



# ЗМІСТ

- 1** Вступ
- 2** Алгоритм роботи
- 3** Вхід в систему
- 4** Адміністративна панель

## **Модулі безпеки:**

- 5** SQL-ін'єкції
- 6** Боти
- 7** Проксі
- 8** Спамери
- 9** Логи
- 10** Бани

## **11** Особливості

- 12** Всі функції



# 1. Вступ



UKEY SECURITY використовує інтелектуальні алгоритми (аналогічні тим, що використовуються великими галузевими компаніями) для виявлення всіх відомих хакерських атак, а також нових невідомих загроз з використанням розпізнавання коду та шаблонів.

Система включає в себе потужну адміністративну панель, з якої ви можете переглядати всі журнали загроз, а також з діючу систему заборон, за допомогою котрої можуть бути заблоковані відвідувачі (IP-адреси), країни, діапазони IP-адрес, інтернет-провайдери (ISP), браузерери, операційні системи (ОС).

## 2. Алгоритм роботи



Невідоме ПЗ атакує веб-додаток



Використовуючи алгоритми та бази даних ПЗ визначається, як шкідливе



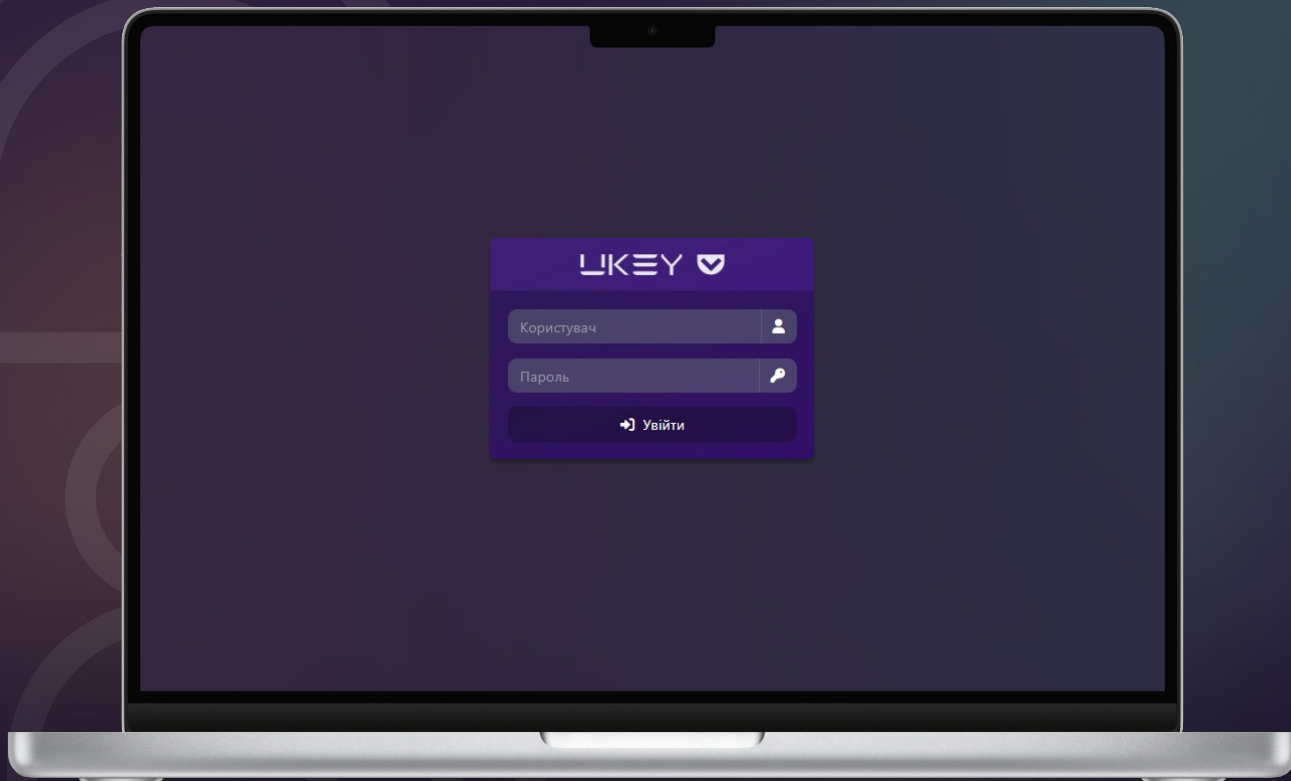
Блокування будь-якого впливу даного ПЗ на веб-додаток



