

Захист веб-додатків надзвичайно важливий у сучасному кіберпросторі, де кількість атак та їхня складність постійно зростають. Acunetix – це провідний інструмент автоматизованого сканування вразливостей веб- додатків, який допомагає організаціям проактивно виявляти й усувати потенційні загрози. У цьому розділі ми детально розглянемо процес застосування Acunetix для сканування веб-додатків, а також проаналізуємо отримані дані для максимального підвищення рівня безпеки[7].

Процес сканування веб-додатків з Acunetix

1. Підготовка до сканування

Перш ніж почати сканування, необхідно правильно налаштувати Acunetix. Це включає в себе кілька ключових кроків:

- Встановлення інструменту: Завантажте та встановіть Acunetix на відповідний сервер або робочу станцію.

- Конфігурація облікового запису: Налаштування користувачів і прав доступу для забезпечення безпечного використання інструменту. Додавання цільових веб-додатків: Введіть URL-адреси веб-додатків, які будуть скануватися.

- Налаштування параметрів сканування: Визначте тип сканування, методи аутентифікації, винятки (наприклад, сторінки з конфіденційними даними) та інші специфічні налаштування, щоб зробити сканування максимально ефективним і безпечним.

2. Проведення сканування

Після завершення підготовки можна приступати до процесу сканування. Acunetix автоматично проводить детальний аналіз цільових веб-додатків, використовуючи різні методи для виявлення широкого спектра вразливостей. Сканування може займати від кількох хвилин до кількох годин, залежить від розміру та складності веб-додатка. Важливо забезпечити, щоб сканування проходило безперервно, без шкоди для продуктивності веб-додатка.

3. Моніторинг процесу сканування

Під час сканування адміністратори можуть стежити за його ходом через інтерфейс Acunetix. Це дає змогу бачити поточний статус сканування, які області вже було просканово і які вразливості було виявлено на цей момент. Такий моніторинг допомагає оперативно виявляти й усувати можливі проблеми, які можуть виникнути під час сканування.

Аналіз отриманих даних

1. Інтерпретація результатів сканування

Після завершення сканування Acunetix генерує докладні звіти, що містять інформацію про виявлені вразливості, їхню критичність, розташування у веб-додатку та рекомендації щодо усунення. Звіти Acunetix допоможуть вам зрозуміти, які саме вразливості присутні, який вплив вони можуть мати на безпеку вашого веб-додатка і як їх можна усунути.

2. Пріоритизація вразливостей

Усі виявлені вразливості мають бути класифіковані за рівнем критичності. Acunetix автоматично привласнює кожній уразливості рівень серйозності, даючи змогу командам безпеки зосередити зусилля нанайнебезпечніших загрозах . Наприклад, такі вразливості, як SQL-ін'єкції або XSS (міжсайтовий скриптинг), часто є висококритичними і потребують негайної уваги.

3. Розробка плану дій

На основі аналізу отриманих даних розробляється детальний план дій щодо усунення вразливостей. Цей план має містити конкретні заходи, строки їх виконання та відповідальних осіб важливо, щоб план був чітким і зрозумілим, щоб усі учасники процесу знали свої завдання і терміни їх виконання.

4. Виправлення вразливостей

Після розробки плану дій команда розробників приступає до_усунення вразливостей. Це може включати в себе:

- Оновлення коду: виправлення помилок у вихідному коді веб-додатка, що призводять до виникнення вразливостей.

- Зміна налаштувань сервера: Налаштуйте параметри сервера для підвищення безпеки.

- Застосовуйте додаткові заходи безпеки: Використовуйте такі заходи безпеки, як фаерволи веб-додатків (WAF), для захисту від потенційних атак.

5. Повторне сканування

Після усунення вразливостей слід провести повторне сканування, щоб переконатися, що всі проблеми усунуто. Повторне сканування також допомагає виявити нові вразливості, які можуть з'явитися внаслідок зміни коду або конфігурації. Це важливий крок для забезпечення безперервного моніторингу безпеки веб-додатків.

Роль Acunetix у забезпеченні безпеки

1. Автоматизація процесу виявлення вразливостей

Acunetix значно спрощує і прискорює процес виявлення вразливостей за рахунок автоматизації. Це дає змогу організаціям проводити регулярне сканування без значних витрат часу і ресурсів, що особливо важливо для великих і складних веб-додатків. Автоматизація також мінімізує можливість людської помилки, що підвищує загальну ефективність процесу.

2. Зниження ризиків та підвищення рівня безпеки

Acunetix допомагає організаціям знизити ризики кіберзагроз завдяки своєчасному виявленню та усуненню вразливостей. Це підвищує загальний рівень безпеки веб-додатків, захищаючи конфіденційні дані користувачів і організацій. Зниження ризиків сприяє підвищенню довіри користувачів до веб-додатків і зменшує ймовірність фінансових втрат через можливі атаки.

3. Інтеграція з розробницькими процесами

Acunetix підтримує інтеграцію з популярними CI/CD-системами, такими як Jenkins, GitLab, Bamboo та іншими. Це дає змогу автоматизувати процес сканування на кожному етапі розробки, забезпечуючи безперервний моніторинг безпеки та швидке виявлення вразливостей. Інтеграція з CI/CD-системами вкрай важлива для сучасних процесів розробки, де швидкість і безпека є ключовими вимогами.

