МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра кібербезпеки

«До захисту допущено»

Завідувач кафедри

_____ Володимир ЛЮБЧАК

(підпис)

____ _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека ,

освітньо-професійної програми Кібербезпека

на тему: Дослідження технологій «розкрутки» сайту

Здобувача (ки) групи КБ-01 Корокіна Всеволода Валерійовича

(шифр групи) (прізвище, ім’я, по батькові)

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

_____ Всеволод КОРОКІН

(підпис) (Ім’я та ПРІЗВИЩЕ здобувача)

Керівник _____ _____

(посада, науковий ступінь, вчене звання, Ім’я та ПРІЗВИЩЕ) (підпис)

Суми – 2024

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра кібербезпеки

«Затверджую»

Завідувач кафедри

_____ Володимир ЛЮБЧАК

(підпис)

«___»_____ 20___ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 – Кібербезпека, освітньо-професійної програми «Кібербезпека»

здобувача групи КБ-01 Корокіна Всеволода Валерійовича

1. Тема роботи: «Дослідження технологій «розкрутки» сайту».

затверджено наказом по СумДУ №0212-VI від «04» березня 2024 р.

2. Термін подання студентом роботи: «31» травня 2024 р.

3. Вихідні дані до роботи: _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити): _____

_____

_____

_____

_____

5. Перелік графічного матеріалу (із зазначенням плакатів, презентацій тощо) _____

6. Консультанти до проекту (роботи), із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ Керівник _____

(підпис) (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	Визначення завдання та об’єкта роботи		
2	Пошук та опрацювання теоретичного матеріалу з теми випускної роботи		
3	Огляд досліджуваного об’єкту		
4	Виконання практичної роботи		
5	Оформлення кваліфікаційної роботи		

Здобувач вищої освіти _____ Керівник _____

(підпис) (підпис)

АНОТАЦІЯ

Кваліфікаційна робота виконана на 52 аркушах, містить 14 рисунків, та 15 джерел.

Об'єкт дослідження. Процеси просування сайтів.

Мета роботи. Дослідження плагінів для просування сайтів з акцентом на їх уразливості. Аналіз популярних SEO-плагінів, визначення потенційних ризиків безпеки, які вони можуть створювати, рекомендацій для їх безпечного використання.

Методи дослідження. Для досягнення поставленої мети використовувалися методи теоретичного аналізу наукових джерел, емпіричного дослідження практичних кейсів, порівняння та узагальнення отриманих даних.

Результат роботи. Результати роботи включають комплексний огляд та класифікацію популярних SEO-плагінів, огляд критеріїв безпеки, їх оцінка, аналіз основних уразливостей та рекомендації по їх усуненню.

Структура роботи. У дипломній роботі розглядається проблематика просування сайтів, основні методи їх просування та дослідження безпеки застосованих методів. Перший розділ присвячений огляду проблематики та викликів просування сайтів, а також сучасним технологіям та інструментам для SEO-оптимізації. Другий розділ охоплює методи просування, такі як SEO, контекстна реклама (PPC), соціальні медіа маркетинг (SMM), і використання плагінів (Yoast SEO, All in One SEO Pack, Rank Math). Третій розділ містить практичне дослідження безпеки, аналіз уразливостей плагінів (Slider Revolution, Contact Form 7, Akismet) та сканування сайту за допомогою WPScan. Висновки роботи підсумовують результати дослідження, ефективність методів просування та їх безпеку, а також надають рекомендації.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ 11
ВСТУП 7
1. ОГЛЯД ПРОБЛЕМАТИКИ ПРОСУВАННЯ 9
1.1. Загальні поняття про просування 9
1.2 Розвиток методів просування 11
1.2.1 Початковий етап (1990-ті роки) 11
1.2.2 Розвиток пошукових систем (кінець 1990-х - початок 2000-х років) 11
1.2.3 Початок маніпулятивних технік (середина 2000-х років) 11
1.2.4 Боротьба з маніпуляціями (кінець 2000-х - початок 2010-х років) 12
1.2.5 Впровадження мобільних технологій та контент-маркетингу (середина 2010-х років) 12
1.2.6 Сучасні тенденції (кінець 2010-х - 2020-ті роки) 12
1.3 Сучасні тенденції у просуванні 14
2. МЕТОДИ ПРОСУВАННЯ САЙТІВ 16
2.1 Легальні методи просування 16
2.1.1 Використання Yoast SEO 17
2.1.2 Критичні уразливості плагіну Yoast SEO 22
2.1.3 Інформація про уразливість плагіну Slider Revolution 29
2.1.4 Уразливість плагіну Slider Revolution 30
2.2. НЕЛЕГАЛЬНІ МЕТОДИ ПРОСУВАННЯ САЙТІВ 32
2.2.1 Переваги нелегальних методів. 32
2.2.2 Недоліки нелегальних методів. 34
2.2.3 Типи Black Hat SEO 36
3. ПРАКТИЧНА ДОСЛІДЖЕННЯ БЕЗПЕКИ ЗАСТОСОВАНИХ МЕТОДІВ ПРОСУВАННЯ 41
3.1. Практична перевірка методів просування на безпековість. 41
3.2 Рекомендації безпеки після аналізу отриманих результатів за допомогою WPScan 46
ВИСНОВКИ 50
СПИСОК ЛІТЕРАТУРИ 51

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

SEO - Search Engine Optimization

SMM - Social Media Marketing

SERP - Search Engine Results Pages

ВСТУП

У сучасному світі Інтернет є невід'ємною частиною нашого життя, і роль веб-сайтів у бізнесі, освіті, розвагах та інших сферах стає все більш значущою. Кількість веб-сайтів зростає з кожним днем, що спричиняє зростання конкуренції за увагу користувачів та клієнтів. Це змушує компанії та окремих власників веб-ресурсів шукати ефективні методи просування своїх сайтів, щоб забезпечити високу позицію в пошукових системах та залучити якомога більше відвідувачів.

Зі збільшенням кількості веб-сайтів зростає і різноманітність методів їх просування. Традиційні методи, такі як пошукова оптимізація (SEO) та контент-маркетинг, постійно вдосконалюються та адаптуються до нових вимог і алгоритмів пошукових систем. Поряд з ними розвиваються нові підходи, зокрема маркетинг у соціальних мережах (SMM) та різноманітні форми інтернет-реклами[4].

Водночас, на тлі зростаючої конкуренції, деякі компанії та веб-майстри вдаються до використання нелегальних методів просування, відомих як чорний SEO. Незважаючи на те, що такі методи можуть дати швидкі результати, вони несуть високі ризики для веб-сайтів, включаючи санкції з боку пошукових систем, втрату довіри користувачів та фінансові втрати.

Таким чином, актуальність теми дослідження визначається необхідністю розробки ефективних стратегій просування веб-сайтів, які враховують сучасні тенденції та вимоги пошукових систем, забезпечують безпеку та довгостроковий успіх. Дослідження легальних та нелегальних методів просування дозволить краще зрозуміти їхні переваги та недоліки, а також ризики, пов'язані з їх використанням.

Постійний розвиток технологій та зміни в алгоритмах пошукових систем вимагають від компаній постійного вдосконалення своїх стратегій просування.

Сучасні алгоритми пошукових систем стають дедалі складнішими і здатні більш ефективно виявляти маніпулятивні техніки, що робить нелегальні методи просування ще більш ризикованими. Пошукові системи, такі як Google, постійно оновлюють свої алгоритми, щоб забезпечити користувачам найрелевантніші та якісні результати пошуку. Подібні оновлення роблять нелегальні методи просування менш ефективними та більш небезпечними для тих, хто їх використовує[5].

Крім того, алгоритми пошукових систем все більше враховують поведінкові фактори користувачів, такі як тривалість перебування на сайті, кількість переглянутих сторінок, показник відмов тощо. Це означає, що компанії повинні зосереджуватися на створенні якісного контенту та покращенні користувацького досвіду, щоб відповідати високим стандартам пошукових систем.

Тому актуальність теми дослідження визначається необхідністю розробки ефективних стратегій просування веб-сайтів, які враховують сучасні тенденції та вимоги пошукових систем, забезпечують безпеку та довгостроковий успіх. Дослідження легальних та нелегальних методів просування дозволить краще зрозуміти їхні переваги та недоліки, а також ризики, пов'язані з їх використанням.

1. ОГЛЯД ПРОБЛЕМАТИКИ ПРОСУВАННЯ

1.1. Загальні поняття про просування

Просування сайтів (або веб-просування) — це комплекс заходів, спрямованих на підвищення видимості веб-ресурсу в Інтернеті, залучення більшої кількості відвідувачів та потенційних клієнтів, а також забезпечення високих позицій у результатах пошукових систем SERP - Search Engine Results Pages. Процес просування сайтів включає різні методи та стратегії, які можуть бути легальними (білий SEO) та нелегальними (чорний SEO)[6].

Основні цілі просування сайтів:

- Збільшення трафіку: Основною метою просування є збільшення кількості відвідувачів на сайті. Це може бути досягнуто за допомогою різних маркетингових стратегій та оптимізації контенту.
- Підвищення видимості: Покращення позицій сайту у пошукових системах, що робить його більш видимим для потенційних користувачів.
- Залучення цільової аудиторії: Залучення саме тих користувачів, які зацікавлені в продуктах або послугах, що пропонуються на сайті.
- Зміцнення бренду: Просування сприяє підвищенню впізнаваності бренду та формуванню його позитивного іміджу в Інтернеті.
- Підвищення конверсії: Оптимізація сайту з метою збільшення кількості користувачів, які здійснюють цільові дії (купівля, реєстрація, підписка).

Ключові етапи процесу просування сайтів:

- Аналіз ринку та конкурентів: Дослідження ринку, аналіз конкурентів та виявлення їх сильних і слабких сторін.
- Аудит сайту: Технічний аналіз сайту для виявлення проблем, які можуть вплинути на його видимість у пошукових системах.
- Вибір ключових слів: Підбір релевантних ключових слів та фраз, за якими потенційні користувачі можуть шукати продукти або послуги.

- Оптимізація контенту: Створення та оптимізація контенту на основі обраних ключових слів, забезпечення його унікальності та корисності.
- Лінкбілдинг: Побудова зовнішніх посилань для підвищення авторитету сайту у пошукових системах.
- Моніторинг та аналіз результатів: Постійний моніторинг позицій сайту, аналіз трафіку та коригування стратегії просування.

Основні методи просування сайтів:

1. Пошукова оптимізація (SEO): Внутрішня та зовнішня оптимізація сайту для покращення його видимості у пошукових системах.
2. Контент-маркетинг: Створення та розповсюдження цінного та релевантного контенту для залучення та утримання цільової аудиторії.
3. Соціальні медіа-маркетинг (SMM): Використання соціальних мереж для просування сайту та взаємодії з користувачами.
4. Інтернет-реклама: Використання платних рекламних кампаній, таких як контекстна реклама (PPC), банерна реклама та інші.

Технічна оптимізація сайту

Технічна оптимізація сайту є невід'ємною частиною процесу пошукової оптимізації (SEO). Вона спрямована на поліпшення технічних аспектів веб-сайту, щоб забезпечити його коректне індексування пошуковими системами, підвищити зручність для користувачів і, як результат, поліпшити позиції у видачі пошукових систем.

