



ТЕМА 1

*ВСТУП ДО ЗАХИСТУ  
ВЕБ-СЕРВЕРІВ ВІД  
КІБЕРАТАК: ПОНЯТТЯ  
ВЕБ-СЕРВЕРА ТА  
КЛАСИФІКАЦІЯ  
ВРАЗЛИВОСТЕЙ ВЕБ-  
СЕРВЕРІВ.*

Леуненко Олексій Володимирович

# *ЗМІСТ*

- Вступ до захисту веб-серверів від кібератак.
- Поняття веб-сервера
- Класифікація вразливостей веб-серверів
- Управлінні вразливостями веб-серверів
- Рекомендації щодо зниження ризиків

# *ВСТУП ДО ЗАХИСТУ ВЕБ-СЕРВЕРІВ ВІД КІБЕРАТАК.*

**Загрози кібербезпеці веб-серверів** викликають значне занепокоєння як у бізнесу, так і у приватних осіб. Скомпрометований веб-сервер може призвести до витоку даних, несанкціонованого доступу, пошкодження веб-сайту і навіть фінансових втрат.

# *ПОНЯТТЯ ВЕБ-СЕРВЕРА*

Визначення веб-сервера.

Основні функції веб-сервера.

Приклади популярних веб-серверів  
(Apache, Nginx, Microsoft IIS).

# *ПОНЯТТЯ ВЕБ-СЕРВЕРА*

**Веб-сервер** - це програмне забезпечення або апаратний пристрій, який обробляє запити від клієнтів (браузерів) і надає їм доступ до веб-сторінок через Інтернет. Він приймає HTTP-запити, обробляє їх і повертає відповідні HTTP-відповіді.

**Веб-сервер** обробляє запит користувача і надсилає відповідь, яка містить дані (HTML, JSON, XML тощо) назад у браузер. Веб-сервери, розміщені на віртуальній машині, використовують обчислювальні потужності віртуальних машин для виконання своїх завдань. Веб-сервер зазвичай відноситься до внутрішніх інфраструктур, таких як база даних, кеш-сервер, черга завдань та інші.

# *ОСНОВНІ ФУНКЦІЇ ВЕБ-СЕРВЕРА*

- **Обробка запитів:** Прийом і обробка запитів від клієнтів.
- **Зберігання та передача контенту:** Зберігання веб-сторінок, зображень, відео та інших ресурсів і їх передача клієнтам.
- **Безпека:** Захист даних і ресурсів від несанкціонованого доступу.
- **Логування:** Ведення журналів запитів і відповідей для аналізу та моніторингу."

# ПРИКЛАДИ ПОПУЛЯРНИХ ВЕБ-СЕРВЕРІВ



[Welcome! - The Apache HTTP Server Project](#)

# NGINX

<https://nginx.org/>



[Home : The Official Microsoft IIS Site](#)