4. Підвищення обізнаності та навчання команди

Acunetix не тільки виявляє вразливості, а й надає докладні рекомендації щодо їх усунення. Це допомагає підвищити обізнаність команди розробників у питаннях безпеки та сприяє їхньому навчанню.

Тому використання Acunetix для сканування веб-додатків і аналізу отриманих даних є найважливішим елементом забезпечення їхньої безпеки. Acunetix надає широкі можливості для автоматичного виявлення вразливостей, генерує докладні звіти та рекомендації, що дає змогу організаціям своєчасно реагувати на загрози та знижувати ризики.

Використання Acunetix у поєднанні з ефективними методами аналізу та усунення вразливостей забезпечує високий рівень захисту веб-додатків і допомагає підвищити загальну кібербезпеку організації. Автоматизація процесів, інтеграція із засобами розробки та постійне навчання команд роблять Acunetix незамінним інструментом для сучасних організацій, які прагнуть забезпечити безпеку своїх веб-додатків.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ НА ОСНОВІ ACUNETIX

3.1 Налаштування Acunetix для проведення сканування

Захист веб-додатків - ключовий елемент кібербезпеки для будь-якої сучасної організації. У зв'язку з постійним зростанням кількості атак на веб додатки необхідність використання ефективних інструментів для виявлення вразливостей стала критичною. Acunetix - один із провідних інструментів для автоматичного сканування веб-додатків на наявність вразливостей. Правильне налаштування цього інструменту дає змогу отримувати точні та релевантні результати, допомагаючи ефективно усувати загрози. У цьому розділі ми детально розглянемо процес налаштування Acunetix для забезпечення максимальної продуктивності сканування і виявлення вразливостей[8].

Початкове налаштування Acunetix

1. Встановлення Acunetix

Встановлення Acunetix - перший і важливий крок у підготовці до сканування веб-додатків. Цей процес передбачає завантаження інсталяційного пакета з офіційного сайту виробника, його розпакування і запуск інсталяційного файлу. Важливо дотримуватися всіх інструкцій, наданих виробником, щоб забезпечити правильне встановлення інструменту. Під час інсталяції необхідно вибрати відповідні параметри, такі як місце інсталяції, тип інсталяції (сервер або клієнт) та інші параметри, що можуть бути специфічними для вашої організації.

2. Конфігурація облікових записів

Після встановлення необхідно налаштувати облікові записи користувачів. Сюди входить створення облікових записів для адміністраторів та інших користувачів, які проводитимуть сканування. Важливо переконатися, що кожен обліковий запис має відповідні права доступу для забезпечення безпеки та зручності використання інструменту. Адміністративні облікові записи повинні мати повний доступ до всіх функцій Acunetix, тоді як інші користувачі можуть мати обмежені права доступу залежно від їхньої ролі.

Налаштування параметрів сканування

1. Додавання цільових веб-додатків (рисунок 3.1)

Наступним кроком буде додавання URL-адрес веб-додатків, які будуть переглядатися. Це можна зробити через інтерфейс Acunetix, де ви вводите URL кожного веб-додатка і, за необхідності, додаєте додаткові параметри, як-от імена піддоменів, конкретні маршрути або параметри запиту.

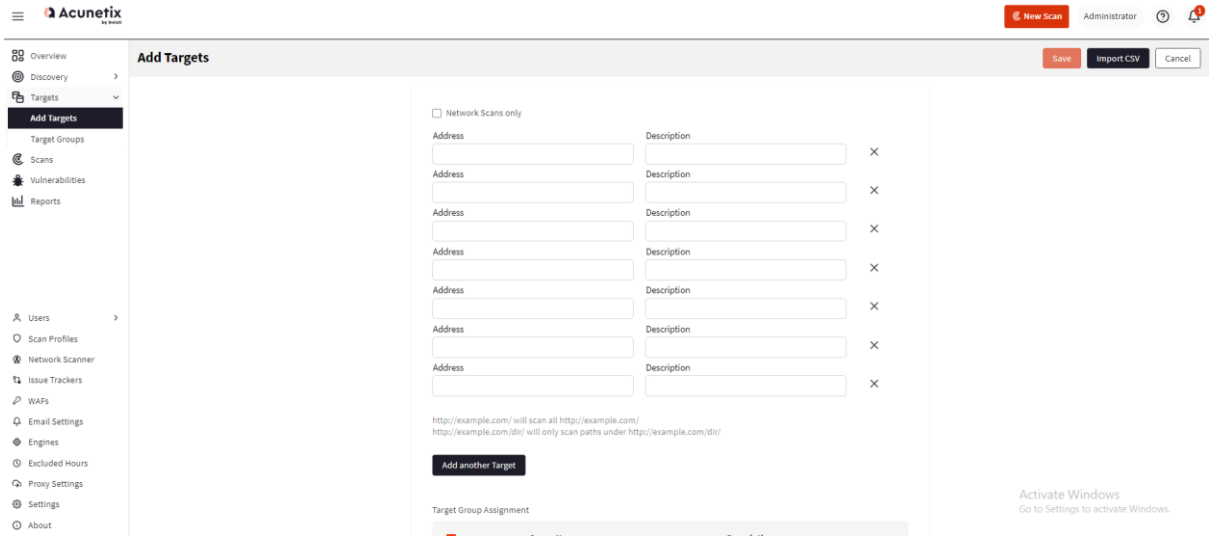

Рис. 3.1. Додавання цільових веб-додатків

2. Конфігурація методів автентифікації

Для того щоб Acunetix міг перевірити всі частини веб-додатка, важливо налаштувати методи аутентифікації. Acunetix підтримує різні типи автентифікації, включно з базовою автентифікацією, автентифікацією на основі форм, автентифікацією за допомогою маркера та іншими. Правильне налаштування аутентифікації дає змогу інструменту отримати доступ до захищених розділів веб-додатка і виконати повне сканування. Сюди входить введення облікових даних, налаштування сценаріїв входу і виходу з системи, а також налаштування обробки сеансів і маркерів.

