**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА КОМП'ЮТЕРНИХ НАУК**

# ВИПУСКНА РОБОТА

**на тему:**

## «Порівняльна характеристика систем керування вмістом для створення безпечних сайтів»

**Завідувач випускаючої кафедри** — **Довбиш А.С.**

**Керівник роботи** — **Лаврик Т.В.**

**Студента групи КБ – 71** — **Лоцько С.П.**

**СУМИ 2021**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

**Кафедра комп'ютерних наук**

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____" _____2021 р.

# ЗАВДАННЯ

## до випускної роботи

Студента четвертого курсу, групи КБ-71 спеціальності "Кібербезпека" денної форми навчання Лоцько Святослава Петровича.

**Тема:** "**Порівняльна характеристика систем керування вмістом для створення безпечних сайтів**"

Затверджена наказом СумДУ

№_____ від _____2021 р.

**Зміст пояснювальної записки**: 1) аналіз систем керування вмістом; 2) характеристика методів та інструментарію дослідження інформаційної безпеки; 3) тестування рівня захищеності вебресурів; 4) порівняльний аналіз систем керування вмістом.

Дата видачі завдання "_____"_____2021 р.

Керівник випускної роботи _____ Лаврик Т. В.

Завдання приняв до виконання _____ Лоцько С.П.

# РЕФЕРАТ

**Записка:** 63 стор., 25 рис., 2 табл., 20 джерел.

**Об’єкт дослідження** — системи керування вмістом.

**Мета роботи** — оцінювання систем керування вмістом для створення вебресурсів з точки зору таких критеріїв як:

- простота використання;
- доступність додаткових модулів;
- рівень безпеки отриманого ресурсу;
- швидкість реагування команди розробників CMS у випадку проблем з безпекою самої CMS.

**Методи дослідження** — метод аналітичного огляду, метод порівняння, метод експертних оцінок.

**Результати** — проведено порівняльний аналіз систем керування вмістом. Аналіз проведений на основі критеріїв тісно пов’язаних з безпекою ресурсів. У процесі дослідження детально розглядався кожен з критеріїв для обраних систем керування вмістом. У результаті було отримано порівняльну характеристику систем, рекомендації щодо їх доцільного використання та усереднені оцінки кожної системи. Усереднені оцінки були отримані з використанням методу експертного аналізу, основним пріоритетом якого була безпека систем та ресурсів, тобто всі критерії були розглянуті з точки зору впливу на загальний рівень безпеки.

СИСТЕМА КЕРУВАННЯ ВМІСТОМ, ІНФОРМАЦІЙНА БЕЗПЕКА, МОДУЛІ, ПЛАГІНИ, WORDPRESS, JOOMLA, WIX, DRUPAL, ВЕБ-РЕСУРСИ, ЗАХИСТ, АНАЛІЗ, ХАМРР, ПОРІВНЯННЯ, ОБСЛУГОВУВАННЯ, МЕТОДОЛОГІЯ

**ЗМІСТ**

ВСТУП ..... 3
1. АНАЛІЗ СИСТЕМ КЕРУВАННЯ ВМІСТОМ ..... 5
1.1. Загальний огляд систем керування вмістом ..... 5
1.2. Аналіз існуючих систем керування вмістом ..... 7
1.3. Постановка задачі ..... 17
2. ХАРАКТЕРИСТИКА МЕТОДІВ ТА ІНСТРУМЕНТАРІЮ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ..... 18
2.1. Аспекти інформаційної безпеки ..... 18
2.2. Інструменти для аналізу рівня захищеності вебресурсів ..... 23
3. ПОРІВНЯЛЬНИЙ АНАЛІЗ СИСТЕМ КЕРУВАННЯ ВМІСТОМ ..... 31
3.1. Простота використання системи ..... 31
3.2. Доступність додаткових модулів ..... 36
3.3. Рівень обслуговування CMS ..... 42
3.4. Безпека ..... 46
ВИСНОВКИ ..... 57
СПИСОК ЛІТЕРАТУРИ ..... 60

# ВСТУП

Інформація завжди була одним з найбільш цінних ресурсів у світі, починаючи з древніх часів, коли люди тільки освоїли певні засоби комунікації та до наших днів. Інформація займає своє місце у світі як найбільш дорогоцінний ресурс, оскільки в деяких випадках її вартість може в рази перевищувати цінність золота, або взагалі бути неоціненною. Звісно не будь-яка інформація має високу вартість, на її вартість впливає безліч факторів починаючи від складності її отримання та закінчуючи рівнем вигоди сторони в випадку отримання даної інформації.

В часи минулого навіть книги були дуже дорогими та вважались ознакою статусу в суспільстві, в наш же час, завдяки розвитку всесвітньої мережі, доступ до інформації припинив бути настільки яскраво вираженою проблемою.

З розвитком мережі все більша частина підприємств створює собі представлення в ній, а деякі підприємства взагалі цілком переходять в онлайн простір, спочатку це дозволяло їм приваблювати нових клієнтів, а потім дозволило спробувати себе в відносно ніші відносно вільній від конкурентів. Вебресурс є дуже зручним інструментом, який підвищує зручність взаємодії з підприємством, а також дає можливість захопити новий сегмент клієнтської бази в мережі Інтернет. Наприклад, якщо це сайт ресторану, то клієнт може за допомогою вебресурсу обрати собі їжу та оформити замовлення онлайн. У такому випадку знадобиться тільки дзвінок з ресторану для підтвердження замовлення, а це набагато швидше та зручніше ніж телефонувати в ресторан, слухати меню та обирати, спираючись лише на слух. Це лише один з наочних прикладів. Але насправді подібна ситуація складається з більшою частиною підприємств.

Створення якісного сайту з нуля є доволі важкою роботою, особливо для тих, хто раніше ніколи цим не займався, але для таких людей є багато Content Management System (CMS) платформ. CMS платформи це системи керування вмістом, за допомогою яких навіть далека від веброзробок людина має можливість створити свій сайт. Зазвичай ці системи мають інтуїтивно зрозумілий графічний інтерфейс, завдяки

якому для створення сайту людині не потрібно знати навіть мови розмітки HTML. Користувач просто створює дизайн свого сайту (тобто, те як він має виглядати), а CMS займається конвертацію цього дизайну в код.

Звісно, якщо створювати сайт з нуля, то розробник має повну свободу в засобах, які буде використовувати. У випадку з CMS засоби, які використовуються, для різних CMS є сталими та своїми для кожної CMS.

В наш час уже існує безліч вебресурсів та онлайн-магазинів, але це ще далеко не фінал, з кожним днем їх стає все більше і більше, що з одної сторони підтверджує актуальність та перспективність мережі, але з іншого надає все більше можливостей шахраям які працюють в ній. Тому є важливим забезпечити безпеку інформації в мережі, а для цього необхідно розглянути які аспекти інформаційної безпеки бувають в загальному, за що саме відповідає кожний з них, та як зробити так, щоб всі ці аспекти доповнювали одне одного та надавали на виході надійну систему захисту. Маючи про це уявлення є можливим розглядати системи захисту реалізовані в різних системах керування вмістом, та проводити порівняльний аналіз з визначенням слабких та сильних сторін кожної з них, а на результатах цього аналізу зробити висновки, щодо пріоритетності використання систем.

Основною задачею роботи є розгляд основних аспектів організації безпеки інформації в вебресурсах створених за допомогою систем керування вмістом, а також визначення рівнів пріоритетності різних аспектів відносно до специфіки створюваного ресурсу.

# 1. АНАЛІЗ СИСТЕМ КЕРУВАННЯ ВМІСТОМ

## 1.1. Загальний огляд систем керування вмістом

Система керування вмістом (далі в роботі буде використана абревіатура *CMS (Content Management System)* ) — програмне забезпечення для організації вебресурсів в мережі Інтернет, а також окремих комп'ютерних мережах.

В загальному існує велика кількість різних CMS, основа задача яких є однаковою, але разом з тим засоби її реалізації відрізняються, тому різні структури та компанії використовують різні системи відповідно до своїх потреб. Не зважаючи на відмінності в апаратних та програмних засобах, які використовують різні CMS, їх все-таки можна розглянути як одне ціле відповідно тим факторам, які властиві практично всім CMS.

Історія CMS розпочалась в якості спеціалізованого програмного забезпечення, основною функцією якого була організація роботи з документацією в великих корпораціях, такі системи були відносно далекі від того поняття CMS, яке відоме нам зараз. В 1995 році від американської медіа компанії Computer Network відокремилась окрема компанія під назвою Vignette, цю компанію можна вважати основоположником ринку платних CMS [1].

Всі наявні на даний момент CMS є можливим поділити на дві загальні категорії: комерційні та безкоштовні. Доступ до безкоштовних CMS систем є вільним та кожен може ознайомитись або працювати використовуючи їх, також користувач може безкоштовно отримати спеціалізовану допомогу від технічної підтримки в разі проблем в роботі з системою. У свою чергу комерційні CMS є платними, але в багатьох випадках більш надійними та широко профільними ніж свої безкоштовні аналоги. Комерційні CMS можуть бути двох видів

- з закритим кодом (вихідний код є закритим та користувач не має можливості вносити в нього зміни);

- з відкритим кодом (код системи є відкритим та користувач може вносити в нього зміни).

Кожен з цих типів має, як свої недоліки, так і переваги, наприклад системи з закритим кодом є більш захищеними, тоді як системи з відкритим кодом більш вразливі до атак, але водночас системи з відкритим кодом дають вмілому користувачу більше простору для роботи з ними.

CMS значно спрощують роботу пов’язану зі створенням сайту та його подальшим адмініструванням, але з іншого боку їх використання може привести до певних проблем з безпекою вебресурсів. Як було сказано вище, при знаходженні вразливості в CMS з відкритим кодом, небезпека поширюється на всі сайти, які працюють на даній CMS. Крім цього при створенні сайту за допомогою CMS є можливість використати вже заражені матеріали, що в результаті призведе до зараження всього ресурсу. Також зазвичай при використанні CMS використовуються сторонні плагіни та модулі, які можуть мати в собі певні вразливості, використовуючи які можна отримати несанкціонований доступ до ресурсу.

Також цілком можливі репутаційні втрати для компанії, у вигляді того, що обслуговуванням та безпекою вебресурсів підприємства займається людина без досвіду в цій сфері(наведений приклад справедливий в випадку, коли CMS використовувалась тільки через простоту використання).

Неможливо на всі 100% захистити ресурс від загроз, але є можливим по максимуму мінімізувати їх, для цього необхідно завжди тримати CMS в найновішій версії, це звісно не врятує від індивідуальних атак, але хоча б захистить від загальновідомих уразливостей з минулих версій. Також у випадку коли загального функціонала CMS недостатньо, необхідно використовувати, або перевірені надійні модулі, які можуть додати необхідний користувачу функціонал, або дати задачу на написання нового модуля, досвідченим програмістам, які добре розбираються в інформаційній безпеці.

Взагалі, не зважаючи на те створений сайт з нуля чи за допомогою CMS, найкращим фактором, що гарантує його безпеку з інформаційної точки зору, є досвідчені та кваліфіковані співробітники, які будуть займатись його підтримкою.

## 1.2. Аналіз існуючих систем керування вмістом

### 1.2.1. Wix

Wix.com це міжнародний хмарний сервіс призначений для створення вебресурсів та їх подальшого розвитку. Використовуючи Wix можна створювати сайти навіть без навичок програмування та веброзробки, все що необхідно, це створити макет сайту(уявлення про те, як він має виглядати) та реалізувати його на Wix.com за допомогою наявних інструментів. Завдяки наявності багатьох програмних модулів можливо також розширювати функціональність сайту в будь-якому необхідному розробникові напрямі(наприклад додати модулі з функціоналом соціальних мереж). Також перевагою даної системи можна вважати можливість використання сторонніх модулів, тобто модулі представлені на платформі розроблені не тільки розробниками Wix, а також і сторонніми розробниками, це і дає можливості для розширення функціоналу ресурсів. Хоч сам сервіс і є безкоштовним, але в ньому існує система преміум, яка надає користувачу багато переваг, наприклад можливість під'єднати власний домен, отримати окреме місце для зберігання даних, та прибрати рекламу.

Основні переваги Wix:

- безкоштовні шаблони;
- безкоштовний хостинг;
- автоматична оптимізація пошуку;
- можливість під'єднати свій домен;
- створений сайт можна оптимізувати під мобільні пристрої;
- захист створених ресурсів;

- багато модулів нарізну потребу;
- зручна статистика

Використовуючи Wix.com в вас є два варіанти створення сайту, ви можете пройти опитування, щодо специфіки сайту, який ви хочете отримати та WIX ADI сам згенерує сайт відповідно вашим вимогам, або ви можете обрати шаблон із багатьох доступних та відредагувати його вручну, під свої вимоги [2].