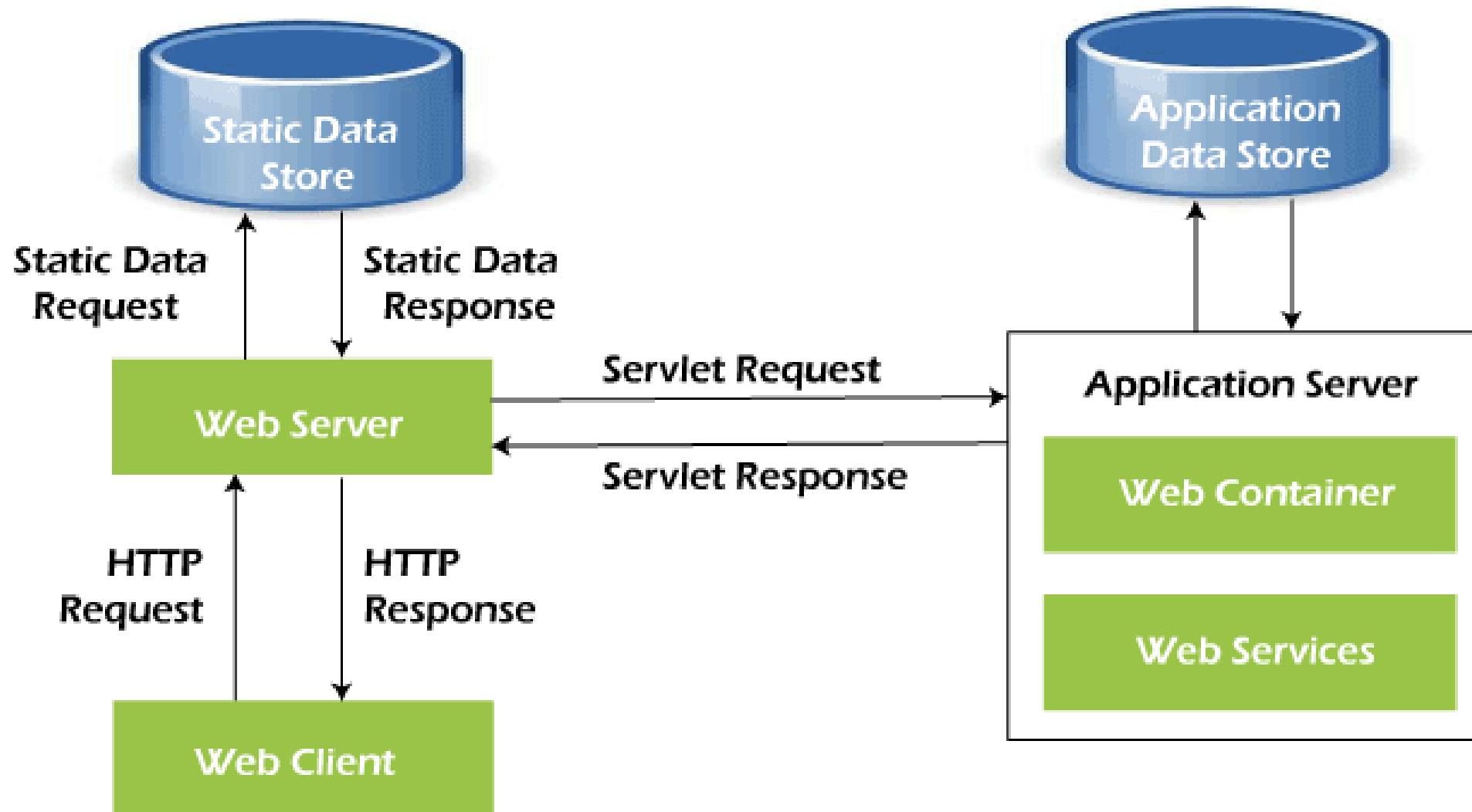
# ***АРХИТЕКТУРА ВЕБ-СЕРВЕРА***



# *ОСНОВНІ КОМПОНЕНТИ ВЕБ-СЕРВЕРА*

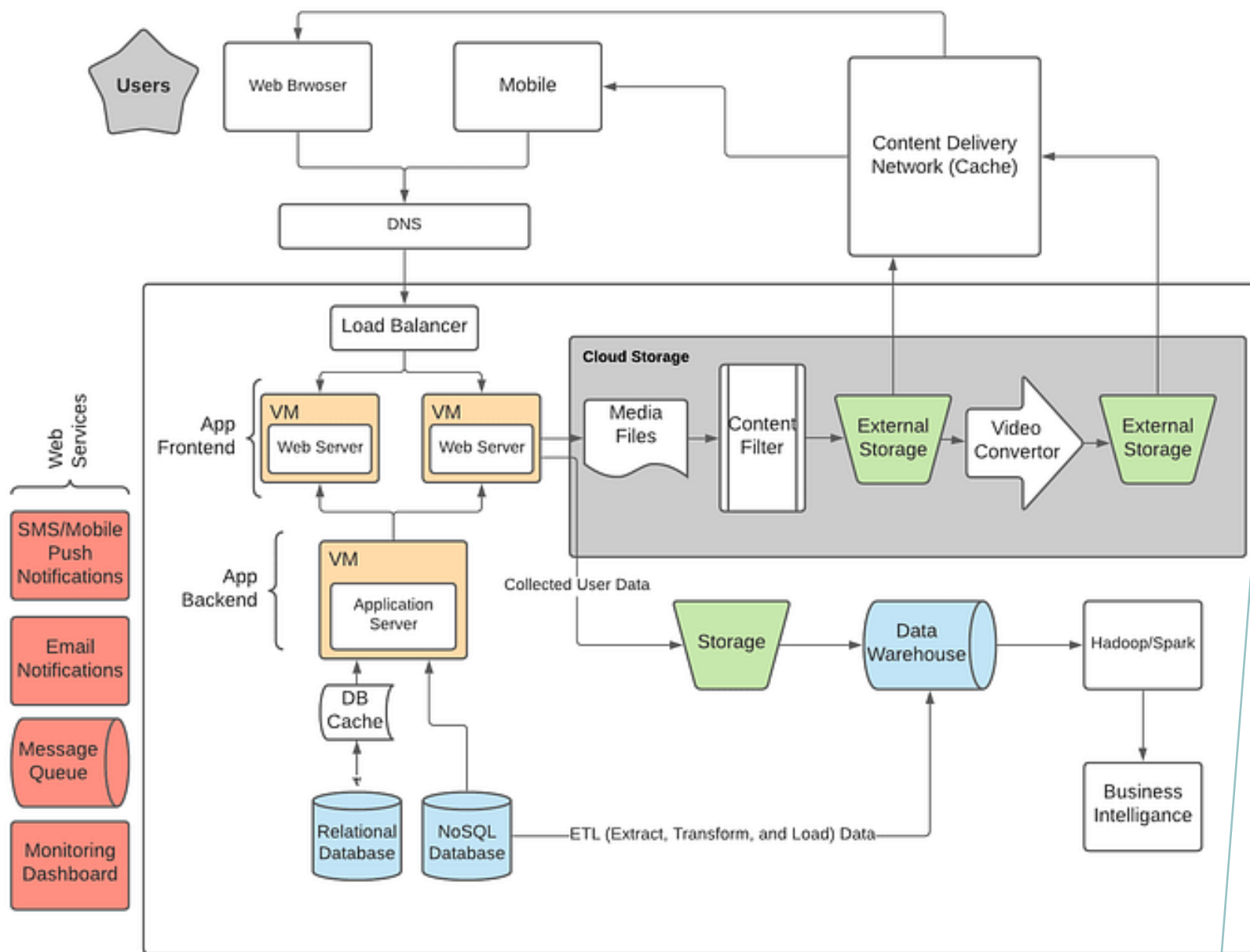
- 1. HTTP-сервер.** Основний компонент, який обробляє HTTP-запити та відповіді.
- 2. Файлова система.** Зберігає веб-сторінки, зображення, відео та інші ресурси.
- 3. Модулі розширення.** Додають додаткові функції, такі як підтримка різних мов програмування (PHP, Python, .NET, Java) або безпекові модулі.
- 4. Журнали:** Ведуть записи про всі запити та відповіді для аналізу та моніторингу."