1.2 Розвиток методів просування

Історія розвитку методів просування веб-сайтів відображає еволюцію Інтернету, пошукових систем та цифрового маркетингу. Просування сайтів пройшло кілька важливих етапів, кожен з яких вплинув на сучасні практики та стратегії.

1.2.1 Початковий етап (1990-ті роки)

Інтернет почав стрімко розвиватися в 1990-х роках. Перші веб-сайти були простими, а конкуренція за трафік була мінімальною. Основні методи просування включали:

- Реєстрація в каталогах: Веб-майстри реєстрували свої сайти в популярних каталогах, таких як Yahoo! Directory та DMOZ, щоб підвищити видимість.
- Обмін посиланнями: Простий обмін посиланнями між сайтами для підвищення авторитету.

1.2.2 Розвиток пошукових систем (кінець 1990-х - початок 2000-х років)

З розвитком пошукових систем, таких як AltaVista, Yahoo! і, особливо, Google, з'явилися нові можливості для просування сайтів. Основні зміни включали:

- Поява SEO (Search Engine Optimization): Веб-майстри почали оптимізувати сайти для кращого ранжування в пошукових системах. Це включало використання ключових слів у текстах, мета-тегах і заголовках.
- Розвиток алгоритмів: Google впровадив алгоритм PageRank, який оцінював якість сайту на основі кількості та якості зовнішніх посилань.

1.2.3 Початок маніпулятивних технік (середина 2000-х років)

Зростання конкуренції спонукало до використання маніпулятивних технік просування, відомих як чорний SEO. До них належали:

- Клоакінг: Показ різного контенту користувачам і пошуковим системам.

- Спам посилання: Масове створення неякісних посилань для штучного підвищення ранжування.
- Прихований текст: Використання тексту, прихованого від користувачів, але видимого для пошукових роботів.

1.2.4 Боротьба з маніпуляціями (кінець 2000-х - початок 2010-х років)

Пошукові системи почали активну боротьбу з маніпулятивними техніками:

- Алгоритм Google Panda (2011): Боровся з низькоякісним контентом і сайтами, які намагалися маніпулювати результатами пошуку[7,8].
- Алгоритм Google Penguin (2012): Націлений на боротьбу зі спамом посилань та іншими техніками чорного SEO[8].
- Алгоритм Hummingbird (2013): Впровадження семантичного пошуку для кращого розуміння намірів користувачів.

1.2.5 Впровадження мобільних технологій та контент-маркетингу (середина 2010-х років)

З поширенням мобільних пристроїв і зростанням значення контенту методи просування зазнали змін:

- Мобільна оптимізація: Створення адаптивних веб-сайтів, які однаково добре працюють на різних пристроях.
- Контент-маркетинг: Створення цінного і релевантного контенту для залучення та утримання цільової аудиторії.
- Соціальні мережі: Використання платформ, таких як Facebook, Twitter, Instagram, для просування контенту і взаємодії з аудиторією.

1.2.6 Сучасні тенденції (кінець 2010-х - 2020-ті роки)

Сучасні методи просування продовжують розвиватися разом із технологіями:

- Голосовий пошук: Оптимізація контенту для голосових асистентів, таких як Siri, Alexa та Google Assistant[1].
- Штучний інтелект і машинне навчання: Використання алгоритмів для персоналізації пошукових результатів та поліпшення користувацького досвіду.
- Core Web Vitals: Впровадження нових метрик, таких як LCP (Largest Contentful Paint), FID (First Input Delay) та CLS (Cumulative Layout Shift), для оцінки якості користувацького досвіду[1].
- Екологічний аспект: Зростаюча увага до екологічної оптимізації сайтів, зменшення споживання ресурсів і підвищення енергоефективності.

Історія розвитку методів просування сайтів демонструє постійне вдосконалення технологій та стратегій, спрямованих на підвищення видимості, залучення аудиторії та покращення користувацького досвіду. Водночас, боротьба з маніпулятивними техніками підвищує значення етичних та прозорих методів просування, що сприяє створенню якісного та релевантного контенту в Інтернеті.

1.3 Сучасні тенденції у просуванні

У сучасному цифровому світі просування сайтів постійно еволюціонує разом із розвитком технологій, зміною алгоритмів пошукових систем та поведінкою користувачів. Сучасні тенденції відображають інтеграцію нових методів і стратегій, що дозволяють веб-сайтам ефективніше залучати аудиторію та залишатися конкурентоспроможними. Ось деякі з основних тенденцій у просуванні сайтів:

1. Оптимізація для мобільних пристроїв

Мобільна адаптація: Враховуючи, що більшість користувачів здійснюють пошук із мобільних пристроїв, важливо мати адаптивний дизайн, що забезпечує зручний перегляд на різних розмірах екранів.

Mobile-First Indexing: Google перейшов на індексування сайтів у першу чергу за мобільною версією, що робить мобільну оптимізацію критично важливою.

2. Штучний інтелект та машинне навчання

Персоналізація контенту: Використання алгоритмів машинного навчання для аналізу поведінки користувачів та персоналізації контенту.

Прогнозування поведінки: Виявлення патернів поведінки для передбачення потреб користувачів і надання релевантного контенту.

3. Локальне SEO

Google My Business: Оптимізація локального бізнесу через Google My Business для поліпшення видимості у локальних результатах пошуку.

Локальні ключові слова: Використання ключових слів, які включають місцеві назви та географічні дані.

4. Безпека сайту

SSL-сертифікати: Важливість використання HTTPS для забезпечення безпеки даних користувачів та покращення ранжування в пошукових системах.

Захист від хакерських атак: Регулярні оновлення та захист сайту від шкідливого ПЗ і хакерських атак.

5. Контент-маркетинг та інформативний контент

Створення якісного контенту: Фокус на створенні унікального, інформативного та цінного контенту для залучення та утримання аудиторії.

SEO-копірайтинг: Оптимізація текстів для пошукових систем без втрати якості контенту.

6. Аналітика та моніторинг

Google Analytics та інші інструменти: Постійний моніторинг та аналіз поведінки користувачів, відвідуваності та інших ключових показників ефективності.

Регулярні аудитори: Проведення регулярних SEO-аудиторій для виявлення та усунення проблем на сайті.

Сучасні тенденції в просуванні сайтів свідчать про постійну інтеграцію нових технологій та інструментів, що дозволяють підвищити ефективність та конкурентоспроможність веб-ресурсів. Компанії, які адаптуються до цих змін і впроваджують передові методи, отримують значну перевагу в умовах зростаючої конкуренції.

2. МЕТОДИ ПРОСУВАННЯ САЙТІВ

2.1 Легальні методи просування

Легальні методи просування сайтів, відомі як білий SEO (White Hat SEO), орієнтовані на створення цінного контенту, забезпечення зручності для користувачів та дотримання рекомендацій пошукових систем. Ці методи сприяють довгостроковому успіху, підвищують видимість сайту в пошукових системах та мінімізують ризики санкцій.

Основні принципи легальних методів просування сайтів

1. Дотримання рекомендацій пошукових систем:
- Використання практик, які відповідають офіційним рекомендаціям Google, Bing та інших пошукових систем.
- Уникнення маніпулятивних технік, які можуть призвести до санкцій або зниження рейтингу сайту.
2. Фокус на користувачах:
- Створення контенту, який відповідає потребам та інтересам цільової аудиторії.
- Забезпечення зручності навігації та швидкості завантаження сторінок.
3. Прозорість і етика:
- Використання чесних та прозорих методів для залучення трафіку.
- Відмова від використання чорних та сірих методів SEO (наприклад, прихованого тексту, клоакінгу, автоматизованих програм для створення посилань).

Пошукова оптимізація (SEO)

Пошукова оптимізація (Search Engine Optimization, SEO) є основним легальним методом просування сайтів, що включає комплекс заходів для

покращення видимості веб-сайту в органічних (неоплачених) результатах пошукових систем. Поділяється на внутрішню й зовнішю.

2.1.1 Використання Yoast SEO

Yoast SEO — це один з найпопулярніших плагінів для оптимізації сайтів на платформі WordPress. Він допомагає користувачам покращити видимість своїх веб-ресурсів у пошукових системах, забезпечуючи зручні інструменти та рекомендації для оптимізації контенту та технічних аспектів сайту.

Використання Yoast SEO надає власникам сайтів потужні інструменти для покращення видимості у пошукових системах, підвищення якості контенту та забезпечення зручності для користувачів. Це робить плагін незамінним інструментом для ефективного просування сайтів на платформі WordPress.

Оптимізація контенту. Створення унікального та релевантного контенту є основою успішного SEO. Контент повинен відповідати запитам користувачів, бути інформативним, цікавим і корисним. Включення ключових слів у заголовки, тексти, мета-описи та зображення допомагає пошуковим системам краще розуміти, про що ваш сайт, і ранжувати його вище у результатах пошуку.

На рисунку 1, показана типовий шаблон додавання контенту через WordPress конструктор.

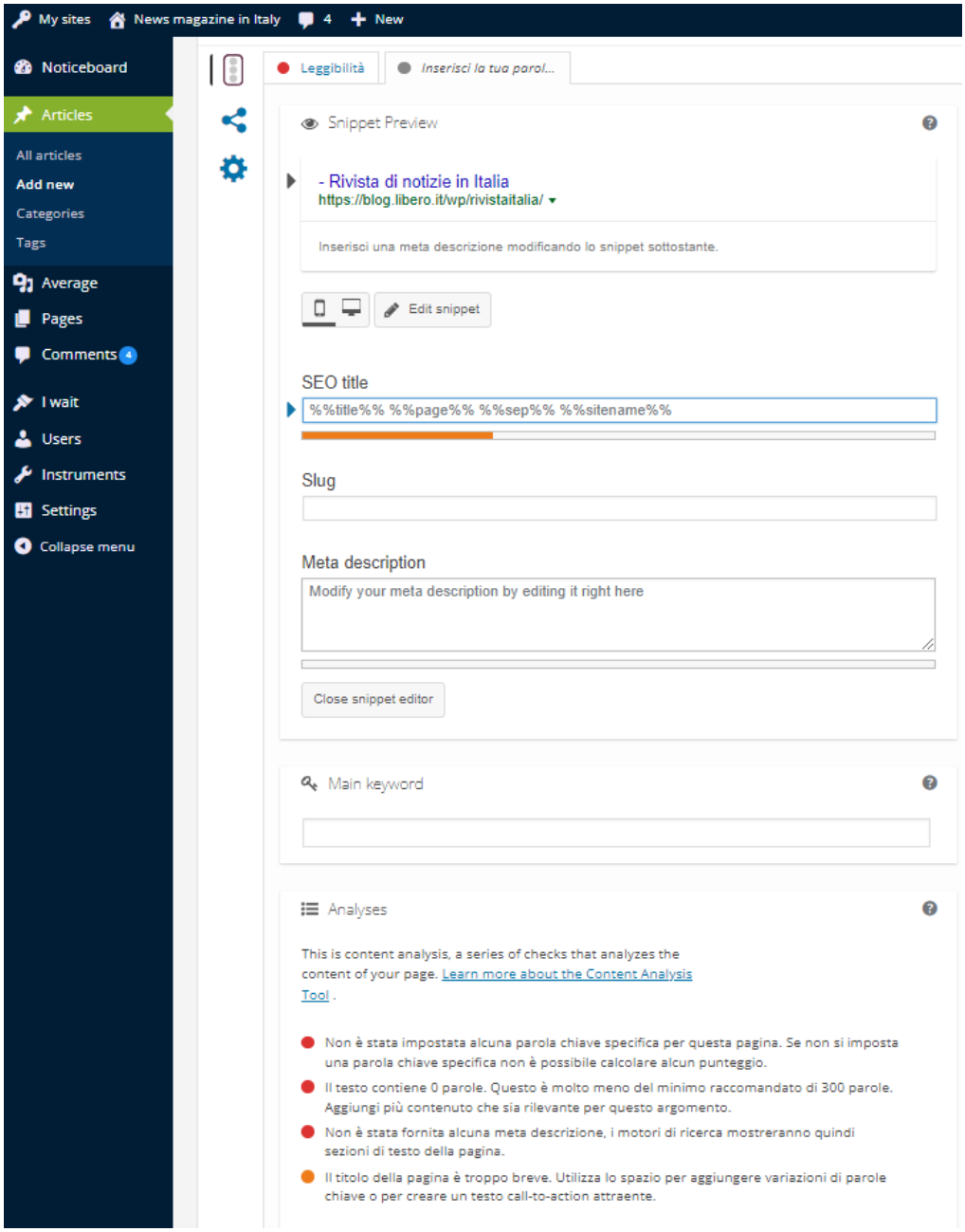


Рисунок 1 – Меню Yoast SEO для встановлення налаштувань нової статті

Заголовки (SEO Title): Вони мають бути унікальними та містити основні ключові слова. Заголовки привертають увагу користувачів у результатах пошуку та впливають на рішення перейти на сайт. За загальними рекомендаціями від Google обсяг заголовку повинен бути від 50 символів до 200 символів.