3. Визначення типу сканування

Тип сканування визначає, наскільки детально Acunetix аналізуватиме веб-додаток. Для критично важливих застосунків рекомендується проводити глибоке сканування, яке включає перевірку всіх сторінок, включно з підсторінками та динамічними елементами. Acunetix дає змогу налаштовувати тип сканування,

вибираючи між швидким, стандартним і глибоким режимами. Глибоке сканування зазвичай займає більше часу, але дає змогу виявити більше вразливостей, що робить його ідеальним для критично важливих і складних веб-додатків.

4. Налаштування виключень

Іноді деякі частини веб-додатків не потребують сканування, наприклад, сторінки з конфіденційними даними або сторінки, що створюють високе навантаження на сервер. Acunetix дає змогу налаштовувати винятки, що дає змогу уникнути зайвих накладних витрат і забезпечує точніші результати сканування. Винятки можна налаштувати за URL, типом файлу або іншими критеріями відповідно до специфічних вимог вашої організації.

Оптимізація налаштувань для ефективного сканування

1. Використання шаблонів сканування

Acunetix пропонує різні шаблони сканування для різних типів веб-додатків. Використання шаблонів дає змогу швидко налаштувати інструмент для сканування стандартних застосунків, заощадивши час і зусилля. Шаблони містять опції для сканування CMS-систем, інтернет- магазинів, корпоративних сайтів тощо. Кожен шаблон має попередньо налаштовані параметри, що дають змогу оптимізувати процес сканування для певного типу веб-додатків.

2. Налаштування обмежень сканування

Для великих веб-додатків корисно встановлювати ліміти сканування, що дає змогу контролювати час і ресурси, що витрачаються на сканування. Це може включати обмеження кількості одночасних запитів, таймаути встановлення запитів та інші параметри, що дають змогу оптимізувати процес сканування. Ці налаштування дають змогу уникнути перевантаження сервера і забезпечити стабільність роботи веб-додатка під час сканування.

3. Використання планувальника завдань (рисунок 3.2)

У Acunetix є вбудований планувальник завдань, що дає змогу автоматизувати процес сканування. Це особливо корисно під час регулярного сканування, яке можна налаштовувати в певні дні та час для забезпечення постійного моніторингу безпеки. Планувальник завдань також дає змогу уникнути пікових навантажень на сервер у робочий час,що мінімізує вплив на продуктивність веб-додатків.

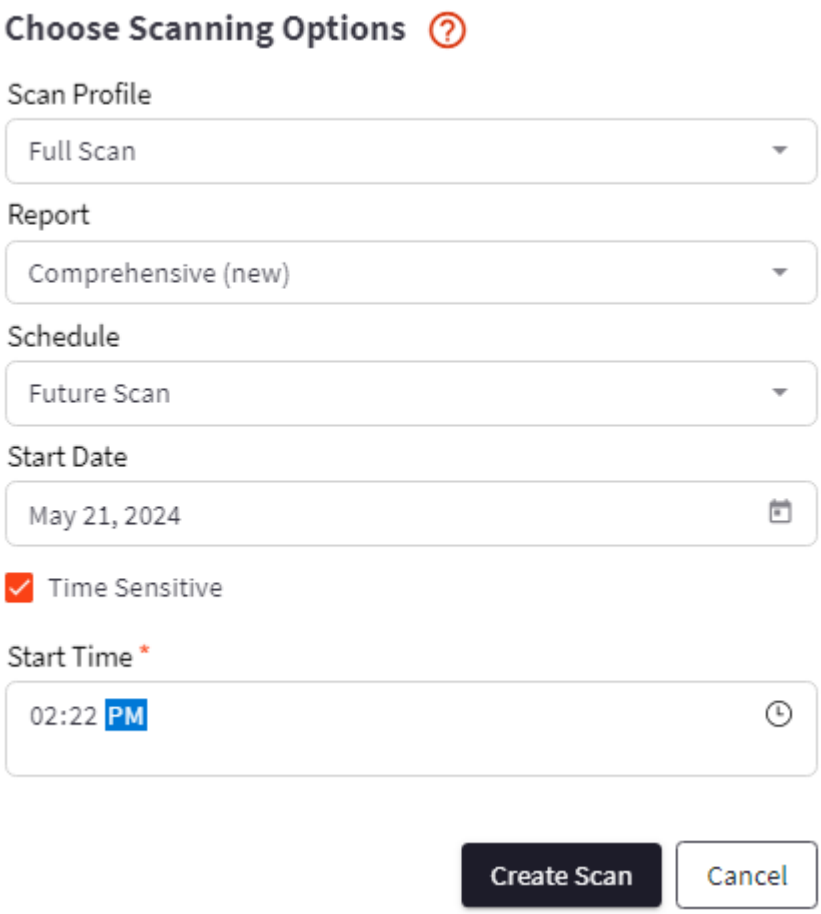

Рис. 3.2. Використання планувальника завдань

Проведення тестового сканування

1. Перевірка налаштувань

Перед проведенням повного сканування рекомендується виконати тестове сканування, щоб перевірити правильність налаштувань. Це дає змогу виявити та виправити можливі помилки в налаштуваннях до початку основного сканування.