## Working of web servers



# СТАТИЧНІ ВЕБ-СЕРВЕРИ ПРОТИ ДИНАМІЧНИХ ВЕБ-СЕРВЕРІВ

№	Статичні веб-сервери	Dynamic Web Servers
1	Статичні веб-сервери - це сервери, які обслуговують лише статичний вміст, тобто вміст фіксований і відображається таким, яким він є.	Динамічні веб-сервери відносяться до серверів, на яких вміст сторінки може оновлюватися і змінюватися.
2	Статичний веб-сервер включає в себе комп'ютер і програмне забезпечення HTTP (Hyper Text Transfer Protocol - протокол передачі гіпертексту).	Динамічний веб-сервер також включає в себе комп'ютер з великою кількістю іншого програмного забезпечення, на відміну від сервера додатків і моделі бази даних.
3	Він називається статичним; вміст веб-сторінок не змінюється, якщо користувач не змінює його вручну, а сервер доставляє веб-файли у веб-браузер у тому вигляді, в якому вони є.	Він називається динамічним, тому що сервер додатків використовується для оновлення файлів веб-сторінок на стороні сервера, і через це він може змінюватися при кожному запиті веб-браузера.
4	Статичні веб-сервери потребують менше часу для завантаження даних.	Динамічний веб-сервер може генерувати дані лише тоді, коли вони запитуються з бази даних. Тому він займає більше часу і є складнішим у порівнянні зі статичними веб-серверами.



# СХЕМА АРХІТЕКТУРИ ВЕБ- ДОДАТКІВ

# РОЛЬ ВЕБ-СЕРВЕРА У ВЕБ-ІНФРАСТРУКТУРІ

Веб-сервер є критично важливим компонентом веб-інфраструктури, оскільки він забезпечує доступ до веб-ресурсів для користувачів. Він взаємодіє з іншими компонентами, такими як бази даних, сервери додатків та мережеві пристрої, щоб забезпечити безперебійну роботу веб-додатків і сервісів.

# *КЛАСИФІКАЦІЯ ВРАЗЛИВОСТЕЙ ВЕБ-СЕРВЕРІВ*

# *СКАНУВАННЯ ПОРТІВ*

**Сканування портів** — це ключовий етап у визначенні стану безпеки веб-сервера. Під час цього процесу виявляються вразливості та ризики, пов'язані з використанням конкретних портів. Ефективне сканування дозволяє фахівцям забезпечити належний рівень захисту та приймати необхідні заходи для усунення виявлених проблем.

# *СКАНУВАННЯ ПОРТІВ*

## Етапи сканування портів:

1. Визначення портів
2. Виявлення відкритих та закритих портів
3. Аналіз конфігурації портів
4. Використання спеціалізованих інструментів для сканування
5. Виявлення специфічних вразливостей на портахВиявлення специфічних вразливостей на портах
6. Захист від сканування портів



# *АНАЛІЗ ВЕБ-ДОДАТКІВ*

**Аналіз веб-додатків** є важливою складовою стратегії забезпечення безпеки в онлайн середовищі. Зловмисники часто використовують різноманітні методи для атак на веб-додатки, спрямовані на отримання несанкціонованого доступу, витік конфіденційної інформації та поширення шкідливого коду.

# *АНАЛІЗ ВЕБ-ДОДАТКІВ*

Процес аналізу вразливостей веб-додатків та заходів щодо їх ефективного управління:

1. Перевірка коду додатку
2. Тестування на переповнення буфера
3. Перевірка налаштувань безпеки
4. Тестування ідентифікації та автентифікації
5. Тестування на захист від XSS та CSRF атак
6. Виявлення вразливостей за допомогою автоматизованих інструментів
7. Розробка інструкцій та рекомендацій з покращення безпеки

# *АНАЛІЗ КОНФІГУРАЦІЇ СЕРВЕРА*

Аналіз конфігурації сервера є важливим етапом у забезпеченні безпеки інтернет-систем. Невірна конфігурація може викликати серйозні вразливості, які можуть бути використані зловмисниками для атак та несанкціонованого доступу.

# *АНАЛІЗ КОНФІГУРАЦІЇ СЕРВЕРА*

1. Налаштування безпеки сервера
2. Налаштування безпеки сервера
3. Захист від DoS-атак
4. Налаштування протоколу HTTPS
5. Управління правами доступу
6. Захист від вразливостей віддаленого виконання коду
7. Автоматизація управління конфігурацією

# *ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ*

Виявлення вразливостей є невід'ємною частиною стратегії забезпечення безпеки ІТ-систем. Зловмисники постійно шукають можливості для атак, і використання спеціалізованих інструментів є ефективним способом виявлення та усунення потенційних загроз.