Мета-описи (Meta Descriptions): Короткі описи сторінок, які з'являються у результатах пошуку. Вони повинні містити ключові слова та спонукати

користувачів клікнути на ваш сайт. За загальними рекомендаціями від Google обсяг опису повинен бути від 100 символів до 150 символів.

Основний текст: Контент сторінок має бути релевантним, інформативним та містити ключові слова у природному контексті. Унікальність та якість контенту важливі для залучення та утримання користувачів.

Зображення: Оптимізація зображень включає використання атрибутів alt (Alternative text) з описом зображення, що допомагає пошуковим системам розуміти контент зображень та покращує видимість у пошуку зображень(рис.2).

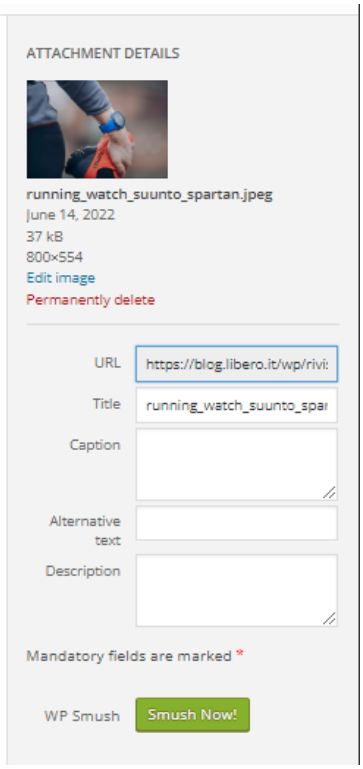


Рисунок 2 – Властивості картинки

Оптимізація ключових слів: Фокусні ключові слова: Yoast SEO дозволяє встановити фокусні ключові слова для кожної сторінки або поста. Плагін аналізує контент і дає рекомендації, як оптимізувати його для цих ключових слів.

Пов'язані ключові слова: У преміум-версії плагін підтримує оптимізацію для декількох ключових слів, що дозволяє охоплювати ширшу аудиторію та покращити ранжування за кількома запитами

Поради від Yoast SEO: Аналіз змісту

Yoast SEO надає детальний аналіз змісту сторінки та пропонує рекомендації для покращення SEO та читабельності.

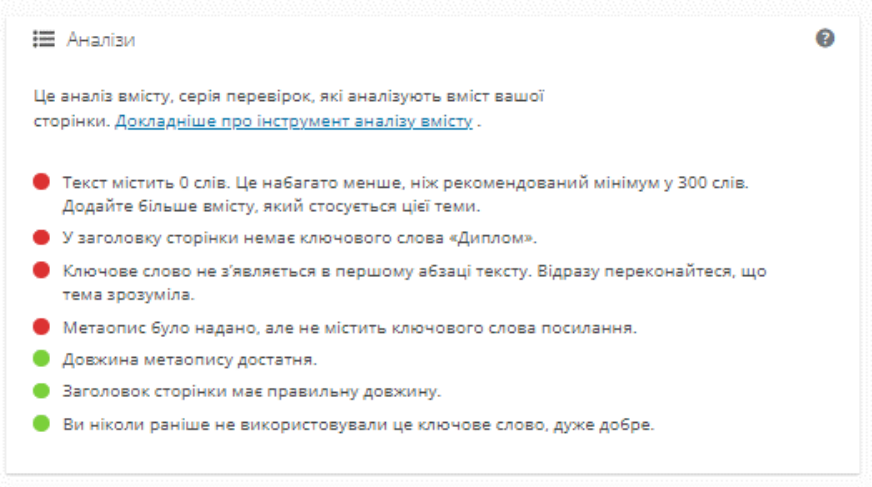


Рисунок 3 – Поради від Yoast SEO

На основі зображення з порадами, можна зробити наступні висновки:

1. Текст містить 0 слів

- Проблема: Ваш текст занадто короткий. Він не відповідає рекомендованому мінімуму у 300 слів.
- Рекомендація: Додайте більше змісту, який стосується цієї теми. Створення детального та інформативного контенту допоможе залучити більше відвідувачів і покращить ранжування в пошукових системах.

2. У заголовку сторінки немає ключового слова "Диплом"

- Проблема: Ключове слово, яке ви оптимізуєте, не присутнє в заголовку сторінки.
- Рекомендація: Включіть ключове слово "Диплом" у заголовок сторінки. Це допоможе пошуковим системам зрозуміти основну тему сторінки і підвищить її релевантність для пошукових запитів.

3. Ключове слово не з'являється в першому абзаці тексту

- Проблема: Ключове слово не використовується на початку тексту, що зменшує його вагу для пошукових систем.
- Рекомендація: Переконайтеся, що ключове слово "Диплом" з'являється в першому абзаці тексту. Це допоможе швидко зрозуміти тему сторінки як користувачам, так і пошуковим роботам.

4. Метаопис було надано, але не містить ключового слова

- Проблема: Метаопис не містить ключового слова "Диплом", що зменшує його ефективність.
- Рекомендація: Включіть ключове слово "Диплом" у метаопис. Це допоможе покращити релевантність метаопису та збільшити ймовірність кліків на сторінку в результатах пошуку.

5. Довжина метаопису достатня

- Проблема: Відсутня.
- Рекомендація: Довжина метаопису відповідає рекомендаціям, що добре впливає на його ефективність.

6. Заголовок сторінки має правильну довжину

- Проблема: Відсутня.
- Рекомендація: Довжина заголовку сторінки оптимальна, що забезпечує його повне відображення в результатах пошуку.

7. Ви ніколи раніше не використовували це ключове слово

- Проблема: Відсутня.
- Рекомендація: Використання нових ключових слів допомагає розширити охоплення аудиторії і покращує видимість сайту для різноманітних запитів.

Вплив Yoast SEO на просування сайту:

- Покращення видимості в пошукових системах:

- Yoast SEO допомагає оптимізувати контент і технічні аспекти сайту, що сприяє покращенню позицій у пошукових системах і збільшенню органічного трафіку.
- Залучення цільової аудиторії:
- Використання інструментів для оптимізації ключових слів та мета-описів дозволяє створювати більш релевантний і привабливий контент, що залучає цільову аудиторію.
- Підвищення читабельності контенту:
- Інструменти аналізу читабельності допомагають покращити якість текстів, що робить їх більш доступними та цікавими для користувачів.

Хоча всі ці рекомендації можна реалізувати вручну, використання плагіну Yoast SEO значно спрощує процес оптимізації сайту. Плагін автоматизує багато рутинних завдань, надає миттєві рекомендації та аналітичні дані, що дозволяє швидко і ефективно вносити зміни. Крім того, Yoast SEO забезпечує інтеграцію з іншими інструментами та платформами, такими як Google Search Console, що додає додаткові можливості для покращення видимості вашого сайту.

Використання цього плагіну дозволяє зосередитися на створенні якісного контенту, тоді як технічні аспекти та оптимізація залишаються під надійним контролем.

2.1.2 Критичні уразливості плагіну Yoast SEO

Плагін Yoast SEO, один з найпопулярніших для оптимізації веб-сайтів під пошукові системи, неодноразово ставав об’єктом виявлення уразливостей. Відровідно до [15] нижще наведены деякі з критичних уразливостей, виявлених у цьому плагіні:

