**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

***Спеціальність: 123 «Комп'ютерна інженерія»***

***Освітня програма: «Комп'ютерна графіка і Web-дизайн»***

***Група: 4КГ-05***

# Дипломний проект

**здобувача освіти денної форми навчання**
**КГ.05.29.000.ДП**

***Тюлькіної Віри Олексіївни***

**м. Одеса**
**2022 р.**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Комп'ютерна графіка і Web-дизайн»**

Група: **4КГ-05**

# ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

## Розробка алгоритму проведення аудиту Web-сайтів за допомогою інструментів тестування на проникнення

Проектний матеріал складається з пояснювальної записки на _____ сторінках та графічного (презентаційного) матеріалу на 11 аркушах (слайдах).

Дипломник _____ (Тюлькіна В.О.)

Керівник _____ (Шевцов Ю.С.)

**Консультанти:**

з економічної частини _____ (Копайгородська Т.Г. )

з охорони праці_____ ( Чорновол Н.І. )

з дотримання вимог ЄСКД _____ ( Петрашова В.І.)

старший консультант _____ ( Скорнякова О.В. )

**До захисту допущений**

Голова циклової комісії _____ ( Скорнякова О.В. )

Завідувач відділення _____ (Суліма Ю.Ю.)

Захист «____»____ _____ 2022 р. Протокол ДКК №_____

Оцінка ДКК _____

Секретар ДКК _____

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

Відділення **комп'ютерних систем** Комісія **КТ та ПІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Комп'ютерна графіка і Web-дизайн»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР_____

_____

"_____"_____2022 р.

# З А В Д А Н Н Я

## на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти **Тюлькіній Вірі Олексіївні**

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи): **Розробка алгоритму проведення аудиту Web-сайтів за допомогою інструментів тестування на проникнення**

затверджена наказом по коледжу від "**30**" **січня** 202**1** р. № **306-А2-ОД**

2. Термін здачі закінченого проекту (роботи) _____

3. Вихідні данні до проекту (роботи): **Usability аудит. Файл robots.txt. Kali Linux. Тестування на проникнення - білий ящик. Тестування на проникнення – чорний ящик. Тестування на проникнення - сірий ящик. Damn Vulnerable Web Application (DVWA). Утиліта Nmap. Визначення реальності IP сайту за допомогою Cloudflare. Пошук субдоменів з Amass. JavaScript.**

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

**ВСТУП.**

1. **ТЕХНОЛОГІЧНИЙ РОЗДІЛ**
2. **ЕКОНОМІЧНИЙ РОЗДІЛ**
3. **ОХОРОНА ПРАЦІ**
4. **ВИСНОВКИ**

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

**Створення презентаційного матеріалу, кількість слайдів не менше 10**

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

| Розділ | Консультант | Підпис, дата | |
|---|---|---|---|
| | | Завдання видав | Завдання прийняв |
| Вступ, 1 | Шевцов Ю.С. | | |
| 2 | Копайгородська Т.Г. | | |
| 3 | Чорновол Н.І. | | |
| Нормоконтроль | Петрашова В.І. | | |
| | | | |

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

| № з/р | Назва етапів дипломного проекту (роботи) | Термін виконання етапів дипломного проекту (роботи) | Відмітка про виконання |
|---|---|---|---|
| 1. | Огляд літератури. Огляд існуючих рішень. | | |
| 2. | Формування кінцевого завдання на розробку. Вступна частина дипломного проекту. | | |
| 3. | Технологічний розділ. Комплексний аудит сайту. | | |
| 4. | Технологічний розділ. Тестування на проникнення. | | |
| 5. | Технологічний розділ. Розробка алгоритму проведення аудиту Web-сайтів. | | |
| 6. | Економічний розділ. | | |
| 7. | Виконання розділу «Охорона праці». | | |
| 8. | Підготовка доповіді та презентації для захисту | | |
| 9. | Підготовка до попереднього захисту, підготовка до захисту | | |
| 10. | Отримання рецензії, відповіді на зауваження рецензента | | |
| 11. | Захист роботи | | |

Дипломник _____
(підпис)

Керівник _____
(підпис)

| Формат | Зона | Поз. | Позначення | Назва | Кіл. | Примітка |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | Документація | | |
| | | | | | | |
| | | | КГ.05.29.000.ДП | Дипломний проект | | |
| | | | | | | |
| А4 | | | КГ.05.29.000.ДП. ПЗ | Пояснювальна записка | 1 | |
| | | | | | | |
| | | | | Презентація | 11 | |

| Ізм. | Арк. | № докум. | Підпис | Дата | КГ.05.29. 000.00 ДП ПЗ | | |
|---|---|---|---|---|---|---|---|
| Розробив | | Тюлькіна В.О. | | | Розробка алгоритму проведення аудиту Web-сайтів за допомогою інструментів тестування на проникнення | Літ. | Аркуш |
| Перевірив | | Шевцов Ю.С. | | | | Н Д П | |
| | | | | | | ВСП ОТФК ОНТУ | |
| Н. Контр. | | Петрашова В.І. | | | | | |
| Затверд. | | Скорнякова | | | | | |

# *АНОТАЦІЯ*

Метою даної роботи є розробка алгоритму проведення аудиту Web-сайтів за допомогою інструментів тестування на проникнення.

В даній випускній роботі молодшого спеціаліста розглянуто внутрішній і зовнішній аудит сайту, види тестування та типи випробувань на проникнення. Проведено дослідження вразливих середовищ для практики зі злому сайтів. Представлені елементи збору інформації: дослідження периметра, пошук чутливої інформації, початковий аналіз веб-програми. В рамках розробки алгоритму проведення аудиту Web-сайтів, були протестовані різноманітні сервіси сканування вразливостей веб-додатків: безкоштовний сканер уразливостей веб-сайтів під Windows із графічним інтерфейсом IronWASP, сканер веб-серверів Nikto, WPScan

**ЗМІСТ**

# ВСТУП

Кожен комерційний сайт, є ефективним інструментом для розвитку бізнесу. При грамотному вкладенні коштів у власний ресурс, доходність від нього можна порівняти з іншими видами підприємницької діяльності. Однак багато власників сайтів стикаються з типовою ситуацією, коли улюблений інтернет-ресурс працює нестабільно, потрапляє в немилість пошукових систем або відвідувачі оминають його.

Головна мета аудиту та всебічного аналізу – якісна оцінка поточного стану комерційного ресурсу. Виявлення помилок та недоліків, розробка заходів для покращення позицій ресурсу у пошуковій видачі, щодо збільшення трафіку та зростання конверсії. В даний час власники комерційних сайтів та веб-майстри можуть провести аудит самостійно, скористатися різними онлайн-сервісами або звернутися до послуг професіоналів. Аудит може бути вузько спрямованим або комплексним.

Конкуренція у світі вийшла на новий рівень. Раніше кібер-шпигунство було доступне тільки великим компаніям, то з розвитком технологій стало доступним малому та середньому бізнесу. В даному випадку йдеться про комерційні сайти компаній, інтернет-магазини, веб-ресурси, що приносять дохід. Тестування на проникнення сайту – комплексний підхід до пошуку не якісного коду ресурсу, виявлення вразливостей ПЗ сервера, завдяки яким можна атакувати та зламати веб-ресурс.

Ви не раз чули новини про те що зламаний сайт, та в мережу викладено облікові дані сотні тисяч користувачів. Що це означає для веб-сайту? Веб- ресурс отримав репутаційні збитки, компанія втратила довіру клієнтів. Адже цього могло й не статися, якби вчасно було проведено тест на проникнення, виявлено можливість злому та проведено заходи щодо виправлення вразливостей.

# РОЗДІЛ 1. КОМПЛЕКСНИЙ АУДИТ САЙТУ

Аудит сайту – це загальний аналіз ресурсу, який допомагає знайти технічні проблеми у його роботі, покращити характеристики сайту для пошукових систем та користувачів. Такий аудит дає можливість визначити причини, через які веб-ресурс не може вийти в топ пошукових систем, а також дозволяє заощадити значну частину фінансів, які йшли на неефективне просування.

Для того щоб робота ресурсу давала результат, він повинен бути привабливим як для користувачів, так і для пошукових систем. Скільки б посилань не було куплено, без якісного аудиту сайт не підніметься у топ позицій, а значить, залишиться непоміченим для більшості потенційних клієнтів. Аудит дозволяє:

• проаналізувати загальну роботу ресурсу та дати статистику;

• знайти помилки та причини їх появи;

• виключити всі неефективні витрати під час просування;

•отримати рекомендації щодо покращення юзабіліті, конверсії та продажу.

Весь аналіз можна розділити на дві складові, це внутрішній і зовнішній аудит сайту.

Внутрішній аналіз - процес, що займає приблизно 80% часу від усього аудиту. Він допомагає виявити всі помилки, недоліки при верстці, биті посилання та недоробки. Якісний внутрішній аналіз дозволить вирішити проблему з нестабільною відвідуваністю веб-ресурсу, відсутністю зворотного зв'язку від клієнтів, низькою конверсією.

Оскільки кожен проект є унікальним, під нього має бути розроблена своя стратегія просування сайту. Тому самостійний аналіз без урахування величезної кількості дрібних деталей може не мати сенсу. Найкращим варіантом буде звернутися до компанії, що займається seo-оптимізацією. Зазвичай фахівці

пропонують два варіанти аналізу: експрес-аудит або повний аудит інтернет-сайту.

У першому випадку веб-ресурс проходить лише поверхневу перевірку, де виявляються лише критичні помилки. До повноцінного аналізу обов'язково входять два види аудиту: технічний та пошуковий. Також існує маркетинговий аудит та аудит юзабіліті, проте їх наявність краще обговорити з фахівцями, оскільки не завжди ці два види включені до послуг.

Зовнішній аудит сайту - включає аналіз зовнішніх факторів ранжування:

• загальна видимість сайту у ПС;

• перевірка та подальша відмова від спамних донорів;

• аналіз анкор-листа веб-сайту для усунення спаму;

• аналіз приросту маси посилань;

• відповідність маси посилань тематиці сайту;

• аналіз маси посилань конкурентів.

Такий аудит в першу чергу проводиться для того, щоб сформувати правильну стратегію посилань, яка допоможе веб-ресурсу не потрапити під санкції пошукових систем або ж вийти з-під них. Також він проводиться з метою виходу сайту в топ за високочастотними, середньочастотними та низькочастотними запитами, що відповідно збільшує трафік та продажі.

Аудит може бути вузькоспрямованим або комплексним. Вузконаправлений аудит сайту – це швидкий та поверхневий аналіз, що дозволяє знайти найвидніші проблеми веб-ресурсу та визначити першочерговий напрямок для більш глибокого аналізу. Комплексний аудит містить:

1) Технічний аудит. Включає виявлення помилок на сайті, що впливають на просування і загальну працездатність веб-ресурсу. Сюди входить:

• склеювання основного дзеркала – головної версії веб-сторінки;

• швидкість завантаження сторінки (не повинна перевищувати трьох секунд);

• виявлення проблем з SSl-протоколом та правильне настроювання HTTPS;

• наявність та правильне відображення мобільної версії на різних пристроях;

• правильна індексація – аналіз індексації сайту та його доступність пошуковим роботам;

• наявність битих посилань;

• неправильні коди відповіді сервера;

• правильність встановлення лічильників веб-аналітики;

• перевірка URL-сторінок сайту.

2) Пошуковий аудит. Усі пошукові системи висувають певні вимоги до сайту. Їхнє невиконання заважає ресурсу просуватися вгору в позиціях пошукових систем. Якщо за результатом запиту аналізованого веб-ресурсу немає хоча б на перших трьох сторінках, це явна ознака помилок, які допоможе виправити пошуковий аудит. Він включає в себе:

• прорахунок кількості вихідних посилань зі сторінки;

• наявність дублюючих сторінок, які частково або повністю копіюють інші сторінки веб-ресурсу;

• аналіз Title, keywords, description, мета-тегів, robots.txt, sitemap для основних сторінок сайту;

• коректність заголовків тексту (h1-h6);

• вживання та щільність ключових слів;

• правильність та наявність перелінкування всередині сайту;

• наявність/створення мікророзмітки та карти веб-ресурсу;

• виявлення прихованого тексту;

• повний аналіз семантичного ядра, трафіку;

• аналізу обсягу та якості зовнішньої посилальної маси;

• наявність Яндекс Метрики та Google Analytics.

3) Usability аудит. Аналіз юзабіліті допомагає визначити, наскільки сайт зручний та комфортний у використанні для користувачів. Хорошим вважається

ресурс, де орієнтир відбувається на інтуїтивному рівні: людина не замислюється, куди йому потрібно натиснути, щоби отримати потрібну інформацію. Також враховується дизайн веб-сторінки, який візуально подобається потенційному клієнту.

Такий аудит можливий у трьох випадках: з погляду експертів; з погляду рядового користувача інтернет-мережі; за допомогою статистики у системах веб-аналітики. Усі ці три підходи допомагають провести аналіз загальної зручності веб-ресурсу. Якщо відбувається зниження позицій сайту та падіння трафіку, причиною може бути поганий поведінковий фактор, виявлений під час аналізу: показник відмов, глибина перегляду, час, проведений на сайті.

Також зокрема аналізуються:

• зручність та зрозумілість веб-ресурсу для потенційного клієнта;

• загальне візуальне враження від сайту;

• зрозумілість навігацій та функціоналу;

• унікальність та відповідність контенту тематики веб-сторінки, його медійності;

• зручність зворотного зв'язку;

• рівень довіри (особливо актуальний для інтернет-магазинів з дорогою продукцією).

• здатність коректно відображатись на всіх можливих типах пристроїв.

Поліпшення всіх цих показників та виправлення помилок на сайті допоможуть залучити клієнтів на веб-ресурс, значно підвищивши конверсію.

4) Маркетинговий аудит. Маркетинговий аудит потрібен для побудови стратегії просування сайту, конкурентоспроможності та підвищення прибутку. Для досягнення певних бізнес-цілей проводиться таке:

• аналізується цільова аудиторія сайту;

• розглядаються унікальність та вигідність торгових пропозицій;

• визначаються недоліки і слабкі сторони в порівнянні з головними конкурентами;

• аналізується якість трафіку;

• виділяються найпопулярніші теми на сайті;

• оцінюють витрати на просування веб-сторінки.

Аналіз показників ресурсу дозволяє скласти статистику, в основі якої слід вибудовувати подальшу маркетингову стратегію. Якщо не внести певні коригування або не зробити редизайн, який необхідний, виходячи зі звіту маркетингового аудиту, сайт може втратити значну частину клієнтів та загальний прибуток.

Виходячи з цього варто зробити висновок, що для якісної роботи ресурсу, високих позицій у пошукових системах та підвищення продаж, професійний аудит сайту просто необхідний. Якщо прийнято рішення отримувати прибуток та просувати свій веб-ресурс, найкращим варіантом буде звернутися до спеціальної компанії. Досвідчені фахівці проведуть комплексну перевірку та допоможуть у подальшому розвитку.

### 1.1 Внутрішній аудит сайту

Внутрішній аудит сайту мається на увазі повний аналіз стану сайту. Проводиться великий обсяг роботи з виявлення всіх пунктів, які ускладнюють просування пошукових систем. До ряду робіт можна віднести такі пункти як:

1) Аналіз контенту на всіх сторінках інтернет-ресурсу.

Наповнення сайту контентом – складний процес, він потребує багато часу та сил. Тим більше, якщо завдання полягає у створенні великого інформаційного чи комерційного порталу. В цьому випадку аналізувати весь вміст сайту, недоцільно. Вирішити проблему можна за допомогою аналізу контенту окремих сторінок, які дають найбільший результат. Дізнатися про них можна через звіт "Сторінки входу". Отримавши статистичні дані, стане зрозумілим, які сторінки відвідують найчастіше. Аналіз змісту тексту має відповідати наступним параметрам:

- відповідність тексту ключовим словам, за якими на сторінку приходить аудиторія;

- актуальність матеріалу та спосіб його подачі;
- відсутність дублювання контенту;
- відсутність битих посилань, які ведуть до неіснуючих розділів або повертають код помилки 404.

Ці опції допоможуть оптимізувати сторінку для зручності відвідувачів. Важливо також пам'ятати про технічні характеристики: використовувати заголовки H1-H6, ключові слова, списки і т.д.

2) Аналіз коду сайту на наявність помилок (додаткові роботи відділу розробки).

Після розробки дизайну програмісти верстають сторінки сайту – наводять їх до єдиної структури у форматі HTML. Завдання верстальника – зробити так, щоб сторінки відображалися коректно у всіх користувачів на будь-яких пристроях і браузерах. Така верстка називається кросплатформною та кросбраузерною - це обов'язкова вимога при розробці будь-яких сайтів. Для цього є спеціальні стандарти: якщо їм слідувати, сторінку будуть коректно розпізнавати всі браузери та гаджети. Такий стандарт розробив Консорціум всесвітньої павутини - W3C (The World Wide Web Consortium). HTML-код, який відповідає, називають валідним. Валідність також стосується файлів стилю - CSS. Якщо у CSS є помилки, візуальне відображення елементів може порушитись. Розробникам рекомендується дотримуватись критеріїв цих стандартів при верстці – це допоможе уникнути помилок у коді, які можуть зашкодити сайту.

Типові помилки коду — це незакриті або дубльовані елементи, неправильні атрибути або їх відсутність ( відсутність кодування UTF-8 або вказівки типу документа).

Які проблеми можуть виникнути через помилки в HTML-коді:

• сторінки завантажуються повільно;

• сайт некоректно відображається на різних пристроях або браузерах;

• відвідувачі бачать не весь вміст;

• програміст не помічає приховану рекламу та шкідливий код.

3) Аналіз розмітки контенту спеціальними тегами.

Пошукові системи бачать сайт не так як ми. Для нас контент веб-сторінки складається з різноманітної текстової інформації, картинок, аудіо-доріжок, відеороликів. Для пошукового робота будь-яка сторінка - полотно коду з розміткою. Метод верстки web-сайтів, за якого всі блоки всередині коду сторінки розмічені спеціальними тегами називають - семантичною версткою.

Іншими словами це створення веб-сторінки мовою HTML5 шляхом використання html5-тегів відповідно до їх значення. Семантична розмітка дозволяє створити структуру сторінки сайту з певною логікою та послідовністю. Якісна семантична верстка шаблонної сторінки сайту така ж важлива як правильно закладений фундамент будівлі. Теги розмітки є індикаторами для пошукових роботів у плані розуміння призначення та ступеня важливості того чи іншого елемента. Вихід 5-ї версії мови HTML ознаменувало появу безлічі нових тегів. Це значно розширило можливості веб-розробок, адже тепер можна і потрібно помічати кожен елемент контенту сторінки. Завдяки розмітці коду спеціальними тегами, пошукові системи краще розуміють вміст сайту і як його складові пов'язані між собою:

• розрізняють важливі, другорядні та не варті уваги текстові блоки;

• знаходять важливі слова та словосполучення, що передають суть сторінки;

• розпізнають слова/фрази у прямому та переносному значенні;

• визначають рекламні блоки;

• розуміють приналежність зображення (для дизайну сторінки чи як фото товару каталогу) тощо.

Таким чином, семантична верстка допомагає машинним веб-агентам коректно аналізувати сторінку, підвищувати ранжованість, готувати розширений опис сайту для його відображення в пошуковій видачі і т.д. Причому візуально веб-сторінка із семантичною версткою не має видимих відмінностей від сайту, де цієї верстки немає і близько.

4) Аналіз та оптимізація посадкових сторінок.

Практика показує, що одні цільові сторінки миттєво зацікавлюють відвідувачів і змушують зробити ту чи іншу дію, інші залишають байдужими, викликаючи єдине бажання покинути сторінку. Секрет полягає в тому, чи оптимізовані посадкові сторінки під привернення уваги користувачів та залучення трафіку на сайт. Тобто, оптимізація лендингу є невід'ємною умовою конвертації потоку відвідувачів сайту в активних клієнтів.

Способи оптимізації посадкових сторінок. Оптимізувати готову посадкову сторінку можна такими шляхами:

• Структурувати інформацію. Для високої конверсії контент посадкової сторінки необхідно структурувати. Зробити це можна шляхом розміщення заголовків і підзаголовків, що розпалюють цікавість, деталізують списки, що спрощує сприйняття інформації користувачами.

• Включити ключові слова у заголовок, мета-теги та контент. Продумуючи заголовок посадкової сторінки, необхідно вставити ключовий запит. При написанні мета-тегів для title та description також варто використовувати один або кілька ключових слів відповідно, що підштовхне користувача до переходу на сторінку. При описі характеристик та переваг товару чи послуги слід використовувати ключові фрази, за якими лендинг індексуватиметься пошуковими системами.

• Зробити привабливий дизайн. Сформувати у відвідувачів позитивне враження про сторінку допоможуть гарні ілюстрації та шрифти, а діяти негайно закличе яскрава кнопка CTA(call to action) . При цьому зі сторінки потрібно виключити всі зайві зображення, кольори та інші деталі, що відволікають користувачів.

• Наповнити масою посилань. Розміщення на сторінці природних посилань із авторитетних інтернет-майданчиків здатне підвищити позиції лендингу у пошуковій видачі.

5) Перевірка файлу robots.txt, генерація карт сайту .xml та .html.