# *ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ*

1. Сканування вразливостей
2. Тестування вразливостей веб-додатків
3. Аналіз коду
4. Тестування на проникнення
5. Виявлення вразливостей в мережі
6. Автоматизовані інструменти управління вразливостями
7. Моніторинг та інцидент-відгук

# *ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ*

Виявлення вразливостей за допомогою інструментів є критичним етапом у забезпеченні безпеки ІТ-систем. Використання спеціалізованих інструментів дозволяє швидко та ефективно виявляти потенційні загрози, зменшуючи ризики та забезпечуючи стійкість до атак. Комбінація різноманітних інструментів та тщательний аналіз допомагають організаціям підтримувати високий рівень безпеки в постійно змінюючомуся цифровому середовищі.

# *УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ВЕБ-СЕРВЕРА*

Управління вразливостями веб-сервера є важливим компонентом загальної стратегії забезпечення безпеки в онлайн середовищі. Веб-сервери, що є витокom для численних атак, вимагають систематичного аналізу та усунення потенційних ризиків.

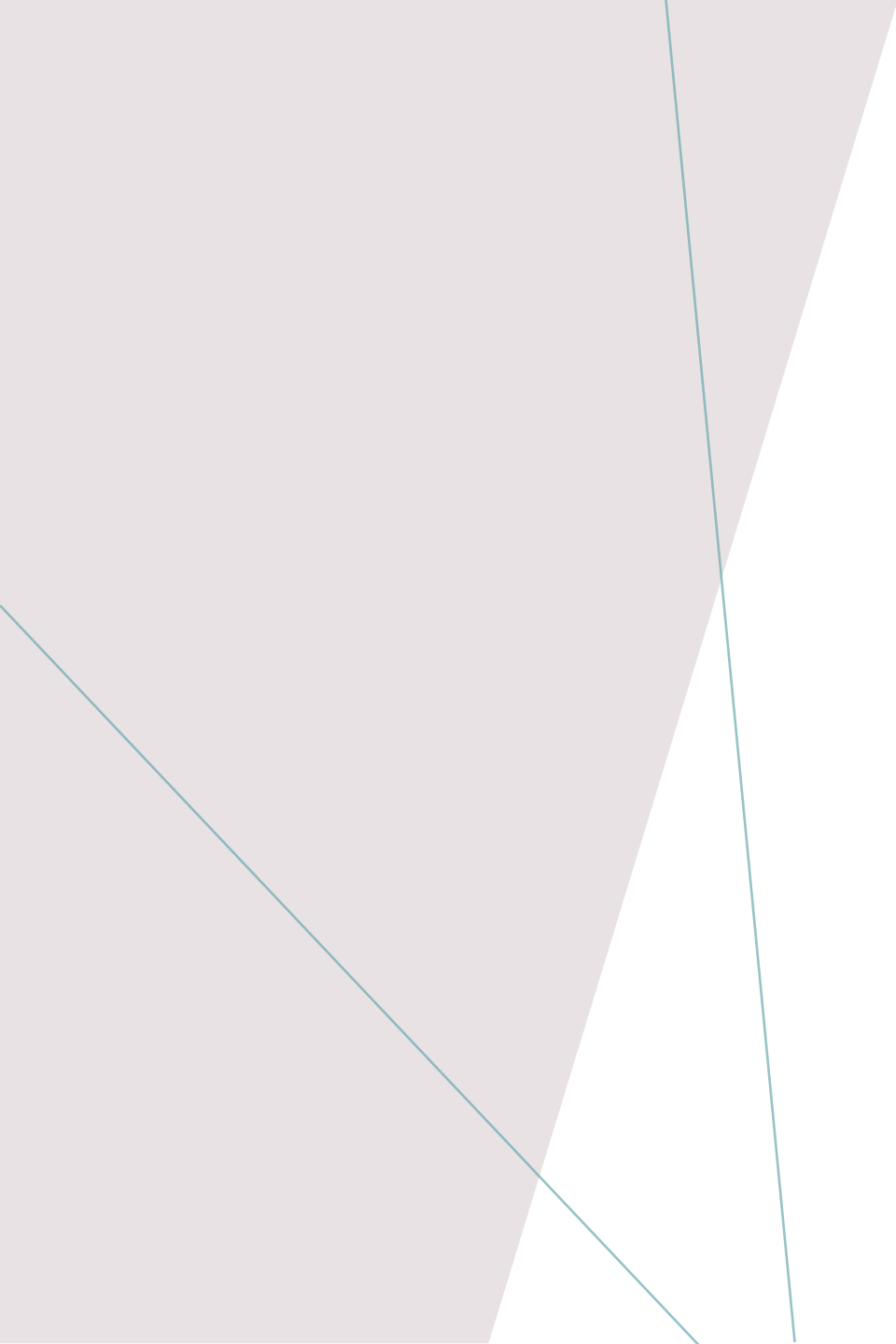


# *УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ВЕБ-СЕРВЕРА*

1. Систематичне сканування та аналіз вразливостей
2. Постійне оновлення та встановлення патчів
3. Спостереження та аналіз журналів подій
4. Конфігураційний аналіз та оптимізація
5. Захист від DDoS атак
6. Валідація та фільтрація введених даних
7. Аудит та звітність

# *УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ВЕБ-СЕРВЕРА*

**Ефективне управління вразливостями веб-сервера** – це необхідна умова для стійкої безпеки в онлайн середовищі. Систематичний аналіз, постійне оновлення та реагування на потенційні загрози дозволяють підтримувати високий рівень безпеки веб-сервера та забезпечувати безпечну роботу онлайн ресурсів. Тільки комплексний підхід до управління вразливостями дозволить досягти оптимального рівня безпеки в інтернет-середовищі.