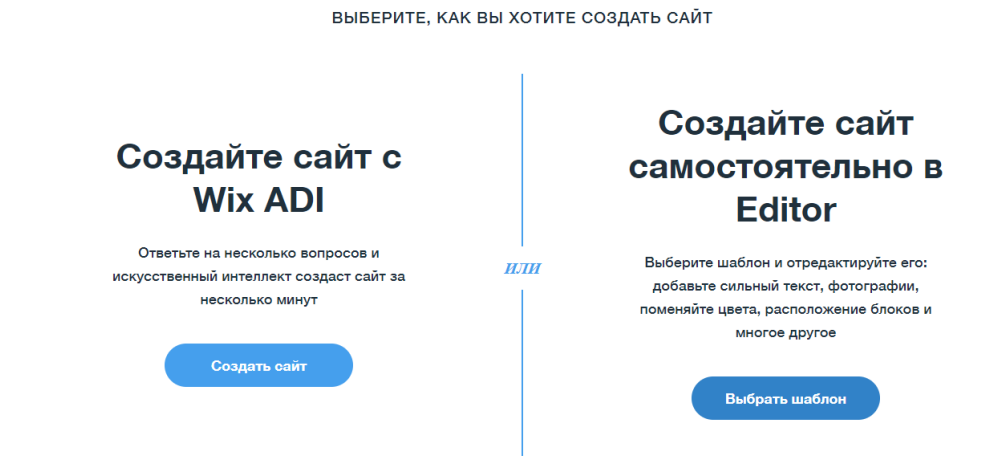


Рисунок 1.1. – Інтерфейс Wix.com

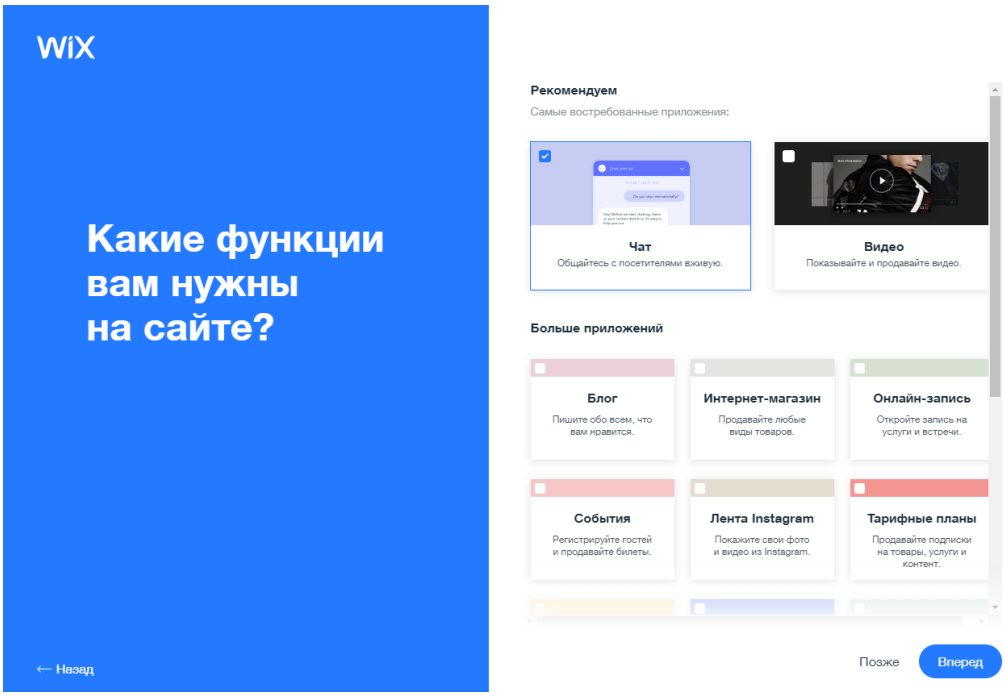


Рисунок 1.2. – Інтерфейс Wix.com

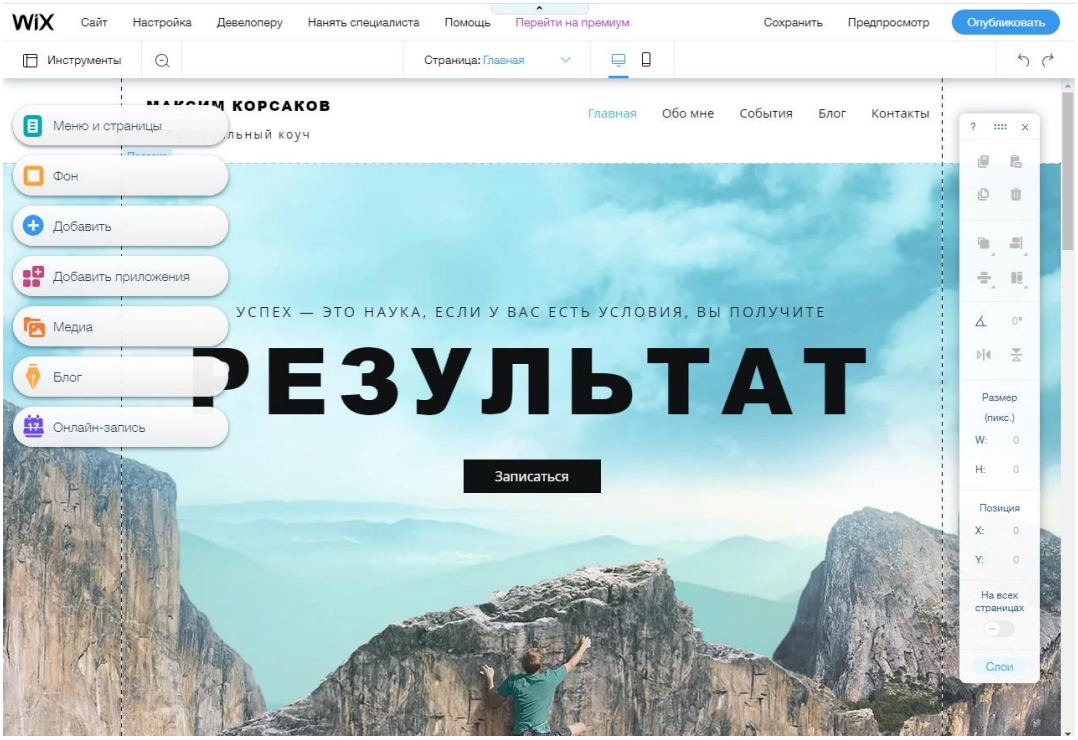


Рисунок 1.3. – Інтерфейс Wix.com

### 1.2.2. Joomla

Joomla це відкрита унікальна CMS, яка використовується для створення вебресурсів та їх подальшого адміністрування. Широкий функціонал та інтуїтивно зрозумілий інтерфейс дозволяє створити ресурс на будь-яку потребу, від невеликого сайту-візитки для компанії до онлайн магазину.

Основними особливостями даної CMS є:

- широкий інструментарій для управління обліковими записами;
- зручний інтерфейс для роботи з медіа;
- можливість зручної локалізації ресурсів;
- система управління рекламою;
- багато готових модулів;
- безліч шаблонів;
- візуальний редактор;

- XML-виклик віддалених процедур;
- вбудований пошук;
- можливість кешування сторінок.

Joomla! написана на мові PHP за архітектурним шаблоном Model-view-controller, завдяки цьому система є гнучкою та зручною в разі розширення. При роботі з Joomla! Використовуються такі системи управління базами даних (далі СУБД) як MySQL, PostgreSQL або MS SQL.

Joomla! захищена ліцензією GPL, ця ліцензія дає користувачам право вільно модифікувати та копіювати систему, але також вона гарантує, що всі похідні продукти від основної системи також будуть вільними. Така ліцензія дозволяє користувачам самим покращувати початковий продукт та в результаті з кожною ітерацією отримувати, щось нове в основі якого лежить стартовий продукт.

CMS Joomla! при початковій установці містить тільки необхідні для роботи системи інструменти без надлишків, додатковий інструментарій є можливим встановити за потреби, це зроблено заради того, щоб запобігти захаращення панелі управління та зробити процес роботи з системою максимально зручним [3].

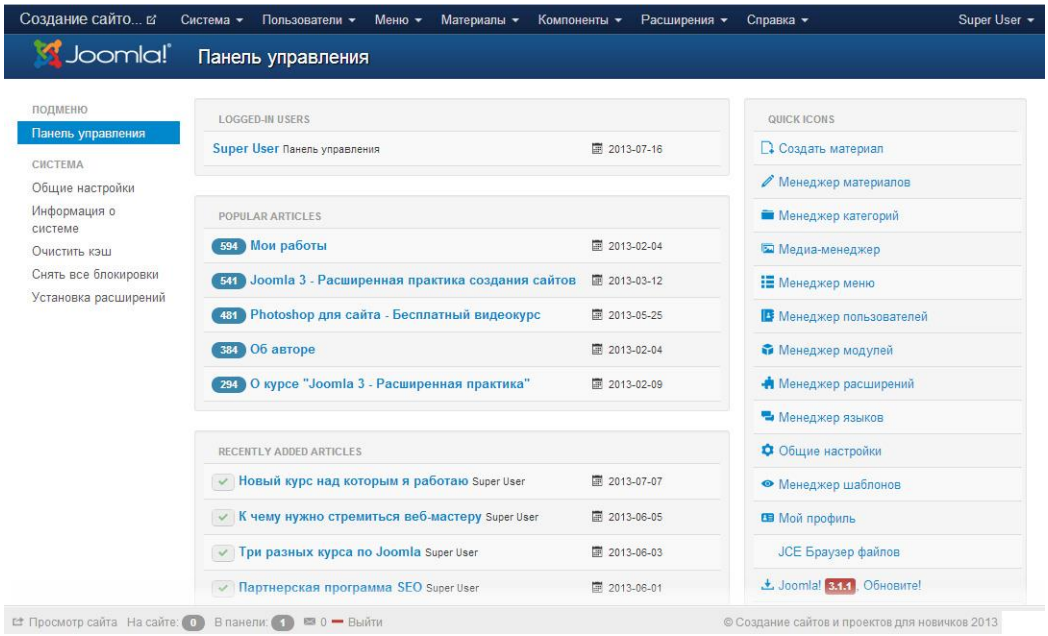


Рисунок 1.4. – Інтерфейс Joomla

### 1.2.3. Drupal

Drupal це вільно розповсюджувана CMS написана на PHP та захищена ліцензією GPL, про цю ліцензію та в чому її особливості було сказано в попередньому розділі присвяченому Joomla.

Зазвичай Drupal використовують для написання back end частин різних сайтів, незалежно від їх функціональності та призначення.

В загальному Drupal працює з такими вебсерверами як Apache, Nginx, Lighttpd та Microsoft IIS.

Основними можливостями даної CMS є:

- Підтримка RSS, RDF, Atom;
- зручне ведення блогу або форуму;
- посилання повідомлень;
- можливості зручної локалізації системи;
- можливість змінити назв посилання для підвищення рівня зручності;
- профілі для користувачів, які можуть налаштовуватись;
- пошук за ключовими словами;

- статистика;
- можливість сортування матеріалів;.

Система Drupal завдяки своїм модулям та структурі дозволяє доволі просто створювати різноманітні вебресурси високого рівня якості.

Drupal підтримує різні теми оформлення та дозволяє створювати свої теми оформлення.

Також спільнотою Drupal створено багато побічних модулів, які допоможуть в роботі з цією системою та зроблять наші сайти ще більш функціональними та різноплановими [4].

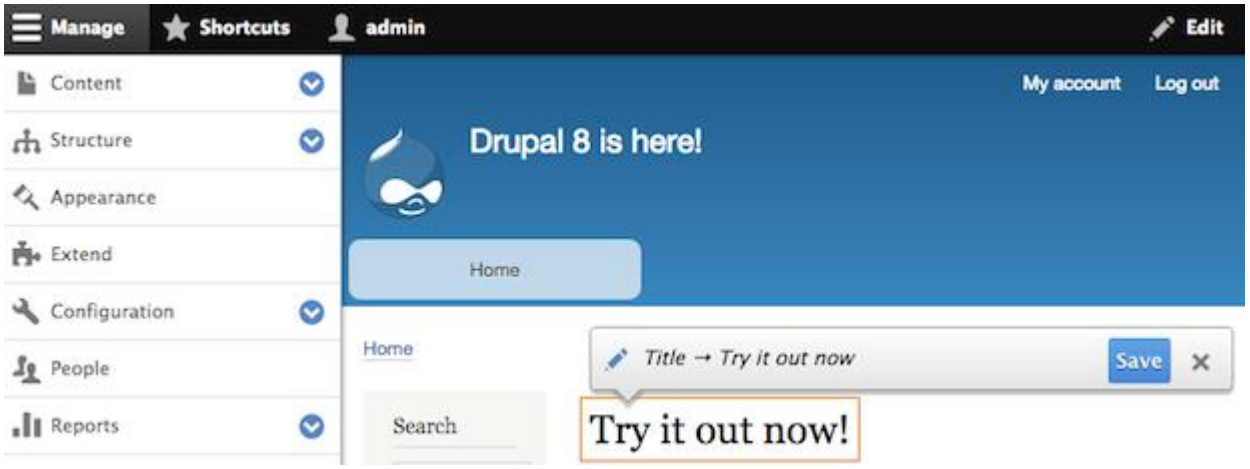


Рисунок 1.5. – Інтерфейс Drupal

### 1.2.4. WordPress

WordPress CMS з відкритим початковим кодом, через свою простоту в встановленні та використанні є дуже відомою на ринку CMS, вона широко застосовується для створення та подальшого просування вебресурсів різної величини починаючи з маленьких проектів та закінчуючи сайтами великих компаній.

Написана за використанням мови програмування PHP з використанням СУБД MySQL. Початковий код поширюється під захистом ліцензії GPL.

Основні переваги:

- просто встановити;

- просто налаштувати;
- підтримка основних вебстандартів;
- інтуїтивно зрозуміле використання плагінів;
- можливість оновлювати систему безпосередньо з панелі адміністратора;
- підтримка тем;
- можливість редагування шаблонів з панелі адміністратора;
- велика бібліотека тем та модулів;
- SEO-оптимізована система;
- українська локалізація;
- миттєве публікування;
- підтримка RSS, Atom, trackback, pingback;
- наявність URL інтуїтивно-зрозумілого для рядового користувача;
- підтримка візуального редактора;
- можливість поставити таймер на публікацію;
- підтримка медіа та мультимедіа [5].

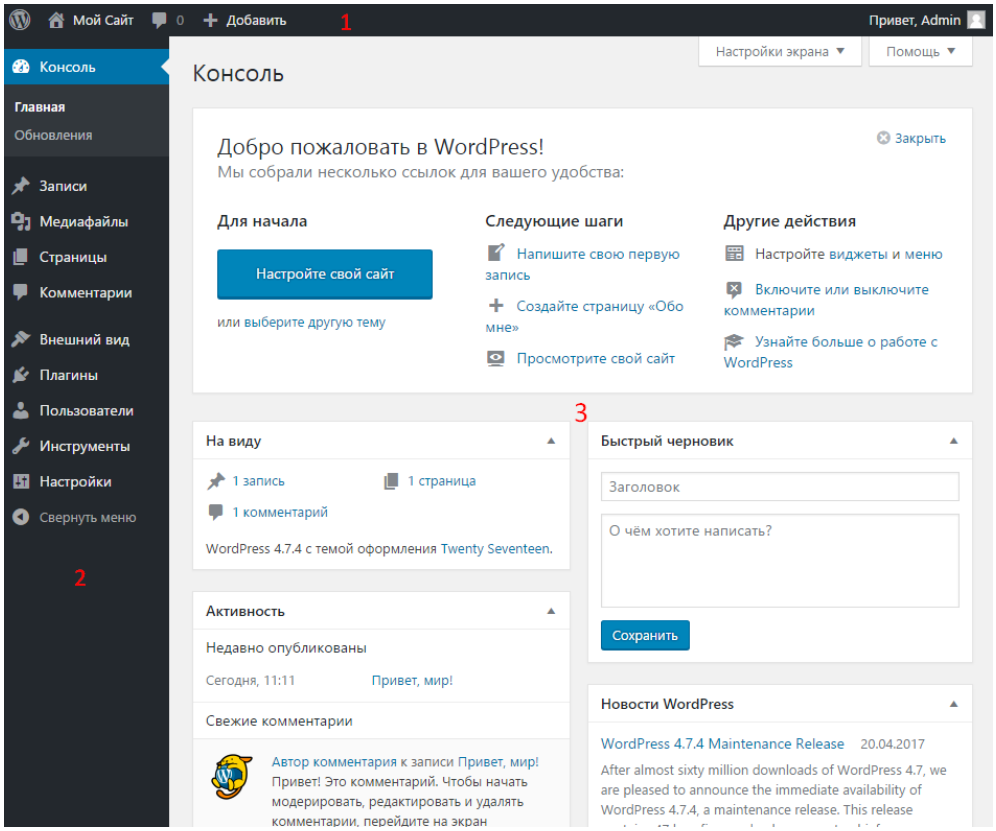


Рисунок 1.6. – Інтерфейс WordPress

### 1.2.5. Особливості CMS для створення безпечних сайтів

В загальному, загрози безпеки для вебресурсів можуть бути прямими та прихованими. До загроз прямого типу належать атаки з використанням брутфорсу або використання уразливостей в структурі ресурсу для отримання неавторизованого доступу, вразливості можуть бути в системах керування вмістом (CMS), плагінах та шаблонах використаних при створенні сайту або розширеннях та змінах. До атак прихованого типу відноситься: компрометація сервера, атаки від “сусідів”, злам SSH/FTTP, Nulled- шаблони, перехват та витік доступів, соціальна інженерія. Відповідно статистичним даним більшість атак реалізуються через загрози прямого типу (74-75% від загальної кількості), але в останні роки помітно стійке зростання кількості атак прихованого типу, заслуговує уваги також той факт, що близько 5% від всіх атак пов’язані з

діяльністю сторонніх фрілансерів або підрядників, які займаються обслуговуванням ресурсів та апаратури [6].

У випадках з використанням CMS, для створення сайту та його подальшого супроводу безпека ресурсів на значному рівні залежить від самої системи керування контентом (CMS) та вчасного встановлення оновлень необхідних для безпеки ресурсу. Таким чином у 2018 році спеціалістами компанії Sucuri було проведено дослідження за результатами якого вони прийшли до висновку, що з точки зору безпеки найбільш небезпечною CMS є WordPress, за результатами їх дослідження 90% ресурсів захист яких зловмисникам вдалось обійти, були сайтами які використовують WordPress. Також в основному дірки в безпеці сайтів існували через ігнорування нових оновлень, необхідних для коректної роботи систем захисту [7].