Файл robots.txt – це текстовий файл, який розміщується на веб-сайтах для інформування роботів пошукових систем (наприклад, Google), які сторінки в

цьому домені можна сканувати. Перш ніж роботи пошукових систем просканують сайт, вони спочатку знайдуть файл robots.txt сайту. Таким чином вони побачать інструкції, які сторінки сайту можна індексувати, а які не слід індексувати консоллю пошукової системи. За допомогою цього простого файлу налаштовуються параметри сканування та індексування для роботи пошукових систем. У файлі robots.txt містяться інструкції, які говорять пошуковим роботам, які URL-адреси на сайті їм дозволено обробляти. З його допомогою можна обмежити кількість запитів на сканування і цим знизити навантаження на сайт. Файл robots.txt не призначений для заборони показу матеріалів у результатах пошуку Google.

Xml карта сайту створюється для пошукових роботів. За допомогою xml карти можна вказати, як часто слід індексувати ту чи іншу сторінку, як часто вона оновлюється, наскільки вона важлива в рамках сайту. За допомогою картки сайту фіксуються всі посилання на сайті. Іншими словами, структура сайту стає прозорою для пошукових роботів. Для «живих» користувачів xml карта марна.

Html карта сайту створюється для відвідувачів сайту, вона аналог змісту в книзі. Часто буває, що при складній або не дуже прозорій структурі відвідувач губиться в навігації по сайту і не доходить до сторінок (він їх просто не знаходить), які йому були б потрібні та йде з сайту незадоволений. Конверсія сайту при цьому знижується. Якщо html карта є і зроблена якісно, правильно і ємно озаглавлені розділи, то будь-який розділ, будь-яка сторінка сайту потрібної тематики легко знайдеться відвідувачем сайту.

6) Складання максимально повного семантичного ядра під всі види послуг, товари тощо.

Семантичне ядро – набір слів та словосполучень, що відображають тематику та структуру сайту. Складаючи смислове ядро, ми відповідаємо на глобальне питання: яку інформацію можна знайти на сайті? Оскільки одним із головних принципів бізнесу та маркетингу вважається клієнтоорієнтованість, створення семантичного ядра можна дивитися з іншого боку. Потрібно

визначити, за допомогою яких пошукових запитів користувачі шукають інформацію, яка буде надрукована на сайті.

Побудова смислового ядра вирішує ще одне завдання. Йдеться про розподіл пошукових фраз на сторінках ресурсу. Працюючи з ядром, визначається, яка сторінка найточніше відповідає на конкретний пошуковий запит або групу запитів. Є два підходи до вирішення цього завдання:

- Перший передбачає створення структури сайту за результатами аналізу запитів користувача. І тут семантичне ядро визначає каркас і архітектуру ресурсу.
- Другий підхід передбачає попереднє планування структури ресурсу до аналізу пошукових запитів. В цьому випадку семантичне ядро розподіляється по готовому каркасу.

Обидва підходи так чи інакше працюють. Але логічніше спочатку планувати структуру сайту, а потім визначати запити, за якими користувачі зможуть знайти ту чи іншу сторінку. Спочатку потрібно вирішити, яку інформацію транслювати аудиторії за допомогою сайту. Для цього необхідно добре знати свою галузь та бізнес. Спочатку потрібно запланувати приблизну структуру сайту та попередній список сторінок. Після цього під час побудови семантичного ядра треба дізнатися, як аудиторія шукає інформацію. За допомогою контенту необхідно відповідати на запитання, які задає аудиторія.

7) Аналіз наявності внутрішньої перелінковки між розділами, сторінками сайту.

Власне, внутрішня перелінковка має систему зв'язків між сторінками сайту з допомогою посилань, тобто. Якийсь елемент контенту, меню або навігації однієї сторінки є посиланням на іншу сторінку, яка, можливо, також посилається на певну сторінку. У будь-якій роботі потрібна система, тому і внутрішня перелінковка повинна вибудовуватися не бездумно, а з урахуванням пріоритетних для проекту завдань. Перерахуємо найважливіші моменти, на які можна вплинути, грамотно розміщуючи внутрішні посилання на сайті:

- Посилання дозволяють передати статичну вагу сторінок розділу, що просувається, підкресливши його важливість.
- За допомогою внутрішніх посилань можна підвищити релевантність сторінок.
- Наявність посилань дозволяє позитивно вплинути на швидкість індексації сторінок із високим рівнем вкладеності.
- Посилання дозволяють затримати користувача на сайті, зацікавивши його новою інформацією, що дозволить збільшити такі показники як: тривалість перебування користувача на сайті та кількість переглядів сторінок користувачем.

Важливо розуміти, що у довідці для веб-майстрів від Google зафіксовано, що чим більше внутрішніх посилань ведуть на конкретну сторінку, тим вона важливіша. Розглянемо типи та схеми перелінкування:

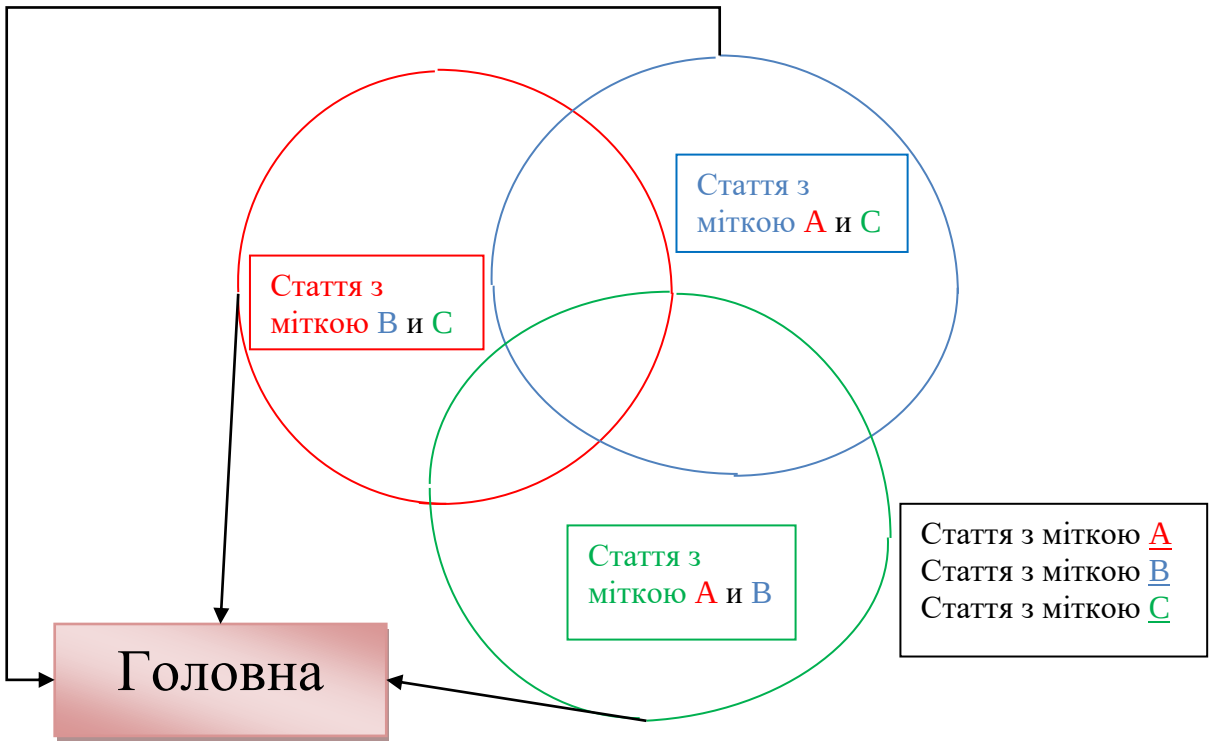


Рисунок 1.1 –Кругова схема внутрішньої перелінковки

Якщо говорити про різновиди внутрішнього перелінкування, то за місцями розміщення посилань виділяють перелінкування в контентній частині

(зокрема, посилання в тексті), а також розміщення посилань у блоках (наприклад, у блоках товарів), у меню та навігації (наприклад, “хлібні крихти”).

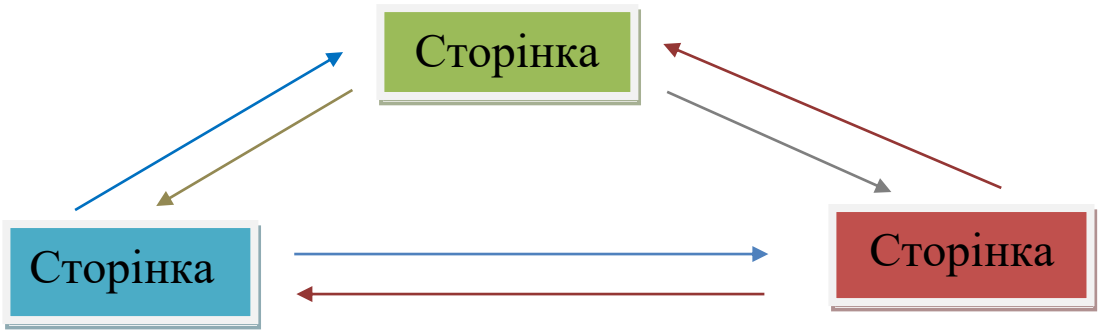


Рисунок 1.2 –Зіркоподібна схема внутрішньої перелінковки

Що стосується схем внутрішньої перелінковки, то виділяють три класичні варіанти: кругова, зіркоподібна та ієрархічна. Розглянемо особливості кожного з них:

- Кругова (Рис.1.1). Всі сторінки сайту посилаються на розділ, що просувається, і один на одного. Такий варіант зазвичай використовується для просування високочастотних запитів.
- Зіркоподібна. Дана схема (Рис.1.2) ґрунтується на тому, що всі сторінки сайту посилаються одна на одну.
- Ієрархічна (Рис.1.3). Суть такого рішення зводиться до того, що при перелінку дотримується чітка ієрархія сторінок сайту - головна посилається на розділи, розділи - на сторінки контенту, сторінки контенту - на головну.

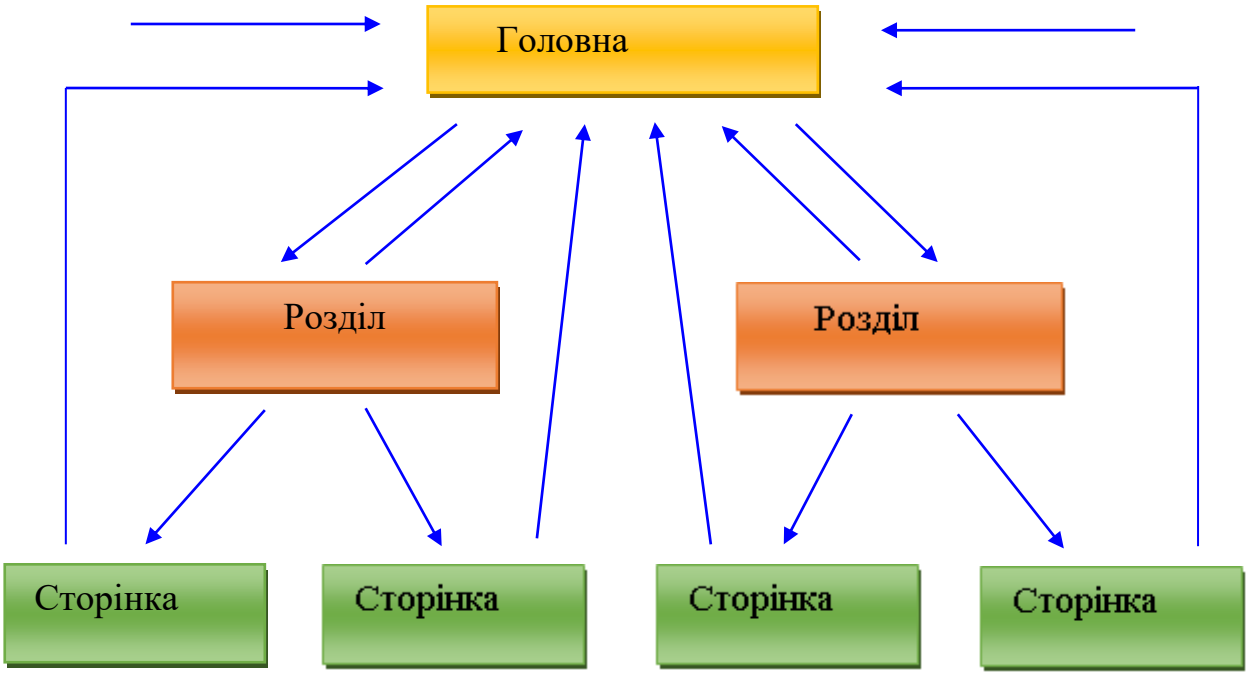


Рисунок 1.3 –Ієрархічна схема внутрішньої перелінковки

Існують і складніші варіанти. Вибирати схему здійснення перелінкування слід, спираючись на стратегію пошукового просування сайту. Здійснити грамотну роботу із внутрішніми посиланнями вам допоможуть спеціальні інструменти. Цілком достатньо даних із Google Search Console та можливостей таких сервісів, як Keycollector та Serpstat.

"Звіт про внутрішні посилання" Google Search Console дозволяє отримати дані про поточну ситуацію та проаналізувати їх, а "Аналіз пошукових запитів" надає дані про запити, які можна використовувати як анкори для внутрішніх посилань.

Keycollector - це інструмент, функціональні можливості якого дозволяють зібрати семантичне ядро, а також отримати рекомендації щодо перелінкування, що ґрунтуються на даних видачі пошукових систем.

Serpstat – широко-функціональний інструмент для аналізу сайту. Він може бути корисним тим, що надає інформацію про запити, за якими сайт знаходиться на другій сторінці видачі.

Запити та сторінки для перелінкування. Використання випадкових запитів для організації перелінкування малоефективне, тому спочатку слід отримати інформацію про запити, за допомогою яких користувачі приходять на сайт. Таку інформацію можна отримати з Google Search Console. Після цього потрібно визначити частотність цих запитів, щоб відмовитися від ключових фраз із запитуваністю, яка близька до нуля. Далі слід опрацювати отриманий масив запитів з метою отримання інформації про позицію, що вони займають. Фахівці рекомендують брати в роботу запити на другій сторінці видачі.

Що стосується сторінок, то слід визначити сторінки сайту, які пошукова система вважає найбільш релевантними конкретному запиту. Для цього можна використовувати той самий Keycollector або провести цю роботу по кожному із запитів вручну через пошукову систему, скориставшись оператором site: “site:mysite.com запит”.

Існує ряд правил, яких варто дотримуватись, працюючи з внутрішніми посиланнями сайту:

- Обмежуватись одним посиланням зі сторінки А на сторінку Б.
- Відмовитися від анкорів у вигляді безладних "спамних" формулювань.
- Розміщувати посилання там, де це зручно для користувача.
- Слідкувати за битими посиланнями та відкритістю сторінок для індексування.

Грамотна внутрішня перелінковка дозволить без особливих зусиль підтягнути в ТОП-10 запити з другої сторінки видачі, проте це лише один з багатьох аспектів, на які слід звертати увагу, працюючи з оптимізацією сайту під вимоги пошукових систем.

## 1.2 Зовнішній аудит сайту

Зовнішній аудит сайту – це комплекс заходів, які зводяться до визначення помилок та слабких місць сайту при роботі з масою посилань. За допомогою такої перевірки, можна з'ясувати за рахунок чого можливе просування сайту в пошукових системах та ліквідувати помилки та недоліки, які «гальмують» розвиток сайту з погляду пошукових алгоритмів.

Серед заходів такого аудиту можна виділити такі як:

- проведення аналізу розподілу посилальної маси;
- проведення робіт з аналізу посилальних донорів;
- аналіз вихідних посилань.

В цілому проведення перевірки сайту, покликане допомогти уникнути помилок при просуванні його в пошукових системах. Грамотний і ретельно організований аудит дозволяє істотно скоротити час на проведення оптимізації сайту, а так само зменшити з в'язані з цим процесом витрати при цьому значно підвищивши ефективність його роботи.

1) Проведення аналізу розподілу маси посилань.

Посилальна маса - поняття, яке має на увазі всі посилання на ваш ресурс з інших сайтів. Посилальну масу нарощують, щоб просувати сайт у мережі інтернет і вивести його в топ-запити пошукових систем. Нарощування якісної маси сайту - процес, що вимагає певного часу. Тому здатність робити це плавно, креативно і з розумом – запорука успіху.

У сукупності із внутрішньою оптимізацією ресурсу та поведінковими факторами, посилальна маса є найбільш популярним способом просування ресурсу. Спочатку використання маси посилань як способу просування, прийнято було вважати, що саме кількість посилань на сайт з інших джерел визначає шанси потрапити на перші сторінки видачі. Але тепер недостатньо мати велику масу посилань — потрібно стежити за її якістю (вагою). Це означає, що сайт із зовнішнім посиланням на ресурс (донор) повинен розпізнаватись пошуковими системами як авторитетний. Посилання, розміщене

неавторитетним донором, може негативно вплинути на позицію сайту, що просувається. У зв'язку з тим, що все частіше можна зустріти покупні посилання, пошукові системи навчилися розпізнавати їх серед природних і не враховувати при формуванні рейтингу ресурсу.

Для перевірки маси сайту та визначення її ліквідності, потрібно провести аудит: перевірити сайт на наявність посилань, дізнатися їхню релевантність, подивитися, на які ресурси йде перелінковка, перевірити стан анкор листа.

2) Виконання аналізу посилань із різних соціальних мереж.

Донори аналізують за такими параметрами:

• сайти-сателіти, партнерки;

• спамні сайти;

• сайти на одному IP або одній підмережі;

• відвідуваність сайту-донора;

• індексація сайту-донора;

• відповідність до тематики ресурсу;

• унікальність контенту на сайті.

3) Аналіз вихідних посилань.

Вихідні посилання - це посилання, розміщені на конкретному сайті та які ведуть інші ресурси.

Вихідні посилання є на будь-якому сайті і не є чимось особливим. Вони можуть мати як позитивні, так і негативні сторони. До позитивних можна віднести:

• докладний розгляд тієї чи іншої інформації при короткому огляді матеріалу на вашій сторінці;

• посилання на джерело тематики, на якій ви робите свій оригінальний аналіз або огляд;

• супутні ресурси та реклама партнерських сайтів.

Таким чином, корисні релевантні посилання допомагають користувачам сайту та підвищують до нього довіру.

Негативна сторона може формуватися через «сіру» рекламу, а також особливо згенеровані посилання. Крім цього, є й інші суттєві мінуси:

• скупчення великої кількості посилань на сторінці, наявність яких відштовхує відвідувачів (рекомендується не більше ста посилань на сторінку);

• розміщення оплачуваних посилань, що негативно впливають на довіру до сайту;

• пам у коментарях;

•користувач, який перейшов за посиланням, може не повернутись на ваш ресурс. Слід грамотно розміщувати посилання на джерела, та попутну інформацію так, щоб відвідувач захотів повернутися на попередню сторінку;

• шкідливі посилання на сайт, що згодом потрапив під фільтр пошукових систем;

• розміщення великої кількості посилань на молодому сайті може загрожувати фільтрами.

Це далеко не весь перелік необхідних робіт для внутрішнього та зовнішнього аудиту сайту. Адже комплекс робіт охоплює абсолютно весь сайт, для виявлення та усунення всіх актуальних помилок. Проведення внутрішнього та зовнішнього аудиту сайту може зайняти як 2 – 3 дні, так і 1 – 2 тижні, все залежить від обсягу, структури та особливостей сайту. Але можна точно сказати, що без аудиту – робота та просування сайту практично неможлива.

# РОЗДІЛ 2. ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Тестування на проникнення є одним із пріоритетних напрямків в інформаційній безпеці. Воно дозволяє отримати оцінку того, наскільки легко здійснити несанкціонований доступ до комп'ютерної системи. Поглянути на саму систему з погляду зловмисника, а саме зрозуміти, як можна скомпрометувати обрану систему і які шкідливі дії в ній можна зробити. Описано способи подолання зловмисником встановлених засобів захисту та набір дій, які він зможе вчинити, отримавши несанкціонований доступ до комп'ютерної системи.

Тестування на проникнення є однією з методик виявлення областей системи, вразливих для вторгнення та компрометації цілісності та достовірності з боку неавторизованих та зловмисних користувачів. Процес тестування проникнення включає навмисні санкціоновані атаки на систему, здатні виявити як її найбільш слабкі області, так і прогалини в захисті від сторонніх проникнень, і тим самим поліпшити атрибути безпеки.

Прогалини в безпеці з'являються на різних стадіях процесу і залежать від багатьох факторів:

• помилка проектування (наприклад, недоробки в дизайні – один із найважливіших факторів виникнення лазівок у безпеці);

• некоректне налаштування та невдала конфігурація пов'язаного обладнання та програмного забезпечення;

• проблеми підключення до мережі (безпечне підключення усуває можливість шкідливих атак, а небезпечна мережа забезпечує шлюз хакерам для нападу на систему);

• людська помилка (помилка, вчинена навмисно або ненавмисно окремою особою або командою при проектуванні, розгортанні та обслуговуванні системи або мережі);

• похибка комунікації (неправильна або відкрита передача конфіденційних даних та інформації серед команд чи окремих осіб);

• надмірна складність системи (контролювати механізм безпеки простої мережної інфраструктури легко, а відстежувати витоки або будь-яку зловмисну діяльність у складних системах важко);

• недостатність навчання (відсутність знань та належної підготовки з питань безпеки як у внутрішніх співробітників, так і тих, хто працює за межами організаційної структури).