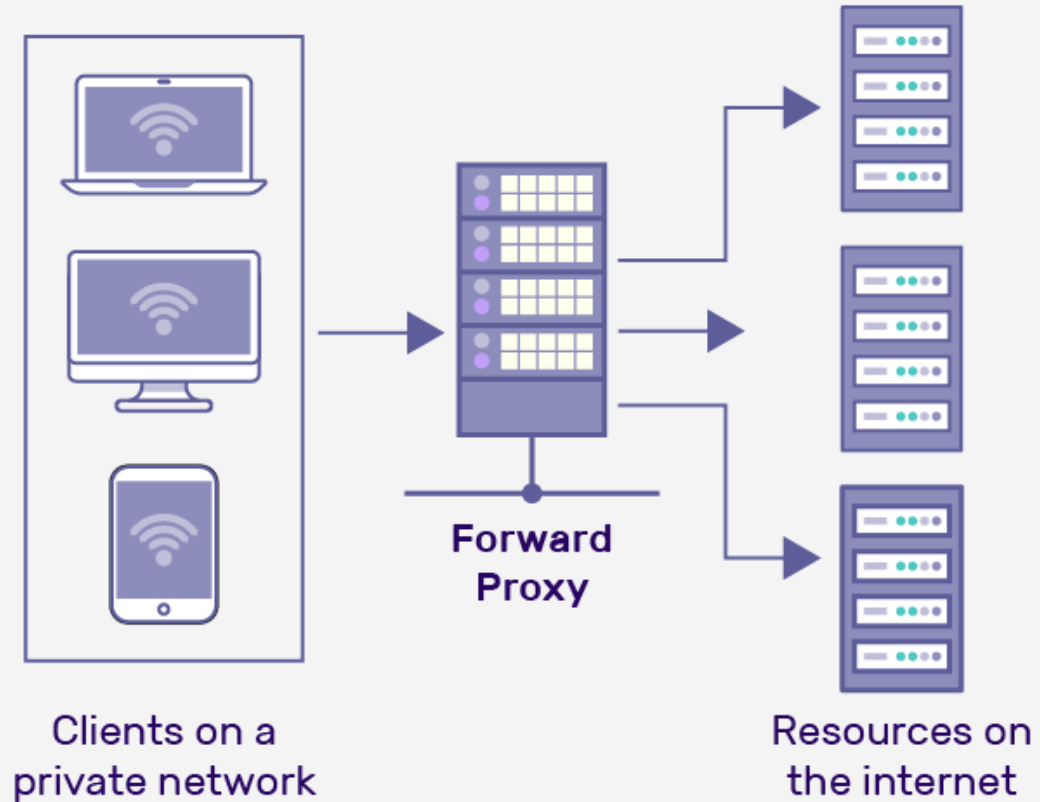


# *УПРАВЛІННІ ВРАЗЛИВОСТЯМИ ВЕБ-СЕРВЕРІВ*

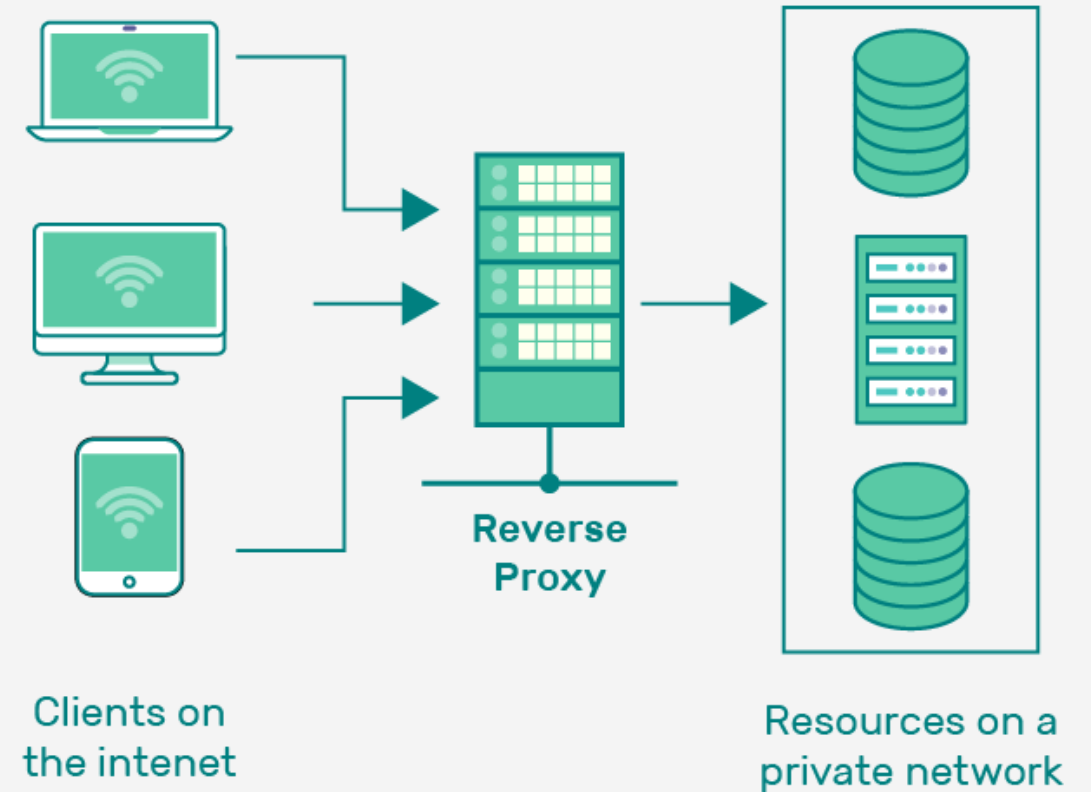
# *МЕТОДИ ЗАХИСТУ ВЕБ-СЕРВЕРІВ*

- Зворотний проксі (reverse proxy)
- Обмеження доступу (Access restriction)
- Підтримка веб-серверів у належному стані та оновлення
- Моніторинг мережі
- Використання брандмауера і SSL