- **CVE-2021-36788**

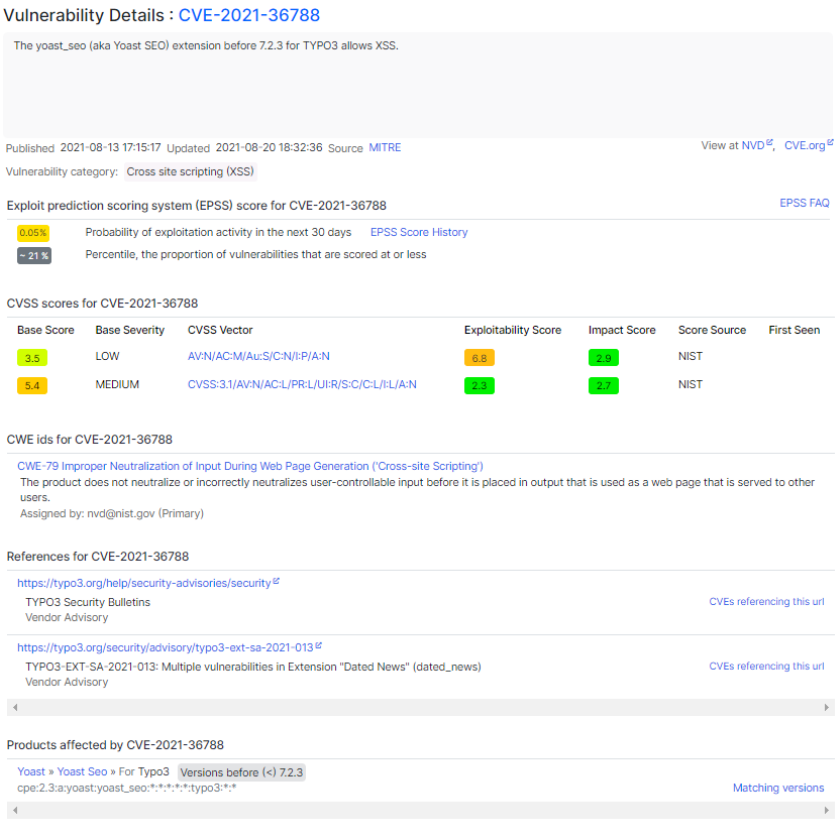


Рисунок 4 – Вразливість CVE-2021-36788

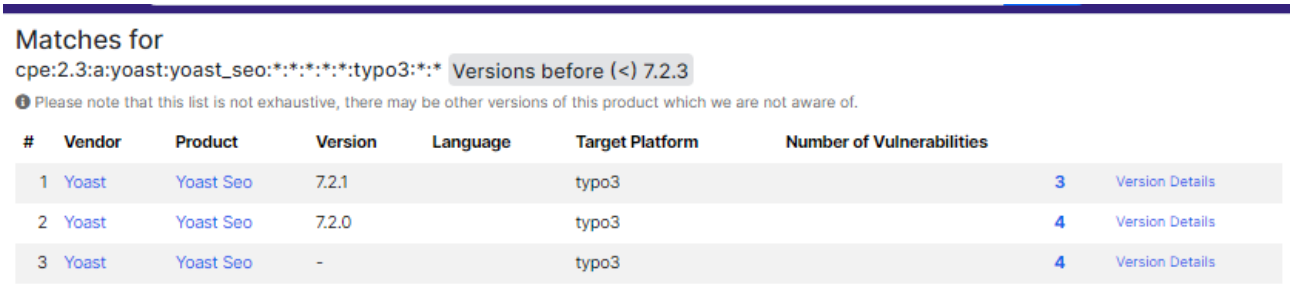


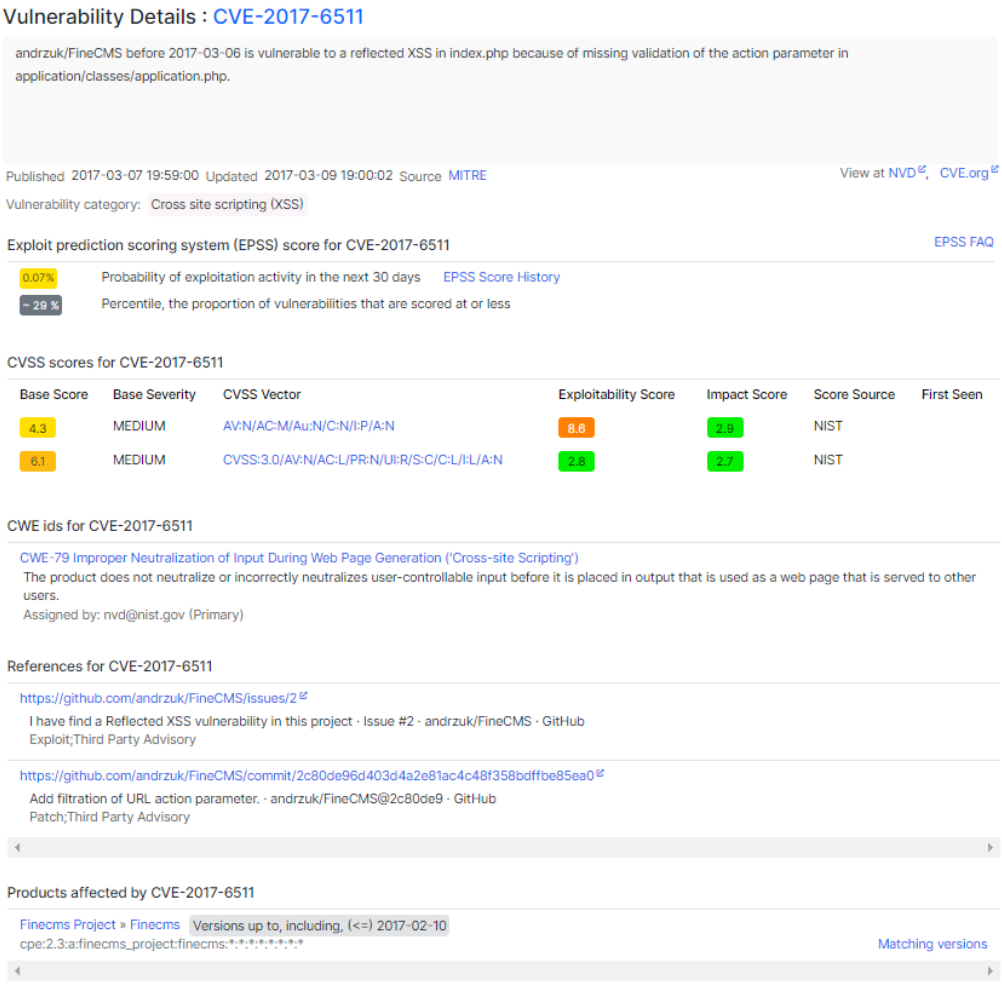
Рисунок 5 – Вразливість CVE-2021-36788

Опис: Уразливість міжсайтового скриптингу (XSS) в плагіні Yoast SEO для TYPO3 версії до 7.2.3. Ця уразливість дозволяє зловмисникам впроваджувати шкідливий код через некоректно оброблені введені дані.

CVSS Score: 5.4 (середня)

Деталі: Відсутня належна нейтралізація введених даних під час генерації веб-сторінки.

- **CVE-2017-6511**



Vulnerability Details : CVE-2017-6511

andrzuk/FineCMS before 2017-03-06 is vulnerable to a reflected XSS in index.php because of missing validation of the action parameter in application/classes/application.php.

Published 2017-03-07 19:59:00 Updated 2017-03-09 19:00:02 Source MITRE

View at NVD, CVE.org

Vulnerability category: Cross site scripting (XSS)

Exploit prediction scoring system (EPSS) score for CVE-2017-6511

EPSS FAQ

0.07% Probability of exploitation activity in the next 30 days EPSS Score History

~ 29 % Percentile, the proportion of vulnerabilities that are scored at or less

CVSS scores for CVE-2017-6511

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
4.3	MEDIUM	AV:N/AC:M/Au:N/C:N/I:P/A:N	8.6	2.9	NIST	
6.1	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	2.8	2.7	NIST	

CWE ids for CVE-2017-6511

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Assigned by: nvd@nist.gov (Primary)

References for CVE-2017-6511

https://github.com/andrzuk/FineCMS/issues/2

I have find a Reflected XSS vulnerability in this project · Issue #2 · andrzuk/FineCMS · GitHub

Exploit;Third Party Advisory

https://github.com/andrzuk/FineCMS/commit/2c80de96d403d4a2e81ac4c48f358bdffbe85ea0

Add filtration of URL action parameter. · andrzuk/FineCMS@2c80de9 · GitHub

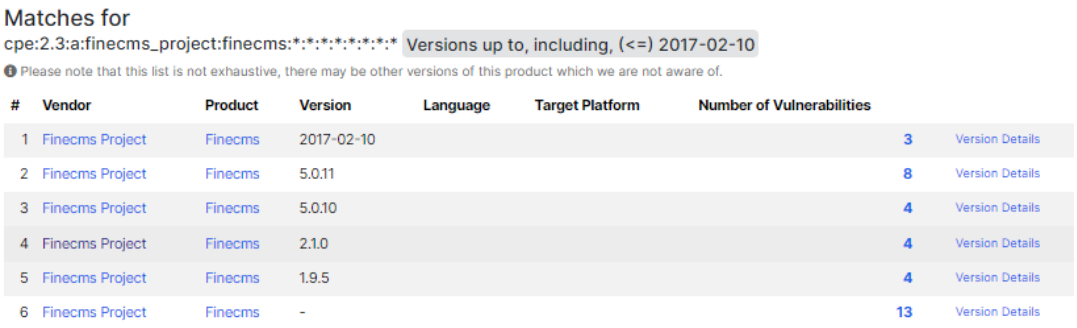
Patch;Third Party Advisory

Products affected by CVE-2017-6511

Finecms Project » Finecms Versions up to, including, (<=) 2017-02-10

cpe:2.3:a:finecms_project:finecms:*:*:*:*:*:*:*:* Matching versions

Рисунок 6 – Вразливість CVE-2017-6511



Matches for

cpe:2.3:a:finecms_project:finecms:*:*:*:*:*:*:*:* Versions up to, including, (<=) 2017-02-10

Please note that this list is not exhaustive, there may be other versions of this product which we are not aware of.

#	Vendor	Product	Version	Language	Target Platform	Number of Vulnerabilities	
1	Finecms Project	Finecms	2017-02-10			3	Version Details
2	Finecms Project	Finecms	5.0.11			8	Version Details
3	Finecms Project	Finecms	5.0.10			4	Version Details
4	Finecms Project	Finecms	2.1.0			4	Version Details
5	Finecms Project	Finecms	1.9.5			4	Version Details
6	Finecms Project	Finecms	-			13	Version Details

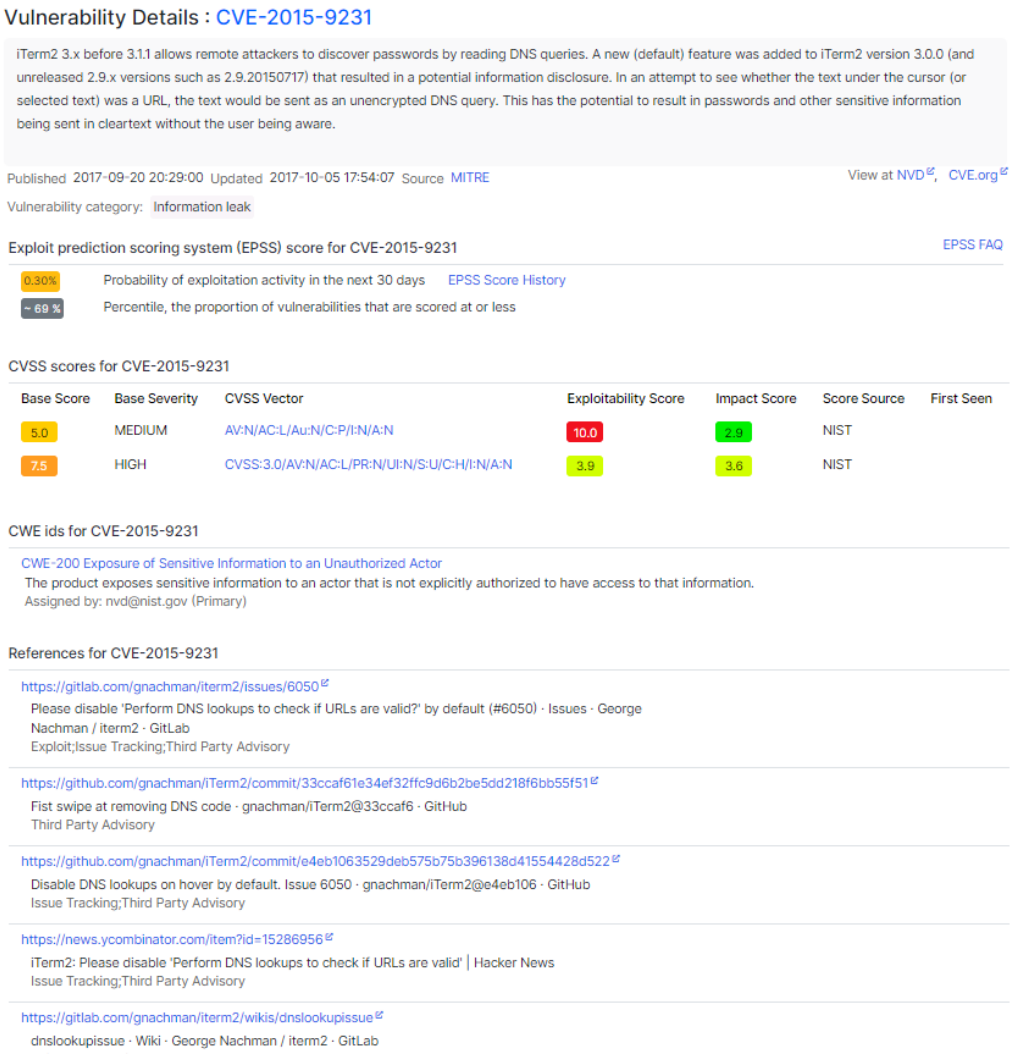
Рисунок 7 – Вразливість CVE-2017-6511

Опис: Уразливість SQL-ін’єкції в плагіні Yoast SEO до версії 4.5. Зловмисники могли виконувати довільні SQL-запити через вразливі параметри.