Тестування на проникнення – це перевірка у реальному часі вручну чи з допомогою інструментів автоматизації. Система та пов'язаний з нею компонент піддаються впливу семульованих зловмисних атак для виявлення недоліків безпеки.

Як зазначалося раніше, прогалини у безпеці забезпечують неавторизованому користувачеві або незаконному об'єкту можливість атакувати систему, що впливає на її цілісність і конфіденційність. Таким чином, тестування програмних продуктів на проникнення допомагає позбавитися цих вразливостей і зробити систему достатньо компетентною для захисту від очікуваних і навіть несподіваних шкідливих загроз і атак.

Розглянемо результати застосування цієї методики докладніше. Отже, тестування на проникнення надає:

• Спосіб виявлення слабких та вразливих областей системи ще до того, як їх помітить хакер. Часті та складні оновлення системи можуть вплинути на відповідне обладнання та програмне забезпечення, що призводить до проблем безпеки, тому доречно контролювати всі ці оновлення.

• Можливість оцінки наявного механізму безпеки системи. Це дозволяє розробникам оцінити свою компетентність у захисті та підтримувати рівень стандартів безпеки, встановлений у системі. Крім вразливості системи рекомендується також за допомогою бізнес- та технічної команд оцінювати різні бізнес-ризики та проблеми, включаючи будь-який компроміс із дозволеними та конфіденційними даними організації. Це допомагає організації

структурувати та встановлювати пріоритети, пом'якшуючи або повністю виключаючи різні бізнес-ризики та проблеми.

• Нарешті (але не в останню чергу) інструмент для виявлення та задоволення певних основних стандартів, норм та практик безпеки.

Тестування на проникнення системи може здійснюватися за допомогою будь-якого з наступних підходів:

• ручне тестування;

• автоматичне тестування;

• поєднання ручного та автоматичного тестування.

Виконується для: Веб-порталів, інтернет-магазинів, мобільних додатків.

## 2.1 Ручне тестування на проникнення

Для проведення ручного тестування на проникнення програмного продукту використовується стандартний послідовний підхід, що включає наступні етапи:

• Планування тестування проникнення. Цей етап включає збір вимог, визначення сфери застосування, стратегій і цілей тестування проникнення відповідно до норм безпеки. Крім того, він може містити оцінку та перерахування областей, що перевіряються, типи планованих випробувань та інші пов'язані з цим перевірки.

• Розвідка. Збір та аналіз максимально докладної інформації про системні та пов'язані з ними атрибути безпеки, корисні для націлення та атаки на кожен блок, для ефективного та результативного тестування проникнення в систему.

Розрізняють дві форми збору та аналізу інформації про цільову систему: пасивна та активна розвідка (у першому випадку не передбачається пряма взаємодія із системою).

• Аналіз уразливості. На цьому етапі тестувальники виявляють уразливі області системи, які надалі використовуватимуться для входу та атаки за допомогою тестів на проникнення.

• Експлуатація. Фактичне випробування на проникненні в систему, що включає внутрішні та зовнішні атаки. Зовнішні атаки – це семульовані атаки з боку зовнішнього світу, що переважають за межами системи/мережі (наприклад, отримання несанкціонованого доступу до функцій та даних системи, що стосуються додатків та серверів, звернених до громадськості). Внутрішні атаки починаються вже після вторгнення авторизованих об'єктів у систему чи мережу і мають на меті різні дії (при досягненні компромісу з цілісністю та правдивістю системи), які здатні навмисно чи ненавмисно скомпрометувати систему.

• Пост-експлуатація. Наступний крок – аналіз кожної атаки на систему для оцінки її мети та завдання, а також її потенційного впливу на системні та бізнес-процеси.

• Звітність. Насправді, звітність включає документаційну роботу по заходах, що проводяться на всіх згаданих етапах. Крім того, вона може описувати різні ризики, виявлені проблеми, уразливі області (використані чи ні) та запропоновані для усунення недоліків рішення.

Ручне тестування на проникнення - це тестування, яке здійснюють люди. У таких видах тестування вразливості і ризик машини перевіряється експертом-інженером. Як правило, інженери з тестування виконують наступні дії (рисунок 2.1).


Рисунок 2.1 – Складники тестування на проникнення

Після проникнення тестер готує заключний звіт, який описує все про систему. Нарешті, звіт аналізується, щоб вжити коригувальних заходів для захисту цільової системи.

Типи ручного тестування на проникнення. Ручне тестування на проникнення зазвичай класифікується за двома наступними способами:

- Цілеспрямоване ручне тестування на проникнення - це набагато більш цілеспрямований метод, який перевіряє конкретні вразливості та ризики. Автоматичне тестування на проникнення не може виконати це тестування; це роблять лише фахівці-люди, які вивчають специфічні вразливості додатків в межах цих доменів
- Комплексне ручне тестування на проникнення - це тестування цілих систем, пов'язаних одна з одної, для виявлення всіх видів ризику та вразливостей. Проте функція цього тестування є більш ситуативною, наприклад, вивчення того, чи можуть кілька несправностей з нижчим ризиком принести більш вразливий сценарій атаки, тощо.

## 2.2 Автоматичне тестування на проникнення

Цей корисний та ефективний підхід до проведення випробувань на проникнення передбачає використання спеціалізованого інструментарію. Автоматичне тестування надійне, зручне, воно відбувається дуже швидко та легко піддається аналізу. Інструменти перевірки є ефективними для точного виявлення дефектів безпеки, присутніх у системі, за короткий проміжок часу, а також для створення «кришталевих» звітів.

Назвемо лише деякі з популярних та широко використовуваних інструментів тестування на проникнення:

• Nmap;

• Nessus;

• Metasploit.

Багато інструментів для автоматизованого тестування можна знайти у готових збірках Linux (Kali Linux, Mantra OS).

Для роботи над конкретним проектом доведеться вибирати інструмент, який відповідає цілій низці вимог та критеріїв:

• зручність розгортання, використання та обслуговування;

• забезпечення простого та швидкого сканування системи;

• можливість автоматизації процесу перевірки виявлених уразливостей;

• доступність перевірки раніше виявлених уразливостей;

• здатність створення простих та докладних звітів про вразливість.

## 2.3 Поєднання ручного та автоматичного тестування на проникнення

Також проводиться спільне використання ручного тестування на проникнення, та автоматичного тестування на проникнення. Єдина різниця між ними полягає в тому, як вони проводяться. Як випливає з назви, ручне тестування на проникнення здійснюється людьми (фахівцями цього напряму), а автоматичне тестування на проникнення здійснюється самою машиною. Даний підхід може бути визнаний оптимальним, так як він поєднує в собі переваги перших двох варіантів та забезпечує оперативний контроль за допомогою надійного та точного проникнення у програмний продукт. Поєднання ручного та автоматичного тестування на проникнення, направлене на максимальну перевірку безпеки системи, а також оцінку цілісності підходу до захисту сайту від несанкціонованого доступу і захисту конфіденційних даних.

## 2.4 Типи випробувань на проникнення

Тестування на проникнення в залежності від елементів і об'єктів, що використовуються, може бути віднесено до наступних типів:

• Соціальна інженерія. Тестування з підключенням «людського контингенту», здатного чітко виявляти та отримувати конфіденційні дані та іншу інформацію через Інтернет або телефон (до цієї групи можуть належати співробітники організації або будь-які інші уповноважені особи, присутні у мережі організації).

• Веб-додаток. Використовується для виявлення недоліків у безпеці та інших проблем у кількох варіантах веб-додаток та сервісів, розміщених на стороні клієнта або сервера.

• Мережева служба. Тестування проникнення в мережу для виявлення та виявлення можливості доступу до хакерів або будь-якого неавторизованого об'єкта.

• Клієнтська частина. Як видно з назви, цей тест використовується для тестування програм, встановлених на клієнтському сайті/додатку.

• Дистанційне підключення. Тестування vpn або аналогічного об'єкта, який може забезпечити доступ до підключеної системи.

• Бездротові мережі. Тест призначений для бездротових додатків та сервісів, включаючи їх різні компоненти та функції (маршрутизатори, фільтраційні пакети, шифрування, дешифрування тощо).

Класифікувати тестування на проникнення також можна і на основі підходів до тестування, що використовуються:

• Білий ящик. При такому підході тестувальник матиме повний доступ до глибоких знань про функціонування та основні атрибути системи. Це тестування дуже ефективне, оскільки розуміння кожного аспекту системи дуже корисно під час проведення великих випробувань проникнення.

• Чорний ящик. Тестувальникам надається лише високорівнева інформація (наприклад, URL або IP-адреса організації) для проведення тестування на проникнення. Фахівець може відчути себе хакером, який нічого не знає про систему/мережу. Це дуже трудомісткий підхід, тому що тестувальнику потрібна значна кількість часу для вивчення властивостей та

деталей системи; крім того, висока ймовірність пропустити частину областей через брак часу та інформації.

• Сірий ящик. Тестувальник отримує обмежену інформацію (наприклад, знання алгоритму, архітектури, внутрішніх станів) для імітації зовнішньої атаки на систему.

### 2.4.1 Тестування на проникнення - білий ящик

Це комплексне тестування, оскільки тестувальникові було надано цілий спектр інформації про системи та / або мережі, такі як схема, вихідний код, деталі операційної системи, IP-адреса тощо. Зазвичай, це розглядається, як симуляція атаки з боку внутрішнього джерела. Він також відомий як структурний ящик, прозоре вікно або тестування з відкритою коробкою.

Тестування на проникнення - білий ящик, перевіряє код і проводить тестування потоку даних, тестування шляхів, тестування циклів тощо.

Переваги тестування на проникнення білий ящик.

•Забезпечує виконання всіх незалежних тестів модуля.

•Гарантує, що всі логічні рішення перевірені разом з їх істинним і помилковим значенням.

•Виявляє друкарські помилки та перевіряє синтаксис.

•Знаходить помилки, які можуть виникнути внаслідок різниці між логічним потоком програми та фактичним виконанням.

### 2.4.2 Тестування на проникнення - чорний ящик

У тестуванні на проникнення - чорний ящик тестер не має уявлення про системи, які він збирається перевірити. Він зацікавлений зібрати інформацію про цільову мережу або систему. Наприклад, у цьому тестуванні тестер знає

лише, який повинен бути очікуваний результат, і він не знає, як досягнути результату. Він не розглядає ніяких програмних кодів.

Переваги тестування на проникнення - чорний ящик.

• Тестер не обов'язково повинен бути експертом, оскільки він не вимагає конкретних знань мови програмування.

• Тестер перевіряє протиріччя в реальній системі та специфікаціях.

• Тест, як правило, проводиться з точки зору користувача, а не дизайнера.

Недоліки тестування проникнення чорного ящика:

• Особливо важко розробити такі типи тестів.

• Можливо, конструктор системи вже провів тест.

• Не проводити все тестування.

### 2.4.3 Тестування на проникнення - сірий ящик

У цьому типі тестування тестер зазвичай надає часткову або обмежену інформацію про внутрішні деталі програм системи. Його можна розглядати як атаку зовнішнього хакера, який отримав незаконний доступ до документів мережевої інфраструктури організації.

Переваги тестування на проникнення сірий ящик.:

• Оскільки тестер не вимагає доступу до вихідного коду, він не є нав'язливим та неупередженим.

• Оскільки існує чітка різниця між розробником і тестером, тому існує найменший ризик особистого конфлікту.

• Вам не потрібно надавати внутрішню інформацію про функції програми та інші операції.

У тестування на проникнення існує низка обмежень:

- брак часу та висока вартість тестування;
- обмежений обсяг випробувань, що базується на вимогах за цей період часу (що може призвести до ігнорування інших важливих областей);

- можливість руйнування системи або втрати системи у стані відмови у результаті випробування на проникнення;
- вразливість даних (втрата, корупція чи шкоду).

Хакери, озброєні вдосконаленими технологіями з широким спектром ресурсів та інструментів, часто легко вриваються в систему або мережу з наміром заподіяти шкоду репутації та активам компанії. Перевірка на проникнення більшою мірою, ніж інші види тестування, може розглядатися як інструмент виявлення різних прогалин у безпеці, що допомагає звести нанівець потенційні загрози для системи в цілому.

Тестування на проникнення має важливе значення, оскільки:

- ідентифікує середовище моделювання, тобто, як зловмисник може атакувати систему через атаку білого капелюха;
- допомагає знайти слабкі зони, де зловмисник може атакувати, щоб отримати доступ до даних і можливостей комп'ютера;
- підтримує запобігання атаці чорного капелюха і захищає вихідні дані;
- оцінює масштаби нападу на потенційний бізнес;
- надає докази того, чому важливо збільшити інвестиції в аспект безпеки технології.

# РОЗДІЛ 3. РОЗРОБКА АЛГОРИТМУ ПРОВЕДЕННЯ АУДИТУ WEB-САЙТІВ.

## 3.1 Добірка вразливих середовищ для практики зі злому сайтів (0 крок)

Нульовим кроком є встановлення OWASP Mutillidae II або Damn Vulnerable Web Application (DVWA) в Kali Linux. OWASP Mutillidae II та Damn Vulnerable Web Application (DVWA) – це вразливі веб-програми, які спеціально призначені для тренування в пошуку та експлуатації різних вразливостей (тобто в тестуванні на проникнення), на них можна тренуватися з злому сайтів або тестувати інструменти для сканування веб-сайтів.

### 3.1.1 OWASP Mutillidae II у Kali Linux

Після завершення встановлення OWASP Mutillidae II буде доступним за посиланням http://localhost/mutillidae/. При першому запуску ми побачимо:

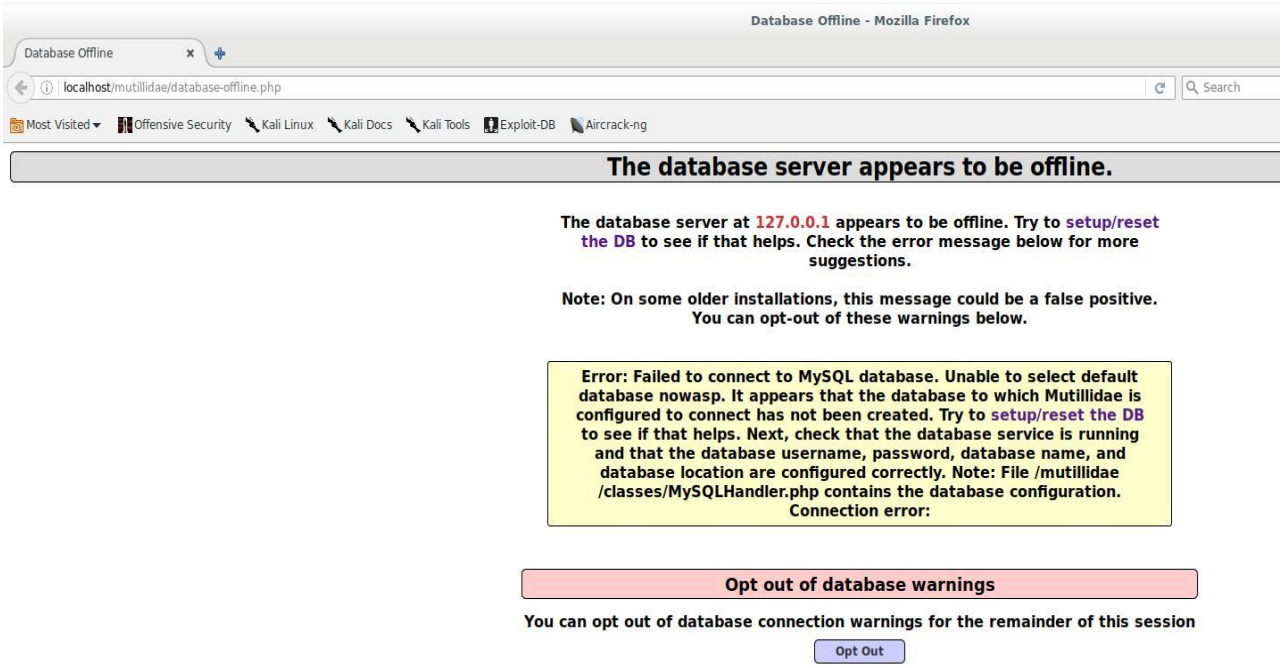

Рисунок 3.1 –Початкова сторінка сайту OWASP Mutillidae II

Натисніть "setup/reset the DB" і дочекаємося створення бази даних (рис.3.2).

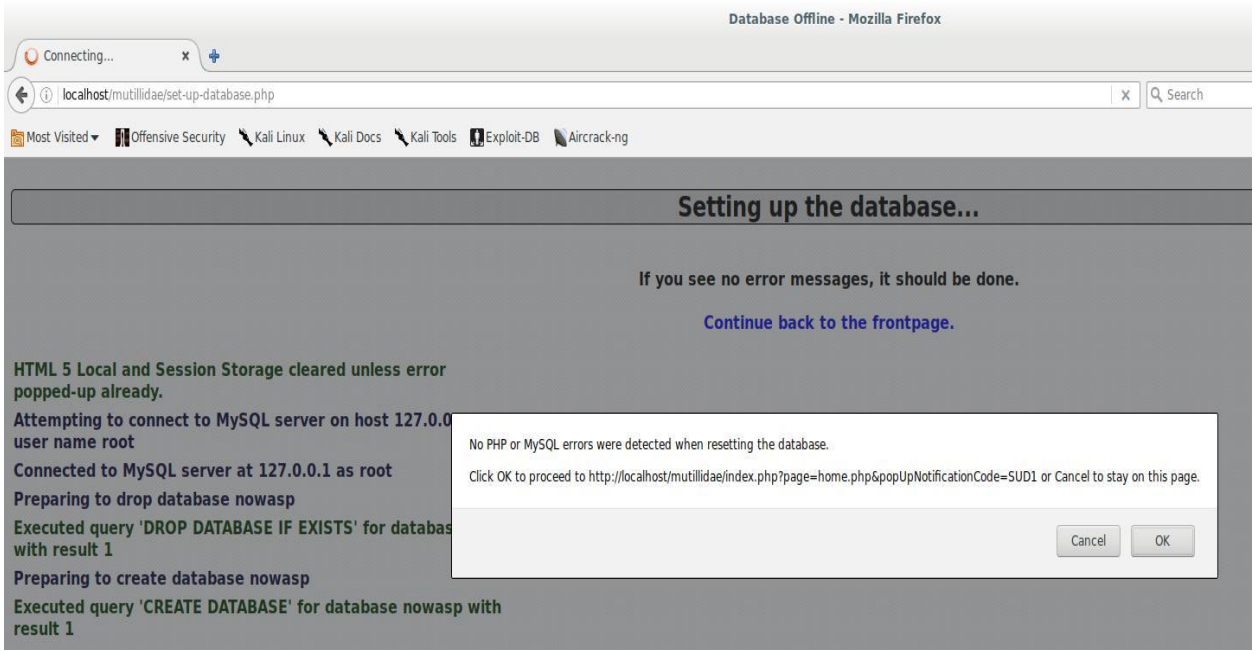


Рисунок 3.2 – Етап створення бази даних

Потім у спливаючому вікні просто натисніть «ОК».

Для ініціалізації бази даних слід перейти за посиланням: http://localhost/mutillidae/set-up-database.php

Тепер ми повністю готові для навчання злому веб-сайтів:

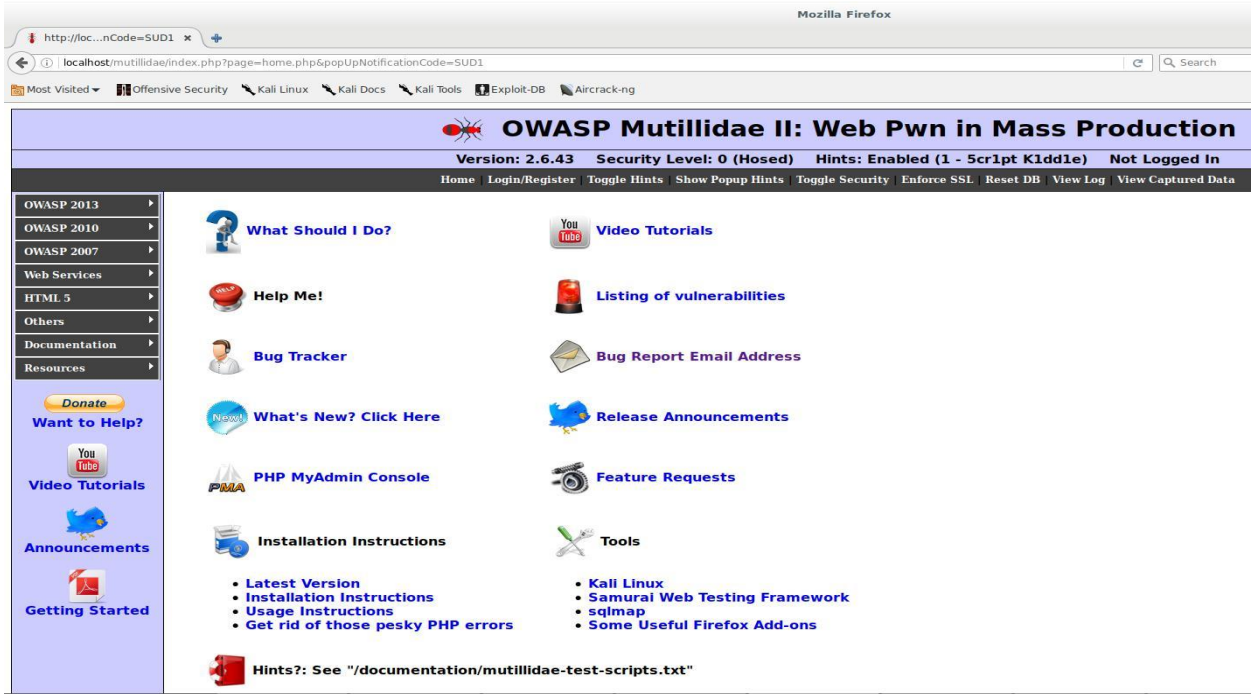

Рисунок 3.3 – OWASP Mutillidae II

### 3.1.2 Damn Vulnerable Web Application (DVWA) у Kali Linux

Після установки необхідно перейти на сторінку Setup/Reset DB у DVWA та виконати скидання/перестворення бази даних.