Тестове сканування також допомагає оцінити тривалість і ефективність процесу, що важливо для планування ресурсів і часу.

2. Аналіз результатів тестового сканування

Після завершення тестового сканування важливо ретельно проаналізувати результати. Це дасть змогу виявити можливі проблеми в налаштуваннях і внести необхідні корективи. На цьому етапі також можна оцінити точність виявлення вразливостей і ефективність налаштованих параметрів. Аналіз результатів тестового сканування допоможе вам підготуватися до основного сканування і забезпечити його максимальну ефективність.

Підготовка до основного сканування

1. Остаточне налаштування

Після успішного завершення тестового сканування і внесення коригувань можна переходити до остаточного налаштування Acunetix для основного сканування. Сюди входить підтвердження всіх параметрів і винятків, налаштування аутентифікації та глибини сканування. Важливо переконатися, що всі налаштування відповідають вимогам і специфікаціям вашої організації.

2. Запуск основного сканування

Основне сканування може бути запущено після завершення підготовчих сканувань. етапів. Важливо контролювати процес сканування, щоб своєчасно реагувати на можливі проблеми. Acunetix надає інструменти моніторингу в режимі реального часу, які дають змогу бачити поточний статус сканування і виявлені вразливості.

Тому правильне налаштування Acunetix для виконання сканування - ключовий крок у забезпеченні безпеки веб-додатків. Від ретельності налаштувань залежить точність і ефективність виявлення вразливостей. Підготовка до сканування передбачає встановлення інструменту, налаштування облікових записів, додавання цільових веб-додатків, а також налаштування параметрів сканування і винятків. Оптимізація налаштувань допомагає підвищити ефективність сканування і забезпечити максимальну безпеку. Проведення

тестового сканування дає змогу виявити та виправити можливі помилки до початку основного сканування. Правильно налаштувавши Acunetix, організації зможуть ефективно захистити свої веб-додатки від кіберзагроз і забезпечити безпеку конфіденційних даних.

Постійне вдосконалення налаштувань і адаптація до нових загроз дає нам змогу забезпечувати високий рівень захисту веб-додатків, що вкрай важливо в сучасному кіберпросторі. Використання Acunetix у поєднанні з іншими методами та інструментами кібербезпеки створює комплексну систему захисту, що дає змогу вчасно виявляти й усувати вразливості, мінімізувати ризики та забезпечувати безперервну роботу веб-застосунків.

3.2 Ідентифікація та класифікація виявлених вразливостей

Виявлення вразливостей у веб-додатках є ключовим етапом у процесі забезпечення їхньої безпеки. Після виявлення вразливостей важливо правильно їх ідентифікувати та класифікувати для подальшого усунення. У цьому розділі детально розглядається процес ідентифікації та класифікації виявлених вразливостей, зокрема за допомогою інструменту Acunetix, що є лідером у галузі автоматизованого сканування веб-додатків[9].

Ідентифікація вразливостей

1. Процес ідентифікації

Процес виявлення вразливостей починається зі сканування веб- додатків за допомогою Acunetix. Для виявлення потенційних загроз Acunetix використовує різні методи і технології, включаючи аналіз вихідного коду, сканування на основі сигнатур, евристичний аналіз та інші. Важливою особливістю Acunetix є його здатність виявляти широкий спектр вразливостей, включно з як відомими, так і новими загрозами.

2. Типи виявлених вразливостей

У процесі сканування Acunetix може виявити різні типи вразливостей, включно з:

- SQL-ін'єкції: атаки, що дають змогу зловмисникам виконувати довільні SQL-запити до бази даних.
- XSS (Cross Site Scripting): Атаки, що дають змогу вставляти шкідливий код на веб-сторінки, який потім виконують у браузерах користувачів.
- CSRF (Cross-Site Request Forgery): Атаки, які змушують користувача виконувати небажані дії на сайті, на який він зайшов.
- Вразливіості аутентифікації та сеансів управління: проблеми, що дають змогу зловмисникам обходити процеси аутентифікації або викрадати сеанси користувачів.
- Небезпечне завантаження файлів: Вразливіості, що дають змогу завантажувати на сервер шкідливі файли.
- Необґрунтоване розкриття інформації: Вразливіості, що призводять до витоку конфіденційної інформації.

3. Інтеграція з іншими інструментами

Для ефективнішого виявлення вразливостей Acunetix можна інтегрувати з іншими інструментами безпеки, як-от системи управління вразливостями (Vulnerability Management Systems), системи аналізу безпеки коду (Static Application Security Testing, SAST) та інші. Така інтеграція дає змогу отримати повнішу картину загроз і підвищити ефективність процесу ідентифікації.