## Forward Proxy



## Reverse Proxy



# *КЛАСИФІКАЦІЯ ВРАЗЛИВОСТЕЙ*

Першим кроком в управлінні вразливостями є їхнє класифікування за рівнем загрози та можливістю використання зловмисниками. Це дозволяє визначити пріоритетність усунення кожної вразливості та спрямовувати ресурси на найбільш критичні аспекти безпеки.

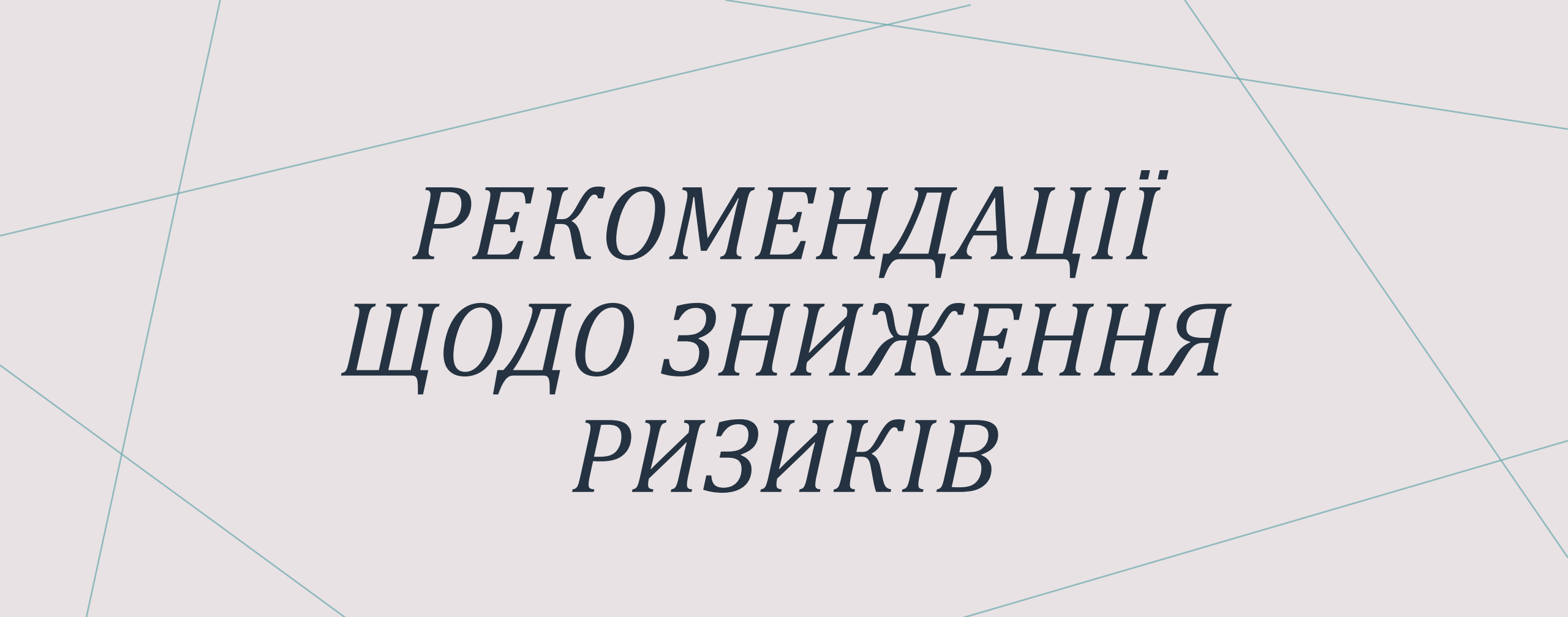
# *ПЛАНУВАННЯ ТА ВПРОВАДЖЕННЯ ПАТЧІВ*

Регулярне видача та впровадження патчів є ключовим елементом управління вразливостями. Виробники програмного забезпечення регулярно випускають оновлення для усунення виявлених проблем безпеки. Ефективне планування та вчасне впровадження цих патчів є важливою складовою стратегії забезпечення безпеки.

# *МОНІТОРИНГ ТА АУДИТ БЕЗПЕКИ*

Моніторинг безпеки веб-серверів — це постійний процес, що дозволяє вчасно виявляти нові вразливості та атаки. Аудит безпеки дозволяє систематично перевіряти стан безпеки та ефективність вжитих заходів. Регулярний моніторинг та аудит забезпечують постійний контроль за безпекою веб-сервера.