Формування докладного звіту про загрозу та внесення даних в логи

### 3. Вхід в систему

Після інсталяції продукту на вашу веб-платформу, адміністратор видасть дані для входу в систему Ukey. Вхід здійснюється безпосередньо на вашому сервері або хостингу.



## 4. Адміністративна панель

Після входу в систему захисту, ви будете перенаправлені до адміністративної панелі, де можете переглядати всю доступну інформацію про веб-сайт який захищає система, а також контролювати активність додаткових модулів.



8 МОДУЛІВ БЕЗПЕКИ:

ДІЄВІ:

- SQL-ін'єкції
- Боти
- Проксі
- Спамери

ДОДАТКОВІ:

- Логи
- Бани
- Виявлення Adblocker
- Фільтр цензури (в тестовому режимі)

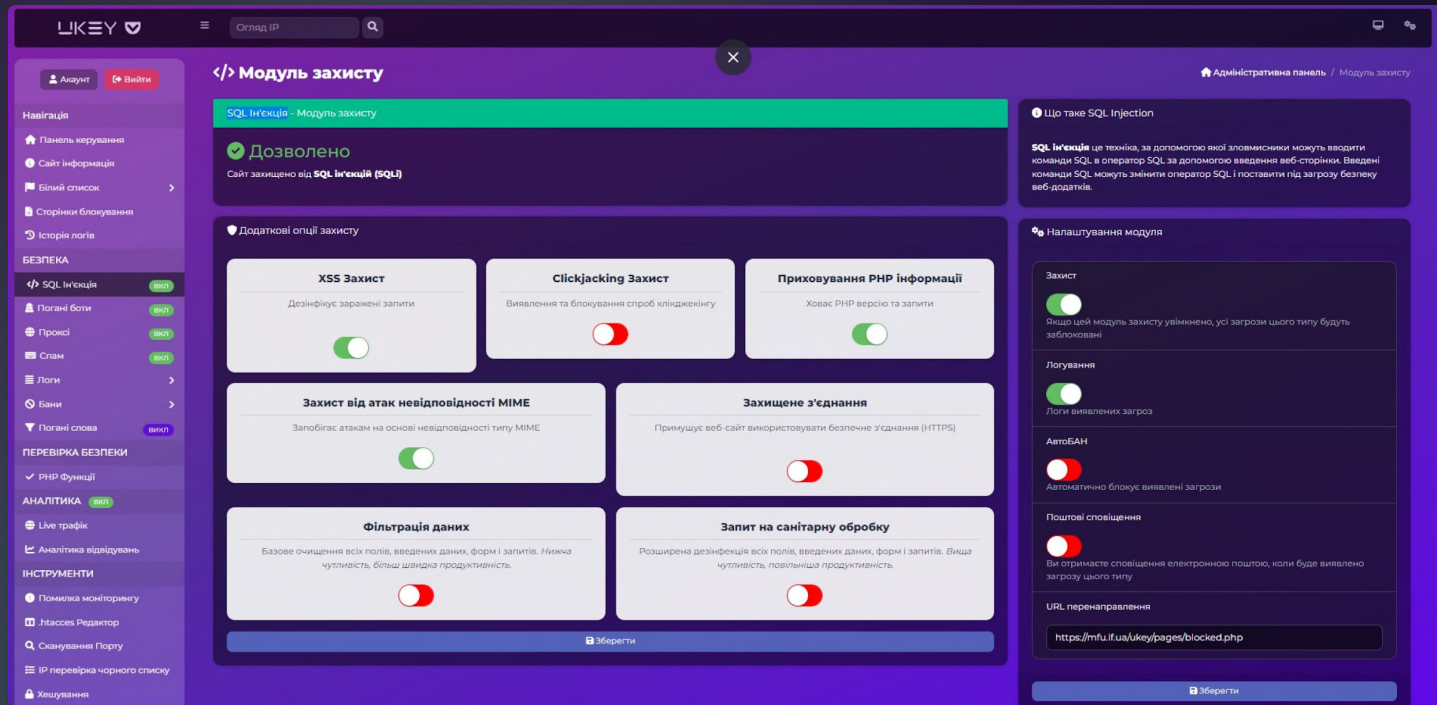


**МОДУЛІ  
БЕЗПЕКИ**



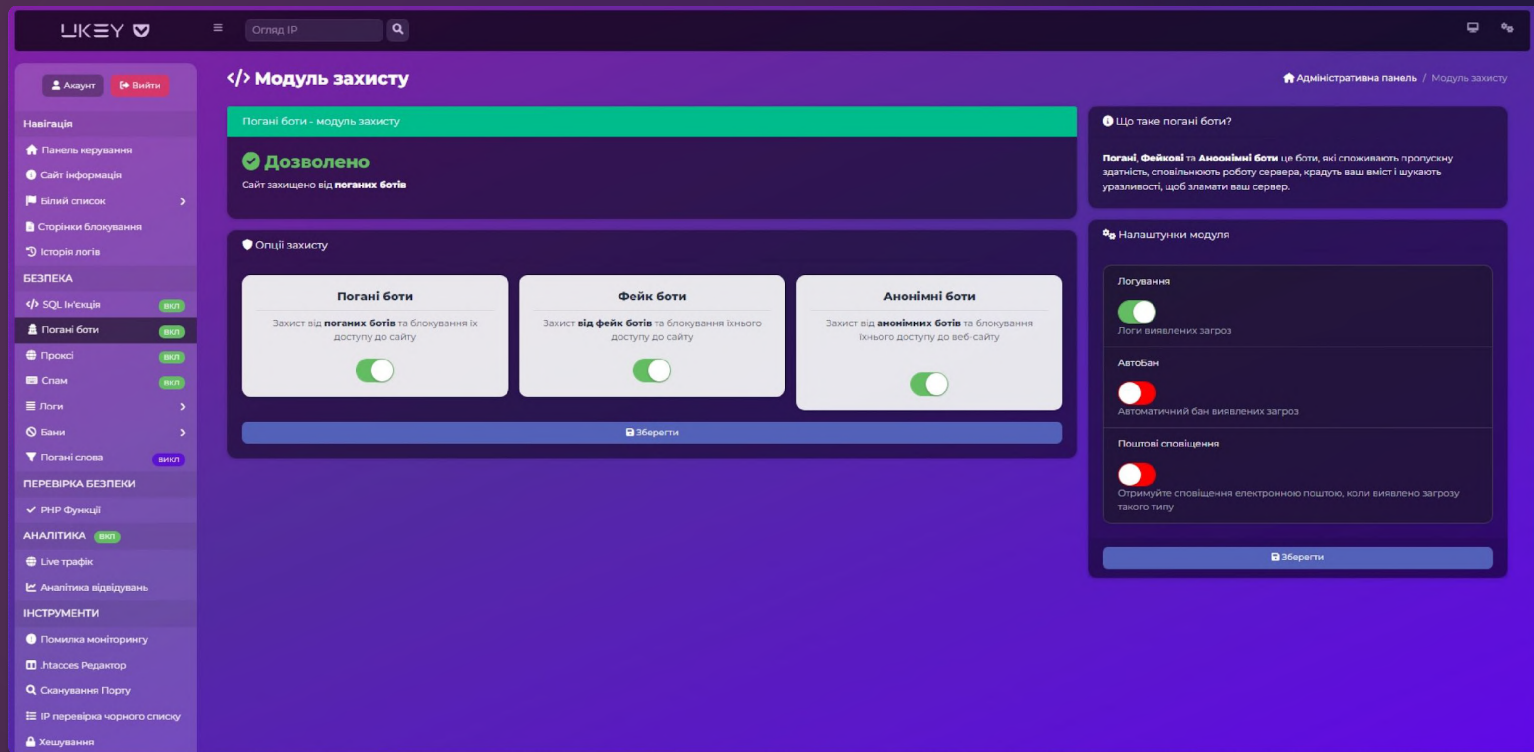
# 5. SQL-ін'єкції

SQL Injection — це технологія, за якої зловмисні користувачі можуть вводити команди SQL в оператор SQL на веб-сторінці. Ін'єкційні команди SQL можуть змінити оператор SQL та порушити безпеку веб-програми. Щоб запобігти цьому UKEY запускає модуль протидії SQL-ін'єкціям.