Як було сказано в пункті 1.1, CMS може бути комерційною та загальнодоступною, цей факт теж значно впливає на рівень захисту ресурсів, за результатами досліджень сайти побудовані за допомогою комерційних систем управління контентом в 4 рази рідше піддаються нападам та потрапляють в чорні списки, але і серед безкоштовних CMS ситуація не рівномірна, так наприклад в чорні списки потрапляє кожний двадцятий сайт на Datalife Engine, і одночасно тим серед сайтів на TYPO3 не було знайдено ні одного з уразливостями, швидше за все, це пов’язано з тим, що команда розробників TYPO3 дуже піклується про безпеку та постійно публікує знайдені вразливості. Серед комерційних систем управління контентом все приблизно рівномірно та визначити однозначного лідера неможливо. Згідно з дослідженням з усіх перевірених сайтів що працюють на Joomla та WordPress лише 3% використовували останню версію CMS Joomla та 15% CMS WordPress, це у свою чергу призвело до того що доля проблемних сайтів на Joomla в 3 рази більше ніж на WordPress [8].

Можна помітити, що спочатку було сказано про те що 90% зламаних сайтів використовували WordPress, потім про те, що доля проблемних сайтів з

використанням Joomla більше ніж тих, що використовують WordPress, це пов’язано з тим, що в загальному огляді WordPress є найпоширенішим серед всіх CMS і кількість сайтів на ньому банально в рази більша ніж на інших системах керування вмістом, і виходячи з цього він може бути більш безпечним ніж більшість CMS, але через поширеність, кількість зломів сайтів на ньому буде більшою ніж кількість зломів на сайтах з меншим рівнем захисту.

Значними загрозами для сайтів створених з використанням CMS є сторонні плагіни, які використовуються для роботи ресурсів, бувають випадки коли розробники продають свої плагіни стороннім особам, а вони можуть внести в них певні зміни, які приведуть до шкоди для ресурсів. Наприклад, у 2017 році WordPress заблокував три плагіни, які були продані своїми розробниками, а нові власники додали в них бекдори. Також існує варіант з плагінами, які мають критичні уразливості та були закинуті своїми розробниками, іноді такі плагіни досі використовуються на багатьох сайтах, а їх власники навіть не підозрюють про проблему. В списку літератури буде наведений ресурс під номером [9], на якому можна знайти багато цікавої інформації про такі плагіни та не тільки. Також бувають проблеми з неправильно написаними з точки зору безпеки модулями, наприклад у 2018 році в системі управління контентом Drupal було знайдено дві критичні для безпеки вразливості в модулях, перша була пов’язана з вбудованою системою посилання e-mail, вона дозволяла виконувати довільний код при обробці повідомлення, а друга проблема була пов’язана з модулем Contextual Links він дозволяє модифікувати елементи сторінки без переходу на сторінку управління, відсутність перевірки параметрів, могла призвести до виконання довільного коду, обидві ці загрози є дуже схожими, але різниця в тому, що другою вразливістю може скористатись тільки людина, яка вже має доступ до панелі управління сайтом, в той час як першою може користуватись людина, у якої такий доступ відсутній. Отже, перша вразливість є набагато більш критичною [10].

## 1.3. Постановка задачі

Аналіз показав, що на даний час в мережі Інтернет існує безліч сайтів, створених за допомогою CMS платформ. Ці сайти мають різноманітний функціонал та цілі, починаючи від звичайних односторінкових сайтів-візиток та закінчуючи доволі потужними інтернет-магазинами. Станом на кінець лютого 2021року на одному тільки Wordpress працює 28 183 568 вебресурсів. На інших платформах працює набагато менше сайтів у порівнянні з Wordpress. Наприклад, на Wix працює 4 565 423 сайтів, на Joomla! – 1 662 593. Найнижчі показники стосуються CMS платформи Drupal, на якій працює лише 562 655 сайтів [1].

Виходячи з наведеної вище інформації, можна зробити висновки про те які CMS-системи мають вищі показники за певними критеріями, а які нижчі показники. Але чи будуть ці висновки коректними і обґрунтованими для користувачів CMS, які не особливо детально розбираються в тому з чим вони працюють.

Метою цієї роботи є оцінювання систем керування вмістом для створення вебресурсів з точки зору таких критеріїв як:

- простота використання;
- доступність додаткових модулів;
- рівень безпеки отриманого ресурсу;
- швидкість реагування команди розробників CMS у випадку проблем з безпекою самої CMS.

Результатом роботи буде порівняльна таблиця з оцінками різних критеріїв для кожної з CMS, на основі якої будуть зроблені висновки щодо доцільності використання різних CMS за різних обставин. Оцінювання безпеки буде проводитись за допомогою спеціальних інструментів, визначених у розділі 2.

# 2. ХАРАКТЕРИСТИКА МЕТОДІВ ТА ІНСТРУМЕНТАРІЮ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1. Аспекти інформаційної безпеки

Захист інформації це набір певних засобів, які забезпечують дотримання основних властивостей інформації(цілісності, конфіденційності та доступності) в умовах коли реалізація певних загроз має можливість чинити шкоду власникам та користувачам даної інформації.

- Конфіденційність – захищає інформацію від можливості несанкціонованого доступу до неї.
- Цілісність – захист оригінального вигляду інформації, захищає інформацію від несанкціонованих змін.
- Доступність – захист доступу до інформації, забезпечує можливість отримати доступ до інформації в той момент коли вона буде необхідна, також ця властивість відповідає за підтримання обладнання в робочому стані та резервне відновлення даних в разі помилок.

Відповідно до наведених властивостей інформації, дотримання яких гарантує коректний рівень захисту інформації існують певні загрози, які призводять до їх порушення.

- порушення цілісності:
  - знищення інформації, або якоїсь її частини;
  - несанкціоноване внесення змін;
- порушення доступності:
  - блокування доступу до інформації;
  - знищення інформації, або якоїсь її частини;
- порушення конфіденційності:
  - неавторизований доступ до інформації;
  - витік даних, який призводить до порушення конфіденційності;

- розголошення інформації, яка є конфіденційною.

Інформація є дуже важливим ресурсом, який потребує захисту, тому необхідно розглянути аспекти з яких складається коректний захист більш детально, такий розгляд дозволяє більш детально вивчити тему, та потім робити об’єктивні висновки щодо рівня захисту інформації який використовується при роботі з системами керування вмістом вмістом.

В загальному, захист інформації, що використовується вебресурсом можна розділити на два аспекти, кожний з яких має багато більш спеціалізованих напрямків. В основному цими аспектами є :

- безпека системи;
- безпека інформації.

### 2.1.1. Безпека системи

Під безпекою системи мається на увазі загальний захист системи інформаційної безпеки та всіх її складових, є можливим сказати, що цей аспект відповідає за захист вебресурсу від несанкціонованого доступу та можливих несанкціонованих модифікацій. Якщо безпека системи добре організована та підтримується кваліфікованими спеціалістами, то шанси проникнення зловмисника в систему є дуже малими, та навіть у випадку успішного проникнення, він буде швидко знайдений та видалений з системи, що не дозволить вчинити шкоду системі.

Безпеці системи необхідно приділяти значну увагу починаючи зі стадії розробки вебресурсу, оскільки якщо будувати систему захисту паралельно з самим ресурсом, який вона буде захищати, то є можливість мінімізувати затрати часу необхідні на побудову системи та максимізувати рівень захисту системи. Наприклад у випадку побудови системи захисту постфактум потрібно буде будувати систему з нуля виходячи тільки з інформації про ресурс, а при паралельній розробці у розробників буде можливість більш глибоко зрозуміти вимоги ресурсу та відобразити їх в системі, в такому випадку розробники

практично беруть участь в розробці ресурсу, тоді як по розробці постфактум вони лише отримують поверхневе ТЗ на основі вже існуючого ресурсу.

Одним з найбільш важливих компонентів системи інформаційної безпеки є програмне забезпечення, а саме для забезпечення стійкої системи захисту інформації, насамперед необхідно забезпечити безпеку програмного забезпечення яке буде використано. Будь-яке програмне забезпечення не є ідеальним, в ньому можуть виникати якісь помилки або неточності, які призводять до помилок. Оскільки повністю ліквідувати всі потенційні помилки практично неможливо, то необхідно мінімізувати їх, наприклад за допомогою відключень непотрібних опцій та внесенням своєчасних оновлень в програмне забезпечення.

Також важливо завжди перевіряти наскільки добре працює програмна частина системи, навіть якщо обов’язки по її підтриманню лежать на інших структурах, наприклад при використанні власного налаштованого вебсервера для роботи вебресурсу ви відповідаєте за коректність роботи і своєчасне виявлення помилок та дірок в безпеці зі сторони серверної частини програмного забезпечення, але в загальному набагато простіше є використати послуги інтернет хостингу для підтримання роботи сайту, використовуючи послуги інтернет хостингу ви делегуєте роботу, щодо своєчасного оновлення серверного програмного забезпечення та виявлення неполадок, але все-таки не буде зайвим слідкувати за своєчасним виконанням цих процесів.

При роботі з системами керування вмістом вмістом для створення вебресурсів основний пріоритет надається зручності в користуванні, тому рядовому користувачу не доводиться розмірковувати про безліч аспектів роботи, наприклад в більшості систем керування вмістом є вбудований безкоштовний хостинг, який дозволяє викласти створений сайт в мережу відразу після його створення.

Також необхідно не забувати про можливі дефекти в програмному забезпеченні, вони є найбільш непередбачуваним фактором, оскільки можуть призвести до проблем роботи системи навіть в випадку її стабільного обслуговування та своєчасного оновлення. Зазвичай відомі постачальники програмного забезпечення не допускають критичних дефектів у своїй продукції, але ніхто не застрахований від помилки, сам по собі дефект, це помилка в роботі програми, яка викликає її неправильну або некоректну роботу, самі по собі дефекти не несуть значної шкоди для системи, їх швидко виявляють та виправляють, але невиявлені дефекти можуть бути використані зловмисниками, для отримання несанкціонованого доступу до системи. Для мінімізації ймовірності використання дефектів стороннім особами достатньо вчасно оновлювати програмне забезпечення та контролювати процеси та запити всередині системи.

### 2.1.2. Безпека інформації

Даний аспект інформаційної безпеки відповідає за безпеку даних, які використовуються в ході роботи вебресурсу, наприклад якщо в роботі сайту передбачена реєстрація користувача, то є необхідність в захисті отриманих даних. Звісно на деяких сайтах не зберігається інформація яка має певну цінність, наприклад у випадку зі звичайним сайтом-візиткою вся інформація представлена на самому сайті в відкритому доступі, на сайтах подібного типу не потребується забезпечення безпеки інформації, оскільки немає потреби забезпечувати захист того, що і так перебуває в відкритому доступі, але якщо на сайті є форма реєстрації, то з’являється необхідність в захисті конфіденційної інформації користувачів, а сам рівень необхідного захисту залежить від рівня конфіденційних даних наданих користувачем.

Як зазначено вище, рівень захисту інформації залежить від самої інформації. Наприклад, якщо на сайті зберігаються тільки імена користувачів, то навіть у випадку порушення конфіденційності цих даних шкоди практично не

буде. Однак, якщо на сайті зберігаються паспортні дані користувачів або інформація про їхні доходи, то в випадку порушення конфіденційності цих даних власник сайту зазнає значних втрат за усіма напрямками. Для побудови оптимального захисту інформації на вебресурсах необхідно спочатку розділити всю наявну інформацію, яка зберігається на сайті, за рівнем пріоритетності, а потім побудувати захист відповідно визначеним пріоритетам.

Крім забезпечення безпеки інформації, що зберігається, необхідно забезпечити безпеку в каналах передачі даних, так наприклад у випадку з інтернет-магазином, який дозволяє оплатити покупку на сайті відразу після її замовлення, необхідно забезпечити захищений канал при вводі даних картки для оплати, та організувати захищений зв'язок з банком для оплати, оскільки при незахищеному зв’язку зростає шанс перехоплення даних, що у свою чергу призводить до втрати банківських даних користувача, а винним в цьому є власник сайту та його адміністратор, який не організував коректний рівень передачі даних відповідно до рівня їх цінності. Отже, крім зберігання даних на сайті та їх захисту необхідно прораховувати шляхи якими ці дані можуть бути відправлені та захистити їх на цих шляхах.

Звісно навіть при використанні найсучасніших засобів захисту інформації та найкращих спеціалістів для моніторингу ситуації рівень захищеності сайту ніколи не рівний 100 відсотків, тому в будь-якому випадку необхідно забезпечити мінімізацію збитків, наприклад організувати захищений канал для переправлення даних з сайту на локальний сервер, який не має доступу до мережі, в такому випадку всі дані будуть зберігатись на захищеному відокремленому сервері, і тоді в випадку коли зловмисник отримає доступ до сайту, він зможе отримати тільки ту інформацію, яка в даний момент циркулює на сайті, тоді як решта інформації буде захищена на сервері, такий спосіб, хоча і не підвищить сам рівень захисту інформації на сайті, але дозволить зменшити збитки в випадку провалу цього самого захисту.

З точки зору державного регулювання захисту даних існує нормативний документ НД ТЗІ 2.5-010-03 “Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу”, цей документ встановлює мінімальний необхідний рівень реалізації послуг забезпечення інформаційної безпеки в вебресурсах в мережі інтернет, за допомогою цього документу є можливим побудувати стандартизовану систему захисту інформації, цей документ є обов’язковим до дотримання для державних структур, але в випадку, коли ресурс не відноситься до державної власності, вимоги викладені в цьому нормативному документі можуть бути виконані, або не виконані, на власний розсуд власника ресурсу, або його адміністратора. Отже, цей документ є доволі корисним при необхідності забезпечити інформаційну безпеку вебресурсу, але водночас через дату релізу у 2003 році в деяких пунктах він може здаватись трохи застарілим.

В загальному, захист інформації та захист системи невіддільні одне від одного і пов’язані між собою. Також кожен з цих аспектів безпосередньо залежить від іншого. Наприклад, у випадку проблеми захисту інформації на сайті, немає потреби в захисті системи, оскільки зловмисник вже наніс достатню шкоду для сайту. У випадку проблеми захисту системи отримання доступу до інформації не буде проблемою взагалі, оскільки всі методики захисту інформації спрямовані від зовнішніх загроз, тоді як у випадку провалу системи захисту зловмисник входить в систему та стає загрозою зсередини, від якої методики захисту не можуть захиститись. Тому варто звертати увагу на обидва ці аспекти на однаковому рівні, та при організації повноцінного системного захисту тримати обидва ці аспекти в балансі.

## 2.2. Інструменти для аналізу рівня захищеності вебресурсів

При створені вебресурсів за допомогою систем управління вмістом, важливою частиною буде перевірка рівня захищеності отриманого на виході додатку. Ця перевірка може проходити двома способами:

- за допомогою автоматизованих засобів;
- вручну.

Оптимальним варіантом проведення аналізу рівня захищеності вебресурсу буде початкове дослідження рівня безпеки за допомогою автоматизованих засобів та подальше проведення аналізу вручну.

Оскільки існує дуже велика кількість різних методів атаки на вебресурси, то спеціалізовані програми для автоматизованої перевірки не можуть охопити весь спектр загроз. Тому для аналізу рівня захищеності вебресурсу бажано використовувати декілька подібних програм одночасно для перекривання проблемних зон та отримання максимальної інформації про недоліки захисту вебструктури.