Тепер встановлені DVWA доступні за адресою http://localhost/dvwa/

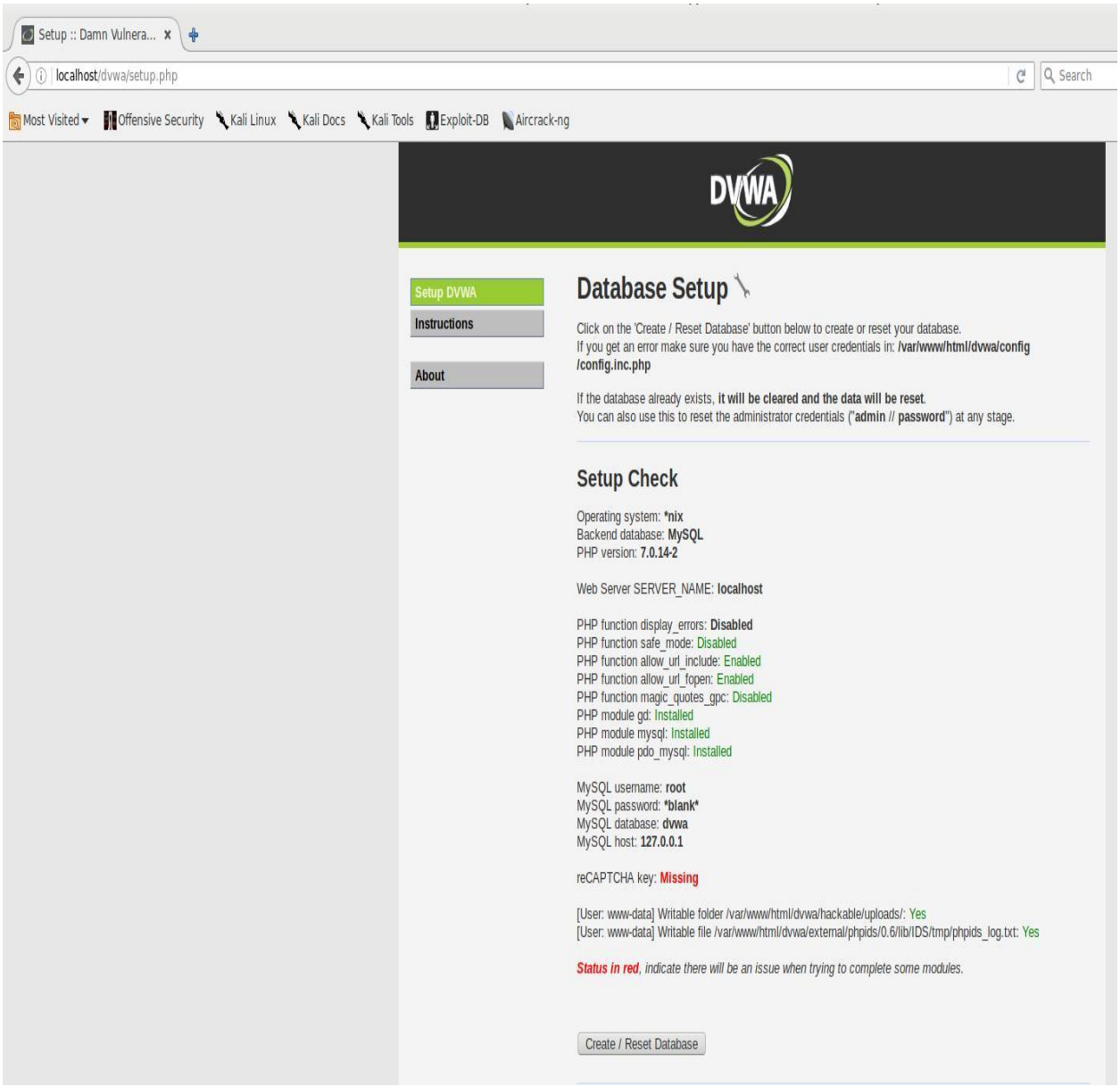


Рисунок 3.4 – DVWA http://localhost/dvwa/

### 3.2 Збір інформації (1 крок)

#### 3.2.1 Інформація про використовувані технології, структуру веб-сайту

1) Ідентифікація технологій, на яких працює веб-сайт (WhatWeb).

WhatWeb – це кросплатформова програма, вона написана на Ruby та працює на популярних платформах, таких як Windows, Mac OSX та Linux. WhatWeb використовується для визначення на яких програмах, яких версій працює веб-сайт. Збірну інформацію умовно можна поділити на три групи:

• про веб-сервер (чи використовується Apache, nginx або ще щось, їх версії; чи використовується PHP і якої версії, які заголовки надсилаються; чи використовується OpenSSL і якої версії тощо)

• про платформу веб-сайту (яка використовується система управління контентом та якою версією; які використовуються бібліотеки JavaScript; які фреймворки та яких версій задіяні в роботі веб-сайту тощо)

• супутня інформація про веб-сайт (IP сайт, країна розташування веб-сервера, поштові адреси, популярні інструменти аналітики та статистики та інше)

Інформація, що використовується, може використовуватися для різної аналітики, а також при тестуванні на проникнення та при розслідуванні на основі відкритих джерел (для зіставлення приналежності сайтів одній особі, встановленню особи власника). В даний час WhatWeb також має плагіни для ідентифікації різноманітних вбудованих пристроїв.

WhatWeb – це утиліта програмного рядка, тому всі дії потрібно виконувати у консолі. Для використання базових функцій програми, достатньо вказати адресу сайту:

```
1  whatweb адреса_сайту
```

Замість адреси сайту може бути IP.Приклад:

```
1 whatweb suip.biz
```

Або:

```
1 whatweb 185.117.153.79
```

Буде виведена приблизно така інформація:

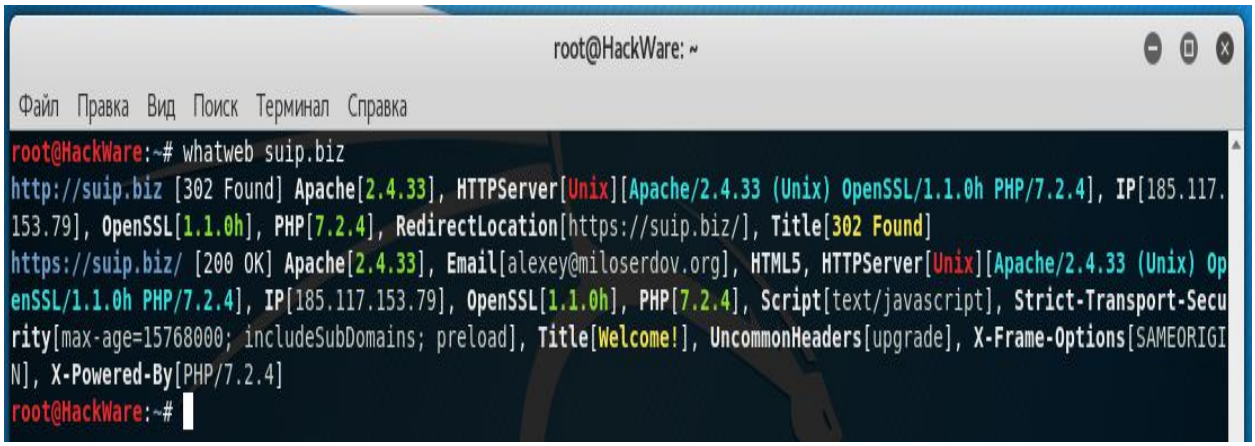


Рисунок 3.5 – Результат роботи WhatWeb

Проаналізуємо результат роботи WhatWeb. По-перше, видно, що зібрана інформація поділена на дві групи. Перша:

```
1 |http://suip.biz [302 Found] Apache[2.4.33], HTTPServer[Unix][Apache/2.4.33 (Unix) OpenSSL/1.1.0h PHP/7.2.4], IP[185.117.153.79], OpenSSL[1.1.0h], PHP[7.2.4], RedirectLocation[https://suip.biz/], Title[302 Found]
```

Друга:

```
1 https://suip.biz/ [200 OK] Apache[2.4.33], Email[alexey@miloserdov.org], HTML5, HTTPServer[Unix][Apache/2.4.33 (Unix) OpenSSL/1.1.0h PHP/ 7.2.4], IP[185.117.153.79], OpenSSL[1.1.0h], PHP[7.2.4], Script[text/javascript], Strict-Transport-Security[max-age=15768000; includeSubDomains; preload], Title[Welcome!], UncommonHeaders[upgrade], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/7.2.4]
```

На початку нам показаний просканований хост і протокол (http://suip.biz). Потім йде відповідь сервера [302 Found] – ця відповідь означає, що запитуваний документ доступний іншою адресою, тобто переміщений. Далі нам говориться, що хост працює з використанням веб-сервера Apache версії 2.4.33 на платформі Unix. У цьому використовується програма OpenSSL версії 1.1.0h, і навіть PHP версії 7.2.4. Нам показаний IP сервера – 185.117.153.79. Рядок RedirectLocation [https://suip.biz/] говорить про те, що відбувається редирект

(перенаправлення), у квадратних дужках вказана адреса, куди нас перекидає. У рядку Title[302 Found] вказано ім'я веб-сторінки.

WhatWeb самостійно переходить за вказаною для переадресації адресою (це можна змінити в налаштуваннях) і також збирає інформацію. З нових рядків у другій секції ми бачимо [200 OK] – це код сервера, який означає, що все гаразд і буде надіслано запитаний документ. На веб-сторінці виявлена адреса електронної пошти Email[alexey@miloserdov.org], також веб-сторінка використовує HTML5. На сторінці використовуються скрипти - text/javascript, а саме JavaScript, сервер надсилає заголовки Strict-Transport-Security[max-age=15768000; includeSubDomains; preload], X-Frame-Options[SAMEORIGIN], X-Powered-By[PHP/7.2.4], є нерозповсюджений заголовок upgrade. Заголовок сторінки "Welcome!". Також за допомогою WhatWeb можна дізнатися CMS (систему управління контентом), платформу сайту та зробити обхід систем виявлення вторгнень (IDS).

2) Використання Nmap для сканування відкритих портів та визначення запущених мережевих служб та їх версій.

Nmap ("Network Mapper") - це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Вона була розроблена для швидкого сканування великих мереж, хоча чудово справляється і з одиничними цілями.

Nmap використовує IP пакети оригінальними способами, щоб визначити які хости доступні в мережі, які служби (назва програми та версія) вони пропонують, які операційні системи (і версії ОС) вони використовують, які типи пакетних фільтрів/брандмауерів використовуються та ще дюжини інших характеристик. У той час як Nmap зазвичай використовується для перевірки безпеки, багато мережевих і системних адміністраторів знаходять її корисною для звичайних завдань, таких як контролювання структури мережі, управління розкладами запуску служб і облік часу роботи хоста або служби.

Ця програма з легкістю може відповісти на такі запитання:

- Що за комп'ютери працюють у вашій локальній мережі?
- 2. Які IP використовуються у локальній мережі?

- 3. Які порти відкриті на віддаленій машині?
- 4. Яка операційна система у цілі?
- 5. Які служби запущені на цільовій машині, яка версія?
- 6. Дізнатися, чи заражена система шкідливим кодом чи вірусом.
- 7. Пошук неавторизованих серверів або мережевих служб у вашій мережі.
- 8. Пошук та видалення комп'ютерів, які не відповідають мінімальному рівню безпеки організації.

Nmap має такі основні функції.

Сканування одиничної IP адреси:

```
1| nmap 192.168.1.1
```

Сканування хоста на ім'я:

```
1| nmap suip.biz
```

Сканування хоста на ім'я у вербальному режимі (більше інформації):

```
1| nmap -v suip.biz
```

Сканування множини IP адрес або підмережі (IPv4):

```
1| nmap 192.168.1.1 192.168.1.2 192.168.1.3
```

Робота з однотипними підмережами, наприклад, 192.168.1.0/24:

```
1| nmap 192.168.1.1,2,3
```

Також можна просканувати діапазон IP адрес:

```
1| nmap 192.168.1.1-20
```

Можна просканувати діапазон IP адрес, використовуючи символ підстановки:

```
1| nmap 192.168.1.*
```

Нарешті, можна просканувати всю підмережу:

```
1| nmap 192.168.1.0/24
```

Можна дізнатися, чи хост/мережа фаєрволом захищений:

```
1| nmap -sA 192.168.1.254
```

```
2| nmap -sA suip.biz
```

І зробити сканування хоста при захисті фаєрволом:

```
1| nmap -Pn 192.168.1.1
2| nmap -Pn suip.biz
```

Nmap також має багато інших можливостей.

3) Розширений пошук в Google.

Пошукові системи сканують інформацію та становлять пошукову видачу на основі своїх алгоритмів і навіть штучного інтелекту. Це означає, що пошукова машина могла просканувати мережу, сайт або окремі сторінки не через те, що їй хтось це дозволив, а просто через те, що вона змогла туди дістатися. Тепер пошукові машини не чекають, що їм хтось розповість про нові сторінки – вони активно їх шукають самі і добираються до найдальших куточків всесвітньої мережі та до нетрі веб-сайтів. При цьому пошукові системи виходять із принципу: «все, що не заборонено, є дозволеним для аналізу». Іноді навіть сканують те, що явно закрито від індексування. Пошукові системи не лише шукають посилання на нові сайти та сторінки з раніше просканованих сайтів – так було раніше. Тепер вони отримують інформацію з кількох, мабуть, не зовсім прозорих джерел. Мабуть, тепер Google може дізнатися про сторінку, навіть якщо ви її просто відкрили в браузері. А якщо на цій сторінці є посилання на інші розділи, то все це буде просканово та розміщено у загальнодоступному індексі.

Майстерне володіння пошуком Гугла - це інструмент, який корисний і звичайним користувачам, які бажають використовувати потужність цієї пошукової системи для точного отримання того, що вони шукають; і для тих, хто займається розслідуваннями на основі відкритих джерел; і навіть для хакерів, які хочуть зібрати інформацію про сайт, що атакується, або знайти вразливі цілі. Більшість операторів можна використовувати в одному запиті у поєднанні з іншими. Можна різноманітним чином групувати елементи запиту та за допомогою дужок та логічних операторів створювати дуже точні запити, які дозволяють, з одного боку, знайти необхідні сторінки, та при цьому

виключити зайві дані. Використовуючи оператори, можна відфільтрувати документи з певним вмістом або які мають певні слова в заголовку або тексті, знайти чутливу інформацію, наприклад, конфігураційні файли та документи з паролями, а також просто – дуже майстерно користуватися пошуком – гуглити як професіонал.

Розширені можливості пошуку в Google включають в себе такі елементи: пошук по одному слову, уточнений пошук, примусове логічне АБО (пошук будь-якого слова або фрази), угруповання слів пошуку за допомогою дужок, виняток певних слів, виключення кількох слів з пошуку, виключення точної фрази , пошук слів поруч один з одним, пошук фраз, що стоять поруч, пошук по певному сайту, пошук вмісту за певними доменами верхнього рівня, пошук матеріалу на декількох доменах верхнього рівня, пошук по синонімах і зразковим значенням, використання точного збігу для блокування синонімів, точне збіг одного слова, пошук тільки за текстом сторінки та багато іншого. Окреме місце для нас займає пошук у Google для хакерів. Google дозволяє аналізувати цільовий сайт, навіть не роблячи на нього запити. Через Google можна знайти вразливі сайти, а також чутливу інформацію.

4) Створення дзеркал сайтів, клонування сторінки входу з HTTrack.

З програмою HTTrack ми можемо створити копію сайту на диску. Програма доступна всім популярним платформам.

У плані пентестингу HTTrack може бути корисним для:

• дослідження структури сайту (підкаталоги, сторінки сайту);

• пошук файлів на сайті (документи, зображення);

• пошук за документами та метаданими файлами з сайту;

• клонування сторінок входу з метою подальшого використання для фітингу.

Думаю, немає потреби пояснювати, навіщо пентестер може знадобитися клон сторінки входу. При цьому слід враховувати таке:

• у сайту можуть бути різні сторінки для входу з мобільного пристрою та для входу з комп'ютера;

• адреса сторінок для входу з мобільного пристрою та з комп'ютера може бути однаковою;

• нам не потрібно клонувати весь сайт – достатньо лише однієї сторінки.

5) Масовий пошук геотегів на сайтах та в локальному сховищі.

На етапі розвідки, а також при криміналістичному дослідженні метадані – це дуже хороше джерело інформації. При цьому потрібно розуміти та оцінювати ризик фальшування даних, оскільки ця інформація може бути легко підмінена.

Слід звернути увагу на дослідження метаінформації на такі можливості:

• Як переглянути або редагувати метадані pdf або зображення з командного рядка Linux.

• Як видалити метадані файлу на Linux.

• Insiderer (потужна програма із вилучення всієї можливої метаінформації).

• Mat (набір інструментів аналізу/видалення метаданих).

• Геолокація фотографій по GPS мітках у метаданих (онлайн сервіс).

• Mat2: нова версія програми для видалення метаданих.

Геотеги – це метаінформація, отримана від GPS датчика про географічні координати, де зроблено фотографію. Вони можуть сприяти:

• масовий пошук GPS інформації у фотографіях на локальному диску;

• пошуку інформації GPS у фотографіях на сайтах.

6) Використання наступальної платформи дослідження веб-додатках TIDoS-Framework.

Програма TIDoS-Framework є платформою для автоматизації збору інформації та пошуку вразливостей у веб-додатках. Це не типовий універсальний сканер, це швидше інструмент для автоматизації отримання інформації про веб-сайт та веб-сервер. Тобто, це асистент для ручного дослідження веб-ресурсу. Багато завдань викликаються вибором опції в текстовому меню. Введення потрібно при запуску програми – для цього вказуємо ім'я сайту, що цікавить нас, також введення з боку користувача

потрібно при аналізі деяких вразливостей. TIDoS-Framework - це (ще одна) програма, яка зібрала різні техніки збору інформації та сканування. Серед функцій збору інформації є дуже цікаві, що не часто зустрічаються в інших фреймворках. Ручне сканування, на мій погляд, поступається просунутим комбайнам з пошуку вразливостей, але саме такий «точковий» формат може бути цікавим для більш просунутих користувачів, які знають який параметр/URI треба вказати.

7) badKarma: Просунутий набір інструментів для розвідки.

Пошук вразливостей на хості (хостом може бути веб-сайт, веб-сервер, мережевий пристрій (роутер та інші), комп'ютер кінцевого користувача) починається зі збору базової інформації. Ця інформація включає виявлення хостів (якщо ми досліджуємо підмережу), сканування їх портів для пошуку відкритих, визначення запущених служб на цих портах. Визначення версій служб і пошук вразливостей для даних версій, перевірка на використання слабких паролів (брут-форс), запуск додаткових сканувань різними інструментами залежно від виявлених мережевих служб. Зазвичай це досить типовий набір дій, який варіює від виявлених на хості запущених мережевих служб. Тому вже є різні інструменти автоматизації, які можуть просканувати діапазон мережі та, наприклад, запустити брут-форс знайдених служб. У badKarma графічний інтерфейс, в якому достатньо клацати мишкою - вводити команди необов'язково (хоча їх можна підправити для тонкого налаштування). badKarma в цілому цікава програма-помічник, за допомогою якої можна швидше виконувати рутинні дії і тримати отримані результати в одному місці, зручному для візуального сприйняття. badKarma є модульною програмою, і ви можете додати свій власний модуль.

### 3.2.2 Дослідження периметра

1) Пошук субдоменів та отримання даних мережі з Amass.