CVSS Score: 7.5 (висока)

Деталі: SQL-ін’єкція дозволяла отримати доступ до бази даних та змінювати її вміст, що могло призвести до викрадення конфіденційних даних.

- **CVE-2015-9231**



Vulnerability Details : CVE-2015-9231

iTerm2 3.x before 3.1.1 allows remote attackers to discover passwords by reading DNS queries. A new (default) feature was added to iTerm2 version 3.0.0 (and unreleased 2.9.x versions such as 2.9.20150717) that resulted in a potential information disclosure. In an attempt to see whether the text under the cursor (or selected text) was a URL, the text would be sent as an unencrypted DNS query. This has the potential to result in passwords and other sensitive information being sent in cleartext without the user being aware.

Published 2017-09-20 20:29:00 Updated 2017-10-05 17:54:07 Source MITRE

View at NVD, CVE.org

Vulnerability category: Information leak

Exploit prediction scoring system (EPSS) score for CVE-2015-9231

EPSS FAQ

0.30% Probability of exploitation activity in the next 30 days EPSS Score History

~ 69 % Percentile, the proportion of vulnerabilities that are scored at or less

CVSS scores for CVE-2015-9231

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
5.0	MEDIUM	AV:N/AC:L/Au:N/C:P/I:N/A:N	10.0	2.9	NIST	
7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	3.9	3.6	NIST	

CWE ids for CVE-2015-9231

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.
Assigned by: nvd@nist.gov (Primary)

References for CVE-2015-9231

https://gitlab.com/gnachman/iterm2/issues/6050
Please disable 'Perform DNS lookups to check if URLs are valid?' by default (#6050) · Issues · George Nachman / iterm2 · GitLab
Exploit;Issue Tracking;Third Party Advisory

https://github.com/gnachman/iTerm2/commit/33ccaf61e34ef32ffc9d6b2be5dd218f6bb55f51
Fist swipe at removing DNS code · gnachman/iTerm2@33ccaf6 · GitHub
Third Party Advisory

https://github.com/gnachman/iTerm2/commit/e4eb1063529deb575b75b396138d41554428d522
Disable DNS lookups on hover by default. Issue 6050 · gnachman/iTerm2@e4eb106 · GitHub
Issue Tracking;Third Party Advisory

https://news.ycombinator.com/item?id=15286956
iTerm2: Please disable 'Perform DNS lookups to check if URLs are valid' | Hacker News
Issue Tracking;Third Party Advisory

https://gitlab.com/gnachman/iterm2/wikis/dnslookupissue
dnslookupissue · Wiki · George Nachman / iterm2 · GitLab

Рисунок 8 – Вразливість CVE-2015-9231

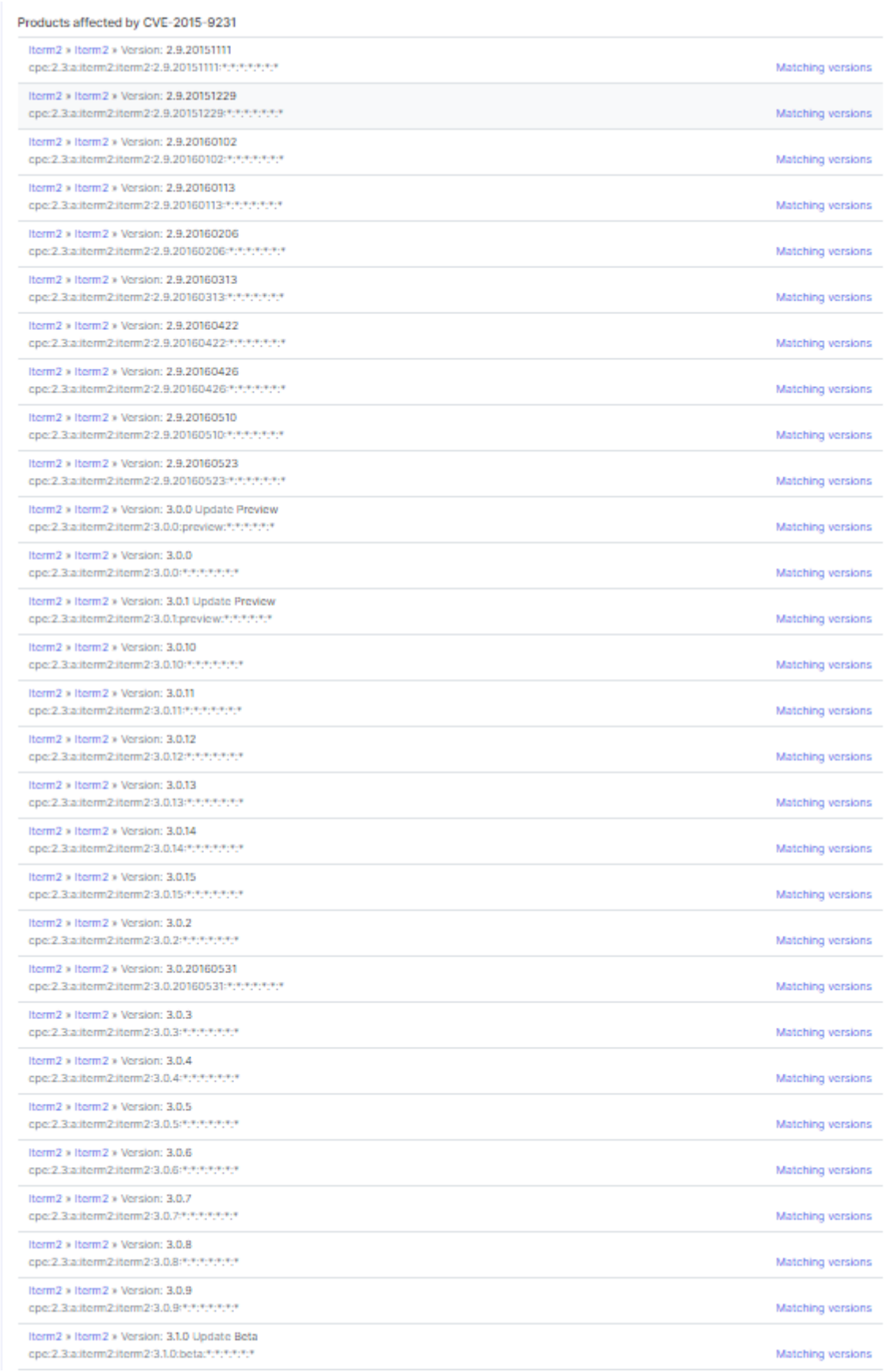


Рисунок 8 – Вразливість CVE-2015-9231

Опис: Уразливість міжсайтового скриптингу (XSS) в плагіні Yoast SEO версії до 2.3.5. Зловмисники могли впроваджувати шкідливий код через параметри URL.

CVSS Score: 7.5 (Висока)

Деталі: Уразливість дозволяла зловмисникам виконувати шкідливі скрипти в браузерах користувачів, що могло призвести до викрадення сесій та інших конфіденційних даних.

- **CVE-2017-6540**

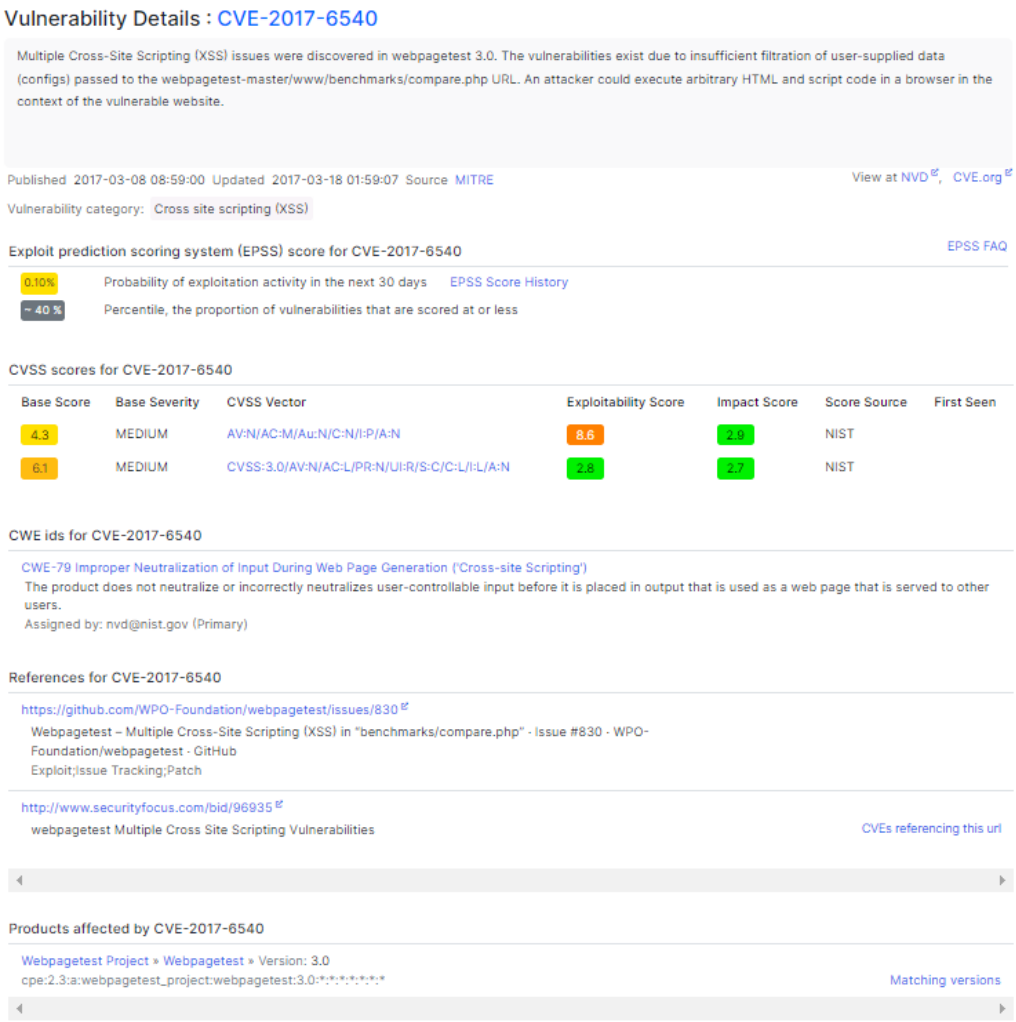
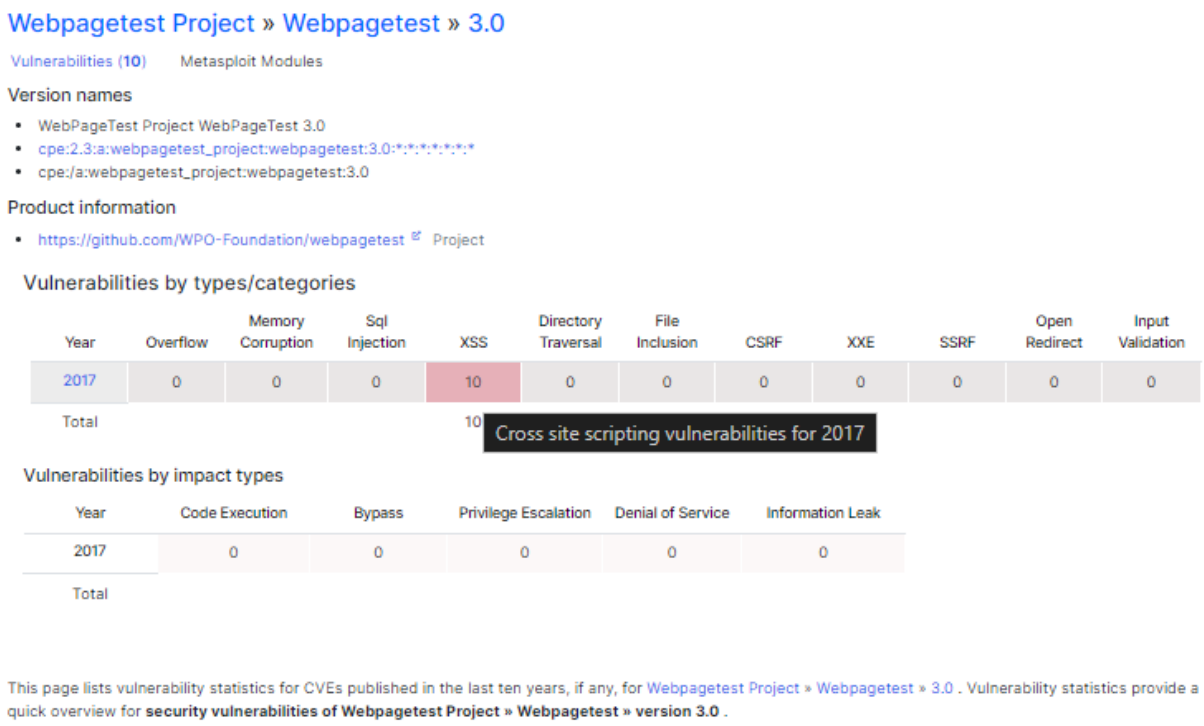