Найбільш відомими засобами для перевірки вебресурсів є OpenVAS, OWASP Xenotix XSS Exploit Framework, Approof від Positive Technologies. Також існують онлайн-сервіси, для використання яких достатньо просто мати доступ до мережі. Такими засобами є SecurityHeaders.io, One button scan, SSL Server Test та CSP Evaluator. Далі розглянемо ці засоби більш детально, оскільки вони будуть використані для оцінки рівня захищеності сайтів, створених за допомогою систем керування вмістом для створення порівняльного аналізу [11].

### 2.2.1. Автоматизовані інструменти

#### OpenVAS

OpenVAS – це сканер розроблений компанією Greenbone Networks, був розроблений у 2009 році та досі займає високе місце на ринку засобів забезпечення інформаційної безпеки, в основному це пов’язано з його широким функціоналом та використанням публічної ліцензії GNU.

Сам сканер є частиною сімейства "Greenbone Security Manager" (GSM), що дозволяє використовувати його разом з іншими модулями сімейства, та створювати дійсно надійний інструмент захисту безпеки інформації.

Завдяки відкритому вихідному коду системи та активній спільноті OpenVAS є одним з лідерів на ринку сканерів вразливостей, основними його можливостями є:

- неавтентифіковане тестування;
- автентифіковане тестування;
- різні високорівневі та низькорівневі Інтернет та промислові протоколи;
- налаштування продуктивності для широкомасштабного сканування;
- потужну внутрішню мову програмування для реалізації будь-якого типу тесту на вразливість [13].

## OWASP Xenotix XSS Exploit Framework

XSS атака це один з видів атаки типу “Впровадження коду”, її суть закладається в тому, що в сторінку, яку видає система, впроваджують шкідливий код, а потім цей код потім виконується на комп’ютері користувача, коли він відкриє дану сторінку.

Основною специфікою таких атак є непередбачуваність, шкідливий код може бути використаний для безлічі різних цілей, та дуже важко захистити свій ресурс від всіх таких можливостей, також шкідливий код може бути впроваджений в систему не тільки через вразливість вебсервера, але й через вразливість на комп’ютері користувача [12].

OWASP Xenotix XSS Exploit Framework це система для виявлення XSS вразливостей в вебресурсах, ця система використовує унікальний сканер Triple Browser Engine, який складається з трьох модулів, це Trident, WebKit та Gecko. Завдяки своєму вбудованому сканеру, модулю для збору інформації та багатьом модулям використання XSS загроз, ця система є дуже корисною при виконанні тестування на проникнення та створення концепції захисту ресурсу [14].

## Approof

Перевіряє конфігурацію вебресурсів, проводить сканування та виявляє шкідливий код, незахищені дані та вразливі компоненти [15].

- Знаходження вразливостей в сторонніх бібліотеках, CMS та фреймворках.
- Перевіряє конфігурацію вебресурсу.
- Виявлення незахищених чутливих даних(Метадані репозиторіїв, ключі шифрування).
- Виявлення шкідливого коду.

**SecurityHeaders.io**

Це служба, яка аналізуватиме заголовки відповідей HTTP інших сайтів, але також існує система оцінок щодо результатів. Заголовки відповідей HTTP, які аналізує цей сайт, забезпечують величезний рівень захисту, і важливо, щоб сайти їх розгортали та проводили перевірку рівня їх захисту. Основною задачею цієї служби є надання простого механізму оцінки заголовків відповідей та додаткову інформацію про те, як розгорнути відсутні заголовки, робота цього сайту повинна активізувати використання заголовків на основі безпеки в Інтернеті.

Цей сайт є дуже простий у використанні, оскільки для його роботи необхідно просто ввести в відповідне поле адресу сайту, а решта процесів пройде автоматично, після виконання сканування ви отримаєте оцінку безпеки вашого ресурсу з точки зору заголовків, ви можете опублікувати результат або приховати його натиснувши на відповідний прапорець [16].

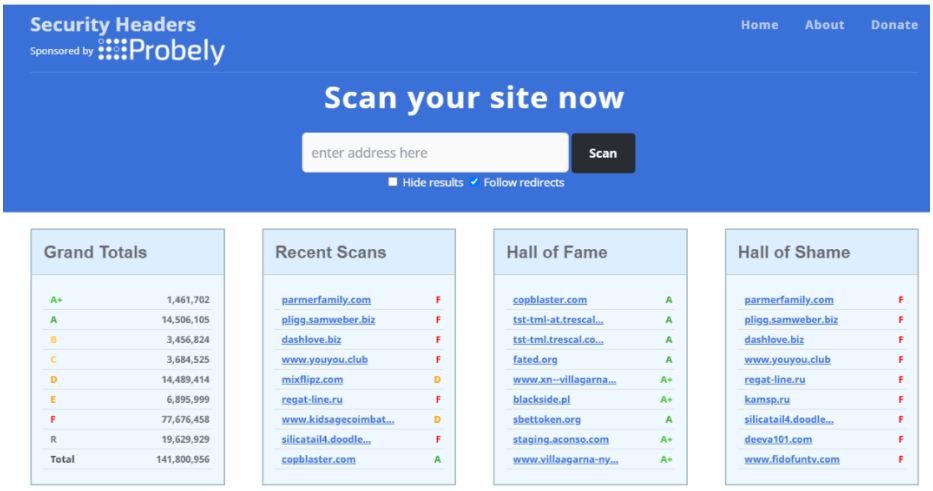


Рисунок 2.1. – Інтерфейс SecurityHeaders.io

**One button scan**

Сканує на наявність вразливостей компоненти ресурсу: DNS, HTTP-заголовки, SSL, чутливі дані, використовувані сервіси.

Сам процес використання сервісу є дуже простим, вам достатньо вставити адресу сайту в відповідне вікно, та натиснути кнопку Scan! Після цього пройде процес сканування та ви отримаєте інформацію щодо вашого сайту, а саме :

- Перевірка DNS на запити AXFR.
- Перевірка DNS на атаки посилення.
- Чутливі файли.
- Перевірка захисних заголовків HTTP.
- Тестування SSL.
- Перевірка daemon memcache.
- Перевірка daemon MongoDB.
- Перевірка daemon Redis.
- Перевірка FTP на наявність анонімного входу.
- Збір інформації через пошукові системи.
- Перевірка XSS через URI запит.
- Перевірка зворотного проксі-сервера.
- Перевірка XSS через заголовок HOST [17].

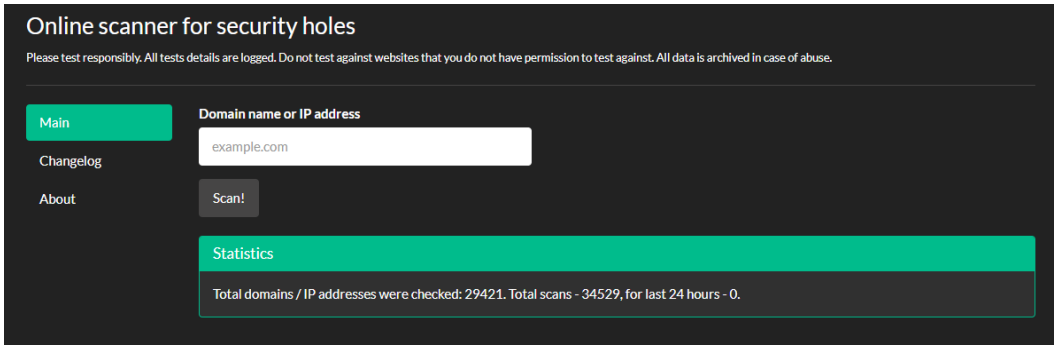


Рисунок 2.2. – Інтерфейс One button scan

## SSL Server Test

Цей безкоштовний онлайн-сервіс проводить глибокий аналіз конфігурації будь-якого вебсервера SSL у загальнодоступному Інтернеті. Зверніть увагу, що інформація, яка подається на даний сайт, використовується лише для надання послуги проведення аналізу конфігурації та не використовується в інших цілях [18].

Користування даним сервісом, як і його інтерфейс, дуже схожий на ресурс SecurityHeaders.io.

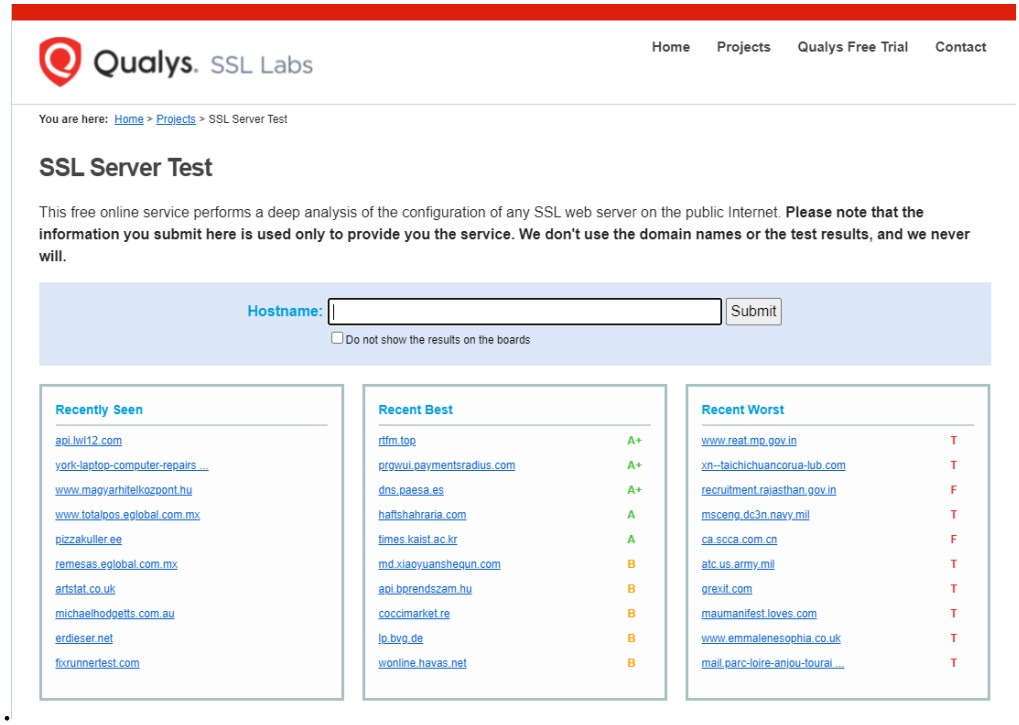


Рисунок 2.3. –Інтерфейс SSL Server Test

## CSP Evaluator

CSP Evaluator дозволяє розробникам та експертам з безпеки перевіряти, чи Політика безпеки вмісту (CSP) служить сильним пом'якшувачем проти атак сценаріїв між сайтами. Це допомагає в процесі перегляду політик CSP, що, як правило, є ручним завданням, і допомагає виявити тонкі обходи CSP, які підривають цінність політики. Перевірки CSP Evaluator базуються на масштабному дослідженні й спрямовані на те, щоб допомогти розробникам зміцнити свою CSP та поліпшити безпеку своїх програм [19].

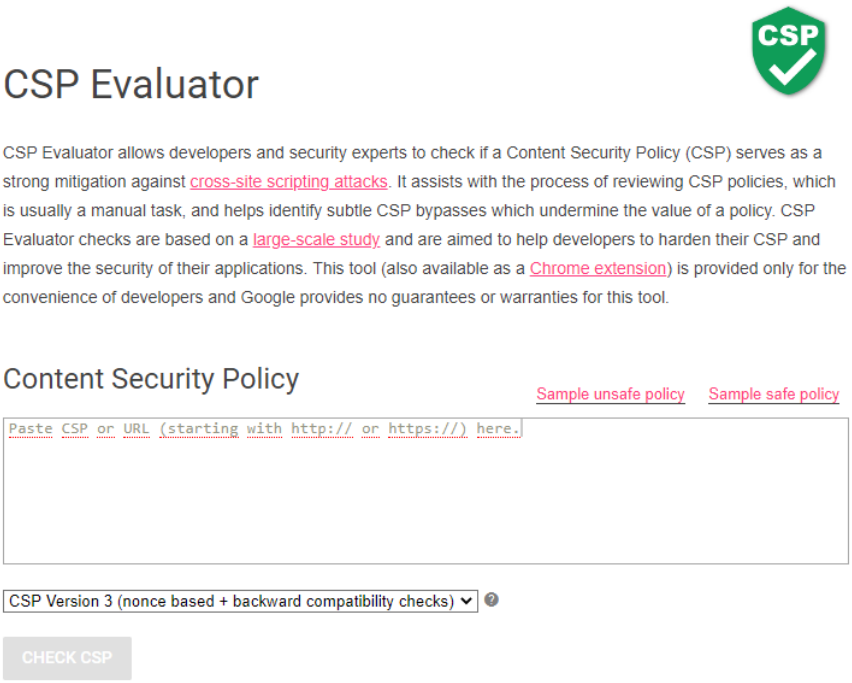


Рисунок 2.4. – Інтерфейс CSP Evaluator

# 3. ПОРІВНЯЛЬНИЙ АНАЛІЗ СИСТЕМ КЕРУВАННЯ ВМІСТОМ

Для того, щоб об’єктивно порівняти обрані CMS, було вирішено окремо розглядати їх з точки зору різних аспектів та присвоювати кожній системі оцінку порівнюючи їх одна з одною, та в результаті отримати таблицю з наведеними в ній загальними оцінками. За результатами таблиці будуть зроблені висновки щодо доцільності використання CMS залежно від потреб користувача.

У якості шкали оцінювання була обрана 5-бальна шкала, оскільки в якості об’єктів дослідження використовуються лише 4 CMS, то 5-бальної шкали буде цілком достатньо для об’єктивного дослідження.

Основна увага під час проведення дослідження буде акцентуватися на рівні безпеки, який забезпечують дані системи. Зокрема будуть розглянуті самі системи та додаткові модулі, використання яких може підвищити рівень безпеки ресурсу.

Також в ході дослідження буде проведений аналіз обраних систем з точки зору простоти використання системи, доступності додаткових модулів та рівня обслуговування CMS.

Отже, результатом проведеного аналізу буде таблиця з внесеними в неї оцінками відповідних CMS та їх обґрунтування, а також висновки зроблені виходячи з цієї таблиці.

## 3.1. Простота використання системи

В першу чергу розглянемо лідера на ринку CMS – WordPress. Щоб установити дану систему та безпосередньо перейти до її використання знадобиться 5 хвилин (в разі наявного встановленого вебсервера) та трохи більше часу в випадку його відсутності. В ході виконання даної використовувався вебсервер XAMMP, та було витрачено 15 хвилин на його встановлення разом з налаштуванням, процес встановлення є автоматизованим та не потребує практично ніяких зусиль від користувача, трохи складніше є налаштувати

віртуальний хост на локальному вебсервері, але в загальному для виконання цієї задачі достатньо лише слідувати інструкціям. Сам процес установки CMS WordPress є дуже простим, достатньо завантажити архів з офіційного сайту та розпакувати його в папку з вашим віртуальним хостом на вебсервері, після цього в браузері ввести назву хоста та пройти коротку процедуру входу в систему WordPress. Після входу в систему, ви отримуєте доступ до її функціоналу, дана система є дуже дружньою по відношенню до новачків та простою в освоєнні, а завдяки локалізації, взагалі дуже важко заплутатись в ній. Як тільки користувач заходить в систему, вона відразу пропонує йому рекомендовані варіанти дій, а також вказує посилання на елементи функціоналу які можуть бути корисними.