Класифікація вразливостей

1. Важливість класифікації

Після виявлення вразливостей важливо розподілити їх за категоріями, щоб розставити пріоритети в процесі усунення. Класифікація дає змогу організації зосередитися на найважливіших загрозах, які мають найбільший потенціал для завдання шкоди. Acunetix надає інструменти для автоматичної класифікації вразливостей на основі різних критеріїв.

2. Критерії класифікації

Основні критерії класифікації вразливостей включають:

- Серйозність: Вразливості класифікують за ступенем серйозності, включно з критичною, високою, середньою та низькою.

- Тип Вразливіості: Вразливіості класифікуються за їхнім типом, наприклад, SQL-ін'єкції, XSS, CSRF тощо.

- Імовірність експлуатації: Оцінює ймовірність того, що вразливість буде використана зловмисниками.

- Вплив на систему: оцінюється можливий вплив Вразливіості на систему, включно з можливістю витоку даних, компрометації системи, втрати доступу тощо.

3. Використання CVSS

Common Vulnerability Scoring System (CVSS) - це стандарт для оцінювання серйозності вразливостей. Acunetix використовує CVSS для визначення рівня серйозності виявлених вразливостей. CVSS оцінює вразливості за кількома параметрами, включно з базовою оцінкою (вплив на конфіденційність, цілісність і доступність), оцінкою часу (ефективність засобів усунення) і оцінкою екосистем (вплив на конкретну організацію).

4. Приклади класифікації

Щоб проілюструвати процес класифікації, розглянемо кілька прикладів:

- SQL-ін'єкція у формах введення даних: Критичний рівень через можливість доступу до бази даних і виконання довільних запитів.

- XSS на сторінці коментарів: Високий рівень, оскільки може призвести до крадіжки сесійних cookie або виконання шкідливого коду в браузері користувача.

- Вразливіість завантаження файлів без перевірки типу файлу: Помірна, оскільки може призвести до завантаження на сервер шкідливих файлів, які можуть бути використані для подальших атак.

- Непотрібне розкриття інформації в HTTP-заголовках: Низький рівень, оскільки розкрита інформація може бути менш критичною, але все одно може бути використана для подальших атак.

Використання результатів ідентифікації та класифікації

1. Планування усунення вразливостей

Після виявлення та класифікації вразливостей важливо розробити план їх усунення. Цей план має враховувати рівень критичність кожної вразливості, її вплив на систему та ресурси, необхідні для усунення. Вразливіості з високим рівнем критичності мають бути усунуті насамперед, а менш критичні можна запланувати на пізніші етапи.

2. Інтеграція з системами управління уразливостями

Процес усунення вразливостей Acunetix може інтегруватися з процесом управління системами. Це дає змогу автоматизувати процеси виявлення, класифікації та усунення вразливостей, а також забезпечити безперервний моніторинг і звітність. Такі системи допомагають відстежувати статус кожної вразливості, призначати відповідальних за її усунення та контролювати виконання завдань

3. Документування і навчання

Важливим кроком є документування виявлених вразливостей і процесу їх усунення. Це допоможе створити базу знань для майбутніх аудитів і навчання персоналу. Навчання співробітників на основі виявлених вразливостей і способів їх усунення допомагає підвищити загальний рівень кібербезпеки в організації

Таким чином, виявлення і класифікація виявлених вразливостей - важливий крок у забезпеченні безпеки веб-додатків. Правильна систематизація виявлених проблем дає змогу ефективно виявляти й усувати потенційні загрози. Цей процес охоплює аналіз результатів сканування, виявлення вразливостей і їхню класифікацію за типами та ступенем серйозності. Дотримання цих кроків дає змогу забезпечити максимальний рівень безпеки веб-додатків і захистити конфіденційну інформацію від потенційних кіберзагроз.

3.3 Рекомендації щодо виявлення вразливостей Web-додатків на основі Acunetix

Acunetix пропонує широкий спектр можливостей аналізу безпеки, однак для максимального використання цього інструменту необхідно правильно налаштувати його та ефективно проаналізувати результати сканування. У цьому розділі ми розглянемо рекомендації щодо оптимізації налаштувань Acunetix і поліпшення процесу аналізу результатів для підвищення загальної ефективності[10].

Оптимізація налаштувань Acunetix

1. Вибір належних профілів сканування

- Acunetix пропонує багато профілів сканування, які можна налаштувати відповідно до конкретних потреб веб-додатку. Використання стандартних профілів сканування ефективне для загальної перевірки безпеки, але для детальнішого аналізу необхідно налаштувати користувацькі профілі.

- Стандартні профілі: Використання стандартних профілів дає змогу швидко виконати базове сканування для виявлення найпоширеніших вразливостей. Ці профілі містять загальні тести, які охоплюють найпоширеніші типи атак, як-от SQL- ін'єкції, XSS, CSRF та інші.

- Користувацькі профілі: Налаштування користувацьких профілів Дозволяє сфокусувати сканування на певних аспектах веб-додатка. Це може включати додавання або видалення певних типів тестів, а також налаштування глибини аналізу. Наприклад, для веб-додатків, що працюють із конфіденційною інформацією, може бути доцільно включати додаткові тести для виявлення слабких місць у системі авторизації та аутентифікації.

2. Конфігурація політик виявлення

Політики виявлення в Acunetix дають змогу визначити, які типи вразливостей шукатимуть під час сканування. Правильне налаштування цих політик - ключ до ефективного виявлення загроз.