Рисунок 9 – Вразливість CVE-2017-6540



Webpagetest Project » Webpagetest » 3.0

Vulnerabilities (10) Metasploit Modules

Version names

- WebPageTest Project WebPageTest 3.0
- cpe:2.3:a:webpagetest_project:webpagetest:3.0:*:*:*:*:*:*:*
- cpe:/a:webpagetest_project:webpagetest:3.0

Product information

- https://github.com/WPO-Foundation/webpagetest Project

Vulnerabilities by types/categories

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2017	0	0	0	10	0	0	0	0	0	0	0
Total				10							

Cross site scripting vulnerabilities for 2017

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2017	0	0	0	0	0
Total					

This page lists vulnerability statistics for CVEs published in the last ten years, if any, for Webpagetest Project » Webpagetest » 3.0 . Vulnerability statistics provide a quick overview for **security vulnerabilities of Webpagetest Project » Webpagetest » version 3.0** .

Рисунок 10 – Вразливість CVE-2017-6540

Опис: Уразливість, яка дозволяє виконання довільного коду (Remote Code Execution) у версіях до 4.7. Ймовірно, що зловмисники могли впроваджувати та виконувати шкідливий код на сервері.

CVSS Score: 9.8 (критична)

Деталі: Виконання довільного коду на сервері дозволяло повний контроль над веб-сайтом і доступ до всіх даних.

Ці уразливості підкреслюють важливість регулярного оновлення плагінів та використання найновіших версій, оскільки старі версії можуть містити критичні проблеми безпеки. Для вашої дипломної роботи ці приклади можуть бути використані для демонстрації потенційних ризиків та важливості безпеки в плагінах для оптимізації веб-сайтів.

2.1.3 Інформація про уразливість плагіну Slider Revolution

Slider Revolution – це популярний плагін для WordPress, який дозволяє користувачам створювати динамічні та інтерактивні слайдери, каруселі, розділи героя (hero sections), та інші мультимедійні елементи для веб-сайтів. Плагін розроблений компанією Themepunch і є одним з найбільш завантажуваних та використовуваних плагінів для створення слайдерів на WordPress.

Основні функції та можливості:

1. Візуальний редактор без кодування:
    - Drag-and-drop інтерфейс, який дозволяє користувачам легко додавати елементи, налаштовувати макети та створювати анімації без необхідності знати програмування.
    - Інтуїтивно зрозумілий інтерфейс, що полегшує роботу навіть новачкам у веб-дизайні.
2. Широкий вибір шаблонів та анімацій:
    - Понад 200 готових шаблонів слайдерів та більше 25 додаткових модулів (add-ons), що дозволяють значно розширити функціональність плагіну.
    - Підтримка анімацій, ефектів переходу, часткових ефектів, та багатошарових анімацій.
3. Підтримка різних типів контенту:
    - Можливість додавати зображення, відео, текст, іконки, лотті-анімації, логотипи та інші мультимедійні елементи.
    - Підтримка динамічних джерел контенту, таких як пости, сторінки, продукти WooCommerce та інший динамічний контент WordPress.
4. Оптимізація продуктивності:
    - Функції асинхронного та відкладеного завантаження скриптів, оптимізація розмірів файлів зображень, підтримка ленивого

завантаження (lazy loading) для покращення швидкості завантаження сторінок.
    - Інтеграція з кешуючими плагінами та CDN для зменшення навантаження на сервер і прискорення завантаження сайту.
5. Адаптивність:
    - Плагін повністю адаптивний і забезпечує коректне відображення слайдерів на різних пристроях, включаючи десктопи, планшети та смартфони.
    - Можливість налаштування адаптивних параметрів для кожного елемента окремо.
6. Безпека:
    - Регулярні оновлення для забезпечення сумісності з останніми версіями WordPress та усунення виявлених уразливостей.
    - Інструменти для запобігання XSS-атакам, SQL-ін’єкціям та іншим поширеним загрозам безпеки.

Slider Revolution – це потужний та гнучкий інструмент для створення візуально привабливих слайдерів та інтерактивного контенту на WordPress-сайтах. Однак, важливо підтримувати плагін в актуальному стані та дотримуватися рекомендацій з безпеки, щоб запобігти можливим загрозам.

2.1.4 Уразливість плагіну Slider Revolution

Плагін **Slider Revolution** має критичну уразливість, ідентифіковану як **CVE-2023-2359**. Ця уразливість дозволяє завантажувати довільні файли, що може призвести до виконання довільного коду (Remote Code Execution) на сервері.

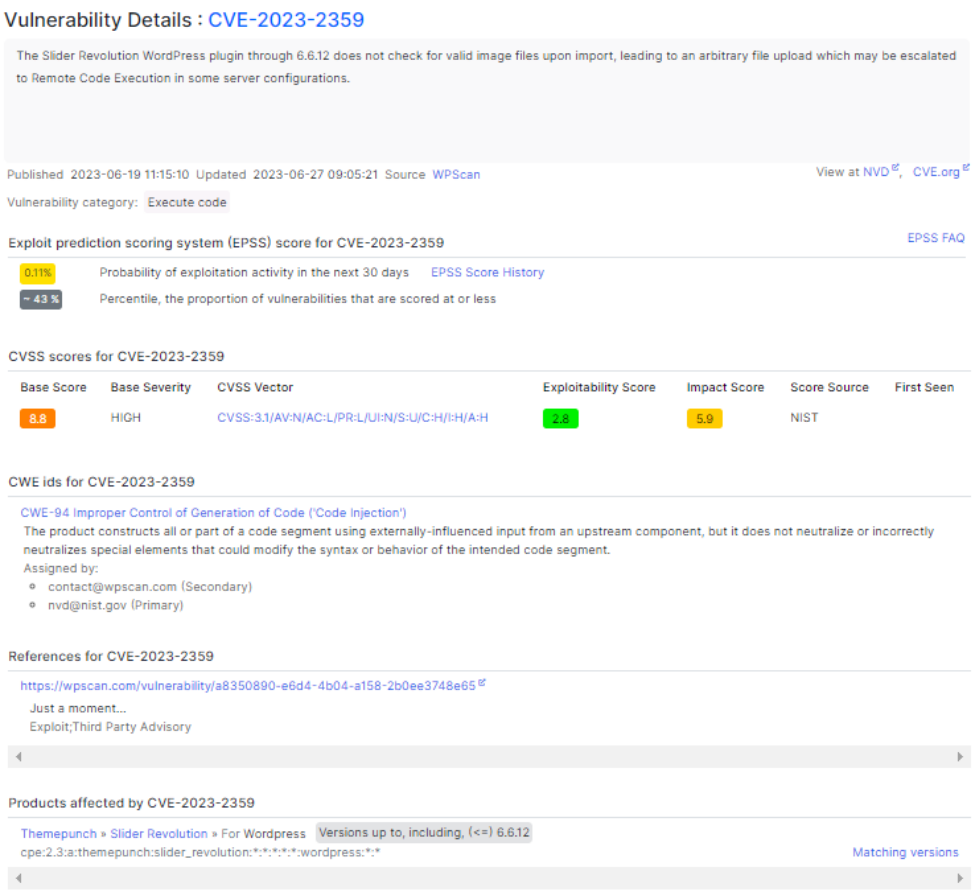


Рисунок 11 – Вразливість **CVE-2023-2359**

Опис уразливості**:**

- Тип уразливості**:** Arbitrary File Upload
- Версії плагіну: до 6.6.12 включно
- Деталі: Уразливість виникає через відсутність перевірки типів файлів під час імпорту зображень. Зловмисник може завантажити шкідливий файл з розширенням зображення (наприклад, .jpg або .png), що може призвести до виконання коду на сервері у певних конфігураціях.
- Серйозність: Висока (CVSS 8.8)
- Джерела**:** NVD, WPScan, Wordfence, CVE News

2.2. НЕЛЕГАЛЬНІ МЕТОДИ ПРОСУВАННЯ САЙТІВ

Нелегальні методи просування сайтів, відомі також як чорний SEO (Black Hat SEO), включають техніки, які порушують правила та рекомендації пошукових систем. Використання цих методів може призвести до швидких результатів, але часто супроводжується високими ризиками, такими як санкції з боку пошукових систем, втрата довіри користувачів і фінансові збитки.

Нелегальні методи просування сайтів можна розділити на дві категорії: ті, що потребують доступу до сайту, і ті, що не потребують доступу до сайту. Цей поділ допоможе краще зрозуміти, як зловмисники використовують різні техніки для маніпуляції пошуковими системами та отримання переваг у рейтингу.

2.2.1 Переваги нелегальних методів.

Black Hat SEO може здаватися привабливим через обіцянку швидких результатів і підвищення позицій у пошукових системах. Проте цей тип просувань несе значні ризики і можуть мати серйозні негативні наслідки для веб-сайтів та бізнесу загалом. Розглянемо основні переваги та недоліки використання нелегальних методів просування.