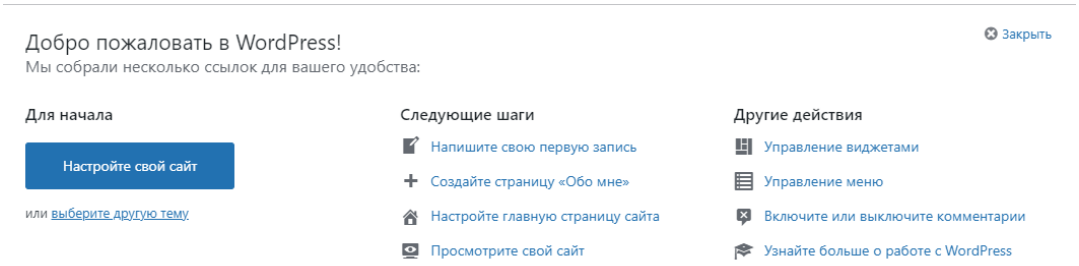


Рисунок 3.1 – Інтерфейс WordPress

Основний функціонал даної системи керування вмістом винесений в окреме меню.

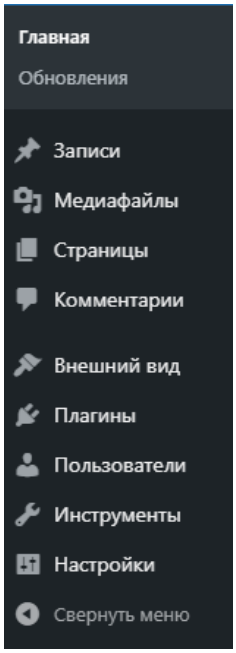


Рисунок 3.2 – Меню WordPress

Звісно для створення професійних сайтів базового інструментарію буде замало, але завдяки своєму відкритому коду та широкій спільноті на WordPress існує багато різноманітних плагінів, які дуже сильно розширюють функціонал системи та є доволі простими в використанні.

Наступною розглянутою системою буде Wix, ця система є ідеальною в плані простоти взаємодії з нею. Вище було сказано, що процес установки WordPress є дуже простим та практично не потребує зусиль, в випадку з Wix цього процесу немає взагалі, для роботи з Wix вам достатньо просто відкрити браузер, ввести в пошук Wix.com, пройти коротку процедуру реєстрації та приступати до роботи над створенням сайту. Взаємодія користувача з системою, є дуже простою, наприклад в самому початку користувач може пройти невелике опитування та отримати готовий шаблон відповідно до тематики та особливостей ресурсу, який він збирався створити, в такому випадку для отримання готового продукту йому залишається просто ввести деякі зміни в наданий йому системою шаблон, також плюсом до простоти використання даної платформи є зручний довідник та служба підтримки, в довіднику ви можете знайти інформацію про всі

доступні елементи функціоналу та їх використання, ну і звісно платформа є локалізованою.

Тепер розглянемо CMS Joomla, дана система в плані установки схожа на WordPress відмінність лише в тому, що для комфортної роботи з нею, окрім основного ядра, яке завантажується з офіційного сайту, необхідно також встановити мовний пакет. Сам процес установки не є важким, він є можливо трохи довшим ніж процес установки WordPress, через мовний пакет, але також варто зауважити, що встановлення мовного пакету не зовсім є частиною установки, так-як можна провести установку англійською мовою та потім вже з інтерфейсу системи встановити мовний пакет. Після установки ви потрапляєте на адміністративну панель Joomla, сама панель є відносно зручною в використанні, на верхній частині наводяться основні пункти при виборі, яких ви можете працювати з обраним функціоналом, також на кожній з обраних сторінок буде відображатись клавіша “Довідка”, яка дасть коротку характеристику сторінки на якій ви знаходитесь. Зручність даної системи для початківців є доволі сумнівною, не є можливим сказати, що вона дуже складна та заплутана, але все-таки деякі з присутніх елементів є надлишковими та зайвими для нового користувача, а для комфортної роботи з самим інтерфейсом необхідно звикнути.

Остання буде представлена CMS Drupal, серед всіх розглянутих в даній роботі систем, вона є найменш відомою, але навіть так на ній працює багато сайтів в мережі, за останніми даними, ця система використовується на 562,655 сайтах. Початок установки даної системи був дуже простим, є можливим сказати, що навіть простішим ніж з Joomla та WordPress, все що необхідно було зробити, це завантажити архів з офіційного сайту та розпакувати його всередину папки з підключеним мною раніше віртуальним хостом, після цієї процедури та введення в браузері назви хоста, користувач опиняється на сторінці установочного процесу Drupal. Процес установки є зрозумілим та розписаним покроково, але на етапі перевірки вимог часто виникає проблема з відключеним розширенням php_db.

Для вирішенння цієї проблеми необхідно зайти в файли конфігурації php та розкоментувати стрічки з даним розширенням, але в моєму випадку це не спрацювало та для вирішення проблеми довелось шукати іншу версію даного розширення (було обране php_gd2.dll), завантажувати його з мережі та додавати в папку php/etx, після чого в файл конфігурації додавати рядок extension=php_gd2.dll, лише після цих дій та перезапуску вебсервера мені вдалось продовжити установочний процес CMS Drupal. Сам процес проходить доволі швидко, все що потрібно від користувача це вводити необхідні дані (наприклад, назву підключеної бази даних, ім'я та пароль користувача). Наступним кроком система встановлення переходить на вкладку встановлення перекладів та працює в автоматичному режимі, користувачеві залишається лише чекати результату. Після завершення процесу користувач вводить дані сайту, який збирається розробляти, та закінчує процес установки. Після того, як система встановлена користувач потрапляє до панелі адміністратора, інтерфейс панелі є доволі заплутаним та складним для розуміння, якщо порівнювати з рештою розглянутих в даній роботі систем, основна складність в великій кількості різних налаштувань та функцій, які не є необхідними для початківця, або рядового користувача. Ймовірніше за все складність інтерфейсу даної системи і є причиною його відносно низького рівня популярності на ринку CMS відносно решти представлених в даній роботі систем.

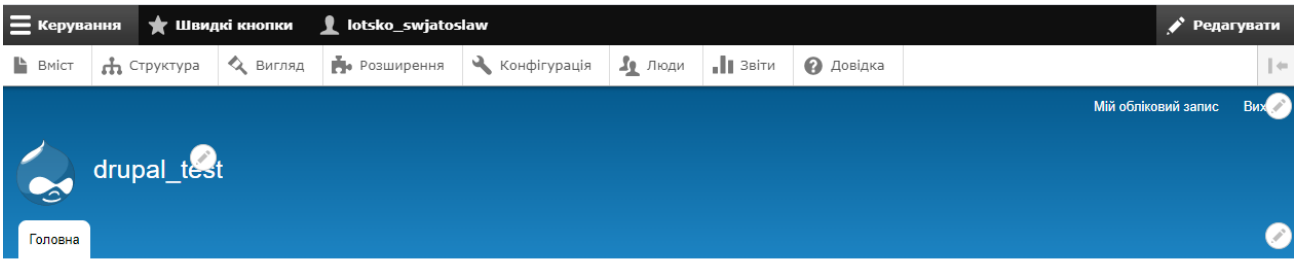


Рисунок 3.3 – Інтерфейс Drupal

В завершення даного розділу буде проведена оцінка обраних систем по визначеній 5-бальній шкалі. Виходячи з аргументації визначеної в даному розділі

об’єктивно буде присвоїти CMS Wix – 5 балів, за відсутність необхідності встановлення та простий інтуїтивно зрозумілий інтерфейс типу drag-and-drop. WordPress отримує 4 за простий процес встановлення та просте лінійне меню. Joomla отримує 3 оскільки її встановлення настільки ж просте як і в WordPress, але інтерфейс є більш складним та може викликати певні затруднення в користувача. Drupal отримує 2, оскільки його інтерфейс є доволі складним відносно решти представлених систем та потребує часу на вивчення перед початком роботи з даною системою.

В результаті ми отримуємо за критерієм простоти використання:

WordPress – 4;

Wix – 5;

Joomla – 3;

Drupal – 2.

### 3.2. Доступність додаткових модулів

Зазвичай основного функціоналу систем недостатньо для роботи з великими та різноплановими проектами, а розширення основного функціоналу так, щоб його вистачало для всіх потреб є занадто нераціонально та складно для CMS, тому для вирішення цієї проблеми використовують додаткові модулі. Завдяки модулям користувач може встановити та використовувати тільки ті модулі, які дійсно необхідні для роботи конкретно його сайту.

Розглянемо систему WordPress, якщо брати до уваги конкретно модулі та їх доступність, то ця система є безперечним лідером, оскільки WordPress це система з відкритим вихідним кодом, а також завдяки її високому рівню популярності, існує безліч модулів. Ці модулі можуть виконувати різні задачі починаючи від аналітичних задач по збору інформації, щодо ресурсу, та закінчуючи повнозначними доповненнями в функціоналі сайту.

Всі існуючі на даний момент модулі діляться на дві категорії: платні та безкоштовні. Платні модулі, як зрозуміло з самої назви необхідно купити перед використанням, безкоштовні ж є вільно доступними. Також існують модулі доступ до яких є частково вільним, тобто користувач отримує доступ до основної частини функціоналу, але для отримання доступу до повного функціоналу необхідно заплатити. В якомусь сенсі система роботи таких модулів є схожою на систему роботи більшості безкоштовних CMS, які надають безкоштовний доступ до ядра, але для отримання інструментів з розширеним функціоналом(модулів) необхідно заплатити.

Щоб додати модуль на WordPress та використовувати його, достатньо перейти в меню “Плагіни” та обрати вкладку “Додати нові”, а потім з понад 50000 доступних модулів обрати необхідний конкретно під свою потребу. Перед завантаженням модуля, рекомендовано перевірити сумісність з поточною версією WordPress, а також звернути увагу на частоту оновлень модуля та рівень його підтримки, це дозволить запобігти непотрібних проблем в роботі ресурсу.

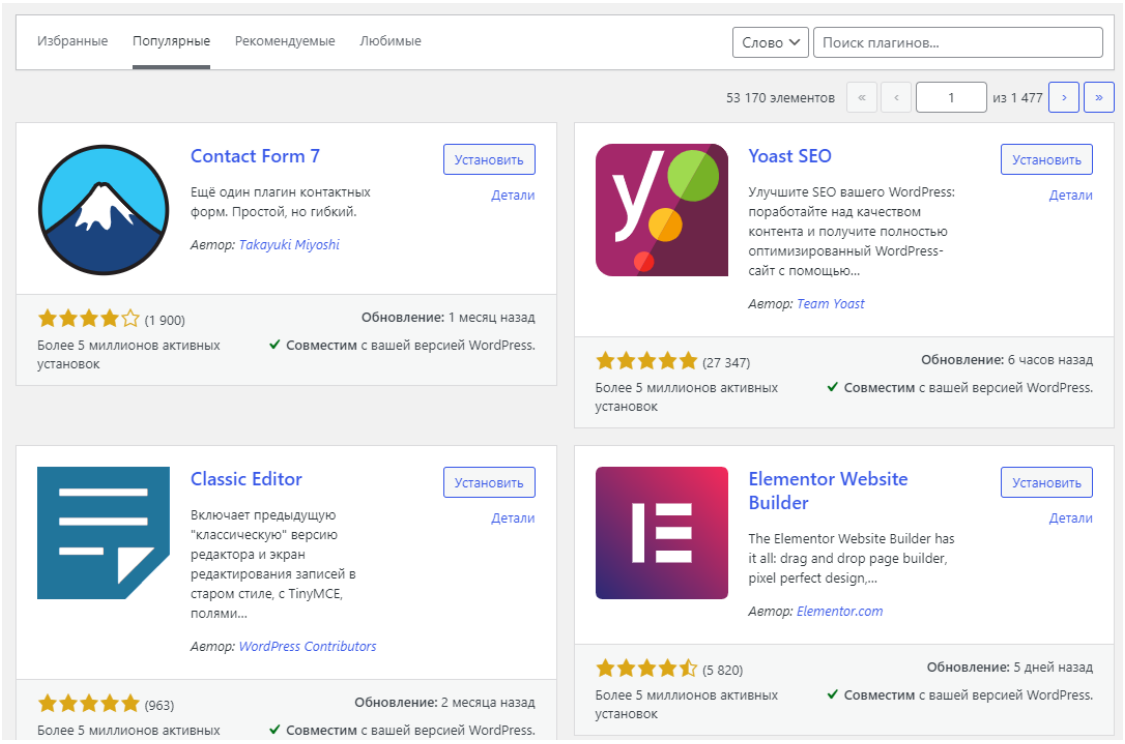


Рисунок 3.4 – Меню плагінів в WordPress

Наступною розглянутою системою буде Wix, система додаткових модулів в даній системі відрізняється від такої системи в WordPress. На відміну від WordPress, дана система є більш закритою в плані додаткових модулів, всі модулі доступні до використання на Wix можна найти на сторінці Wix App Market, на ній представлені різнопланові додатки розроблені, як розробниками Wix, так і сторонніми розробниками. В порівнянні з іншими розглянутими системами на Wix існує не так багато додатків, всього їх більше 100, що є доволі великою кількістю, але якщо порівнювати з іншими системами це доволі мало. Невелика кількість модулів на даній системі компенсується їх якістю, оскільки додатки представлені на Wix App Market є або створені командою розробників самої системи, або вони проходять детальний процес розгляду та рецензування перед тим, як їх додають на Wix App Market. Загалом будь-який додаток представлений в Wix App Market буде корисним інструментом для користувача, варто зауважити, що серед всіх додатків від розробників платформи більшість є безкоштовними, що в свою чергу теж є значною перевагою для використання даної системи.

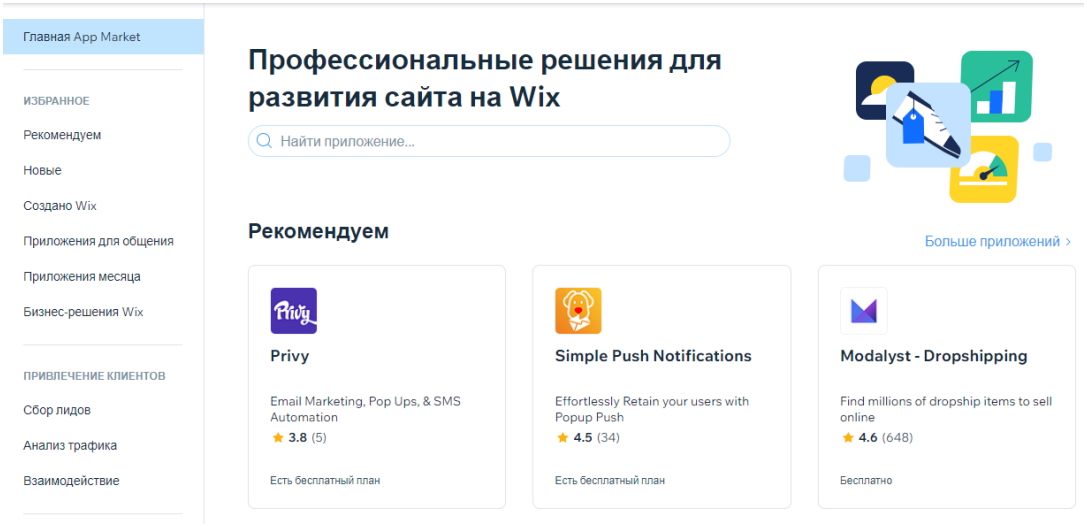


Рисунок 3.5 – Wix App Market

Окрім модулів системи Wix буде доцільно розглянути різні тарифні плани, хоча система і є безкоштовною, вона пропонує різні тарифні плани, які надають

ряд переваг для користувачів. З основних переваг даних планів слід зазначити можливість підключення власного домена, підвищення рівня продуктивності ресурсу, а також простір для зберігання даних представлений платформою.