# *РЕКОМЕНДАЦІЇ ЩОДО ЗНИЖЕННЯ РИЗИКІВ*

# РОЗПОДІЛЕНІ АТАКИ НА ВІДМОВУ В ОБСЛУГОВУВАННІ (DDOS)



- Використовуйте надійну мережу доставки контенту (CDN).
- Налаштуйте брандмауери та системи запобігання вторгненням (IPS).
- Використовуйте обмеження швидкості та моніторинг трафіку.
- Розгляньте можливість використання сервісів або пристроїв, які спеціалізуються на боротьбі з DDoS-атаками.

# АТАКИ НА ВЕБ-ДОДАТКИ

- **Міжсайтовий скриптинг (XSS):** Захистіться від XSS-атак, впроваджуючи перевірку вхідних даних, кодування вихідних даних і використовуючи бібліотеки або фреймворки безпеки.
- **SQL-ін'єкції:** Запобігайте SQL-ін'єкціям, використовуючи параметризовані запити або заздалегідь підготовлені оператори, а також регулярно проводячи аудит безпеки ваших веб-додатків.
- **Підробка міжсайтових запитів (CSRF):** Захистіться від CSRF-атак, використовуючи токени проти CSRF, перевіряючи заголовки рефералів і використовуючи атрибут "SameSite" для файлів cookie.
- **Безпечні методи кодування:** Дотримуйтесь безпечних практик кодування, таких як перевірка вхідних даних, кодування вихідних даних, безпечне управління сесіями та оновлення залежностей програмного забезпечення.



# ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ПРОГРАМИ-ВИМАГАЧІ

- Використовуйте на сервері надійне антивірусне та антивірусне програмне забезпечення і регулярно оновлюйте його.
- Використовуйте надійну стратегію резервного копіювання, щоб забезпечити регулярне резервне копіювання критично важливих даних та їх безпечне зберігання за межами офісу.
- Впроваджуйте суворий контроль доступу, обмежуючи права доступу до файлів і каталогів, щоб запобігти несанкціонованим змінам.
- Регулярно перевіряйте свій веб-сервер на наявність шкідливого програмного забезпечення або вразливостей за допомогою інструментів і служб безпеки.





# АТАКИ ГРУБОЇ СИЛИ

- Впровадження надійних політик паролів для входу на сервер і в додатки.
- Впровадження механізмів блокування облікового запису після певної кількості невдалих спроб входу.
- Використання багатофакторної автентифікації (MFA) для додавання додаткового рівня безпеки до входів користувачів.
- Моніторинг логів сервера на предмет підозрілої активності та впровадження систем виявлення вторгнень (IDS) або систем запобігання вторгненням (IPS) для блокування зловмисних IP-адрес.



# ЗАСТАРІЛЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА ВИПРАВЛЕННЯ



- Регулярно оновлюйте та виправляйте всі програмні компоненти вашого веб-сервера.
- Моніторинг списків розсилки безпеки та оголошень постачальників на предмет останніх оновлень безпеки.
- Вимкнення або видалення невикористаного програмного забезпечення та плагінів для мінімізації поверхні атаки.

# ВІДСУТНІСТЬ ОНОВЛЕНЬ І ВИПРАВЛЕНЬ БЕЗПЕКИ

Налагодьте процес управління виправленнями, щоб забезпечити своєчасне встановлення оновлень безпеки для операційної системи, програмного забезпечення веб-сервера та інших компонентів.

Регулярно перевіряйте наявність рекомендацій з безпеки та патчів від відповідних постачальників і застосовуйте їх якнайшвидше.

Тестуйте патчі в непромисловому середовищі, перш ніж розгортати їх на промислових серверах.

Розгляньте можливість використання інструментів сканування вразливостей для виявлення будь-яких не виправлених вразливостей на вашому веб-сервері.

# РЕГУЛЯРНЕ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

На додаток до оновлень безпеки, переконайтеся, що все програмне забезпечення, яке працює на вашому веб-сервері, є актуальним, включаючи систему управління контентом (CMS), плагіни, теми та будь-які сторонні додатки. Застаріле програмне забезпечення може стати головною мішенню для зловмисників





# СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА ФІШИНГ



- Ознайомте себе та свою команду з поширеними тактиками соціальної інженерії, такими як фішингові електронні листи, телефонні шахрайства або спроби видати себе за іншу особу.
- Будьте обережні, коли ділитеся конфіденційною інформацією, особливо електронною поштою або телефонними дзвінками.
- Впровадьте механізми фільтрації електронної пошти та виявлення спаму, щоб зменшити ризик потрапляння фішингових листів до вашої поштової скриньки. Регулярно оновлюйте та навчайте співробітників про новітні методи соціальної інженерії та найкращі практики виявлення та повідомлення про підозрілі дії.

# НЕБЕЗПЕЧНА ПЕРЕДАЧА ФАЙЛІВ

- Використовуйте безпечні протоколи передачі файлів, такі як SFTP (SSH File Transfer Protocol) або FTPS (FTP Secure) для шифрування передачі файлів.
- Вимкніть незахищені протоколи, такі як звичайний FTP або Telnet, які передають дані відкритим текстом.
- Регулярно перевіряйте журнали передачі файлів на предмет будь-яких незвичних дій або спроб несанкціонованого доступу.
- Впроваджуйте надійні механізми автентифікації, такі як автентифікація з відкритим ключем, для безпечної передачі файлів.