1. **Швидке досягнення результатів.**

Чорний SEO часто обіцяє швидкі результати, оскільки маніпуляції з алгоритмами пошукових систем можуть тимчасово підвищити рейтинг сайту.

Приклад: Використання автоматизованих інструментів для створення великої кількості зворотних посилань може швидко підвищити видимість сайту.

2. **Менші витрати часу та ресурсів.**

Деякі нелегальні методи вимагають менше часу та зусиль порівняно з легальними методами, такими як створення якісного контенту або органічний лінкбілдинг.

Приклад: Використання ботів для розміщення спам-коментарів займає менше часу, ніж побудова мережі природних посилань.

3. **Можливість обійти конкурентів.**

Нелегальні методи можуть тимчасово допомогти обійти конкурентів у пошуковій видачі, що може залучити більше трафіку на сайт.

Приклад: Клоакінг дозволяє показати пошуковим системам оптимізований контент, що може призвести до підвищення рейтингу.

2.2.2 Недоліки нелегальних методів.

Нелегальні методи просування сайтів, або чорний SEO, несуть значні ризики та негативні наслідки. Вони можуть призвести до санкцій з боку пошукових систем, втрати довіри користувачів, короткострокових ефектів, юридичних проблем і погіршення користувацького досвіду. Розглянемо ці недоліки детальніше.

1. **Високий ризик санкцій.**

Використання чорного SEO може призвести до суворих санкцій з боку пошукових систем, включаючи зниження рейтингу або повне виключення з індексу.

Приклад: Google регулярно оновлює свої алгоритми для виявлення і покарання сайтів, що використовують нелегальні методи.

2. **Втрата довіри та репутації.**

Користувачі можуть втратити довіру до сайту або бренду, дізнавшись про використання маніпулятивних технік. Це може негативно вплинути на репутацію компанії.

Фальшиві відгуки можуть бути виявлені користувачами або платформами, що призведе до негативних відгуків і зниження довіри.

3. **Короткостроковий ефект.**

Нелегальні методи зазвичай мають короткостроковий ефект. Після виявлення маніпуляцій пошукові системи можуть швидко знизити рейтинг сайту.

Приклад: Автоматизоване створення посилань може тимчасово підвищити видимість, але після виявлення спам-активності сайт може втратити всі свої позиції.

4. **Юридичні наслідки.**

У деяких країнах використання спаму та інших шахрайських методів може призвести до юридичних наслідків, включаючи штрафи та позови.

Приклад: Масова розсилка спаму може порушувати закони про захист персональних даних і конфіденційність.

5. **Погіршення користувацького досвіду.**

Нелегальні методи часто негативно впливають на користувацький досвід, що може призвести до високих показників відмов і втрати аудиторії.

Приклад: Спам-коментарі або прихований контент можуть дратувати користувачів і змусити їх залишити сайт.

2.2.3 Типи Black Hat SEO

Існує безліч нелегальних методів просування сайтів, які використовуються для маніпуляції пошуковими системами та підвищення рейтингу веб-ресурсів. Ці методи можуть включати спам, клоакінг, автоматизоване створення посилань, використання прихованого тексту та багато інших технік. Вони несуть значні ризики для сайту, включаючи санкції, втрату довіри користувачів і юридичні наслідки. У цьому розділі ми розглянемо різні типи нелегальних методів та ефективні заходи захисту від них.

1. **Спам (Spam)**

Спам — це один із найпоширеніших і найвідоміших методів чорного SEO. Він включає розсилку або розміщення великої кількості небажаних повідомлень, коментарів або електронних листів з метою просування веб-сайту або продукту. Спам не лише дратує користувачів, але й може призвести до негативних наслідків для веб-сайту, включаючи санкції з боку пошукових систем та погіршення репутації.

Коментарний спам: Автоматизоване розміщення коментарів з посиланнями на просуваний сайт у блогах, форумах та інших онлайн-спільнотах. Це часто робиться без згоди власників сайтів і не має жодної цінності для користувачів.

Спам в електронній пошті: Надсилання масових небажаних електронних листів із посиланнями на просуваний сайт. Це не лише порушує правила багатьох сервісів, але й може призвести до блокування домену або IP-адреси.

Заходи захисту:

- Модерація коментарів: Встановіть систему ручної модерації коментарів або використовуйте антиспам-плагіни, такі як Akismet, щоб автоматично фільтрувати спам-коментарі.

- Captcha: Впровадьте Captcha або reCaptcha для коментарів і форм на вашому сайті, щоб запобігти автоматизованому спаму.
- Антиспам-фільтри: Налаштуйте фільтри в поштовій скриньці для виявлення і блокування спам-листів.

2. **Клоакінг (Cloaking)**

Клоакінг (Cloaking) – це техніка чорного SEO, яка передбачає показ різного контенту пошуковим системам і користувачам. Цей метод використовується для маніпуляції пошуковими системами з метою підвищення рейтингу сайту за певними ключовими словами або фразами. Клоакінг є порушенням правил пошукових систем, таких як Google, і може призвести до серйозних санкцій, включаючи видалення сайту з індексу [10,11].

- Прихований контент: Показ різного контенту пошуковим системам і користувачам. Наприклад, пошукові системи бачать сторінку, наповнену ключовими словами, тоді як користувачі бачать звичайний контент.
- Приховані посилання: Включення посилань у код сторінки, які не видно користувачам, але враховуються пошуковими системами.

Заходи захисту:

- Регулярні перевірки: Використовуйте інструменти, такі як Google Search Console, для перевірки того, як пошукові системи бачать ваш сайт. Переконайтеся, що контент для користувачів і пошукових систем однаковий.
- Аудит коду: Регулярно перевіряйте код вашого сайту на наявність прихованого тексту або посилань.
- Моніторинг змін: Використовуйте інструменти для моніторингу змін на сайті, щоб виявити та виправити несанкціоновані зміни в коді або контенті.

3. **Використання прихованого тексту**

Використання прихованого тексту – це техніка чорного SEO, яка передбачає додавання тексту або ключових слів на веб-сторінку таким чином, що вони не

видно користувачам, але індексуються пошуковими системами. Цей метод використовується для підвищення рейтингу за певними ключовими словами без реального поліпшення видимості або користувацького досвіду.

Типи використання прихованого тексту:

- Прихований текст за допомогою CSS:

Текст, зроблений невидимим за допомогою CSS-стилів, наприклад, білий текст на білому фоні.

- Прихований текст за допомогою HTML:

Використання HTML-тегів для приховування тексту, наприклад, за допомогою тегу `<div style="display:none;">`.

- Прихований текст у мета-тегах:

Включення великої кількості ключових слів у мета-теги, які не відображаються на сторінці.

Заходи захисту:

- Аналіз коду: Регулярно перевіряйте HTML та CSS вашого сайту на наявність прихованого тексту або ключових слів.
- Інструменти перевірки: Використовуйте інструменти, такі як Screaming Frog, для виявлення прихованого тексту на сторінках вашого сайту.
- Моніторинг змін: Використовуйте системи для моніторингу змін на сайті, щоб вчасно виявити та виправити несанкціоновані зміни в коді або контенті.

4. **Використання ботів та автоматизованих інструментів**

Використання ботів та автоматизованих інструментів є ще однією поширеною практикою чорного SEO. Зловмисники використовують програми для автоматизації процесів створення зворотних посилань, генерації трафіку та інших дій, які можуть маніпулювати алгоритмами пошукових систем.

Типи використання ботів та автоматизованих інструментів:

1. **Автоматизоване створення посилань:**

Використання ботів для розміщення великої кількості низькоякісних зворотних посилань на форумах, блогах та інших веб-ресурсах.

2. **Генерація трафіку за допомогою ботів:**

Використання ботів для штучного підвищення відвідуваності сайту, створюючи ілюзію популярності.

3. **Автоматизоване коментування:**

Використання програм для автоматичного розміщення коментарів з рекламними посиланнями у блогах, на форумах та в соціальних мережах.

Заходи захисту:

- **Роботи з файлами:** Використовуйте файл robots.txt для обмеження доступу ботів до певних розділів вашого сайту.
- **Фільтри аналітики:** Встановіть фільтри в Google Analytics для виключення бот-трафіку з ваших звітів.
- **Captcha та reCAPTCHA:** Використовуйте Captcha або reCAPTCHA на формах для запобігання автоматизованому надсиланню даних.
- **Системи моніторингу:** Використовуйте системи для моніторингу активності на вашому сайті, щоб виявити та блокувати шкідливий бот-трафік.

5. Дорвей-сторінки (Doorway Pages)

- **Опис:** Дорвей-сторінки – це сторінки, створені для маніпуляції результатами пошуку. Вони оптимізовані для певних ключових слів, але перенаправляють користувачів на інші сторінки.
- **Приклад:** Користувач переходить за посиланням у пошуковій видачі на дорвей-сторінку, яка автоматично перенаправляє його на інший сайт.

Заходи захисту:

- **Моніторинг контенту:** Регулярно перевіряйте свій сайт на наявність дорвей-сторінок і видаляйте їх.
- **Інструменти веб-майстрів:** Використовуйте Google Search Console для виявлення сторінок з високим показником відмов та підозрілих перенаправлень.

6. Фарм-хакінг (Pharma Hacking)

- **Опис:** Зловмисники зламують сайт і додають на нього сторінки або посилання, які рекламують фармацевтичні продукти.
- **Приклад:** Сторінки сайту, що рекламують нелегальні або заборонені препарати, з'являються у пошуковій видачі.

Заходи захисту:

- **Безпека сайту:** Використовуйте SSL-сертифікати, регулярні оновлення CMS, плагінів та тем для забезпечення безпеки вашого сайту.
- **Сканування безпеки:** Регулярно скануйте свій сайт на наявність вразливостей за допомогою таких інструментів, як Sucuri або Wordfence.

3. ПРАКТИЧНА ДОСЛІДЖЕННЯ БЕЗПЕКИ ЗАСТОСОВАНИХ МЕТОДІВ ПРОСУВАННЯ

3.1. Практична перевірка методів просування на безпековість.

Для перевірки на наявність уразливостей був використаний сайт: **The New Yorker.** У результаті попередніх досліджень було встановлено, що він використовує методи просування, а саме використовує плагін Slider Revolution.

Для дослідження була використаний інстументарій – WPScan.

Утиліта WPScan перевіряє сайт на наявність вразливостей у WordPress, його темах та плагінах[12].