| | VIP | Безлимитный | Базовый | Подключить домен |
|---|---|---|---|---|
| | Приоритетная поддержка | Для предпринимателей | Для личных целей | Только домен<br>Этот план показывает рекламу Wix |
| | US$ 12 25 /мес.<br>~~US$24.50~~ | US$ 6 25 /мес.<br>~~US$12.50~~ | US$ 8 50 /мес. | US$ 4 50 /мес. |
| | Выбрать | Выбрать | Выбрать | Выбрать |
| Персональный домен | ✓ | ✓ | ✓ | ✓ |
| Бесплатный домен на 1 год | ✓ | ✓ | ✓ | – |
| Сайт без рекламы Wix | ✓ | ✓ | ✓ | – |
| Бесплатный SSL-сертификат | ✓ | ✓ | ✓ | ✓ |
| Производительность | Безлимитный | Безлимитный | 2 ГБ | 1 ГБ |
| Пространство для хранения | 35 ГБ | 10 ГБ | 3 ГБ | 500 МБ |
| Видеоархив | 5 часов | 1 час | 30 минут | – |
| 75 $ на рекламу | ✓ | ✓ | ✓ | – |
| Приложение Site Booster Бесплатно на 1 год | ✓ | ✓ | – | – |
| Приложение Visitor Analytics Бесплатно на 1 год | ✓ | ✓ | – | – |
| Профессиональный логотип | ✓ | – | – | – |
| Файлы логотипа для соцсетей | ✓ | – | – | – |
| Служба поддержки | Приоритетная поддержка | Поддержка 24/7 | Поддержка 24/7 | Поддержка 24/7 |

Рисунок 3.6 – Тарифні плани Wix.com

Тепер розглянемо Joomla. З точки зору додаткових модулів вона є дуже схожою на WordPress. Завдяки своїй популярності та відкритому вхідному коду, дана система є вільною для всіх користувачів, в її каталозі можна знайти багато плагінів, які можуть бути корисними для будь-якого проекту, на даний момент каталог всіх розширень даної системи становить більше 5 тисяч різноманітних додатків. Ці додатки розсортовані по категоріям та підкатегоріям, тому є дуже зручно шукати саме те, що необхідно користувачеві. Крім функціональних плагінів Joomla також пропонує мовні пакети, які дозволяють локалізувати вашу систему на одну з 75 наявних мов, що значно підвищує рівень комфорту при

роботі з даною системою. Також варто зауважити наявність чорного списку плагінів, в який вносять неблагонадійні додатки, при роботі з якими у користувачів можуть виникнути проблеми, більш детально про цей список буде розказано в пункті “Рівень обслуговування CMS”.

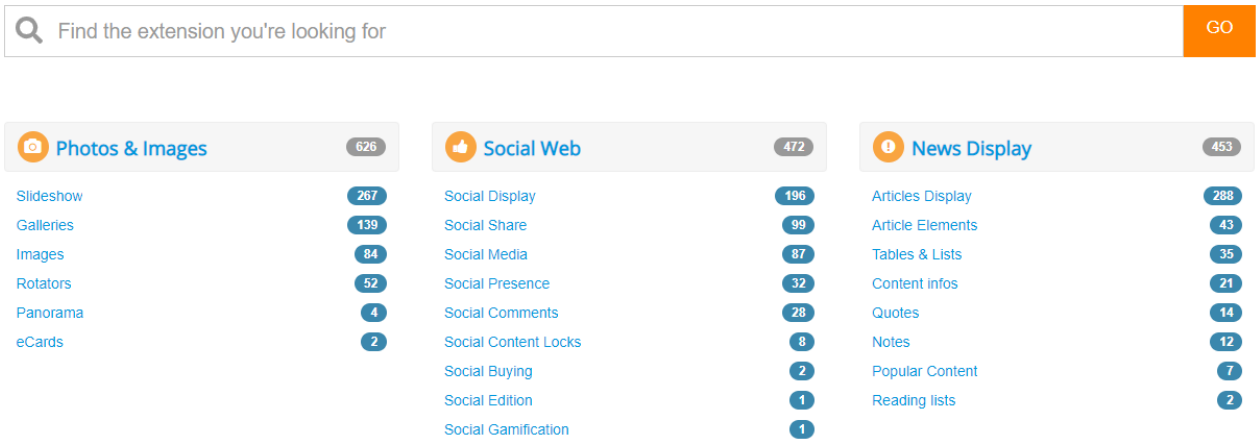


Рисунок 3.7 – Каталог плагінів Joomla

Розширення на систему Drupal теж в основному створюються спільнотою користувачів, вони поділяються на модулі представлені відразу з системою та модулі, які потребують окремої установки. Модулі представлені відразу з системою є встановленні за замовчуванням після інсталяції CMS Drupal, користувач відразу може їх використовувати, потрібно лише зайти на сторінку розширень та ввімкнути необхідне. Також варто враховувати сумісність встановлених розширень використовуючи дану систему, так-як декілька несумісних модулів працюючих одночасно призведуть до проблем в роботі ресурсу.

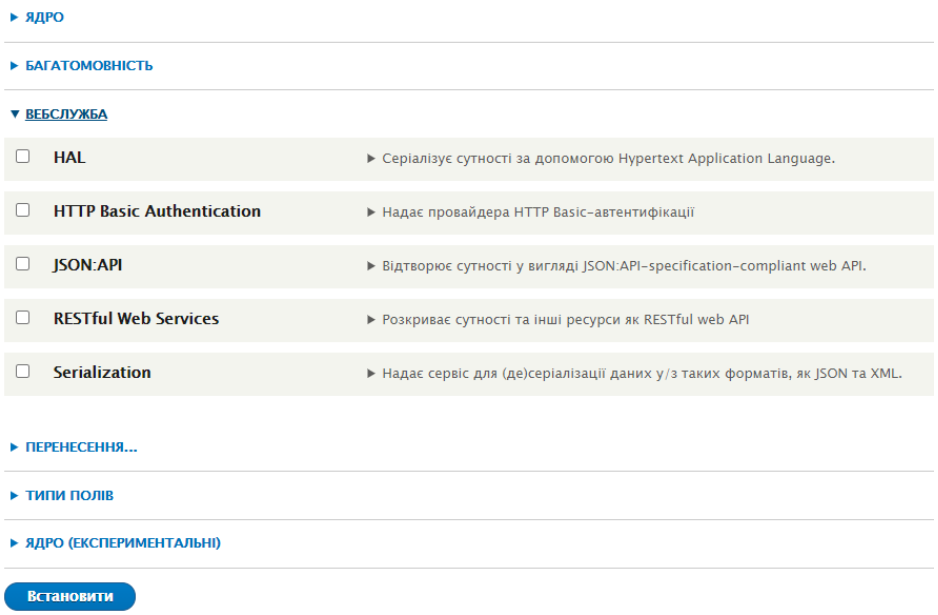


Рисунок 3.8 – Інтерфейс з вбудованими модулями Drupal

Інший тип модулів на дану систему необхідно встановлювати вручну. Для цього користувачу потрібно зайти на офіційний сайт CMS Drupal та завантажити необхідний йому модуль, а потім встановити його з системи, використовуючи опцію “Встановити модуль”.

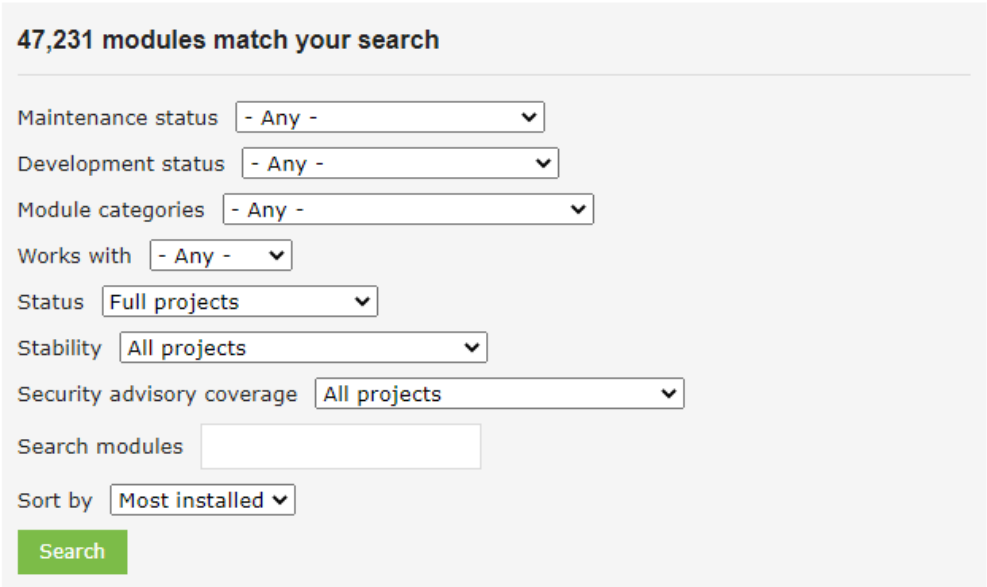


Рисунок 3.9 – Сторінка з модулями на офіційному сайті Drupal

Отже, виходячи з наведеної вище інформації, щодо доступності розширень на системи, що розглядаються, є можливим провести оцінювання та надати системам з відкритим вихідним кодом по 5 балів, оскільки для них доступно багато різноманітних модулів на будь-яку потребу, а в випадку, якщо користувач не знайде необхідний йому модуль, він може сам створити його. Для системи Wix ситуація інша, хоч і існують додатки, але їх набагато менше в порівнянні з модулями інших представлених в роботі систем, з іншого боку багато представлених даною платформою додатків розробляються та підтримуються надійними розробниками, що в свою чергу рятує систему від багатьох проблем, тому лише завдяки якості представлених модулів, Wix буде оцінений в 3 бали, через малі можливості для розширення функціоналу за допомогою модулів.

Отже відповідно критерію доступність додаткових модулів:

WordPress – 5;

Wix – 3;

Joomla – 5;

Drupal – 5;

### 3.3. Рівень обслуговування CMS

Під рівнем обслуговування системи мається на увазі рівень підтримки поточних версій в технічному плані, а також рівень підтримки користувачів в разі проблем з роботою системи.

Система WordPress була випущена на світ у 2003 році, та з того часу активно росла, зараз вона займає вершину на ринку CMS, насамперед завдяки постійним оновленням та покращенням. На цей час актуальною версією системи є версія 5.7, а якщо бути точним, то версія 5.7.2. Сама гілка оновлень 5.7 була випущена 9 березня 2021 року, з того часу пройшло не так багато часу, а вже було випущено 2 версії даної гілки, теперішня версія 5.7.2. була випущена 23 травня 2021 року. Виходячи з цих факторів можна сказати, що розробники турбуються

про свій продукт та постійно додають щось нове, або модифікують старі елементи. На офіційному сайті даної системи також можна знайти довідник, який дає початкові знання для роботи з системою, документацію в якій також є багато корисної інформації, але поданої в доволі важкому для сприйняття стані, і що найголовніше форуми, на яких кожен користувач, має можливість почитати статті від більш досвідчених людей та отримати від них відповіді на свої питання. В загальному цю систему можна розглянути, як систему створену людьми для людей, вона розвивається завдяки спільним зусиллям розробників та рядових користувачів, більш досвідчені користувачі допомагають новачкам, таким чином навіть за відсутності ліній технічної підтримки люди з спільноти WordPress завжди знають де знайти вирішення своїх проблем.

Наступним кроком розглянемо Wix. В плані оновлень та нових версій дана система значно відстає від решти, основна суть оновлень Wix полягає у введені нових технологій в роботу системи або вирішення технічних проблем з системою. Оновлення на даній системі проходять в автоматичному порядку, тому користувачі завжди працюють на актуальних версіях системи та їм не потрібно турбуватись, щодо ручного оновлення системи. Для додавання нового функціоналу платформи в 2012 році був створений Wix App Store, про який розповідалось в попередньому пункті, а в подальшому при необхідності додання функціоналу створювались додатки, в свою чергу підтримкою додатків займаються їх розробники, що є доволі добре, оскільки на Wix App Store можна знайти додатки від таких надійних розробників як Яндекс, Google, LiveChat, Shopify, Instagram, а це означає надійність підтримки їх додатків, за стабільну роботу самого ядра ж відповідають самі розробники Wix.

Також Wix як платформа пропонує доступ до центру підтримки, який дозволяє знайти інформацію практично по будь-якому питанню, крім того платформа при використанні преміум тарифу дає пріоритетний доступ до служби підтримки, яка дозволяє в оперативному темпі вирішити будь-яке запитання. Та

звісно, завдяки тому, що Wix є одним з найвідоміших конструкторів сайтів, в випадку виникнення проблем, які ви не можете вирішити за допомогою вказаних вище засобів, ви маєте можливість звернутись до безлічі форумів в мережі, деякі з яких створені спільнотою Wix.com.

Надалі розглянемо Joomla в контексті рівня обслуговування системи. Свіжа версія даної системи 3.9.27 була випущена 24.05.2021. В загальному плані підтримка системи проходить стабільно, практично кожного місяця виходить пакет оновлень, які допомагають вирішувати найнагальніші проблеми в роботі системі. З точки зору плагінів ситуація така сама, як і в WordPress, оскільки код є відкритим, то більша частина плагінів перебуває в вільному доступі та їх підтримка залежить лише від бажання розробника, в будь-який момент він може припинити підтримку плагіна або передати його в руки іншим людям, що в свою чергу може нести загрозу як для безпеки ресурсу, так і для його стабільності, але на відміну від WordPress у Joomla існують чорні списки плагінів, використання яких може принести шкоду для роботи вашого ресурсу, ці чорні списки можна найти на офіційному сайті системи, звісно в них зазначені не всі плагіни, які можуть чинити загрозу, а лише самі відомі з них, тому користувачам системи необхідно бути обережними при роботі з неперевіреними плагінами в будь-якому випадку. У Joomla немає офіційної технічної підтримки, тому підтримка проходить по принципу форумів, тобто користувачі обмінюються досвідом та допомагають одне одному на спеціалізованих форумах присвячених конкретно даній системі, на відміну від того ж WordPress, на офіційному сайті Joomla є розділення на різні рівні форумів, наприклад окремо є форуми для користувачів де вони діляться своїми проблемами та питають порад у інших, а окремо є форум для розробників на якому обговорюють проблеми при розробці нових елементів для системи. Також окрім форумів на сайті можна знайти багато документації та довідок, щодо функціональних деталей системи.

В загальному можна дійти висновку, що спільнота Joomla є схожа на спільноту WordPress, але якщо розібратись більш детально, стає зрозуміло, що існує безліч дрібних відмінностей, які хоч і є дрібними, але їх кількість в даному випадку відіграє основну роль, тому при більш детальному порівнянні стає зрозуміло, що в цих систем можуть бути спільні основні парадигми, та їх деталі роблять їх унікальними.

Тепер перейдемо до розгляду CMS Drupal з точки зору підтримки та оновлень, на даний момент, актуальною версією є версія Drupal 9.1.9., розрахунок версій в даній системі працює так само, як в WordPress, дана версія була випущена 26 травня в 2021 році, попередня до неї (Drupal 9.1.8.) вийшла 5 травня, виходячи з цього можна зробити висновок, про достатній рівень підтримки зі сторони розробників системи, так-як оновлення виходять доволі часто, а проблеми в безпеці або функціонуванні системи виправляються дуже оперативно.

Наступним кроком є розгляд спільноти Drupal, на відміну від WordPress та Joomla, спільнота Drupal є набагато меншою та більш спеціалізованою, тоді як на інших представлених CMS високий процент новачків Drupal зазвичай працюють люди з досвідом, оскільки сама система є доволі складною для новачка. Також на офіційному сайті, ви можете отримати доступ до довідок та форумів з цікавою інформацією, щодо роботи системи та актуальних новин про неї.