Субдоменами називають домени третього, четвертого та наступних рівнів. Візьмемо як приклад сайт kali.tools. Його субдомен (домен третього рівня) є en.kali.tools. Загальний вигляд субдоменів третього рівня сайту *.kali.tools. Домени можуть бути четвертого test.en.kali.tools, exp.en.kali.tools і наступних рівнів. Субдомени та підпапки це не одне й те саме. Приклад підпапки для kali.tools це kali.tools/all. І на субдоменах, і в підпапках можуть міститися різні файли веб-програми, встановлені різні системи управління контентом, там можуть бути два абсолютно різних сайти. Відмінність субдомену від підпапки в тому, що для субдомену сервер імен DNS може містити запис. Тобто для кожного домену DNS сервер має запис, в якому ім'я домену (kali.tools) зіставлено з адресою IP. Так от, DNS сервер може мати такі записи і для субдоменів. І адреси IP для субдоменів можна вказувати різні. Це означає, наприклад, що kali.tools може бути розміщений на одному сервері, en.kali.tools — розміщено на іншому, а test.en.kali.tools знову ж таки іншому сервері і навіть у іншій країні. Пошук субдоменів є важливою частиною початкового етапу пентестингу, на якому збирається інформація про цільовий сайт/хост/мережа. Оскільки знання інших субдоменів дозволяє розширити периметр для атаки, або отримати уявлення про структуру мережі, організації.

Техніки пошуку субдоменів умовно поділяються на пасивні та активні. Під час пасивного пошуку дані запитуються на сервісах, які збирають цю інформацію — таких сервісів досить багато. Дані також можуть збиратися з інформації про видані сертифікати, шукатися у видачі пошукових систем (просунутий пошук з Google), сюди ж можна віднести техніку зворотного DNS (визначається IP сайту, для цього сайту на сервісах шукаються списки хостів, з цих списків відфільтровуються субдомени цільового хоста ) і т.д.

До активних можна зарахувати брут-форс. Причому це може бути як брут-форс подібний пошуку прихованих файлів - тобто робляться HTTP запити до сайту і якщо повернутий код статусу 200 (припустимо для en.kali.tools) значить такий субдомен є, а якщо повернутий код статусу 404 (наприклад для ch.kali.tools) значить такого хоста немає. Насправді такий брут-форс

застосовується нечасто. Набагато зручніше (і швидше) робити запити до серверів DNS і на основі їх відповідей визначати, чи існує субдомен. Але перший варіант іноді є єдиним можливим у тому випадку, якщо субдомени розміщені на одному IP адресі, а DNS запису вказаний підстановковий символ.

Головне призначення Amass – це пошук субдоменів. Особливість Amass (а подібних інструментів та онлайн-сервісів дуже багато) в тому, що вона зібрала в собі велику кількість різних технік і задіює багато сервісів для отримання даних, а також вміє брут-форсувати субдомени. Програма є кросплатформною – працює у тому числі і на Windows, Linux.

2) Визначення всіх сайтів на одному IP та в одній підмережі.

Веб-сервер може обслуговувати один або більше віртуальних хостів. Отже, на одному IP можуть розміщуватися відразу кілька сайтів. Інформація про сайти на одному IP може бути цікавою як просто якими ще сайтами/проектами займається даний веб-майстер, або під час пентестингу – при початковому зборі інформації для розширення площі атаки. Оскільки різні веб-програми можуть використовувати різноманітне програмне забезпечення, то якщо не вдалося знайти пролом у вразливості одного з сайтів, то варто спробувати успіх з іншим на цьому ж сервері. Як кажуть, «міцність всього ланцюга визначається міцністю найслабшої ланки» - це можна застосувати в даній ситуації.

Оскільки при компрометації веб-сайту, який хоч і не є метою, але розташований на тому ж сервері, що і цільовий сайт, є можливість скомпрометувати весь сервер, або полегшити атаку на цільовий сайт. Можливість знайти сайти на одному IP надають різні сервіси, які як база даних використовують великий обсяг статистичної інформації. Це означає що:

• різні послуги можуть надати інформацію різного обсягу (залежно від повноти накопичених даних);

• дані можуть бути неактуальними (частково або повністю);

• інформація може бути неповною.

Iptodomain, використовуючи архів історичної інформації з Virustotal, дозволяє нам вилучати домени з IP діапазону та зберігати їх у файл. Це корисно, якщо ви хочете дізнатися, які домени прикріплені до цієї IP-адреси. Програма працює з діапазонами IP та не підтримує введення безпосередньо імені хоста (доменного імені). Тому алгоритм роботи наступний:

• дізнаємось IP цікавого сайту;

• вказуємо як початковий і кінцевий IP діапазон один і той же адресу.

Якщо для якогось IP ми знайшли дуже велику кількість сайтів, то, ймовірно, ця IP-адреса може належати хостинг-провайдеру, який надає послуги віртуального хостингу. У цих випадках на одному IP може бути сотні і навіть тисячі веб-сайтів.

3) Аудит безпеки хостингу та інших спільно використовуваних систем на Linux.

Linux – операційна система, розрахована на багато користувачів. Це означає, що в одній операційній системі може бути створено кілька облікових записів користувачів, і що з неї можуть одночасно працювати кілька користувачів. Найбільш типовим прикладом розрахованого на багато користувачів використання Linux, є віртуальний хостинг. Англійською вона називається shared hosting, тобто спільний хостинг. Якщо ви не веб-майстер і думаєте, що ніколи не стикалися із спільним хостингом, ви помиляйтеся.

Віртуальний хостинг працює так: кожному клієнту хостера на сервері виділяється його власна папка. У цій папці веб-майстер розміщує свої сайти – один або кілька. До цих папок веб-майстри мають FTP доступ або доступ через файловий менеджер з веб-інтерфейсом. Багато хостингів в даний час надають також доступ по SSH (відразу або на запит). За задумом, кожен веб-майстр має доступ тільки до своєї папки: возиться там, щось робить, розміщує сайти і так далі. Спільне використання одного «залізного» комп'ютера дуже економічне та зручне. Такий підхід може бути реалізований на комп'ютерах в громадських місцях, в організаціях, навіть ви вдома можете налаштувати роботу в ОС таким способом.

Той же сервер (якщо він досить потужний) може обслуговувати сотні клієнтів і хостити (розміщувати на собі) одночасно тисячі сайтів. І якщо на домашньому комп'ютері питання безпеки не стоять гостро (хоча нікому не приємно, якщо хтось лазить по його особистих папках), то в корпораціях і спільному хостингу це набагато важливіше: можливість «зазирнути» в чужу папку може означати розголошення конфіденційної інформації. А якщо хтось отримав доступ до папки з сайтами, це означає компрометацію, витік паролів, небезпека зараженням веб-ресурсу шкідливим програмним забезпеченням та інші негативні наслідки. Для когось це може стати сюрпризом, бо так як погано налаштованих хостингів вистачає. Для виконання аудиту хостингу можна скористатися, наприклад, програмою LinEnum. Ця програма призначена для перевірки розрахованих на багато користувачів систем на предмет неправильного налаштування та можливості підвищення привілеїв.

4) Визначення реальності IP сайту за допомогою Cloudflare.

Cloudflare – це прокладка між користувачем та сайтом. Вона працює за принципом зворотного проксі, надаючи додаткові послуги, у тому числі кешування сторінок, захист від DDoS, захист від поганих роботів та інше. У тому числі, Cloudflare приховує справжню IP адресу сервера, на якому розміщено сайт. Cloudflare використовує свої сервери імен, що відповідають на DNS запити та перетворюють ім'я хоста на IP адресу.

Тобто, власник сайту налаштовує для свого домену використання NS серверів Cloudflare, ці NS сервери у відповіді на DNS запити надсилають IP, що належить мережі Cloudflare. В результаті запит до сайту надходить на Cloudflare, яка отримує сторінку з сервера, де розміщено сайт (або зі свого кеша) і показує цю сторінку користувачеві, який її запитав. В результаті справжня IP адреса сайту за Cloudflare стає добре прихованою. Якщо Cloudflare налаштована правильно, то справжня IP адреса сайту ніколи не розкривається і не записується будь-куди. Але скільки знаєте людей, які все завжди роблять правильно? З цієї причини існують інструменти, що шукають прорізи в налаштуваннях Cloudflare. Однією з таких програм є CloudFail.

Кожен сайт може мати піддомен виду *.сайт.ua. Де замість зірочки можуть бути підставлені різні значення, наприклад:

• www.сайт.ua

• en.сайт.ua

• forum.сайт.ua

• test.сайт.ua

• admin.сайт.ua

• 111.сайт.ua

• chat.сайт.ua

Таких піддоменів може бути необмежену кількість. Важливий момент: кожен такий піддомен може мати свою IP адресу. Тобто, сервери імен дозволяють вказати IP (або відразу кілька адрес) для сайту.ua, інший IP для test.сайт.ua, інший IP для en.сайт.ua і так далі. Може виникнути ситуація, коли в DNS записах домену сайт.ua прописана IP-адреса Cloudflare, але DNS записи для піддомену test.сайт.ua вказують на інший IP, що не знаходиться під захистом Cloudflare. В результаті розкривається IP адреса, яка:

• може виявитися справжньою IP адресою сайту;

• є IP адресою лише субдомену, але дає нам інформацію про власника або підказку для подальших досліджень.

Ми не можемо просто отримати список усіх субдоменів. Тому необхідно перебирати різні варіанти. Саме це і реалізовано у CloudFail:

• пробуються різні варіанти субдоменів;

• якщо для субдомену існує DNS запис, то для неї отримуємо IP;

• перевіряється, чи входить отриманий IP в діапазон Cloudflare (тобто захищений за допомогою Cloudflare чи ні).

Насправді описаний процес є вже третьою стадією. На першій стадії CloudFail отримує список можливих субдоменів від DNSDumpster.com та перевіряє їх. На другому етапі CloudFail звертається до сервісу CrimeFlare, який зібрав велику базу IP адрес для сайтів, захищений за допомогою Cloudflare. Якщо для сайту відомий IP, він відразу показується. І на третьому етапі

виконується описаний брут-форс субдоменів за словником. В результаті такого комплексного підходу досить часто вдається знайти адреси IP, не захищені Cloudflare. Важливо відзначити, що ми виходимо з припущення коли IP-адреси піддоменів належать або пов'язані з власником основного сайту. Зазвичай це так, але завжди потрібно пам'ятати, що в DNS запису піддоменів власник основного домену може вказати будь-які IP адреси, що навіть не належать йому.

5) Збір інформації про власника сайту. Пошук сайтів однієї особи.

Якщо хтось під час реєстрації домену в якості імені вказав «Слава Україні» або сховався за CloudFlare, це не означає, що його не можна ідентифікувати. Пошук власника сайту, який не хоче представитися, зазвичай полягає у пошуку фрагментів інформації, яка дозволяє його ідентифікувати за іншими джерелами. Наприклад, на сайті «аноніма» (або в SOA запису DNS) знайдено e-mail, а занурення цієї адреси привело на сайт з оголошеннями про пошук співробітників. Це оголошення може містити ПІБ, телефон, місто, додаткову інформацію по особі, що цікавить. Пошук додаткових підтверджень, у тому числі занурення за щойно знайденим номером телефону, – і «справу» можна вважати розкритим (власник сайту ідентифікований). Зовсім безладні аноніми швидко закінчуються, тому залишаються найхитріші, які не залишають таких явних зачіпок. Завдання отримує додатковий етап – намагаючись знайти інші сайти невідомої особи, і вже на цих сайтах знайти зачіпки для ідентифікації особи.

Під час пошуку сайтів одного веб-майстра ми виходимо з наступного:

• іноді власник кількох сайтів розміщує їх на одному сервері. Тобто, для пошуку інших сайтів нам потрібно дізнатися IP сервера, де розміщено сайт і знайти всі сайти на одній IP адресі;

• власник сайту часто використовує унікальні ідентифікатори, що не змінюються на різних сайтах. Це можуть бути фрагменти коду партнерських мереж (наприклад, унікальний для кожного облікового запису індикатор

міститься в коді виклику оголошень Google, AdSense, eBay), лічильники (наприклад, Google Analytics) та інше;

• веб-майстри мають тенденцію використовувати однакові технології на різних серверах, іноді сайти завантажують ресурси (зображення, файли CSS стилів, JavaScript бібліотеки) з інших сайтів цього веб-майстра, або мають взаємні URL посилання.

Для досягнення результату використовуються наступні прийоми та інструменти: пошук сайтів на одному IP, пошукова система за вихідним кодом, визначення справжнього IP сайту за Cloudflare, пошук сайтів одного облікового запису, що ховаються за CloudFlare, експлуатація неправильного настроювання DNS для виявлення справжнього IP сайту за Cloudflare та інші методи.

6) Масовий збір докладних відомостей про хости у великих мережах за допомогою нових програм для сканування.

Розглянута вище програма nmap чудово підходить для збору інформації про один хост або про невелику підмережу. Якщо говоримо про великі мережі, то швидкість nmap досить низька, та й обробляти отримані дані незручно.

Останнім часом з'явилося багато цікавих програм для сканування мереж із різними цікавими функціями. Наприклад, Masscan дозволяє проводити сканування з приголомшливою швидкістю. Якщо встановити відповідний драйвер і якщо ваше Інтернет з'єднання дозволить, то величезні мережі можна сканувати за лічені хвилини! При написанні коду автор насамперед виходив зі швидкості генерування пакетів для відправки. Крім цього, Masscan має іншу відмінну новацію. Як працюють популярні сканери, якщо вказати діапазон адрес? Вони будуть сканувати послідовно IP через IP. В цей час якісь мережі зазнають значного навантаження, а інші мережі просто «чекають», поки до них дійде черга. Masscan перемішує всі IP з переданого йому діапазону і випадково сканує їх - в результаті навантаження на мережі балансується. Masscan має неймовірно простий, але при цьому добре працюючий механізм організації розподіленого сканування.

Програма flashlight є інтелектуальною оболонкою для nmap, вона може прискорювати процес сканування (за рахунок одночасного запуску багатьох екземплярів nmap), вона досить зручно зберігає отримані результати, вміє масово збирати скріншоти. Взагалі, програма flashlight підтримує 3 типи сканування, збір скріншотів – це лише один із них. У цьому ряді нових програм особливо хочеться відзначити IVRE. Програма має хороший обробник зібраних даних, є навіть графічний інтерфейс (веб-інтерфейс). Вона збирає дуже докладну інформацію про всіх хостів. Програма чудово підтримує багатопоточність, а також підтримує розподілене сканування.

### 3.2.3 Пошук чутливої інформації, початковий аналіз веб-програми

1) Приховані директорії та файли як джерело чутливої інформації про веб-додаток.

Приховані директорії та файли, які випадково залишаються на веб-сервері, можуть стати дуже цінним джерелом чутливої інформації. У кореневій папці веб-програми може бути безліч прихованої інформації: файли та папки системи управління версіями вихідного коду (.git, .gitignore, .svn), конфігураційні файли проекту (.npmrc, package.json, .htaccess), файли конфігурацій користувача з популярними розширеннями, такими як config.json, config.yml, config.xml та багато іншого.

Загалом ці джерела можуть бути поділені на кілька загальних категорій:

• Системи керування версіями вихідного коду.

• Конфігураційні файли проекту, які створює IDE (інтегроване середовище розробки – зазвичай це редактор вихідного коду з розширеними функціями).

• Специфічні конфігураційні файли та налаштування для цього проекту або технології.

Давайте подивимося на них уважніше — де їх шукати і на яку інформацію чекати від них.

Системи керування вихідним кодом Git.

Git – це безкоштовна та з відкритим вихідним кодом розподілена система контролю версій, створена для швидкої та ефективної роботи з будь-якими проектами від маленьких до дуже великих. З GitHub.com зараз одна з найпопулярніших систем контролю версія коду, особливо у світі відкритого вихідного коду. Багато компаній використовують їх власні установки GitLab, а також GitHub Enterprise або Bitbucket.

Базова інформація про Git проекти.

Щойно створений Git репозиторій містить кілька стандартних папок та файлів, де зберігатиметься вся інформація. Це приклад папки .git в яку вже було зроблено один commit (цим словом називають будь-яка зміна в проекті, наприклад, зміна вихідного коду будь-якого файлу, створення нового файлу, видалення рядків із файлів або файлу повністю та інше).

Погляньмо на це з погляду атакуючого. Вміст репозиторію Git записано в об'єкти. Усі вони зберігаються у папці .git/objects. Об'єкти можуть бути одного з трьох типів: commit, tree та blob.

Commit — це інформація про коміти з поточним Tree (деревом, тобто структурою папок та файлів) хешей об'єктів.

Tree (дерево) містить інформацію про структуру папок та файлів - і кожна папка або файл має свій власний хеш об'єкт, що зберігається в об'єкті дерева. Це може бути інше дерево (папки, які на один рівень нижче в структурі папок) або файл.

Blob — це тип об'єкта Git, де зберігатиметься вміст файлів. Якщо ви знаєте хеш певного файлу, ми можемо прочитати його вміст, використовуючи команду git cat-file.

Якщо ми знайшли папку .git на веб-сервері, тоді є простий спосіб отримати вміст будь-якого файлу з неї, просто завантажуючи та читаючи об'єкти Git. Іноді, якщо нам пощастило, можна спробувати клонувати репозиторій, використовуючи стандартну команду git clone або просто запустимо команду wget з встановленою опцією -r для рекурсивного

завантаження всієї папки .git. Але це завжди можливо з кількох причин (такі як відсутність необхідних облікових даних чи відсутність команди wget). Припустимо, що всі ці опції неможливі.

Щоб переконатися, що папка .git доступна, просто перевіримо, чи отримаємо ми відповідь HTTP 403 (або щось схоже, головне, щоб це не був код відповіді 404, оскільки він означає, що на цьому сервері або в цьому розташуванні немає папки .git ):

Відповідь 403 говорить про існування папки .git на цьому сервері:


Рисунок 3.6 –Відповідь 403 про існування папки

2) Пошук адмінок (панелей управління) на сайтах.

Адреса адміністративної панелі потрібно знати для введення до неї здобутих облікових даних. Також відмічено, що «внутрішнім» вузлам веб-сайтів, які не призначені для широкого кола відвідувачів, деякі програмісти приділяють менше уваги, там може виявитися, наприклад, уразливість SQL-ін'єкція. Пошук адміністративних панелей – це нескладне завдання, цим можна займатися, вводячи в адресний рядок браузера різні можливі шляхи до сторінки входу в панель. Є досить багато різноманітних утиліт, що дозволяють автоматизувати та прискорити цей процес.

Якщо ми віддаємо перевагу кросплатформенній програмі з графічним інтерфейсом, то для пошуку входу в панелі управління можна скористатися

jSQL Injection. Програма має інструмент, який називається "Пошук адміністративної папки", він розташований на відповідній вкладці програми:

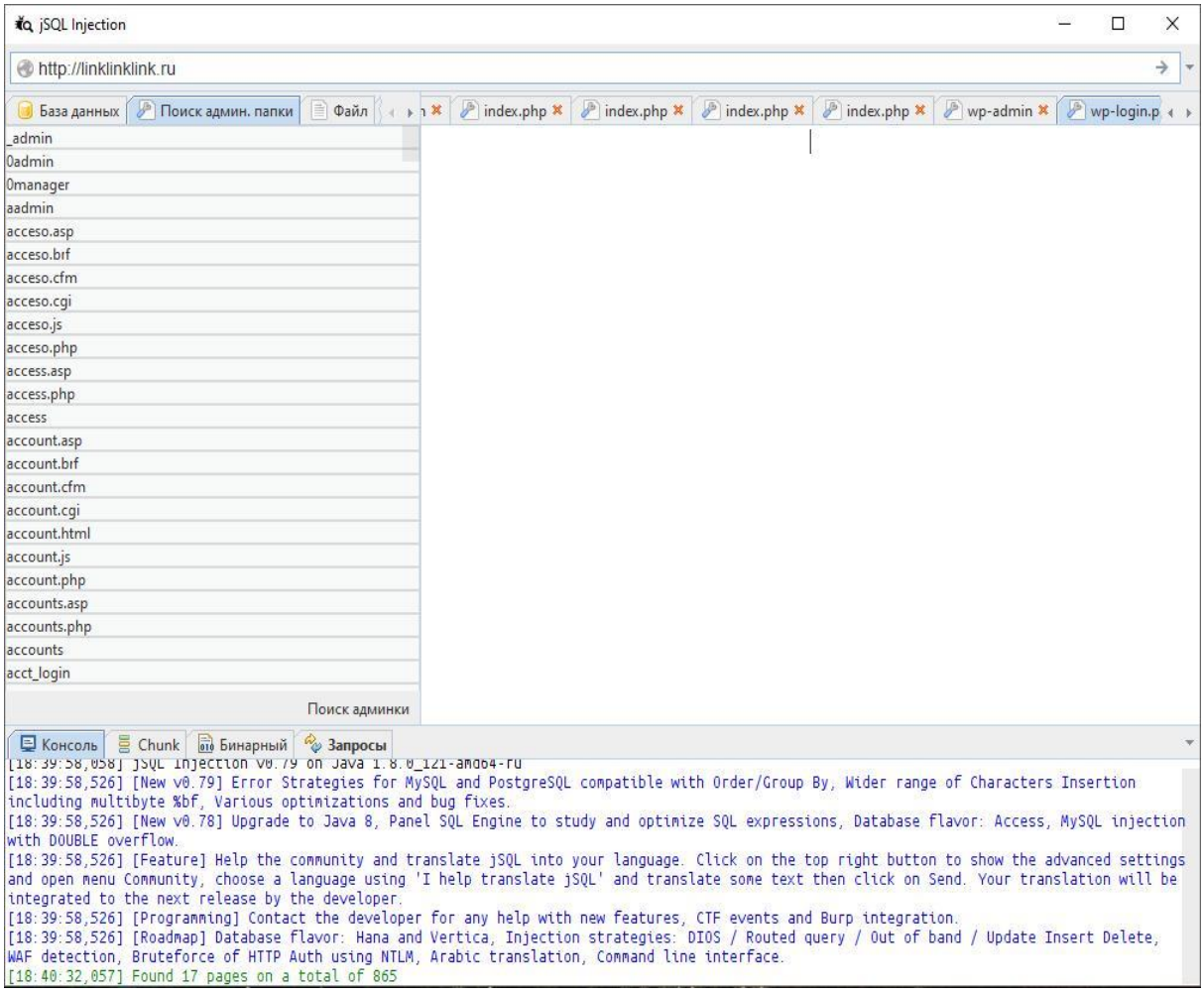


Рисунок 3.7 –Пошук адміністративної папки

У програму вже завантажено досить великий список адрес сторінок, за якими найчастіше розташовуються адмінки. Ми можемо редагувати цей список: додати нові значення або завантажити їх із файлу.