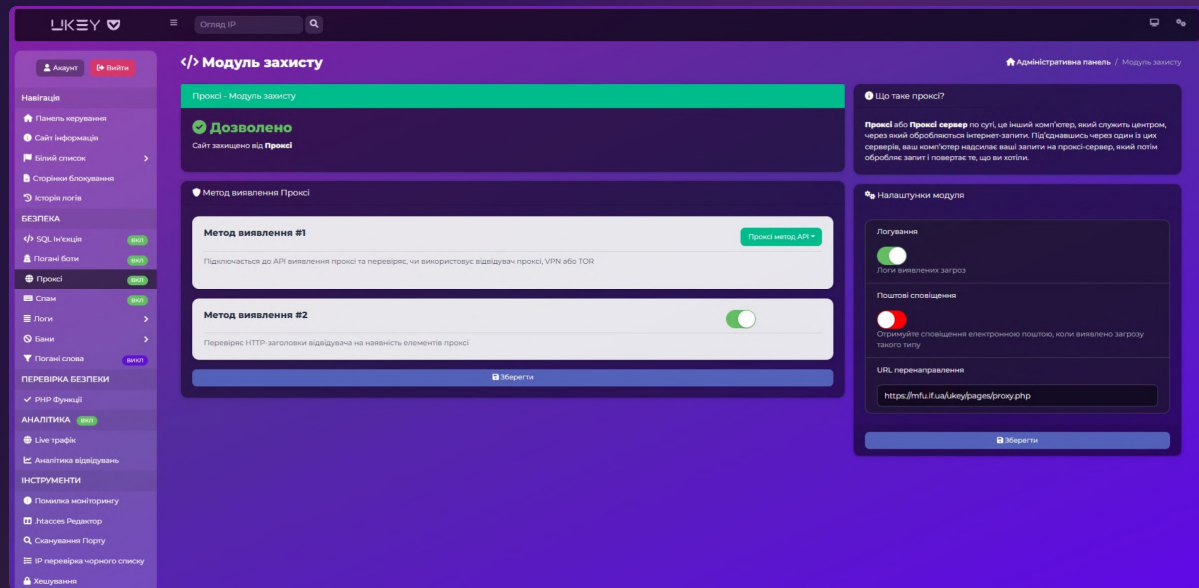
## 6. Боти

Боти, Фейкові боти і Анонімні боти — це боти, котрі споживають пропускну здатність, сповільнюють роботу вашого серверу, крадуть ваш вміст та шукають вразливості для компрометації серверу. Система здійснює жорсткий контроль за підозрілими відвідуваннями та веде журнал загроз від переходів ботів на сайт.



# 7. Проксі

Проксі або проксі-сервер — загалом є ще одним комп'ютером, котрий служить концентратором, за допомоги которого обробляються запити в Інтернеті. Підключившись через один з цих серверів, ваш комп'ютер надсилає запити на проксі-сервер, котрий потім обробляє ці запити і повертає те, що ви хотіли. Даний модуль використовує 3 методи виявлення:



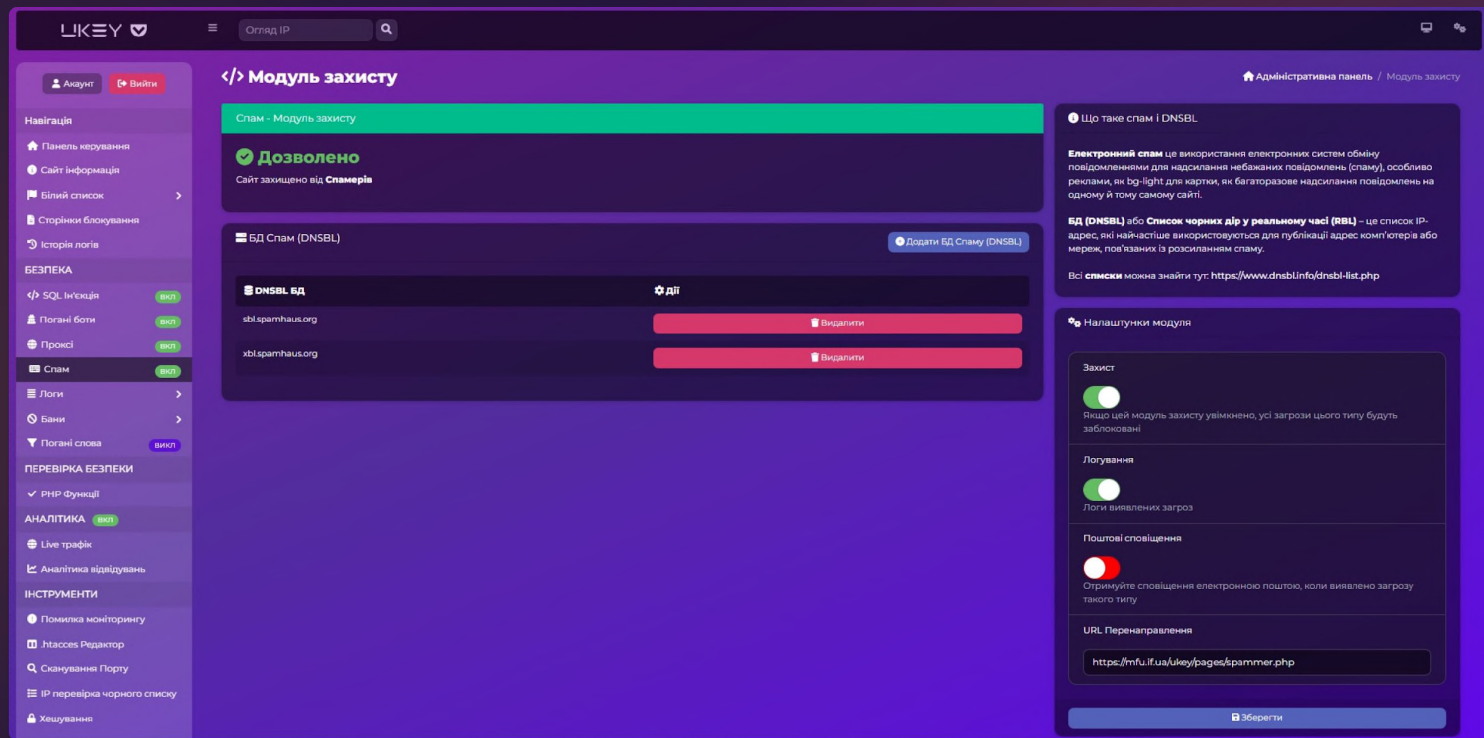
**1** Підключається до API виявлення проксі-серверу та перевіряє, чи використовує відвідувач проксі-сервер, VPN або TOR.

**2** Перевіряє заголовки HTTP відвідувача на наявність елементів проксі.

**3** Сканує порти відвідувача, щоб показати чи знаходиться він за проксі-сервером. Цей метод виявлення в основному використовується для виявлення та блокування проксі сайтів в Інтернеті.

# 8. Спамери

Електронний спам полягає у використанні електронних систем обміну повідомленнями для відправлення небажаних повідомлень (спаму), особливо реклами, таких як картка-тіло bg-light, або повторне відправлення повідомлень на одному веб-сайті.



Список Blackhole на основі DNS (DNSBL) або Список Blackhole в реальному часі (RBL) - це перелік IP-адресов, які частіше за все використовуються для публікації адрес комп'ютерів або мереж, пов'язаних зі спамом.