Отже виходячи з наведених вище факторів можна сказати, що найбільшу підтримку системи від розробників надає Wix.com, оскільки він реалізує все те, що є наявним в інших системах, не потребує ручного оновлення, а також має спеціалізовану технічну підтримку, тому дана система отримує 5 балів. Joomla та WordPress оцінюються в 4 бали, оскільки їх система підтримки є гіршою ніж у Wix, але завдяки значній спільноті, яка бере на себе частину турбот про підтримку системи та користувачів, вона є доволі корисною. Drupal отримує 3,

оскільки система підтримки реалізована на рівні Joomla WordPress, але популярність системи в рази гірше.

За критерієм рівень обслуговування CMS:

WordPress – 4;

Wix – 5;

Joomla – 4;

Drupal – 3;

## 3.4. Безпека

В цьому розділі будуть розглянуті основні вразливості безпеки, які можуть загрожувати коректній та надійній роботі сайтів, написаних з використанням CMS систем. Для об’єктивних оцінок, був проведений аналіз багатьох вебресурсів за допомогою інструментів, наведених у п. 2.2 даної роботи, та за результатами цих досліджень, були виявлені деякі проблеми безпеки, які певною мірою будуть стосуватись всіх представлених в даній роботі систем. Також будуть розглянуті загрози, які стосуються конкретних систем та в кінці, будуть зроблені висновки, щодо загального рівня безпеки різних CMS та поради щодо його підвищення.

Спочатку розглянемо приклад роботи з інструментарієм, використаним для дослідження безпеки ресурсів. Для дослідження було обрано університетський вебресурс cybersecurity.sumdu.edu.ua.

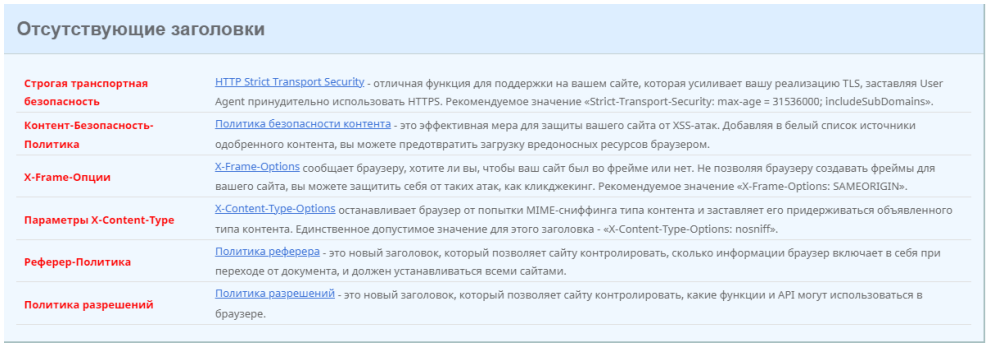


Рисунок 3.10 – Результати дослідження ресурсу cybersecurity.sumdu.edu.ua за допомогою Securityheaders

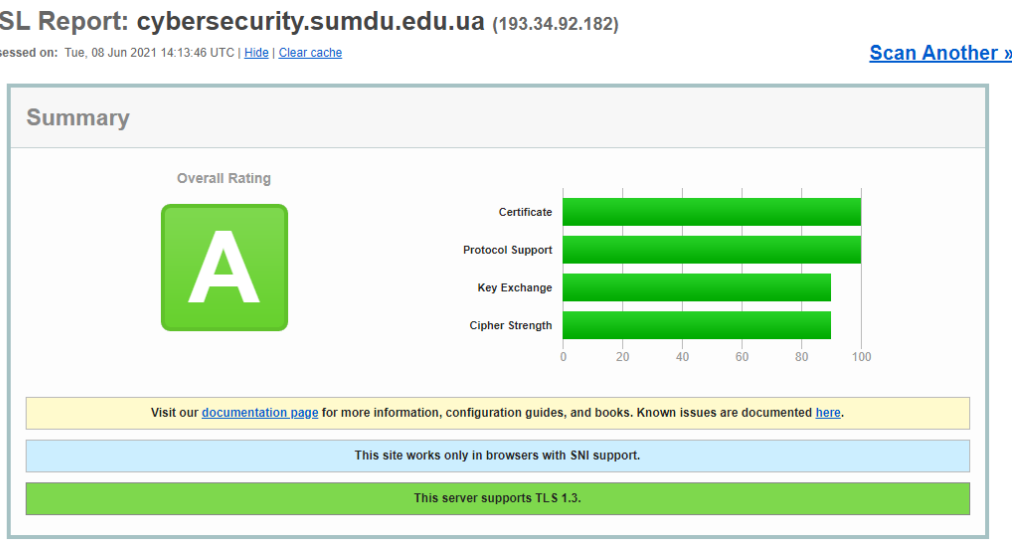


Рисунок 3.11 – Результати дослідження ресурсу cybersecurity.sumdu.edu.ua за допомогою Ssllabs

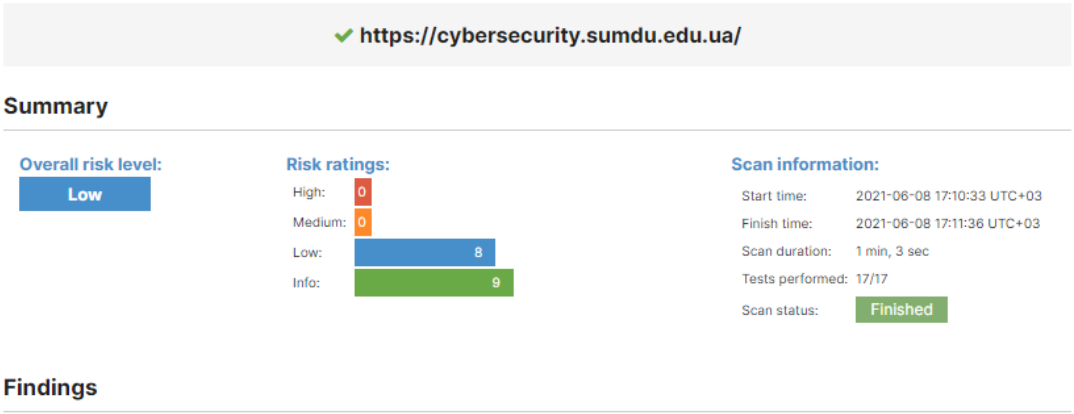


Рисунок 3.12 – Результати дослідження ресурсу cybersecurity.sumdu.edu.ua за допомогою Pentest-tools

Аналіз був проведений з використання ресурсу спеціальності “Кібербезпека”, даний ресурс працює з використанням останньої версії WordPress. У процесі сканування було визначено проблеми з заголовками безпеки, а саме відсутність багатьох з них. В загальному при скануванні даного ресурсу не було виявлено критичних уразливостей, що означає високий рівень організації безпеки ресурсу.

Наступним був перевірений ресурс it.sumdu.edu.ua.

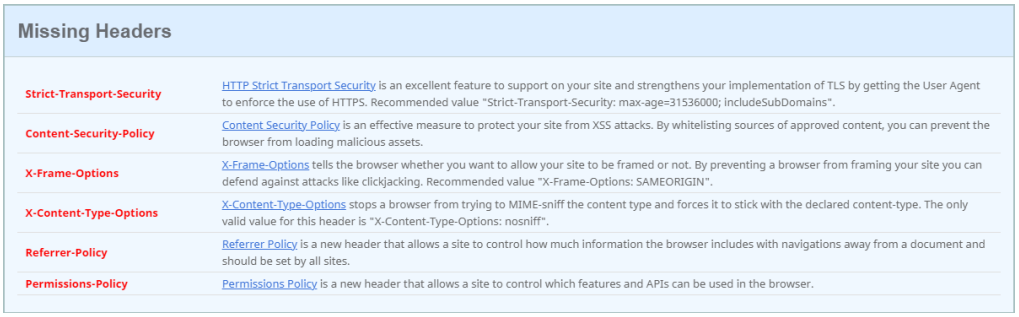


Рисунок 3.13 – Результати дослідження ресурсу it.sumdu.edu.ua за допомогою Securityheaders

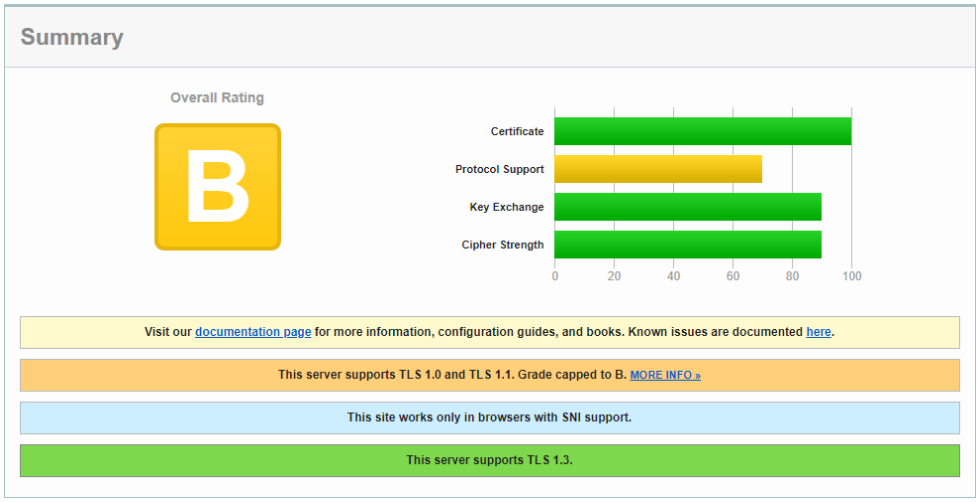


Рисунок 3.14 – Результати дослідження ресурсу it.sumdu.edu.ua за допомогою Ssllabs

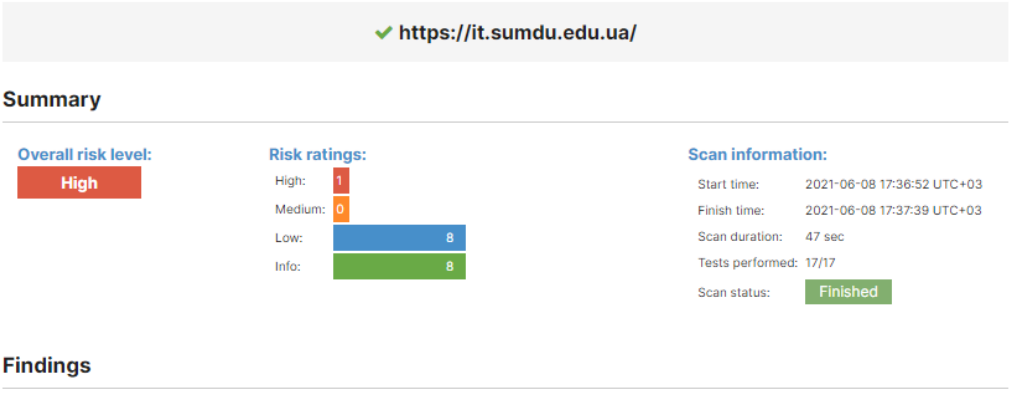


Рисунок 3.15 – Результати дослідження ресурсу it.sumdu.edu.ua за допомогою Pentest-tools

Даний ресурс в плані безпеки, значно відстає від попереднього, відсутності заголовків та проблеми підтримки деяких захисних протоколів, даний ресурс працює на версій WordPress 5.6.4., яка в свою чергу є застарілою та має багато уразливостей. Ці уразливості системи були виявлені за допомогою безкоштовного сканера, що в свою чергу означає низький рівень захисту ресурсу та високий шанс його злому. Загрози високого рівня виявлені в ході сканування виникли через відсутність вчасних оновлень системи, а саме:

1) CVE-2021-29447 (використовуючи проблему синтаксичного аналізу XML файлу існує можливість отримати доступ до файлів внутрішньої бібліотеки ресурсу, дана проблема існує для версій WordPress до 5.7.1.);

2) CVE-2018-19296 (вразливість PHPMailer для атак з вводом об’єкта, актуальна для версій до 6.0.6.);

3) CVE-2020-36326(дозволяє вводити об’єкти через Phar Deserialization з використанням PHPMailer).

Оскільки в даній роботі 3 системи з розглянутих 4 систем мають відкритий вихідний код, то буде варто розглянути загрози, які він становить для безпеки вебресурсів. Системи з відкритим вихідним кодом в останні роки набувають, все більшої популярності, оскільки такі системи масштабуються та розширюються навіть без втручання розробників, а лише завдяки зусиллям рядових користувачів. З іншого боку, такий підхід має свої недоліки, більшість з яких пов’язані з безпекою ресурсів. Наприклад, при використанні продуктів та систем з відкритим вихідним кодом існує можливість аналізу цього самого коду усіма користувачами, в тому числі й зловмисниками. Також при використанні таких ресурсів необхідно приділяти більше уваги адмініструванню, оновленням та додатковим модулям. Оскільки одним з найнадійніших засобів підвищення рівня безпеки є своєчасні оперативні оновлення всіх елементів системи та підтримка їх в робочому стані, особливу увагу слід звернути на безкоштовні модулі, оскільки через вразливості в них зловмисник має можливість отримати доступ до ресурсу

в цілому, а вразливості модулів в свою чергу є дуже поширеними явищами, та виникати вони можуть як випадково через помилки розробників, так і навмисно, для цілей проникнення в ресурси, які використовують даний модуль.

Також існують загрози, на які рядові користувачі не можуть вплинути практично ніяк, наприклад, як було сказано в 2 розділі даної роботи, захист ресурсу поділяється на захист інформації та захист сервера, і тоді як з захистом інформації користувач може працювати сам, та підвищувати його рівень завдяки використанню певних плагінів, додатків та налаштувань безпеки, то з серверною частиною працює його хостинг, на якому був розміщений сайт, тому все, що може зробити користувач, це на стадії підбору хостинга обрати оптимальний та надійний варіант, а потім слідкувати за рівнем наданих ним послуг.

Отже, при використанні систем з відкритим кодом, ви отримуєте практично безмежний простір для розвитку вашого проекту, але водночас підвищуєте рівень ризиків з точки зору безпеки, тому при використанні таких систем необхідно приділяти більше уваги своєчасним оновленням системи та її модулів, а також пам’ятати, що ніяка система не може бути захищеною на всі 100 відсотків та наперед мінімізувати можливу шкоду в випадку злому.

Тепер розглянемо проблеми безпеки виявленні при роботі з системою WordPress. Багато уразливостей виявлених на даній системі направлені на отримання несанкціонованого доступу до ресурсу. Так, наприклад, в стандартній версії WordPress користувач не має обмеження на кількість спроб введення паролю, тому загрозою для системи є навіть елементарний метод грубої сили, але ця загроза не становить значної небезпеки, оскільки існує безліч способів від неї захиститись, починаючи від банального ускладнення пароля та закінчуючи двофакторною аутентифікацією, або ж установкою спеціалізованого плагіна, який надає тільки сталу кількість спроб при вводі пароля, а в випадку невдачі блокує доступ до системи для даної адреси. Також оскільки одною з основних уразливостей системи є панель адміністратора, а саме можливості отримання

несанкціонованого доступу до неї, то необхідно мінімізувати можливість отримання такого доступу. Наприклад за допомогою файлу конфігурації є можливість обмежити доступ до теки адміністратора, змінивши цей файл можна надати доступ до теки тільки за своєю IP-адресою, тобто зайти в адміністративну панель можна буде тільки з вашої адреси, доступ туди для інших адрес буде заблокований. Отримати доступ до панелі адміністратора в WordPress можна багатьма різними способами, однак, не можна сказати, що система сама по собі не є захищеною, оскільки при використанні правильно підібраного набору плагінів та грамотно налаштованої системи, шанси на використання цих загроз різко падають. Під цими загрозами маються на увазі типові загрози такі як XSS (Cross Site Scripting) та SQL–ін'єкції. Також до загроз відноситься відкритість даних ресурсу, навіть ті дані, які на вашу думку не мають ніякого відношення до безпеки ресурсу насправді можуть бути використані проти вас, наприклад елементарний номер версії WordPress на якій працює сайт дає зловмиснику важливу інформацію. Не існує цілком безпечної системи, оскільки з кожною версією системи, розробники закривають одні дірки в безпеці, але водночас відкривають інші, тому знаючи версію на якій працює ваш сайт, зловмисник зазвичай знає і вразливості цієї версії, та може їх використовувати, до цієї ж категорії відносяться і права перегляду, наприклад якщо доступ до перегляду каталогу ресурсу є вільним, то це дає зловмисникам інформацію щодо структуру ресурсу, що у свою чергу буде використано проти вас.