3) Статичний аналіз вихідного коду веб-сайту у браузері.

Будь-який сучасний веб-браузер має набір вбудованих інструментів розробника. Для їх увімкнення ми можемо використовувати **Ctrl+Shift+I**, **CMD+Option+I** (macOS), кнопку **F12** або просто знайдемо потрібну опцію в меню браузера — це залежить від операційної системи та браузера, які ми використовуємо. Якщо у нас є веб-браузер, значить у нас вже є Інструменти розробника. Інший інструмент, який непогано було мати встановленим, це IDE (інтегроване середовище розробки) або будь-який редактор коду з

підсвічуванням синтаксису HTML та JavaScript. Все залежить від наших переваг, ми можемо вибрати Visual Studio Code. Повністю безкоштовна, з відкритим вихідним кодом IDE – це NetBeans, підтримує кілька мов програмування, зокрема підсвічування синтаксису HTML та JavaScript. Інтерпретатор Python – це наступна обов'язкова для нас річ. NodeJS дуже корисний для запуску та тестування коду JavaScript в терміналі (цього ж ми можемо досягти використовуючи браузер). Python корисний для створення власних скриптів. Якщо ви краще знайомі з іншою мовою, що інтерпретується (Ruby, PHP, Perl, Bash і так далі), ви також можете використовувати їх за своїм бажанням. Дослідження: вихідного коду HTML, Кукіз та Сховища браузера, JavaScript дозволять знайти безліч цінної інформації. Веб-браузер це дуже потужний інструмент. Іноді це єдиний інструмент, який потрібен для читання вихідного коду та повного розуміння, як працює програми та ідентифікації його слабкостей.

4) Аналіз динамічно генерованих сайтів за допомогою JavaScript та сайтів з підвантажуваним контентом.

JavaScript, а також численні допоміжні бібліотеки та фреймворки (платформи) дозволяють створювати дивовижні інтерактивні сайти. При цьому вихідний код може містити мінімум елементів. Насправді, цілком реально зробити веб-сторінку у вихідному коді якої в <body> не буде нічого, крім одного підключеного JavaScript файлу, але яка в веб-браузері може показувати цілий портал з відеороликами, картинками, записами, що нескінченно підвантажуються і так далі. При цьому ця сторінка в динамічному стані може мати дуже об'ємний і складний DOM. Спрощено кажучи, про DOM можна думати як про HTML вміст сайту, який сформований у процесі виконання. Кінцевий DOM може бути таким самим як вихідний код — у випадках, якщо не використовується JavaScript для додавання та видалення елементів у процесі роботи веб сторінки, а може кардинально відрізнятися від вихідного HTML коду.

Для багатьох сучасних програм, що активно використовують JavaScript і численні фреймворки, стало дуже важко і майже марно аналізувати вихідний HTML код, оскільки основна функціональність для них перенесена в код JavaScript, який часто ще й «стиснутий» внаслідок чого виглядає нечитаним. З цієї ситуації можна вийти за допомогою Burp Suite або подібних програм, які аналізують запити і отримані відповіді. Але в веб-браузері вбудовані не менш потужні інструменти аналізу запитів. Причому веб-браузер має навіть свої переваги:

• ми працюємо з конкретною сторінкою у конкретній вкладц;

• робота з сайтами на HTTPS нічим не відрізняється від роботи з сайтами на HTTP;

• не потрібно додаткових програм — потрібен лише браузер;

• безліч додаткових можливостей у вигляді відладчика JavaScript;

• множина інформації, наприклад, згрупована за доменними іменами активність конкретної вкладки сторінки.

Інструменти розробника дуже корисні для пентестера, що оцінює безпеку або досліджує веб-сайти та веб-додатки.

### 3.3 Сканування вразливостей веб-додатів (2 крок )

#### 3.3.1 IronWASP: безкоштовний сканер уразливостей веб-сайтів під Windows із графічним інтерфейсом

IronWASP — це безкоштовна програма з відкритим вихідним кодом для сканування безпеки веб-програм. Її автором є Lavakumar Kuppan. Сам автор не соромиться і називає свій автоматичний інструмент пошуку проблем з безпекою на веб-сайтах: «Одним з кращих у Світі сканерів безпеки веб-сайтів і веб-додатків». Найбільшою його особливістю є те, що написано спеціально під Windows. Він абсолютно безкоштовний, у нього відкритий вихідний код,

програма відкрита для додавання нових плагінів та модулів. Інші ключові особливості IronWASP ви знайдете у картці програми IronWASP.

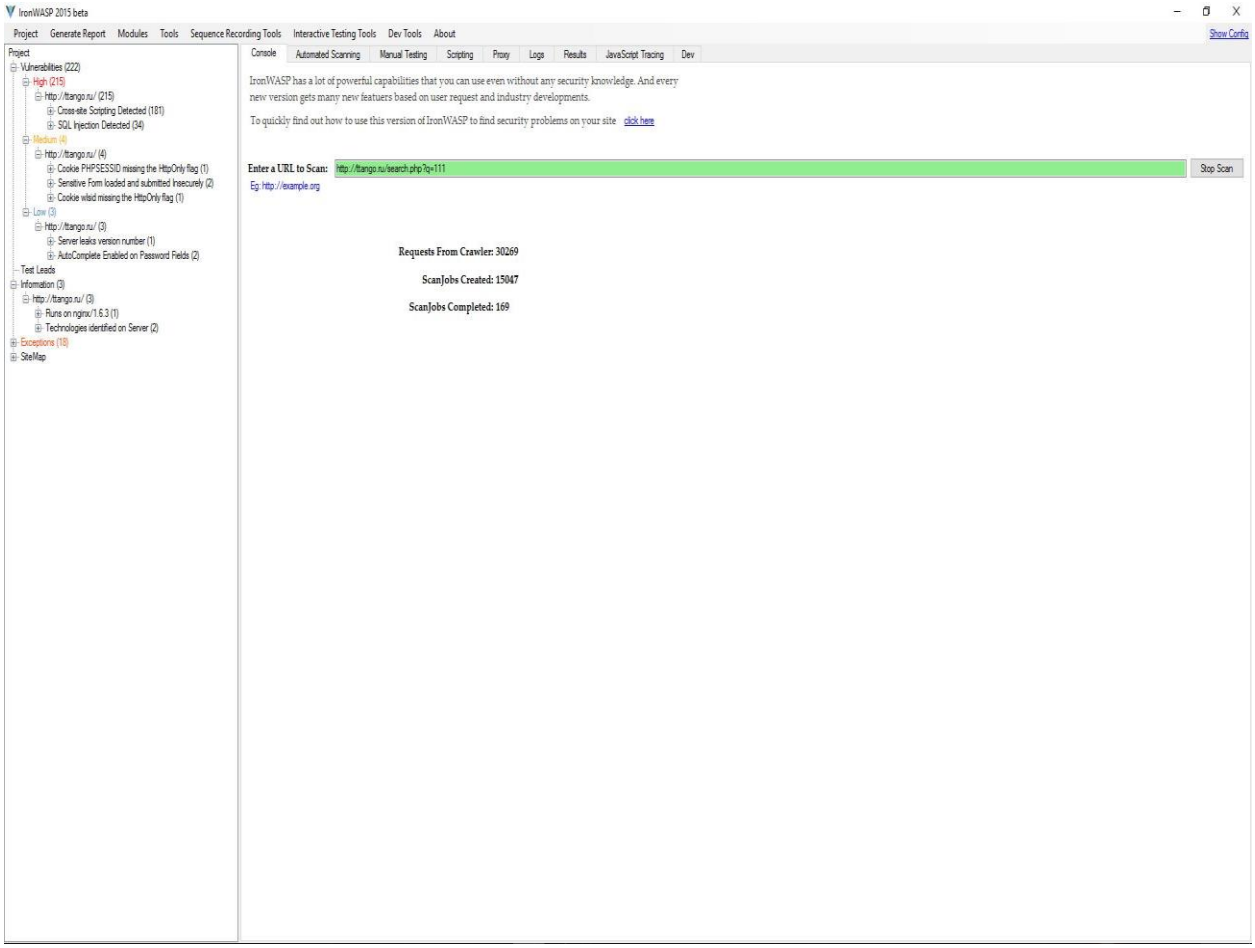


Рисунок 3.8 –Картка програми IronWASP

1) Завантаження та перший запуск IronWASP.

Сторінка програми: http://ironwasp.org/index.html

Сторінка для скачування: http://ironwasp.org/download.html

Після завантаження розраховуємо файл, запустимо IronWASP.exe. Невелике попередження: при скануванні програма зберігає величезну кількість балок, розмір яких може розтягнутися на гігабайти, тому перемістимо папку з програмою на диск з достатньою кількістю місця. До речі, програма є портативною, тобто не вимагає установки.

Якщо ми хочемо одночасно сканувати 2 і більше сайтів, необхідно зробіть кілька папок з програмою і кожну з них запускаємо окремо для певного сайту. При кожному запуску ми бачимо таке вікно:

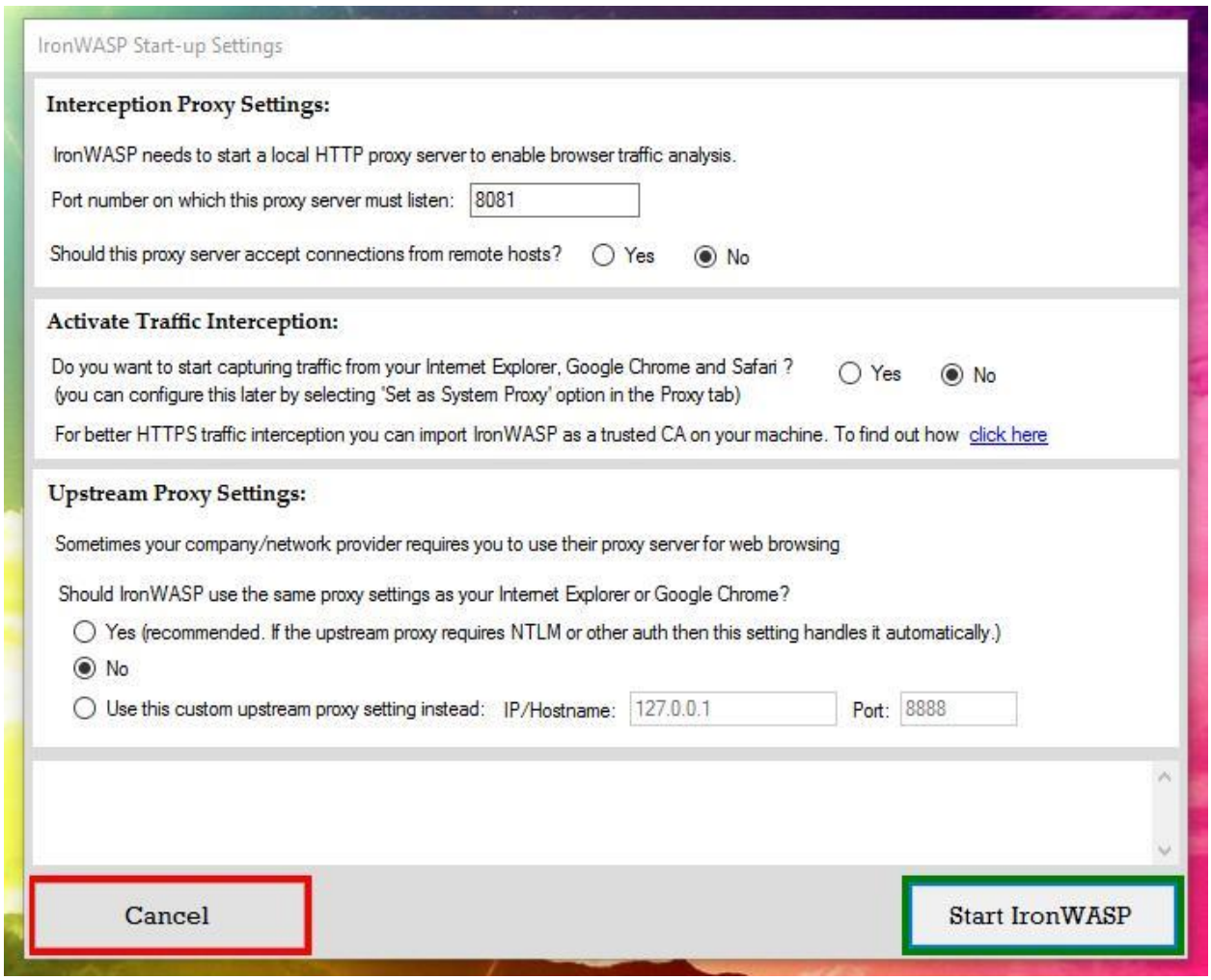


Рисунок 3.9 –Процес сканування сайта

IronWASP необхідний локальний HTTP проксі-сервер, щоб вона змогла аналізувати веб-трафік. Ми можемо змінити порт, встановити, чи може наш проксі сервер приймати підключення з віддалених хостів, включити або відключити активне підслуховування трафіку з веб-браузерів, встановити налаштування вищого проксі (якщо ми хочемо приховати свій реальний IP). За замовчуванням можна залишити всі налаштування — для аналізу веб-сайтів вони підходять. Якщо ви одночасно запускаєте кілька копій IronWASP для паралельного сканування кількох веб-сайтів, для кожного екземпляра IronWASP можна задати свій власний порт HTTP проксі.

2) Аналіз сайтів із IronWASP

Ось так виглядає головне вікно програми ( вже введена адреса сайту для сканування):

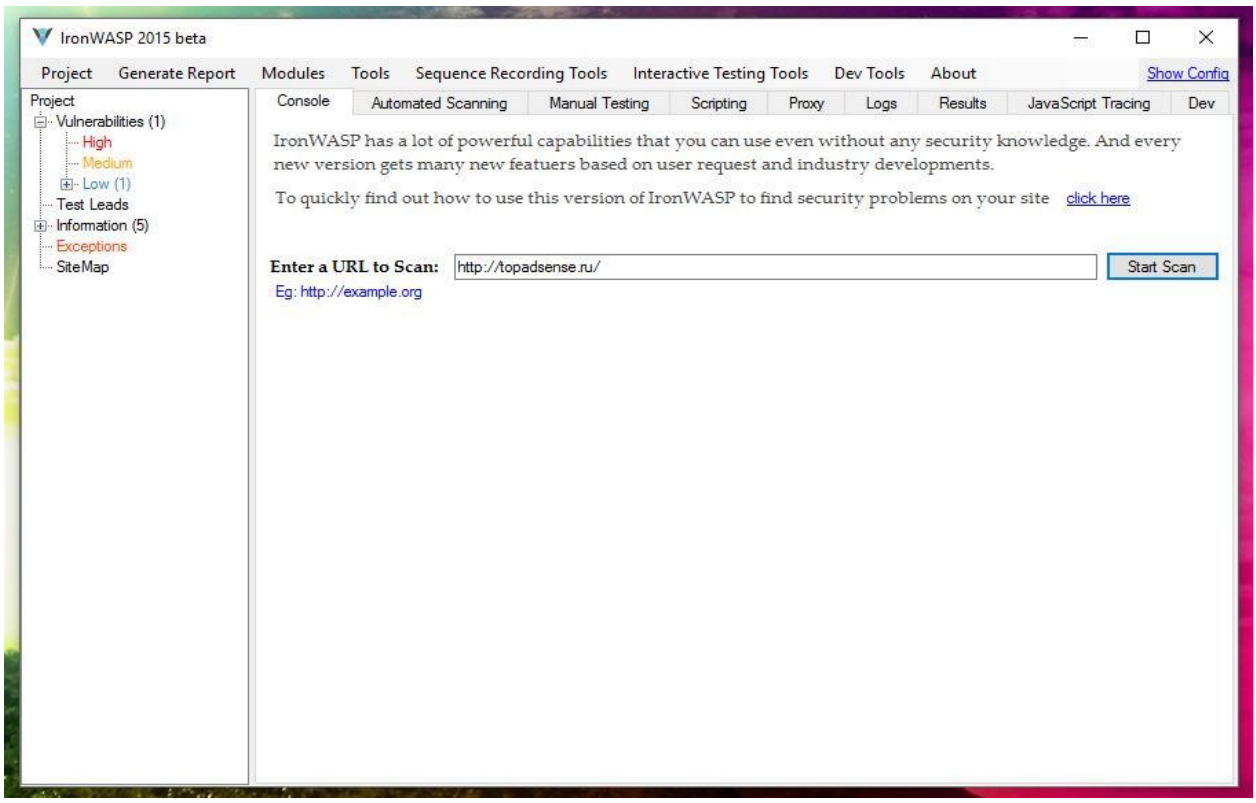


Рисунок 3.10 –Головне вікно програми

Після введення адреси сайту натисніть кнопку Start Scan. Відкриється майстер, який проведе через всі кроки сканування. Усі оптимальні налаштування сканування вибрано за замовчуванням.

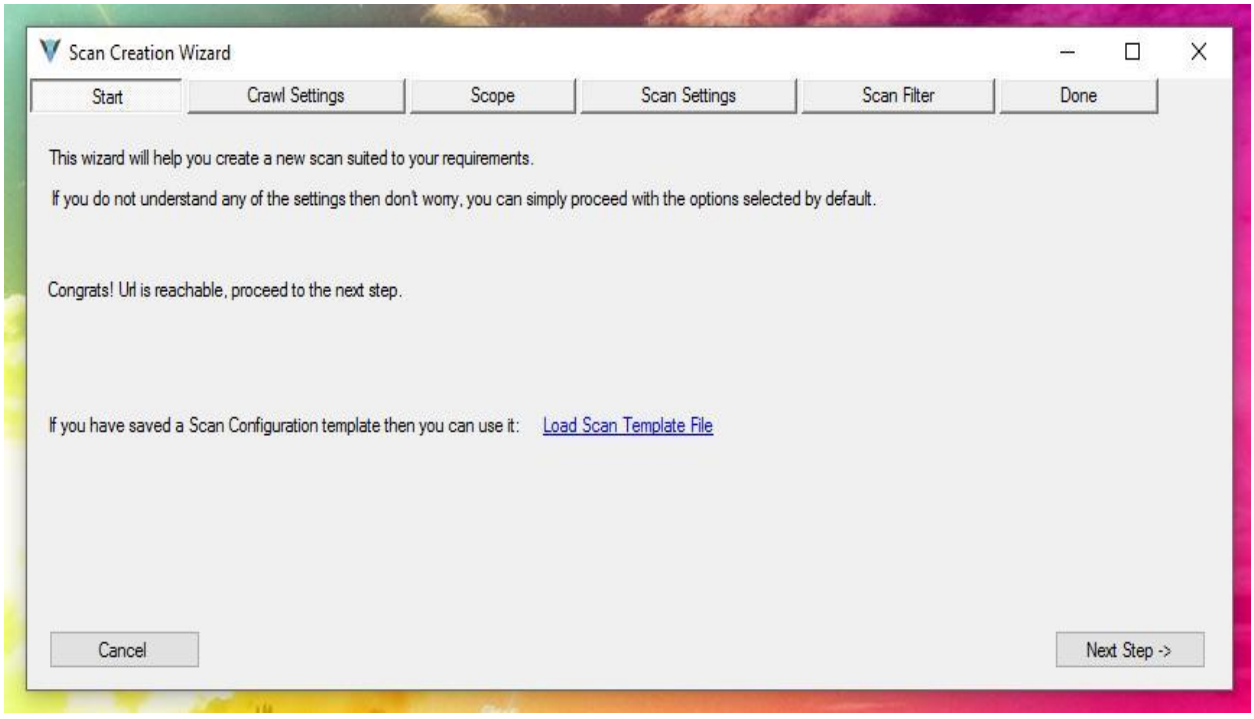


Рисунок 3.11 –Scan Creation Wizard. Start

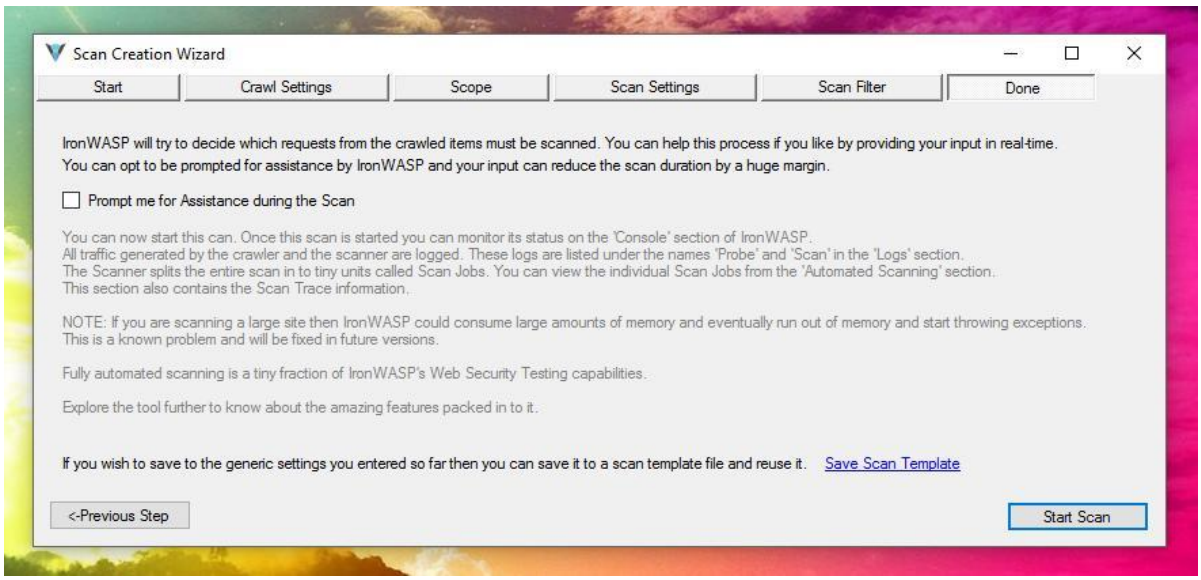


Рисунок 3.12 –Scan Creation Wizard. Done

В останньому вікні показано (рис.3.12) є місце під галочку, якщо натиснути яку IronWASP буде запитувати, які саме запити потрібно просканувати. Це може значно прискорити процес сканування великих сайтів, але ми повинні розуміти, що саме відбувається і що потрібно відповідати. Тому для повністю автоматизованого сканування просто натискаємо Start Scan. Можна зайти у вкладку Automated Scanning і змінити кількість паралельних дозволених потоків (максимум 10).