- Адаптація політик: Політики виявлення мають бути адаптовані відповідно до специфіки веб-додатку та його інфраструктури. Це включає налаштування параметрів для виявлення специфічних вразливостей, таких як SQL-ін'єкції, XSS (міжсайтові скрипти), CSRF (міжсайтові підробки запитів) тощо. Наприклад, для веб-додатку, який використовує API для обміну даними, важливо включити тести для перевірки безпеки API-запитів.

- Детальні політики: Використання детальних політик дозволяє зосередитися на виявленні певних типів вразливостей, які можуть бути найбільш критичними для конкретного веб-додатку. Це може включати налаштування рівня чутливості та глибини аналізу. Наприклад, для додатків з високими вимогами до безпеки, таких як фінансові сервіси, необхідно включити детальні тести для перевірки захисту від атак, спрямованих на викрадення даних.

Налаштування політик виявлення повинно враховувати як технічні характеристики веб-додатку, так і його бізнес-цілі. Це дозволяє зосередитися на найбільш критичних аспектах безпеки. Наприклад, для веб-додатків, що обробляють фінансові транзакції, особливу увагу слід приділити захисту від атак на фінансові дані та транзакції.

3. Оптимізація використання ресурсів

Оптимізація використання ресурсів - важливий аспект для забезпечення ефективності сканування, особливо у великих організаціях з великою кількістю веб-додатків.

- Сканування за розкладом: Налаштування планують сканування, щоб мінімізувати вплив на продуктивність системи під час пікових навантажень. Це дає змогу запобігти зниженню продуктивності веб-додатків під час сканування. Наприклад, сканування можна запланувати на ніч або на вихідні, коли навантаження на систему мінімальне.

- Паралельне сканування: Використовуйте паралельне сканування для прискорення процесу перевірки великих веб- додатків. Це дає змогу одночасно аналізувати різні частини веб-додатка, значно скорочуючи загальний час

сканування. Паралельне сканування може бути особливо корисним для великих веб-додатків з великою кількістю сторінок і функцій.

Покращення процесу аналізу результатів

1. Аналіз звітів та пріоритезація вразливостей

Ефективний аналіз звітів є критично важливим для швидкого та точного виявлення вразливостей.

- Функції сортування та фільтрації Acunetix дають змогу швидко виявити критичні вразливості. Це дає змогу зосередитися на найнебезпечніших загрозах і швидко вжити необхідних заходів. Наприклад, можна відсортувати вразливості за рівнем критичності, щоб насамперед усунути найнебезпечніші.

- Система пріоритезації: Впровадження системи пріоритезації вразливостей, що враховує як технічні аспекти, так і потенційні бізнес-ризики. Це допомагає визначити, які вразливості вимагають негайного усунення, а які можуть бути відкладені на більш пізній термін. Пріоритезація вразливостей може також включати використання метрик ризику, таких як CVSS (Common Vulnerability Scoring System), які дають змогу оцінити потенційний вплив вразливості на організацію.

2. Інтеграція з іншими інструментами безпеки

Інтеграція Acunetix з іншими інструментами безпеки дозволяє створити комплексну систему управління вразливостями та автоматизувати процес усунення загроз.

- Інтеграція з системами управління вразливостями: Інтеграція Acunetix з іншими системами управління вразливостями дає змогу централізовано керувати виявленими вразливостями та відстежувати хід їх усунення. Наприклад, інтеграція з такими платформами, як Jira або ServiceNow, дає змогу автоматично створювати завдання з усунення вразливостей.

- Інтеграція з інструментами CI/CD: Інтеграція з інструментами CI/CD (Continuous Integration/Continuous Deployment) для автоматизації процесу виявлення й усунення вразливостей на всіх етапах розроблення та розгортання веб-додатків. Це дає змогу виявляти вразливості на ранніх стадіях розробки та оперативно реагувати на них. Наприклад, інтеграція з Jenkins або GitLab CI/CD дає змогу автоматично запускати сканування.

- Використання API: Використання API Acunetix для створення індивідуальних рішень у сфері науки про дані. Це дає змогу автоматизувати процеси та інтегрувати Acunetix з іншими системами, що використовуються в організації. Наприклад, API можна використовувати для автоматичного експорту результатів сканування у внутрішні бази даних або системи звітності.

Інтеграція з іншими засобами захисту дає змогу створити єдину систему моніторингу та управління вразливостями, що значно підвищує загальний рівень безпеки. Наприклад, інтеграція з системами SIEM (Security Information and Event Management) дає змогу централізовано відстежувати й аналізувати події безпеки.

3. Навчання та підвищення кваліфікації персоналу

Навчання та розвиток персоналу є важливим елементом для забезпечення ефективного використання Acunetix і правильної інтерпретації результатів сканування.

- Навчання: Проведення тренінгів для співробітників з використання Acunetix та інтерпретації результатів сканування. Це допоможе переконатися, що всі користувачі інструменту володіють необхідними знаннями та навичками для його ефективного використання. Наприклад, регулярне навчання може включати практичні заняття з аналізу звітів і налаштування параметрів сканування.

- Внутрішні інструкції: Розроблення внутрішніх інструкцій і посібників, які допоможуть швидко реагувати на виявлені загрози І правильні варіанти налаштування сканування. Внутрішні інструкції можуть містити покрокові інструкції з використання різних функцій Acunetix і рекомендації щодо оптимізації налаштувань.