Отже, сама система WordPress для початківця не надає суттєвого рівня захисту, щоб організувати достатню систему захисту та налаштувати саму CMS, необхідно мати певний рівень навичок та розбиратись в системі на більш просунутому рівні, але водночас завдяки своєму широкому профілю та наявності багатьох різноманітних плагінів, користувач який має ці навички, зможе організувати відносно високий рівень захисту.

Наступною розглянутою системою в плані захищеності буде Wix.com, дана система відрізняється від решти представлених. Взагалі цю систему не можна віднести до систем з відкритим вихідним кодом, хоча деякі частини системи можна знайти в відкритому доступі, але більша частина є закритою та доступною лише для розробників. В плані безпеки система Wix є дуже простою для рядового користувача, оскільки на відміну від решти систем, розглянутих в даній роботі, вона не потребує практично ніяких налаштувань та додаткових модулів для перекриття проблем безпеки на ресурсі. Всі потреби щодо забезпечення безпеки отриманого ресурсу, у випадку з системою Wix, задовольняються розробниками CMS, а вони у свою чергу дуже відповідально відносяться до цього питання. Система є сертифікованою відповідно вимогам міжнародних стандартів ISO 27001 та ISO 27018, також наявний сертифікат SSL, який забезпечує надійну передачу даних через протокол https, крім того завдяки TLS1.2 забезпечується конфіденційність всіх транзакцій на ресурсах, які працюють під системою Wix. Також варто зауважити, що Wix надає користувачам власний хостинг, обслуговуванням якого займаються кваліфіковані спеціалісти, тобто користувачу нема потреби шукати надійний хостинг для публікації сайту, після створення сайту він може буквально в декілька кліків передати всю роботу, пов’язану з серверною частиною ресурсу на Wix. Також важливим є фактор того, що система Wix є централізованою, а це означає автоматичні оновлення всього, що стосується безпеки вашого сайту, нема потреби оновлювати систему вручну, таким чином ваш сайт завжди буде працювати на найновішій версії системи. Крім того, команда спеціалістів постійно поводить моніторинг та виявляє всі підозрілі діяльності на ресурсах своєї платформи.

Виходячи з наведеної вище інформації, можемо контстатувати, що безпека ресурсів створених за допомогою Wix є доволі високою, але все-таки слід не забувати, що ніякий захист не є ідеальним. Наприклад, зловмисник за допомогою

соціальної інженерії отримує доступ до облікового засобу користувача на Wix та разом з тим отримує доступ до всіх ресурсів підв’язаних до нього.

Наступною на черзі системою є Joomla, розглядаючи її з точки зору безпеки, вона має такі самі вразливості, як і всі системи з відкритим кодом. Зараз будуть розглянути проблеми безпеки притаманні конкретно для системи Joomla. Сама по собі система є слабо захищеною, але завдяки багатьом просунутим плагінам для організації захисту дану систему можна назвати однією з найзахищеніших систем серед інших систем з відкритим вихідним кодом, доказом цьому є статистичні дані, щодо порушення безпеки на ресурсах, що працюють використовуючи Joomla. Joomla займає друге місце у рейтингу використання CMS після WordPress. Така ситуація також впливає на рейтинги серед CMS з точки зору заражених ресурсів, у такому рейтингу Joomla теж займає друге місце, але зі значним відривом, в той час, коли серед всіх заражених сайтів на WordPress працює близько 80%, на Joomla такий відсоток становить лише 4-5% [7]. Дані показники обумовлюються меншою популярністю системи, а також наявністю просунутих Joomla плагінів для забезпечення безпеки ресурсів. Серед таких плагінів найвідомішими та найбільш надійними є RSFirewall, JomDefender та AdminExile. За допомогою цих плагінів можливо налаштувати та захистити найвразливішу частину системи (AdminExile), комплексно захистити систему від найпоширеніших загроз (RSFirewall) та організувати оптимізацію захисту від потенційних загроз (JomDefender).

Загальні парадигми організації захисту ресурсів побудованих за використанням CMS Joomla практично такі самі, як і в випадку WordPress, але існують деякі відмінності, які полягають в інструментарії та плагінах які використовуються. Таким чином, при використанні Joomla ці плагіни є більш розвинуті та частіше обновлюються, через це дана система має більш високий рівень захисту у порівнянні з іншими системами з відкритим кодом представлених в даній роботі.

Тепер розглянемо систему Drupal з точки зору безпеки, з першого погляду дана система здається доволі надійною , через низький процент зламаних сайтів, але в даному випадку основною причиною малого відсотку є лише відносно низький рівень популярності системи серед користувачів, а також те, що люди, які використовують дану систему в більшості своїй мають певний досвід та можуть провести коректні налаштування безпеки ресурсу, сукупність цих факторів приводить до думки про високий рівень захисту системи. Насправді ж система має доволі багато уразливостей, більша частина з яких висвітлюється на спеціалізованих форумах самими користувачами системи. Ці вразливості зберігаються з версії у версію, хоча розробники прикладають багато сил з кожним оновленням для видалення цих уразливостей, або мінімізації шансу їх використання . Наприклад на системі Drupal протягом багатьох версій актуальна проблема хешування паролів, проблема полягає в використанні застарілого механізму зі сталою кількістю ітерацій, що в свою чергу може привести до проблем безпеки, також в даній системі існував користувач з понаднормовими правами, доступ до якого можливо отримати навіть з рядового користувача(якщо є певні права), унікальність цього користувача в можливості надавати та віднімати будь-які права та дозволи у всіх членів системи. Проблема в тому, що явно такий користувач навіть не існує, тому контролювати доступ до нього дуже проблемно. Крім цих проблем існує, ще дуже багато проблем безпеки даної системи, але особливістю цих проблем є відносно складна реалізація. Тобто можна сказати, що безпека Drupal побудована при компетентних спеціалістах в якості адміністраторів та складності реалізації можливих загроз, в сукупності з відносно низьким рівнем популярності даної системи на виході Drupal можна назвати цілком захищеним.

Захистом системи займається спеціальна команда Drupal Security Team [20]. Вони в стані онлайн проводять моніторинг системи та найпопулярніших плагінів, виявляють підозрілу діяльність або загрози та

оперативно виправляють їх, також дана команда публікує бюлетені з знайденими вразливостями на офіційному сайті.

Також для забезпечення безпеки сайтів при використанні системи Drupal варто пам’ятати, про можливість несумісності плагінів та загальні проблеми безпеки викликані використанням ненадійних плагінів. В загальному дана версія Drupal 9 є набагато більш захищеною в порівнянні з версіями 7 та 8, проблеми безпеки яких були одним з основних їх недоліків, але незважаючи на затрачені розробниками зусилля, щодо максимізації рівня безпеки, деякі недоліки існують досі, та щоб максимально захистити свій ресурс необхідно уважно віднестись до налаштувань безпеки та модулів, що використовуються.

Виходячи з отриманих в ході досліджень даних, ми можемо розділити всі системи з точки зору безпеки, найвищий рівень безпеки у Wix оскільки захистом даної системи займаються спеціалісти, а також ядро є закритим, що значно підвищує рівень безпеки, враховуючи також всі технології, що використовуються та сертифікати, Wix отримує 5 балів. Наступною розглянутою системою є Joomla, завдяки доступним та функціональним модулям для забезпечення безпеки та відносно зручним налаштуванням системи вона отримує 4 бали. WordPress та Drupal отримують по 3 бали, оскільки WordPress є дуже поширеним на ринку, а його модулі захисту по рівню якості сильно здають позиції аналогічним модулям модулям Joomla. Система Drupal є доволі складною, але в той же час вразливою для атак, крім того через механізм невідповідності модулів вноситься додаткова складність у роботу з системою та підвищуються шанси виникнення загроз доступності ресурсу.

В плані безпеки системи поділяються як:

WordPress – 3;

Wix – 5;

Joomla – 4;

Drupal – 3;

# ВИСНОВКИ

Складемо таблицю, відповідно наданим раніше оцінками та зробимо висновки, щодо функціональних властивостей систем відповідно до потреб користувачів.

| | Простота | Доступність модулів | Підтримка | Безпека |
|---|---|---|---|---|
| WordPress | 4 | 5 | 4 | 3 |
| Wix | 5 | 3 | 5 | 5 |
| Joomla | 3 | 5 | 4 | 4 |
| Drupal | 2 | 5 | 3 | 3 |

Таблиця 1 – Порівняльний аналіз

Також є необхідним вивести усереднених оцінок для всіх наведених систем, для цього ми використаємо метод експертної оцінки. Спочатку виведемо вагу для кожного критерія, основною умовою є те, щоб сума всіх виведених значень була рівна одиниці. Найважливішим критерієм оцінювання в даній роботі є безпека, тому його вага буде найвищою та рівною 0,4. Оскільки основною характеристикою даної роботи є безпека, то наступним за рівнем важливості значенням буде підтримка, оскільки відсутність оновлень або проблеми з підтримкою системи можуть призвести (та зазвичай приводять) до проблем з рівнем захищеності. Для даного критерію обрана оцінка 0,3. Наступним критерієм в плані впливу на рівень захисту системи є доступність модулів, оскільки відсутність модулів для захисту інформації або проблеми з ними надають відносно високий вплив на безпеку системи та створених за її допомогою ресурсів, але в той же час рівень ризику значно нижчий ніж в попередніх критеріїв, завдяки наявній можливості нівелювання даного ризику, тому призначене значення рівне 0,23. Останнім критерієм є простота

використання. Цей критерій чинить найменший вплив на рівень безпеки ресурсу, але навіть так, його вплив не є нульовим, оскільки простота взаємодії з системою робить простішим процес організації її захисту, тому призначене значення не рівне 0, а рівне 0.07.

Тепер маючи вагу критеріїв та їх оцінки виведені за результатами аналізу, побудуємо нову таблицю, в якій будуть розраховані усереднені значення.

Усереднені значення розраховуються за формулою:

$v_{pr} * n_{pr} + v_d * n_d + v_{pid} * n_{pid} + v_b * n_b$, де

v – вага критерія

n – оцінка критерія

| | Простота | Доступність модулів | Підтримка | Безпека | Усереднені значення |
|---|---|---|---|---|---|
| Вага критеріїв | 0.07 | 0.23 | 0.3 | 0.4 | |
| WordPress | 4 | 5 | 4 | 3 | 3.83 |
| Wix | 5 | 3 | 5 | 5 | 4.54 |
| Joomla | 3 | 5 | 4 | 4 | 4.16 |
| Drupal | 2 | 5 | 3 | 3 | 3.39 |

Таблиця 2 – Розрахунок усереднених значень

Виходячи з отриманих в ході дослідження даних, можна прийти до таких висновків, щодо оптимальності використання кожної з наведених систем:

- Якщо користувачу необхідний сервіс з максимально простою структурою та з мінімальними вимогами до навичок користувача, він може звернутись до Wix, обслуговування ресурсу візьме на себе сама платформа.

Все що необхідне від користувача, це створити ресурс відповідно своїм потребам та наповнювати його контентом в зручній формі.

- Якщо користувачу необхідно провести знайомство з системами керування вмістом або для створення невеликих сайтів без чітких вимог до функціоналу та високого рівня безпеки, то ідеальним варіантом буде WordPress. Він дозволить користувачу почати вивчення систем такого типу з нуля, а безліч матеріалів в мережі та широка спільнота дозволить вирішити будь-які проблеми, які можуть виникнути.
- Якщо потреби такі самі, як в попередньому пункті, але є певні більш чіткі вимоги до функціоналу та безпеки, то Joomla ідеальний варіант, який завдяки плагінам безпеки допоможе організувати коректний рівень безпеки, а завдяки простоті буде зручним для початківців.
- У випадку необхідності створення великого ресурсу при наявності потужного серверу, відмінним варіантом буде Drupal, але для його використання необхідно спочатку отримати певний досвід та навички, він є доволі складним, але при професійному використанні незамінимим для великих проєктів.

Отже, кожна з розглянутих систем має певну сферу діяльності, в якій вона себе добре показує, але лише при кваліфікованому користувачеві вона може розкрити весь свій потенціал, тому навіть при високих навичках роботи з CMS важливо обирати систему відповідно поставленій задачі.

# СПИСОК ЛІТЕРАТУРИ

1. CMS // Wikipedia. [Electronic resource]. – Access mode : https://ru.wikipedia.org/wiki/CMS.

2. Wix.com // Wikipedia. [Electronic resource]. – Access mode : https://ru.wikipedia.org/wiki/Wix.com

3. Joomla.ru [Electronic resource]. – Access mode : https://joomla.ru/

4. Drupal.org [Electronic resource]. – Access mode : https://www.drupal.org/

5. Что такое WordPress. Обзор самой популярной CMS // Hostinger.ru URL: https://www.hostinger.ru/rukovodstva/chto-takoe-wordpress-obzor-populjarnoj-cms/

6. Анализ подходов к повышению безопасности интернет-сайтов, развернутых с использованием систем наполнения контентом. // Cyberlinka [Electronic resource]. – Access mode : https://cyberleninka.ru/article/n/analiz-podhodov-k-povysheniyu-bezopasnosti-internet-saytov-razvernutyh-s-ispolzovaniem-sistem-napolneniya-kontentom

7. 90% взломанных в 2018 CMS составляют сайты на WordPress. // Anti-malware [Electronic resource]. – Access mode : https://www.anti-malware.ru/news/2019-03-05-1447/29063

8. Исследование безопасности сайтов на различных CMS [Electronic resource] // Офіційний сайт проєкту Habr. – Access mode : https://habr.com/ru/company/ruward/blog/209950/

9. Threatpost [Electronic resource]. – Access mode :https://threatpost.com/

10. Security Week 40: уязвимости в CMS Drupal и не только// [Electronic resource] // Офіційний сайт проєкту Habr. – Access mode : https://habr.com/ru/company/kaspersky/blog/427351/

11. Echo.lviv [Electronic resource]. – Access mode : https://echo.lviv.ua/dev/6231

12. Awesomeopensource [Electronic resource]. – Access mode : https://awesomeopensource.com/project/ajinabraham/OWASP-Xenotix-XSS-Exploit-Framework

13. Openvas [Electronic resource]. – Access mode : https://www.openvas.org/

14. Owasp [Electronic resource]. – Access mode : https://owasp.org/projects/

15. Approof.ptsecurity [Electronic resource]. – Access mode : https://approof.ptsecurity.ru/

16. Securityheaders [Electronic resource]. – Access mode : https://securityheaders.com/

17. Sergeybe.love: [Electronic resource]. – Access mode : https://sergeybe.love/one-button-scan/about/

18. Ssllabs [Electronic resource]. – Access mode : https://www.ssllabs.com/ssltest/

19. Csp-evaluator [Electronic resource]. – Access mode : https://csp-evaluator.withgoogle.com/

20. Drupal-security-team [Electronic resource]. – Access mode : https://www.drupal.org/drupal-security-team