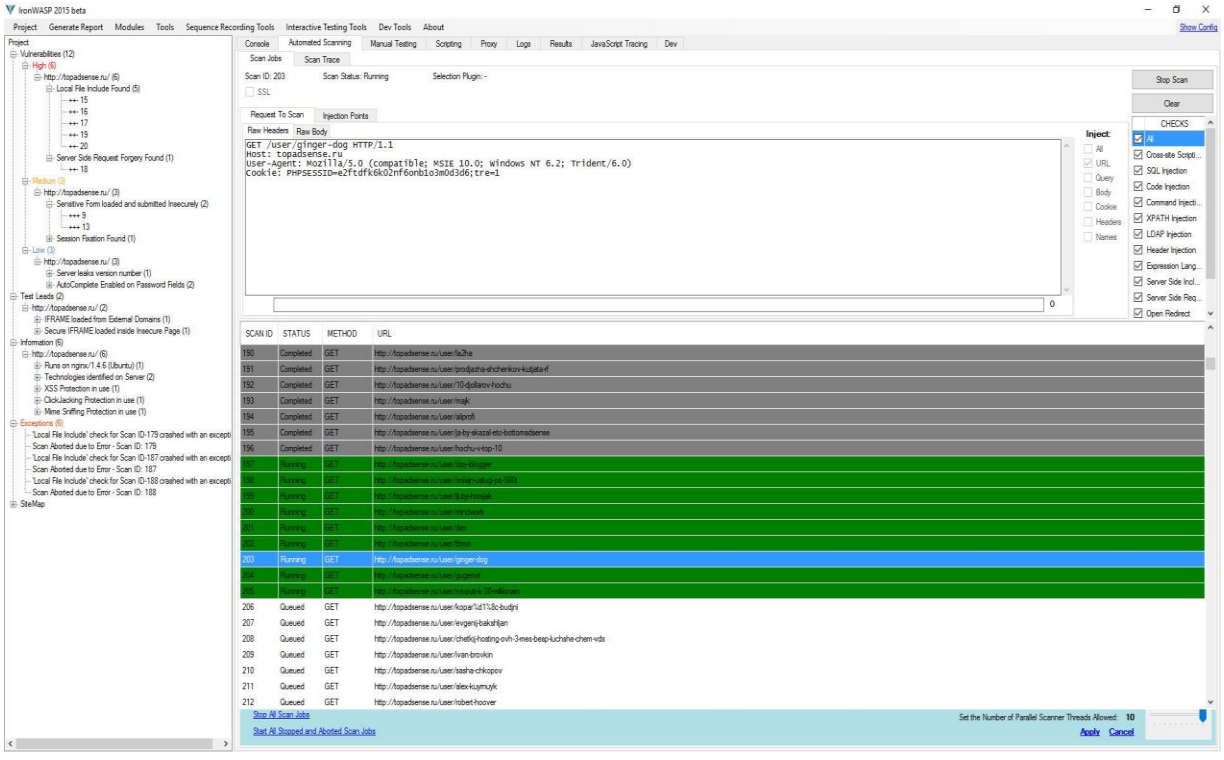


Рисунок 3.13 –Вкладка Automated Scanning

3) Оцінка результатів IronWASP

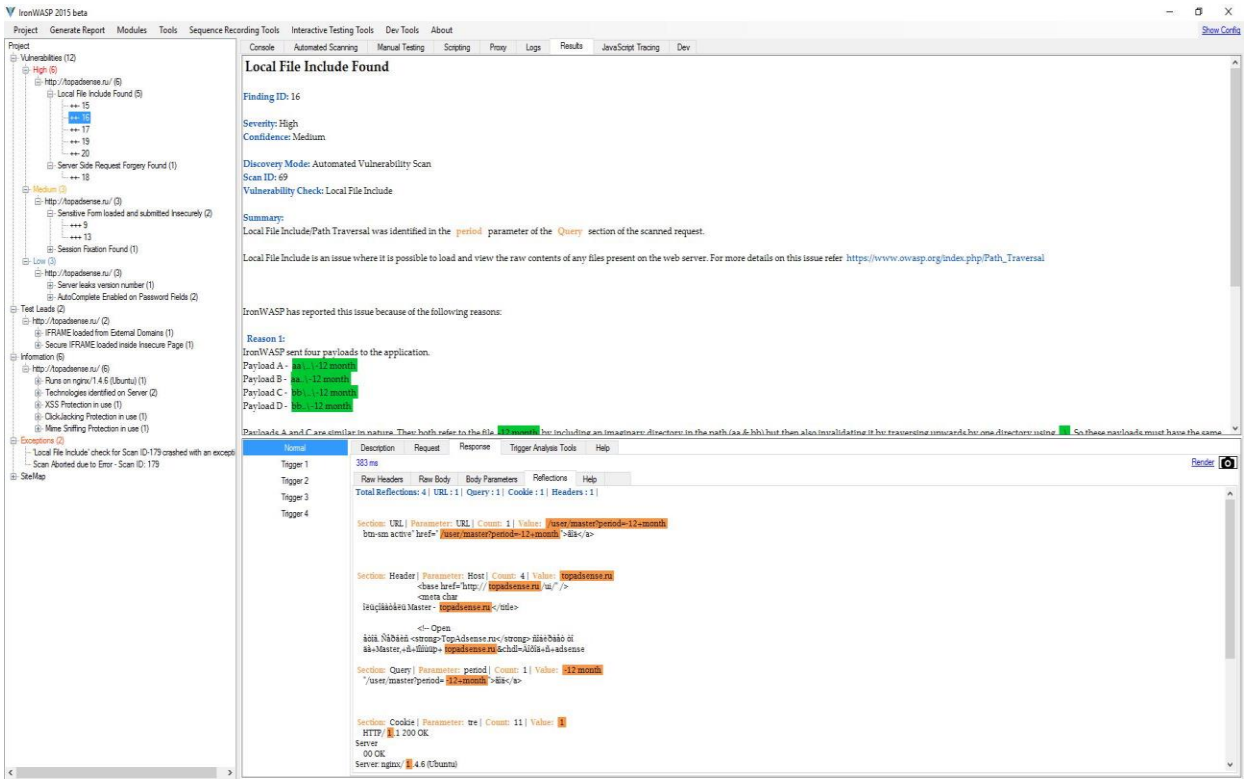


Рисунок 3.14 –Результати IronWASP

Усі результати за рівнем небезпеки позначаються як High (червоний), Medium (оранжевий) та Low (синій). Якщо серед результатів є вразливість рівня High, це вимагає НЕГАЙНИХ дій.

• По-перше, потрібно переконатися, що це не є результатом помилкового спрацьовування. Незважаючи на те, що в IronWASP присутній досить інтелектуальний двигун по фільтрації помилкових спрацьовувань, цих спрацьовувань буває достатньо. Особливо для SQL-ін'єкцій.

• По-друге, якщо підтверджено, що вразливість рівня High на сайті є, то сайт потрібно вважати скомпрометованим і проводити комплекс відповідних заходів (пошук бекдорів, пошук несанкціонованих змін вихідного коду, пошук несанкціонованих змін у базах даних, зміна паролів тощо).

4) Просунуте використання IronWASP

Описане вище сканування дозволяє виявити вразливість веб-сайтів. Таке сканування веб-сайтів може провести будь-який веб-майстер навіть без спеціальної підготовки. Крім описаної базової функціональності, IronWASP

включає інструменти для просунутих фахівців у сфері безпеки. Їх досить багато, тому обмежимося їх перерахуванням.

Вбудовані модулі:

• WiHawk — сканерт уразливостей WiFi роутерів.

• XmlChor — інструмент автоматичної експлуатації XPATH ін'єкції.

• IronSAP — сканер безпеки SAP.

• SSL Security Checker — сканер для виявлення вразливостей установок SSL.

• OWASP Skanda — автоматичний інструмент SSRF.

• CSRF PoC Generator — інструмент для автоматичної генерації експлойтів для уразливостей CSRF.

• HAWAS — інструмент для автоматичного виявлення та декодування закодованих рядків та хешей на веб-сайтах.

Вбудовані інструменти:

• Заснований на браузері павук.

• Аналізатор DOM XSS.

• Кодування/Декодування.

• Пошук відмінностей у двох текстах.

• Візуалізація HTML.

• Сканер потоку.

• Витягувач повідомлень веб-сокету.

• Клієнт веб-сокету.

Інструменти розробника. Вони дозволять вам створити власні помічники, скрипти, плагіни кількома доступними мовами програмування. У тому числі з графічним інтерфейсом.

IronWASP, мабуть, найпростіший інструмент для тестування безпеки веб-застосунків. При цьому дуже потужний та ефективний. Тим не менш, видається, що без розуміння суті знайдених потенційних уразливостей, той, хто запустив цей інструмент, не зможуть:

а) перевірити, чи не є знайдена вразливість помилковою тривогою;

б) самостійно ліквідувати пролом у безпеці;

в) експлуатувати знайдені вразливості.

### 3.3.2 Сканер веб-серверів Nikto

Nikto – це сканер з відкритим вихідним кодом (GPL) для веб-серверів, він виконує комплексні тести щодо серверів за кількома напрямками, включаючи більше 6700 потенційно небезпечних файлів/програм, перевірка на застарілі версії понад 1250 серверів та проблеми, специфічні для версій ніж 270 серверів. Сканер також перевіряє елементи конфігурації сервера, такі як наявність декількох індексних файлів, серверні опції HTTP і намагається визначити ім'я та версії веб-сервера та програмного забезпечення.

Nikto не створювався бути непомітним. Він буде тестувати веб-сервер за найшвидший можливий час, очевидно, що його активність потрапить до логів веб-сервера і в поле зору IPS/IDS (систем виявлення/запобігання вторгненням). Тим не менш, є підтримка анти-IDS методів з LibWhisker – на випадок, якщо ви захочете їх спробувати (або протестувати вашу систему IDS). Не кожна перевірка стосується проблеми безпеки, хоча більшість стосується. Деякі пункти є перевірками типу «тільки для інформації», які шукають речі, які можуть бути не проломами безпеки, але веб-майстер або інженер з безпеки можуть не знати, що це є на сервері. Зазвичай у виведеній інформації ці елементи позначені відповідним чином. Існують також деякі перевірки на невідомі елементи, які були помічені у файлах журналів.

Ось деякі з основних особливостей Nikto:

• Підтримка SSL (Unix з OpenSSL або може бути Windows з Perl/NetSSL у ActiveState).

• Повна підтримка HTTP проксі.

• Перевірка на застарілі компоненти сервера.

• Збереження звіту у вигляді простого тексту, XML, HTML, NBE або CSV.

• Двигун шаблонів для простого налаштування звітів.

• Сканування кількох портів на сервері або кілька серверів, отриманих із файлу введення (включаючи висновок nmap).

• Техніки кодування LibWhisker IDS.

• Ідентифікація встановленого програмного забезпечення за заголовками, іконками (favicon) та файлами.

• Аутентифікація на хості з Basic та NTLM.

• Вгадування під доменів.

• Перелік імен користувачів Apache та cgiwrap.

• Техніки мутації для «рибалки» за контентом веб-серверів.

• Підстроювання сканування, для увімкнення або виключення цілих класів перевірок на вразливості.

• Припущення облікових даних для області авторизації (включаючи безліч стандартних комбінацій логінів/паролей).

• Вгадування авторизації працює з будь-якою директорією, а не лише з кореневою.

• Покращене придушення помилкових спрацьовувань за допомогою кількох методів: заголовки, вміст сторінки та обчислення хешу вмісту.

• Повідомлення про «незвичайні» побачені заголовки.

• Інтерактивний статус, можна поставити на паузу та змінити налаштування вербальності.

• Збереження повних запитів/відповідей для тестів, які дали позитивні результати.

• Повторне відтворення позитивних запитів.

• Максимальний час виконання на одну мету.

• Автоматична постановка на паузу у певний час.

• Перевірки на поширені «паркувальні» сайти.

### 3.3.3 Пошук вразливостей у сайтах на WordPress за допомогою WPScan

Сайти, що використовують популярні системи керування контентом, такі як WordPress, мають у своїй основі однаковий вихідний код, скрипти. Цей код вже багаторазово перевірено. Тобто, використання сканерів загального призначення для пошуку, наприклад, SQL-ін'єкцій, XSS та інших популярних уразливостей у WordPress, навряд чи дасть результати, оскільки це вже багаторазово було зроблено до нас. Тим не менш, дослідники безпеки регулярно знаходять уразливості як в основному коді WordPress, так і в його численних плагінах, темах оформлення. Це означає, що сканувати WordPress потрібно не програмами загального призначення для пошуку вразливість, а спеціалізованою програмою.

Найкращою програмою для сканування WordPress є WPScan. Цей інструмент здатний визначати версію WordPress, а також те, які плагіни та теми яких версій використовуються. WPScan має велику та актуальну базу вразливостей у цих плагінах та темах, тому зіставляючи дані, отримані при скануванні з цією базою, програма повідомляє нам про вразливості, які присутні на досліджуваному сайті.

Вразливими можуть бути:

- сам WordPress;
- встановлені плагіни;
- встановлені теми.

WPScan не працює на Windows. Тому якщо ми хочемо просканувати сайт, але не можемо впоратися з Linux, ми можемо скористатися наступним безкоштовним онлайн сервісом для сканування WordPress за допомогою WPScan: https://suip.biz/ru/?act=wpscan&color=on. Там нам достатньо ввести адресу свого сайту та дочекатися закінчення сканування (10-20 хвилин).

### 3.4 Алгоритм аудиту Web-сайтів

Повністю робочий, який відповідає вимогам пошукових систем та зручний для користувача web-ресурс – це 70% успіху в онлайн просторі. Способів для досягнення такого результату безліч, але вони будуються навколо "правильної" бази.

Комплексна перевірка сайту – це перший, але дуже важливий крок для досягнення високих результатів у мережі Інтернет. Саме на цьому етапі виявляються основні проблеми веб-ресурсу та створюється стратегія щодо підвищення ефективності web-порталу.

Тестування на проникнення використовується для пошуку недоліків у комп'ютерних системах, з метою вжити відповідних заходів безпеки для захисту даних та підтримки функціональності.

В результаті аналізу розроблено методику створення алгоритму аудиту Web-сайтів за допомогою інструментів тестування на проникнення. Алгоритм складається із трьох кроків (рис.3.15). І включає наступні елементи:

• (0 крок) Підбірка вразливих середовищ для практики зі злому сайтів.

• (1 крок) Збір інформації.

• (2 крок) Сканування вразливостей веб-застосунків.

До алгоритму включено різні засоби та інструменти тестування на проникнення, комплексне використання яких підвищить ефективність аудиту Web-сайтів. В алгоритмі застосовують новітні програмні реалізації, що дозволяють поліпшити продуктивність моніторингу сайтів. Даний підхід дозволяє визначити недоліки сайтів і вразливі місця безпеки їх використання.

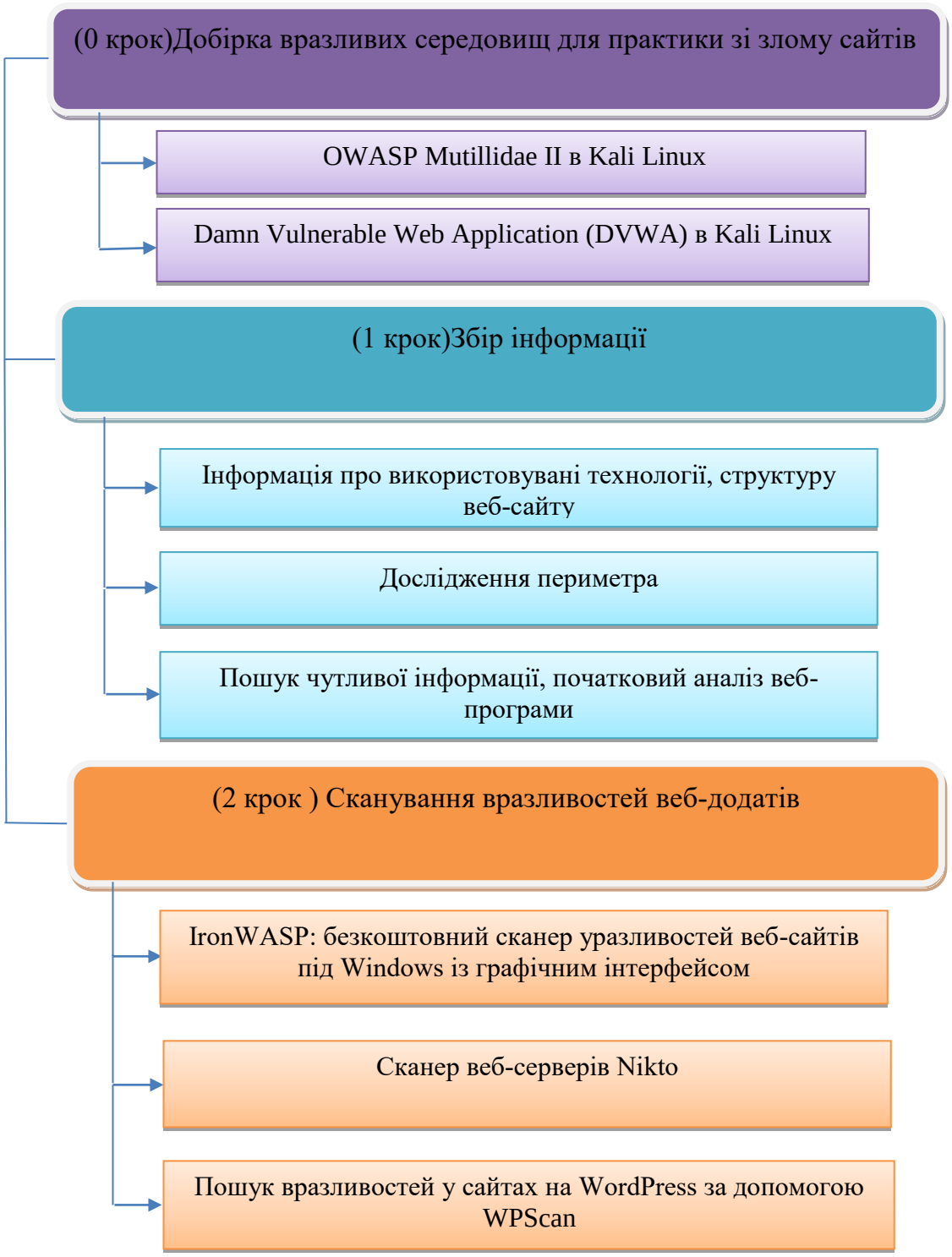


Рисунок 3.15 –Алгоритм аудиту Web-сайтів

Розроблений алгоритм може бути задіяний на підготовчій стадії аудиту (0 крок), а також для виявлення недоліків під час самого аудиту Web-сайтів за допомогою інструментів тестування на проникнення (1 крок) та (2 крок). Алгоритм розрахований вирішувати завдання різної складності, оскільки кожен його крок має кілька варіантів реалізації.