Навчання співробітників також охоплює ознайомлення з новими функціями та оновленнями Acunetix, що дасть вам змогу отримати максимальну віддачу від вашого інструменту для забезпечення безпеки веб-додатків. Наприклад, регулярні вебінари та семінари допоможуть співробітникам бути в курсі останніх інновацій у сфері кібербезпеки.

Практичні рекомендації

Щоб підвищити ефективність використання Acunetix і забезпечити надійний захист веб-додатків, варто взяти до уваги такі практичні рекомендації:

1. Регулярне оновлення інструменту: Забезпечення регулярного оновлення Acunetix до останньої версії, щоб мати доступ до нових функцій і поліпшень. Наприклад, оновлення можуть містити нові функції для виявлення новітніх типів вразливостей.

2. Моніторинг результатів сканування: Постійно відстежуйте результати сканування, щоб своєчасно виявляти нові вразливості та швидко їх усувати. Наприклад, ви можете налаштувати автоматичні повідомлення про критичні вразливості, щоб швидко реагувати на них.

3. Автоматизація процесів: використання автоматизації для скорочення ручної праці та підвищення точності аналізу. Наприклад, автоматизація процесу генерації звітів дає змогу швидко отримувати докладні звіти про результати сканування.

4. Документування процесів: Документування всіх процесів кастомізації та аналіз послідовності й повторюваності дій.

Використання цих рекомендацій допомагає створити безпечніше середовище для веб-додатків, знизити ризик експлуатації вразливостей і підвищити загальний рівень кібербезпеки організації. Постійне вдосконалення процесів і налаштувань, а також підвищення кваліфікації персоналу є ключовими факторами для досягнення високого рівня безпеки веб-додатків.

Таким чином, правильне використання Acunetix у поєднанні з системним підходом до забезпечення безпеки дає змогу забезпечити надійний захист веб-додатків від кіберзагроз і зберегти конфіденційність, цілісність і доступність даних, оброблюваних веб-додатками.

ВИСНОВОК

Забезпечення безпеки веб-додатків є критично важливим аспектом у сучасному світі, де кіберзагрози стають все більш витонченими і масштабними. У своїй бакалаврській роботі ми детально розглянули методи виявлення вразливостей веб-додатків, використання інструменту Acunetix та розробку рекомендацій щодо їх усунення. Ця робота охоплює основні аспекти кібербезпеки, починаючи з аналізу проблеми і закінчуючи практичними рекомендаціями, які можуть бути впроваджені у реальних організаціях.

Основні аспекти роботи

1. Аналіз проблеми та основні поняття безпеки веб-додатків

На початку роботи було розглянуто основні поняття безпеки веб-додатків. Веб-додатки є особливо вразливими до атак через їхню доступність через Інтернет та складну архітектуру. Основні загрози включають SQL-ін'єкції, кросс-сайтовий скриптінг (XSS), CSRF (Cross-Site Request Forgery) та інші види атак, що можуть призвести до витоку конфіденційної інформації, компрометації даних та інших серйозних наслідків. Важливість розуміння цих понять полягає у можливості адекватного захисту додатків і зниження ризиків, пов'язаних із кіберзлочинністю.

2. Аналіз вразливостей та види веб-додатків

У наступному розділі було проведено детальний аналіз вразливостей, характерних для різних видів веб-додатків. Важливо розуміти, що кожен тип веб-додатка має свої особливості і специфічні загрози. Наприклад, для електронних магазинів особливо критичними є вразливості, пов'язані з обробкою платежів, тоді як для соціальних мереж важливо захистити особисті дані користувачів. Це розділення допомагає розробникам і фахівцям з безпеки більш цілеспрямовано підходити до захисту різних типів веб-додатків, зосереджуючись на специфічних загрозах для кожного з них.

3. Визначення ролі і місця сканерів виявлення вразливостей для безпеки веб-додатків

Було розглянуто роль сканерів виявлення вразливостей, таких як Acunetix, у забезпеченні безпеки веб-додатків. Ці інструменти автоматизують процес виявлення вразливостей, що дозволяє знизити ризик людських помилок та прискорити процес ідентифікації загроз. Acunetix, зокрема, пропонує широкий спектр функцій для глибокого аналізу безпеки, включаючи сканування на наявність відомих вразливостей, перевірку на наявність уразливих конфігурацій та інші можливості. Використання таких сканерів є невід'ємною частиною сучасної стратегії забезпечення кібербезпеки, оскільки вони надають змогу оперативно виявляти та усувати вразливості до того, як вони будуть використані зловмисниками.

4. Дослідження сучасних методів та засобів виявлення вразливостей

Було проведено дослідження сучасних методів та засобів виявлення вразливостей, а також їх порівняння. Acunetix було визначено як один з провідних інструментів у цій галузі завдяки його можливостям автоматизації та точності виявлення вразливостей. Інші інструменти, такі як Nessus, Burp Suite, та OpenVAS, також були розглянуті для порівняння їхніх можливостей та особливостей. Порівняння включало такі аспекти, як точність виявлення, зручність використання, можливості інтеграції з іншими системами безпеки, а також вартість. Це дозволяє обрати найбільш підходящий інструмент для конкретних потреб організації, враховуючи їхні ресурси та вимоги.