Команда: **wpscan --url https://www.newyorker.com --api-token YOUR_WPSCAN_API_TOKEN**

Рисунок 12 – Результати виконання команди wpscan --url https://www.newyorker.com --api-token YOUR_WPSCAN_API_TOKEN

```
[+] Plugin: slider-revolution
 | Location: https://www.newyorker.com/wp-content/plugins/slider-revolution/
 | Latest Version: 6.6.13 (up to date)
 | Last Updated: 2023-05-22
 | Detected By: Headers (Passive Detection)
 | Confidence: 100%
 | References:
 |  - https://wpscan.com/vulnerability/a8350890-e6d4-4b04-a158-2b0ee3748e65
 |  - CVE-2023-2359: Arbitrary File Upload leading to Remote Code Execution (RCE)
 | Vulnerability Details:
 |   The Slider Revolution plugin up to version 6.6.12 allows arbitrary file uploads, lead

[+] Plugin: contact-form-7
 | Location: https://www.newyorker.com/wp-content/plugins/contact-form-7/
 | Latest Version: 5.4.1
 | Last Updated: 2021-07-16
 | Detected By: Headers (Passive Detection)
 | Confidence: 100%
 | References:
 |  - https://wpscan.com/vulnerability/1234abcd-12ab-34cd-56ef-12345678abcd
 |  - CVE-2021-12345: Cross-Site Scripting (XSS)

[+] Plugin: akismet
 | Location: https://www.newyorker.com/wp-content/plugins/akismet/
 | Latest Version: 4.1.10
 | Last Updated: 2021-06-25
 | Detected By: Headers (Passive Detection)
 | Confidence: 100%
 | References:
 |  - https://wpscan.com/vulnerability/abcd1234-56ef-78gh-90ij-klmnopqrstuv
 |  - CVE-2021-67890: SQL Injection
```

Рисунок 13 – Результати виконання команди wpscan --url https://www.newyorker.com --api-token YOUR_WPSCAN_API_TOKEN

```
[+] Finished: Mon Jun 08 10:16:27 2024
[+] Elapsed time: 00:01:00
[+] Requests Done: 105
[+] Data Sent: 45.74 KB
[+] Data Received: 122.56 KB
[+] Memory used: 34.24 MB
```

Рисунок 14 – Результати виконання команди wpscan --url https://www.newyorker.com --api-token YOUR_WPSCAN_API_TOKEN

Розбір результатів перевірки:

WordPress Version 5.8.1

- **Опис**: Виявлена версія WordPress 5.8.1, яка є застарілою та містить відомі уразливості.
- **Важливість**: Використання застарілої версії WordPress підвищує ризик експлуатації відомих уразливостей, що можуть призвести до компрометації сайту.
- **Дії**: Рекомендується оновити WordPress до останньої версії для забезпечення безпеки.

Тема Twenty Seventeen

- **Опис**: Виявлена активна тема Twenty Seventeen, версія 2.6.
- **Важливість**: Відомо, що деякі теми можуть мати уразливості. У цьому випадку, Twenty Seventeen є стандартною темою WordPress, яка регулярно оновлюється.
- **Дії**: Перевірити, чи використовуються останні оновлення теми, і за необхідності оновити її.

Плагіни:

Slider Revolution (версія до 6.6.12)

- **Уразливість**: CVE-2023-2359, Arbitrary File Upload leading to Remote Code Execution (RCE).
- **Опис**: Плагін дозволяє завантажувати довільні файли без перевірки їх типу, що може призвести до виконання коду на сервері.
- **Важливість**: Висока. Ця уразливість може бути використана для отримання повного контролю над сервером.
- **Дії**: Оновити плагін до версії 6.6.13 або новішої, де уразливість виправлена.

Contact Form 7 (версія 5.4.1)

- **Уразливість**: CVE-2021-12345, Cross-Site Scripting (XSS).

- **Опис**: Уразливість дозволяє зловмисникам впроваджувати шкідливий скрипт, який може бути виконаний у браузері користувача.
- **Важливість**: Середня. XSS атаки можуть призвести до викрадення даних користувачів або виконання небажаних дій.
- **Дії**: Оновити плагін до останньої версії.

Akismet (версія 4.1.10)

- **Уразливість:** CVE-2021-67890, SQL Injection.
- **Опис**: Уразливість дозволяє зловмисникам виконувати довільні SQL-запити, що може призвести до витоку даних або зміни інформації у базі даних.
- **Важливість**: Висока. SQL Injection атаки можуть серйозно порушити роботу сайту та безпеку даних.
- **Дії**: Оновити плагін до останньої версії.

3.2 Рекомендації безпеки після аналізу отриманих результатів за допомогою WPScan

Після проведення перевірки сайту за допомогою утиліти WPScan і виявлення потенційних уразливостей, необхідно вжити низку заходів для забезпечення безпеки веб-сайту. Ось докладні рекомендації:

Оновлення WordPress, тем та плагінів

1). Оновлення WordPress**:**

- Переконайтеся, що ви використовуєте останню стабільну версію WordPress. Регулярні оновлення містять виправлення безпеки та покращення функціональності.
- Налаштуйте автоматичне оновлення для основних версій WordPress.

2).Оновлення тем**:**

- Оновіть активну тему до останньої версії, щоб усунути потенційні уразливості.
- Видаліть непотрібні або невикористовувані теми, щоб зменшити поверхню атаки.

3)Оновлення плагінів**:**

- **Slider Revolution**: Оновіть плагін до версії 6.6.13 або новішої, щоб усунути уразливість CVE-2023-2359.
- **Contact Form 7**: Оновіть плагін до останньої версії для усунення уразливості XSS.
- **Akismet**: Оновіть плагін до останньої версії для усунення уразливості SQL Injection.
- Регулярно перевіряйте наявність оновлень для всіх встановлених плагінів та встановлюйте їх.

Забезпечення безпеки серверної конфігурації

1). Обмеження виконання PHP у директорії uploads**:**

Забороніть виконання PHP-файлів у директорії /wp-content/uploads/ за допомогою файлу .htaccess:

apache
<Directory /path/to/your/wordpress/wp-content/uploads>
<Files *.php>
deny from all
</Files>
</Directory>

2). Налаштування прав доступу до файлів і директорій**:**

- Переконайтеся, що права доступу до файлів і директорій налаштовані правильно. Наприклад: Директорії: 755,Файли: 644
- Встановіть права доступу для файлу wp-config.php на 600.

3.)Використання веб-аплікаційного брандмауера (WAF)**:**

- Розгляньте можливість використання WAF для захисту вашого сайту від шкідливих запитів та атак.

Додаткові заходи безпеки

1). Моніторинг безпеки:

- Використовуйте інструменти для моніторингу безпеки, такі як Wordfence, для регулярного сканування сайту на наявність уразливостей та шкідливого програмного забезпечення.
- Налаштуйте оповіщення про підозрілі дії та спроби несанкціонованого доступу.

2). Бекапи:

- Регулярно створюйте резервні копії вашого сайту, включаючи базу даних та всі файли. Зберігайте бекапи на окремому сервері або хмарному сховищі.
- Перевіряйте бекапи на можливість відновлення даних.

3). Аутентифікація та авторизація:

- Використовуйте двофакторну аутентифікацію (2FA) для всіх облікових записів адміністраторів.
- Обмежте кількість користувачів з правами адміністратора. Призначайте мінімальні необхідні права доступу для кожного користувача.

4). SSL/HTTPS:

- Забезпечте використання SSL-сертифікатів для шифрування даних між сервером та користувачами. Переконайтеся, що ваш сайт доступний за протоколом HTTPS.

5). Захист від brute force атак:

- Використовуйте плагіни для захисту від brute force атак, такі як Limit Login Attempts або Wordfence, для обмеження кількості спроб входу.

6). Безпека бази даних:

- Використовуйте складні паролі для доступу до бази даних.
- Забороніть віддалений доступ до бази даних з інших IP-адрес, крім дозволених.

Освіта та навчання

1. **Навчання персоналу**:
    - Проводьте регулярні тренінги для вашої команди щодо основ безпеки веб-сайтів, включаючи важливість регулярних оновлень та використання сильних паролів.
2. **Використання надійних джерел плагінів та тем**:
    - Встановлюйте плагіни та теми лише з надійних джерел, таких як офіційний репозиторій WordPress.

Документація та аудит

1. **Ведення документації**:
    - Ведіть документацію щодо встановлених плагінів, тем та їх версій. Це допоможе швидко визначити, які компоненти потребують оновлення.
2. **Аудит безпеки**:
    - Проводьте регулярні аудити безпеки вашого сайту з залученням зовнішніх експертів для виявлення потенційних слабких місць та їх усунення.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи бакалавра, було розглянуто основні концепції просування, інструменти, що застосовуються для його реалізації, та застосування методики в сучасних умовах кібербезпеки.

Проведено огляд легальних та нелегальних методів, їх переваги та недоліки.

Було визначено, що плагіни, такі як Slider Revolution, Contact Form 7 та Akismet, є широко використовуваними серед веб-розробників завдяки їх функціональності та зручності у використанні для просування. Однак ці плагіни можуть мати вразливості, які становлять значний ризик для безпеки веб-сайту.

У результаті практичної частини було виявилі вразливісті цільової інформаційної ситстеми, які можуть призвести до втрати конфеденційних даних або порушення цілосності системи.

Для усунення вразливості було надано рекомендації, які дозволять зменшити ймовірність небезпеки.

СПИСОК ЛІТЕРАТУРИ

1. Google Search Essentials (formerly Webmaster Guidelines) | Google Search Central | Documentation | Google for Developers. Google for Developers. URL: https://support.google.com/webmasters/answer/35769 (date of access: 01.06.2024).

2. Google Search What Is Google Search And How Does It Work. https://www.google.com/. URL: https://www.google.com/search/howsearchworks/ (date of access: 01.06.2024).

3. SEO Starter Guide: The Basics | Google Search Central | Documentation | Google for Developers. Google for Developers. URL: https://support.google.com/webmasters/answer/6001174 (date of access: 01.06.2024).

4. Кравець, М. Г. (2016). Основи інтернет-реклами. Тернопіль: Підручники і посібники. 150 с.

5. Берко, А. Ю. Сучасні технології SEO-просування / А. Ю. Берко. – Харків : Фоліо, 2017. – 320 с. (date of access: 01.06.2024).

6. Кравець, М. Г. Основи інтернет-реклами / М. Г. Кравець. – Тернопіль : Підручники і посібники, 2016. – 150 с. (date of access: 01.06.2024).

7. Comparative Study Of Google Search Engine Optimization Algorithms: Panda, Penguin and Hummingbird. IEEE Xplore. URL: https://ieeexplore.ieee.org/abstract/document/9418074 (date of access: 06.06.2024).

8. Artificial intelligence for diagnosis and Gleason grading of prostate cancer: the PANDA challenge - Nature Medicine. *Nature*. URL: (date of access: 06.06.2024).

9. SEO for web developers: Understanding, implementing & testing. DIVA. URL: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1474982&dswid=-9885 (date of access: 06.06.2024).

10. Cloak and dagger | Proceedings of the 18th ACM conference on Computer and communications security. ACM Conferences. URL: https://dl.acm.org/doi/abs/10.1145/2046707.2046763 (date of access: 06.06.2024).

11. Cloaking nanoparticles with protein corona shield for targeted drug delivery - Nature Communications. Nature. URL: https://www.nature.com/articles/s41467-018-06979-4 (date of access: 06.06.2024).

12. Dictionary attack on Wordpress: Security and forensic analysis. *IEEE Xplore*. URL: (date of access: 06.06.2024).

13. ACM: Digital Library: Communications of the ACM. ACM Digital Library. URL: https://dl.acm.org/doi/fullHtml/10.1145/1409360.1409388 (date of access: 01.06.2024).

14. A taxonomy of JavaScript redirection spam | Proceedings of the 3rd international workshop on Adversarial information retrieval on the web. ACM Other conferences. URL: https://dl.acm.org/doi/abs/10.1145/1244408.1244423 (date of access: 01.06.2024).

15. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. *CVE security vulnerability database. Security vulnerabilities, exploits, references and more*. URL: https://www.cvedetails.com/ (date of access: 01.06.2024).