# 4. ЕКОНОМІЧНІ РОЗРАХУНКИ

Метою даних розрахунків є обчислення вартості виконання науково-дослідної роботи « Розробка алгоритму проведення аудиту Web-сайтів за допомогою інструментів тестування на проникнення». Основна мета даного дипломного проекту є ознайомлення з поняттям аудит веб-сайтів, розробка алгоритму для проведення аудиту сайтів за допомогою тестування на проникнення, яке дозволяє перевірити сайт на безпеку, виявити вразливість ПЗ серверів, знайти неякісні коди ресурсу, завдяки яким можна атакувати та зламати веб ресурс.

Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення. Розрахунок трудомісткості НДР здійснений в наступній послідовності:

1) Складений перелік всіх етапів і видів робіт, які необхідно виконати в ході даної НДР. Після узгодження з керівником проекту допущено виключення, доповнення, об'єднання окремих етапів і видів робіт;

2) По кожному виду робіт визначений кваліфікаційний рівень виконавців.. Розподіл робіт по етапах і видах виконавців вироблений формою, наведено в таблиці 1.

**Розподіл робіт по етапах і видах виконавців.**

Таблиця 4.1.

| **Етап проведення НДР** | **Вигляд робіт** | **Посада виконавця** |
|---|---|---|
| Розробка технічного завдання (ТЗ) | 1.Складання і затвердження ТЗ для НДР «Розробка алгоритму проведення аудиту Web-сайтів за допомогою інструментів тестування на проникнення» | Дипломник, керівник |

| | | |
|---|---|---|
| Вибір напряму дослідження | 1. Збір і вивчення науково-технічної літератури.<br>2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР .<br>3. Вибір напряму проведення досліджень для подальшої розробки.<br>4. Розробка плану проведення досліджень для подальшої розробки. | Дипломник керівник |
| Теоретичні і експериментальні дослідження | 1. Робота над першим розділом дипломного проекту «Комплексний аудит сайту»<br>2. Робота над другим розділом дипломного проекту «Тестування на проникнення»<br>3. Робота над третім розділом дипломного проекту «Розробка алгоритму проведення аудиту Web-сайтів»<br>4. Розрахунок економічної частини. Обчислення вартості виконання роботи<br>5. Написання розділу «Охорона праці».<br>6. Написання висновків та переліку посилань | Дипломник керівник консультанти |
| Узагальнення і оцінка результатів досліджень | 1. Узагальнення результатів попередніх етапів роботи.<br>2. Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття результатів в цілому. | Дипломник керівник консультанти |

В умовах відсутності нормативної бази тривалість виконання окремих робіт розраховується на основі вірогідних оцінок робіт, що задаються виконавцями.

**Очікувана трудомісткість робіт.**

Таблиця 4.2.

| Вигляд роботи | Очікуваний час виконання (дні) |
|---|---|
| 1. Складання і затвердження ТЗ для НДР «Розробка алгоритму проведення аудиту Web-сайтів за допомогою інструментів тестування на проникнення» | 1 |
| 2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів. | 4 |
| 3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка. | 2 |
| 4. Вибір напряму проведення досліджень і способів вирішення поставлених завдань. Розробка плану проведення досліджень для подальшої розробки. | 1 |
| 5. Робота над першим розділом дипломного проекту «Комплексний аудит сайту» | 3 |
| 6. Робота над другим розділом дипломного проекту «Тестування на проникнення» | 3 |
| 7. Робота над третім розділом дипломного проекту «Розробка алгоритму проведення аудиту Web-сайтів» | 5 |
| 8. Розрахунок економічної частини. Обчислення вартості виконання роботи | 2 |
| 9. Написання розділу «Охорона праці». | 2 |
| 10. Написання висновків та переліку посилань | 1 |
| 11. Узагальнення результатів попередніх етапів роботи. | 2 |
| 12. Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття результатів в цілому. | 3 |

| | |
|---|---|
| Всього: | 29 |

Результатом виконання НДР є науково-технічна продукція, що є закінчені науково – дослідницькі роботи, виконані відповідно до вимог, передбачених договором, і прийнятими замовником. Розрахунок собівартості і ціни виконання НДР включає наступні статті витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями, і деякі інші.

1) Витрати на матеріали, купувальні комплектуючі, напівфабрикати визначають на основі розрахунку потреби в них за оптовими цінами, що діють і складають ( ПАПІР формат А4 * вартість друку одного листа ) 85*3=255 грн.

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Розмір основної зарплати встановлюється виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за один робочий день. Відповідно до статті 8 «Закону про Державний бюджет України на 2022» встановлено мінімальну заробітну плату у місячному розмірі з 1 січня 2022 року - 6500 гривень; мінімальну погодинну тарифну ставку – 39,26 грн.

Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

$$Зден = п.т.с. * 8;$$

де п.т.с – погодинна тарифна ставка, грн..;

8 – тривалість робочого дня,год.

Зден дипломника = 39.26*8 = 314,08 грн.

Зден керівника = 60 *8 = 480 грн.

Зден консультантів = 60 *8= 480 грн.

Зден нормоконтролера = 50*8 = 400 грн.

Витрати на основну заробітну плату, НДР, що включаються в собівартість, приведені в таблиці 3.

**Витрати на основну заробітну плату.**

Таблиця 4.3.

| **Виконавець** | **Погодинна тарифна ставка, грн** | **Денна ставка, грн** | **Трудомісткість робочих днів** | **Сума основної зарплати, грн** |
|---|---|---|---|---|
| Дипломник | 39,26 | 314.08 | 29 | 9108,32 |
| Керівник | 60 | 480 | 1 | 480 |
| Консультант по економічній частині | 60 | 480 | 0,25 | 120 |
| Консультант по охороні праці | 60 | 480 | 0,25 | 120 |
| Нормоконтроль | 50 | 400 | 0,25 | 100 |
| Всього (Зо) | | | | 9928,32 |

3) Витрати на додаткову заробітну плату визначаються у відсотках від основної і враховують виплати за час, що не пропрацював, встановлений законом. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

$$Зд=10\%Зо;$$

$$Зд = 0,1 * 9928,32 = 992,832 \text{ грн}$$

4)До складу собівартості НДР включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Відрахування до єдиного соціального внеску складає.

$$Зєсв=0,22*(Зо+Зд);$$

$$Зєсв = 0,22 * (9928,32 + 992,832) = 0,22 * 10921,152 = 2402, 65344 \text{ грн}$$

5) До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР.. У наукових

закладах накладні витрати складають 40 -120% від основної і додаткової заробітної плати.

$$Рнакл= (Зо+Зд)*0,4;$$

$$Рнакл = (9928,32 + 992,832) * 0,4 = 4368,4608 грн$$

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 4.

**Калькуляція планової собівартості**

Таблиця 4.4.

| Статті витрат | Сума, грн. |
|---|---|
| 1. Матеріали | 255 |
| 2. Основна заробітна плата | 9928,32 |
| 3. Додаткова заробітна плата | 992,832 |
| 4. Відрахування до єдиного соціального внеску | 2402, 65344 |
| 5. Накладні витрати | 4368,4608 |
| Планова собівартість (Спл) | 17947,26624 |

Плановий прибуток визначений по формулі:

$$Ппл = 0,1*Спл$$

$$Ппл = 0,1* 17947,26624 = 1794,726624$$

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції.

Договірна ціна визначається по формулі:

$$Цнір = Спл + Ппл$$

$$Цнір = 17947,26624 + 1794,726624 = 19741,992864 грн.$$

Звідси ціна реалізації становить:

$$Цр = Цнір + ПДВ= Цнір+ Цнір*0,2$$

$$Цр = 19741,992864 + 19741,992864 *0,2 = 19741,99 + 3948,398 = 23690,388грн.$$

# 5. ОХОРОНА ПРАЦІ

## 1. Вступ

Охорона праці - це система правових, соціально-економічних, організаційно- технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров’я і працездатності людини в процесі трудової діяльності.

Це визначення свідчить, по-перше, про те, що охорона праці становить сукупність законів, норм, правил, стандартів тощо, а також комплекс різноманітних заходів і засобів, які забезпечують збереження життя, здоров’я та працездатність людей у процесі виконання ними трудових обов’язків, а, по-друге, про те, що однією з пріоритетних функцій держави є турбота про стан здоров’я працівника.

Сучасна концепція охорони праці в економічно розвинених країнах базується на тому, що до нещасних випадків на виробництві та професійних захворювань справа не повинна доходити. До найважливіших функцій сучасної держави належить створення умов, головною метою яких є робота, спрямована на запобігання травматизму та професійним захворюванням, відновлення здоров’я потерпілих на виробництві, виплата компенсацій потерпілим.

Ґрунтуючись на правових та організаційних основах, охорона праці вирішує питання виробничої санітарії, виробничої та пожежної безпеки.

## 2. Аналіз та безпека умов праці працівника на робочому місці з ПК

Працівники, задіяні на роботах, пов'язаних з періодичною або постійною роботою за комп'ютером, піддаються впливу факторів виробничої небезпеки.

До основних шкідливих факторів при роботі з комп'ютером відносять: тривале сидяче положення, електромагнітне випромінювання, навантаження на

зір, перевантаження кистьових суглобів, збільшене нервово-емоційне навантаження на оператора.

Усі шкідливі фактори зазначенні вище, встановленні у нормативному документі ГОСТ 12.003-74 ССБТ «Небезпечні і шкідливі виробничі фактори. Класифікація».

# 3 Розробка заходів з охорони праці

## 3.1 Виробничі приміщення

Об'ємно-планувальні рішення будівель та приміщень, де експлуатуються відео дисплейні термінали мають відповідати вимогам ДСанПіН 3.3.2.007-98.

Розміщення робочих місць з ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях та на цокольних поверхах заборонено.

Площа на одне робоче місце для операторів повинна складати не менше 6,0 м$^2$, а об'єм – не менше 20,0м$^3$. Стіни повинні бути пофарбовані матовою краскою.

## 3.2 Мікроклімат робочої зони працівників, вентиляція.

Мікроклімат у приміщенні, де знаходиться робоче місце, оптимальний:

- температура повітря – 22-25$^0$С;
- відносна вологість – 40-60%;
- швидкість руху повітряних мас – 0,1-0,2 м/сек.

Для підтримки необхідних параметрів мікроклімату робоче приміщення оснащене системами опалення й кондиціювання.

У приміщеннях, де відбувається робота з ПК вимоги до параметрів мікроклімату в цілому виконанні.

### 3.3 Освітлення робочого місця, шум, вібрація

В приміщенні, де розташоване робоче місце присутнє бокове природне освітлення та система комбінованого освітлення. В якості штучного освітлення використовуються світлодіодні лампи. Для місцевого освітлення використовуються світильники з відбивачами, що не просвітлюються.

У приміщенні застосовуються на вікнах світловідбивні жалюзі, що перерозподіляють світловий потік в глибину приміщення. Середня освітленість робочого місця дорівнює 300 лк, рівномірність освітленості зони безпосереднього оточення - 0,54, периферії - 0,18.

Джерелом шуму у виробничому приміщенні є персональні комп'ютери та принтери. Допустимі рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку для широкосмугового постійного та непостійного (крім імпульсного) шуму на робочих місцях, де присутня творча, наукова діяльність, програмування, конструювання слід приймати:

| Рівні звукового тиску, дБ, у октавних смугах із середньогеометричними частотами, Гц | | | | | | | | | Рівні звуку та еквівалентні рівні звуку, дБА |
|---|---|---|---|---|---|---|---|---|---|
| 31,5 | 63 | 125 | 250 | 500 | 1000 | 2000 | 4000 | 8000 | |
| 86 | 71 | 61 | 54 | 49 | 45 | 42 | 40 | 38 | 50 |

Для тонального та імпульсного шуму допустимі рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку - на 5 дБ менше значень, зазначених у таблиці.

На робочому місці рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку для широкосмугового постійного та непостійного (крім імпульсного) шуму дорівнюють 125 дБ при 61 Гц. Рівень шуму дорівнює 40 дБА.

Рівні постійних магнітних полів протягом робочого дня не перевищують 7 кА/м. Рівні напруженості магнітного поля частотою 50 Гц при постійному

впливі протягом робочого дня (8 год) не перевищують 1,1 кА/м. Тобто фактичні норми ЕМВ не перевищують допустимі норми, зазначені у документі ДСНіП 3.3.6.096-2002, у якому встановлено, що рівні постійних магнітних полів протягом робочого дня не повинні перевищувати 8 кА/м, та рівні напруженості магнітного поля частотою 50 Гц при постійному впливі протягом робочого дня (8 год) не повинні перевищувати 1,4 кА/м.

### 3.4 Електробезпека.

Джерелами виділення шкідливих речовин у виробничому приміщенні є персональні комп'ютери та електричне обладнання, яке під'єднується до них (принтери тощо). Вони можуть бути джерелом ураження електрострумом при поломках чи неправильній експлуатації.

Приміщення, в якому знаходиться робоче місце, відносно небезпеки ураження людей електричним струмом належить до приміщень без підвищеної небезпеки.

Для попередження поразок електричним струмом необхідно чітко й у повному обсязі виконувати правила провадження робіт і правил технічної експлуатації. Необхідно виключити можливість доступу оператора до частин устаткування, що працює під небезпечною напругою, до неізольованим частинам, призначеним для роботи при малій напрузі й не підключеним до захисного заземлення, а також підводити електроживлення до ПЕОМ від розетки за допомогою спеціальної вилки із заземлюючим контактом.

### 3.5 Організація робочого місця користувача ПК

Сучасний комп'ютер є електротехнічним пристроєм загального користування, та не є засобом підвищеної небезпеки. Робота за комп'ютером за показниками напруженості трудового процесу належить до допустимого рівня класу умов праці.

При розміщенні робочих місць з персональними комп'ютерами відстань між робочими столами з відеомоніторами (у напрямі тилу поверхні одного відеомонітора і екрану іншого відеомонітора) повинна бути не менше 2,0 м, а відстань між бічними поверхнями відеомоніторів - не менше 1,2 м. При розміщенні декількох робочих місць в одному приміщенні мінімальна площа для одного робочого місця складає 6 м$^2$.

Екран відеомонітора повинен знаходитися від очей користувача на відстані 60-70 см, але не ближче 50 см з урахуванням розмірів алфавітно-цифрових знаків і символів, та бути розташований у вертикальній площині під кутом + 30° до нормальної лінії погляду працівника.

Конструкція робочого столу забезпечує оптимальне розміщення на робочій поверхні використовуваного обладнання з урахуванням його кількості і конструктивних особливостей, характеру виконуваної роботи. Поверхня робочого столу має коефіцієнт відбиття 0,6. Нормою коефіцієнту відбиття е 0,5-0,7. Висота робочої поверхні столу складає 725 мм.

Робочий стіл має простір для ніг висотою 620 мм, шириною - 510 мм, глибиною на рівні колін - не менше 450 мм, на рівні витягнутої ноги - не менше 650 мм.

Конструкція робочого стільця (крісла) забезпечує підтримку раціональної робочої пози під час роботи на персональному комп'ютері, дозволяє змінювати позу з метою зниження статичного напруження м'язів для попередження розвитку втоми. Робочий стілець (крісло) підйомно-поворотний, регульований по висоті і кутам нахилу сидіння і спинки, а також відстані спинки від переднього краю сидіння, при цьому регулювання кожного параметра незалежне, легко здійснюване, має надійну фіксацію. Поверхня сидіння, спинки та інших елементів стільця (крісла) напівм'яка, з нековзним повітропроникним покриттям, що забезпечує легке очищення від забруднень.

Клавіатуру слід розташовувати на поверхні столу на відстані 100-300 мм від краю, зверненого до користувача, або на спеціальній, регульованою по висоті робочої поверхні, відокремленої від основної стільниці.

Для збереження здоров’я працівників, запобігання професійним захворюванням і підтримки працездатності слід передбачати внутрішньозмінні регламентовані перерви для відпочинку:

Для зниження нервово-емоційного напруження і втоми очей, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії доцільно деякі перерви використовувати для виконання комплексу вправ.

Внутрішньозмінні режими праці та відпочинку, норми для виробничих приміщень та організації робочих місць встановлені у ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».

## 4. Пожежна безпека

Метою пожежної безпеки об’єкта є попередження виникнення пожежі на визначеному чинними нормативами рівні, а у випадку виникнення пожежі – обмеження її розповсюдження, своєчасне виявлення, гасіння пожежі, захист людей і матеріальних цінностей.

Часто займання відбуваються через спалах електропроводки через перевантаження електромережі. Можливою причиною вибуху або пожежі у приміщенні, де розташоване робоче місце є електрообладнання - комп’ютер, світильник, принтер. Вибух чи пожежа можуть трапитися тільки внаслідок поломки обладнання чи її неправильної експлуатації.

Приміщення, де знаходиться робоче місце, оснащене переносним вуглекислотним вогнегасником ВВК-2. На підприємстві є засоби пожежної сигналізації, плани евакуації, внутрішні пожежні крани, є пожежний щит із первинними засобами пожежогасіння .

## 5. Висновки

В приміщенні, де знаходиться робоче місце дотримані всі норми організації робочого простору. Робота за комп’ютером за показниками напруженості трудового процесу належить до допустимого рівня класу умов праці. Приміщення, в якому знаходиться робоче місце, належить до приміщень без підвищеної небезпеки. Забезпечені засоби протипожежної безпеки.

# ВИСНОВОК

Аудит Web-сайтів за допомогою інструментів тестування на проникнення проводиться із застосуванням широкого списку спеціалізованих програм та додатків (підбірка вразливих середовищ для практики по злому сайтів, пошук вразливостей сайту, застосування програм та утиліт) та охоплює велику кількість пунктів перевірки:

- Збір інформації.
- Пошук технічної бази.
- Аналіз вразливостей та загроз.
- Експлуатація та обробка даних.
- Формування звіту.

Аудит за допомогою інструментів тестування на проникнення дає найбільш повну картину про стан інформаційної безпеки сайту, дозволяє виявити слабкі та незахищені місця та вчасно вжити заходів щодо покращення безпеки, дати розуміння про поточну роботу сайту, пов'язану з інформаційною безпекою, дає план дій щодо усунення вразливостей. Багато спеціалістів з інформаційної безпеки рекомендують проводити penetration test на регулярній основі. Технології інформаційної безпеки дуже швидко старіють, рішення, оптимальне для підприємства замовника на даний момент, не буде таким через деякий час. Фахівця для проведення аудиту із застосуванням тестування на проникнення краще вибирати з боку, це має бути компетентна людина, незацікавлена та неупереджена. Співробітники служби безпеки організації – замовника на цю роль не підходять, тому що безпосередньо зацікавлені в результаті і можуть просто не мати необхідний рівень знань. Експерт з боку, який має мінімальні знання про архітектуру системи безпеки замовника, з більшою ймовірністю виявить її вразливості.

Аудит Web-сайтів на основі інструментів тестування на проникнення є необхідним елементом забезпечення інформаційної безпеки для будь-якої організації.

## ПЕРЕЛІК ПОСИЛАНЬ


1. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p.
2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p.
3. Wilhelm, Thomas. Professional penetration testing: Creating and learning ina hacking lab. Newnes, 2013, 525 p.
4. BSI - Study A Penetration Testing Model. Federal Office for Information Security, 111 p. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html
5. Najera-Gutierrez, Gilberto, and Juned Ahmed Ansari. Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. Packt Publishing Ltd, 2018.
6. Johansen, Gerard, et al. Kali Linux 2–Assuring Security by Penetration Testing. Packt Publishing Ltd, 2016.
7. Buchanan, Cameron, and Vivek Ramachandran. Kali Linux Wireless Penetration Testing Beginner's Guide: Master wireless testing techniques to survey and attack wireless networks with Kali Linux, including the KRACK attack. Packt Publishing Ltd, 2017.
8. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.
9. Norman, Alan T. Computer Hacking Beginners Guide: How to Hack Wireless Network, Basic Security and Penetration Testing, Kali Linux, Your First Hack. Independently published, 2018.
10. Hertzog, Raphaël, and Jim O'Gorman. Kali Linux Revealed: Mastering the Penetration Testing Distribution. offsec Press, 2017.

11. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.

12. Penetration Testing- A hand on introduction to hacking, Georgia Weidman,no starch press, San Francisco, 2014

13. Chu, Ge, and Alexei Lisitsa. "Penetration Testing for Internet of Things and Its Automation." 2018 IEEE 20th International Conference on High PerformanceComputing and Communications; IEEE 16th International Conference on Smart City;IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE, 2018.

14. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

15. http://www.pentest-standard.org/index.php/Exploitation https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penet ration/penetration_pdf.html

16. Бойчик І. М. Економіка підприємства: навчальний посібник для студентів економічних спеціальностей вищих навчальних закладів І-IV рівнів акредитації. Третє видання, випр. і доп. / І. М. Бойчик, П. С. Харів., М. І. Холчан, Ю. В. Піча. – К.: Каравела, 2016. – 328 с.

17. Закон України Про охорону праці, №235-IV, 22.11.2002

18. ГОСТ 12.003–74 ССБТ. Небезпечні і шкідливі виробничі фактори. Класифікація

19. ДБН В.2.5 - 28:2018 Природне і штучне освітлення

20. ГОСТ 12.1.003-83. Шум. Общие требования безопасности

21. НАПБ Б.03.002-2007 Норми визначення категорій приміщень будинків і зовнішніх установок за вибухопожежною та пожежною небезпекою