5. Аналіз основних можливостей Acunetix

Було детально розглянуто основні можливості Acunetix. Інструмент пропонує широкий набір функцій, включаючи підтримку різних методів автентифікації, можливість налаштування глибини сканування, конфігурацію виключень та використання шаблонів сканування. Acunetix також має вбудований планувальник завдань, що дозволяє автоматизувати регулярні сканування та забезпечити постійний моніторинг безпеки веб-додатків. Крім того, він надає інструменти для звітності та аналізу результатів, що дозволяє фахівцям з безпеки ефективно виявляти та усувати вразливості. Ці можливості роблять Acunetix потужним інструментом у арсеналі кібербезпеки будь-якої організації.

6. Застосування Acunetix та аналіз отриманих даних

Було описано процес застосування Acunetix для сканування веб-додатків та аналіз отриманих даних. Важливо провести тестове сканування перед основним, щоб перевірити правильність налаштувань і оцінити тривалість та ефективність процесу. Після сканування результати повинні бути ретельно проаналізовані, щоб виявити і класифікувати всі вразливості. Acunetix надає можливість детального аналізу вразливостей, включаючи їхнє детальне описання, рекомендації щодо усунення та оцінку ризику. Це дозволяє фахівцям з безпеки пріоритезувати заходи щодо усунення вразливостей і ефективно розподіляти ресурси.

7. Розробка рекомендацій щодо виявлення вразливостей веб-додатків на основі Acunetix

На основі отриманих результатів було розроблено рекомендації щодо виявлення вразливостей веб-додатків з використанням Acunetix. Це включає налаштування інструменту для проведення сканування, ідентифікацію та класифікацію виявлених вразливостей, а також оптимізацію налаштувань для підвищення ефективності та вдосконалення процесу аналізу результатів. Правильне налаштування та використання Acunetix дозволяє значно підвищити рівень безпеки веб-додатків і знизити ризик їх компрометації. Рекомендації також включають постійне моніторинг і оновлення налаштувань, щоб адаптуватися до нових загроз і забезпечити максимальну ефективність захисту.

Ппідсумовуючи все вище сказане робота продемонструвала, що Acunetix є потужним інструментом для виявлення вразливостей веб-додатків, який значно спрощує процес забезпечення їхньої безпеки. Правильне налаштування та використання цього інструменту дозволяє ефективно ідентифікувати та усувати загрози, забезпечуючи захист конфіденційних даних та стабільну роботу веб-додатків. Виконані дослідження і розроблені рекомендації можуть бути корисними для фахівців з кібербезпеки та організацій, що прагнуть підвищити рівень захисту своїх веб-ресурсів від потенційних кіберзагроз.

Крім того, ця робота підкреслила важливість комплексного підходу до кібербезпеки, який включає не тільки використання сучасних інструментів для виявлення вразливостей, але й постійне навчання персоналу, розробку політик безпеки та впровадження найкращих практик у повсякденну діяльність організацій. Лише за умови системного підходу можна забезпечити надійний захист веб-додатків від сучасних кіберзагроз і забезпечити їхню безперебійну та безпечну роботу.

Таким чином, розробка рекомендацій на основі результатів сканування, проведеного за допомогою Acunetix, та їх впровадження в реальні процеси кібербезпеки дозволяє суттєво підвищити рівень захисту веб-додатків. Це, в свою чергу, знижує ризики витоку конфіденційної інформації, компрометації даних та інших негативних наслідків, забезпечуючи стабільність і надійність роботи веб-додатків у сучасному кіберпросторі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Документація Acunetix – Introduction to Acunetix. URL:https://www.acunetix.com/support/ (дата звернення: 23.05.2024).

2. Stuttard, D., Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Глава 2 (стр. 20-45). URL: https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Dafydd%20Stuttard,%20Marcus%20Pinto%20-%20The%20web%20application%20hacker%27s%20handbook_%20finding%20and%20exploiting%20security%20flaws-Wiley%20(2011).pdf

(дата звернення: 23.05.2024).

3. OWASP Injection. URL: https://owasp.org/Top10/A03_2021-Injection/ (дата звернення: 23.05.2024).

4. OWASP Cross-Site Scripting. URL: https://owasp.org/www-community/attacks/xss/ (дата звернення: 23.05.2024).

5. OWASP Testing Framework. URL: https://github.com/OWASP/wstg/tree/master/document (дата звернення: 23.05.2024).

6. Stuttard, D., Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Глава 4 (стр. 60-85). URL: https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Dafydd%20Stuttard,%20Marcus%20Pinto%20-%20The%20web%20application%20hacker%27s%20handbook_%20finding%20and%20exploiting%20security%20flaws-Wiley%20(2011).pdf (дата звернення:23.05.2024).

7. Документація Acunetix – Reporting. URL: https://www.acunetix.com/support/ (дата звернення: 23.05.2024).

8. Документація Acunetix – Scan Profiles. URL: https://www.acunetix.com/support/ (дата звернення: 23.05.2024).

9. Документація Acunetix – Vulnerabilities. URL: https://www.acunetix.com/support/ (дата звернення: 23.05.2024).

10. Документація Acunetix – Types of scans. URL: https://www.acunetix.com/support/ (дата звернення: 23.05.2024).