# НЕДОСТАТНЄ ВЕДЕННЯ ЖУРНАЛІВ І МОНІТОРИНГ

- Увімкніть та налаштуйте детальне ведення журналів на вашому веб-сервері, щоб фіксувати відповідні події та дії, пов'язані з безпекою.
- Впровадьте централізовану систему керування журналами для збору та аналізу логів з різних джерел.
- Налаштуйте моніторинг у режимі реального часу та сповіщення про підозрілі дії, такі як багаторазові невдалі спроби входу або незвичні шаблони трафіку.
- Регулярно переглядайте та аналізуйте дані журналів для виявлення потенційних інцидентів безпеки або вразливостей.





# НЕДОСТАТНІЙ КОНТРОЛЬ ДОСТУПУ



- Впровадження принципу найменших привілеїв, надаючи користувачам лише ті дозволи, які необхідні для виконання їхніх завдань.
- Регулярно переглядайте та оновлюйте привілеї доступу користувачів відповідно до їхніх ролей та обов'язків.
- Впроваджуйте надійну політику використання паролів, включаючи вимоги до складності та регулярну зміну паролів.
- Впроваджуйте двофакторну автентифікацію (2FA) для важливих облікових записів та адміністративного доступу.

# ФІЗИЧНА БЕЗПЕКА



- Зберігайте сервери в захищених і закритих приміщеннях з обмеженим доступом.
- Впроваджуйте системи спостереження, сигналізації та контролю доступу, щоб запобігти несанкціонованому фізичному доступу.
- Регулярно перевіряйте серверні приміщення та обладнання для виявлення та усунення будь-яких вразливостей або потенційних ризиків.



# ОБІЗНАНІСТЬ І НАВЧАННЯ СПІВРОБІТНИКІВ

- Регулярні тренінги з підвищення обізнаності про безпеку, що охоплюють такі теми, як гігієна паролів, обізнаність про фішинг та безпечні звички перегляду веб-сторінок.
- Чіткі політики та інструкції щодо прийнятного використання ресурсів компанії та поводження з конфіденційною інформацією.
- Заохочуйте співробітників негайно повідомляти про будь-які підозрілі дії або потенційні інциденти безпеки.

# ***РЕГУЛЯРНА ОЦІНКА ВРАЗЛИВОСТЕЙ І ТЕСТУВАННЯ НА ПРОНИКНЕННЯ***





# БЕЗПЕЧНА КОНФІГУРАЦІЯ МЕРЕЖІ

- Налаштуйте мережу та брандмауер так, щоб пропускати лише необхідний вхідний та вихідний трафік.
- Застосовуйте принцип найменших привілеїв, обмежуючи доступ до певних IP-адрес, портів і протоколів.
- Регулярно переглядайте та оновлюйте правила брандмауера, щоб переконатися, що вони відповідають вашим вимогам безпеки.





# ***БЕЗПЕЧНА КОНФІГУРАЦІЯ ВЕБ-СЕРВЕРА***

- Дотримуйтесь найкращих практик для захисту конфігурації вашого веб-сервера.
- Вимкніть непотрібні служби, видаліть програми за замовчуванням або типові програми
- Налаштуйте безпечні протоколи шифрування (наприклад, TLS) для захисту даних під час передачі.



# РЕГУЛЯРНЕ РЕЗЕРВНЕ КОПІЮВАННЯ ТА АВАРІЙНЕ ВІДНОВЛЕННЯ



- Впровадьте надійну стратегію резервного копіювання, яка включає регулярне створення резервних копій даних і конфігурацій вашого веб-сервера.
- Зберігайте резервні копії надійно і періодично тестуйте процес відновлення, щоб забезпечити цілісність даних.
- Створіть план аварійного відновлення, щоб швидко відновити веб-сервер у разі інциденту безпеки або збою системи.

# МОНІТОРИНГ БЕЗПЕКИ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ

- Впровадьте план реагування на інциденти безпеки, який окреслює кроки, що мають бути зроблені у випадку порушення безпеки.
- Налаштуйте інструменти моніторингу безпеки в режимі реального часу, щоб оперативно виявляти потенційні інциденти безпеки та реагувати на них



# БУДЬТЕ В КУРСІ ПОДІЙ



- Будьте в курсі останніх тенденцій у сфері кібербезпеки, вразливостей та найкращих практик.
- Регулярно слідкуйте за блогами, форумами та джерелами галузевих новин, щоб бути в курсі нових загроз та методів їх подолання.

# ЗАЛУЧАЙТЕ ФАХІВЦІВ З БЕЗПЕКИ

- Розгляньте можливість залучення фахівців з кібербезпеки або постачальників керованих послуг безпеки (MSSP) для оцінки стану безпеки вашого веб-сервера, забезпечення постійного моніторингу та надання експертних рекомендацій щодо зменшення ризиків.





# **БЕЗПЕКА ВЕБ- СЕРВЕРА – ЦЕ БЕЗПЕРЕРВНА РОБОТА**

Вкрай важливо регулярно переглядати та вдосконалювати свої методи безпеки, щоб випереджати нові загрози

# *ВИСНОВОК*

Оцінка та управління вразливостями веб-серверів – це невід’ємна частина стратегії забезпечення безпеки онлайн середовища. Ретельна ідентифікація та ефективно управління вразливостями дозволяють зменшити ризики, пов’язані з атаками зловмисників, і забезпечують надійний захист веб-серверів. Постійна підтримка безпеки та вдосконалення процесів оцінки стану безпеки є ключовими аспектами в сучасному цифровому світі, де безпека даних та конфіденційність інформації мають величезне значення.