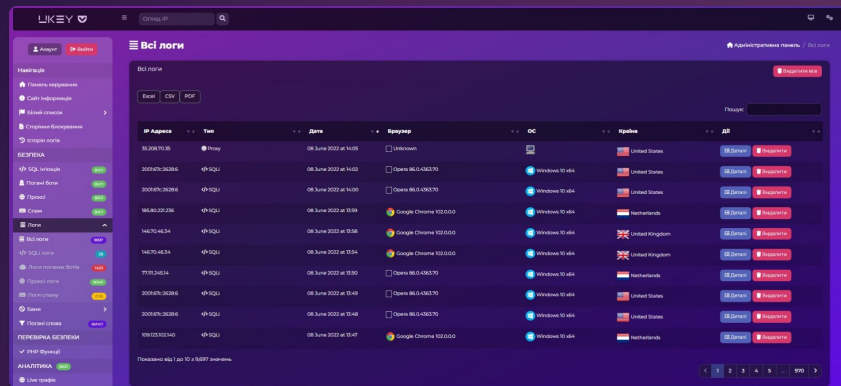
# **ДОДАТКОВІ МОДУЛІ БЕЗПЕКИ**



# 9. Логи

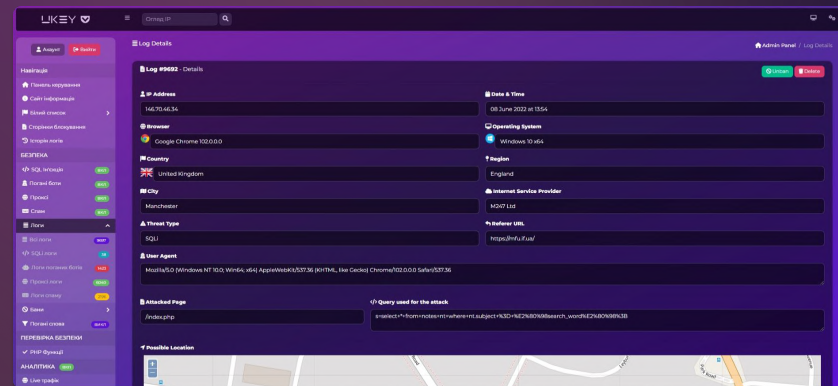
## Логи

Фіксують всі дії користувачів котрі були здійснені на веб-сайті, за всіма модулями безпеки.



## SQLi Логи / Логи проксі / Логи Ботів / Логи спамерів

В даному розділі можна приймати рішення для загроз що були виявлені



# 10. Бани

В цьому розділі можна встановлювати правила для певних загроз, зокрема блокувати їм доступ до ресурсу, якщо система завдала підозрілу активність з тої або іншої адреси. Банити звернення можна за параметрами країни, IP-адреси, або за використання стороннього ПЗ в виді Adblocker.

ЛКЕY

Огляд IP

Акаунт

Вийти

Навігація

Панель керування

Сайт інформація

Білий список

Сторінки блокування

Історія логів

БЕЗПЕКА

SQL ін'єкції

Погані боти

Проксі

Слани

Логи

Бани

IP Бани

Бани за країнами

IP шкала бану

Інші бани

Погані слова

ПЕРЕВІРКА БЕЗПЕКИ

✓ RNP Функції

АНАЛІТИКА

Live трафік

Аналітика відвідувань

IP Бани

Виділити все

Excel

CSV

PDF

Пошук:

IP Адреса

Забанено на

Перенаправлено

Автобан

Дії

146.70.46.34

08 June 2022

Ні

Ні

Редагувати

Розбан

95163.255.137

08 June 2022

Ні

Ні

Редагувати

Розбан

95163.255.209

08 June 2022

Ні

Ні

Редагувати

Розбан

45142.122.34

01 June 2022

Ні

Ні

Редагувати

Розбан

34124.203.16

01 June 2022

Ні

Ні

Редагувати

Розбан

114.119.135.64

01 June 2022

Ні

Ні

Редагувати

Розбан

95163.255.211

01 June 2022

Ні

Ні

Редагувати

Розбан

95163.255.229

01 June 2022

Ні

Ні

Редагувати

Розбан

65154.226.166

01 June 2022

Ні

Ні

Редагувати

Розбан

212143.94.254

01 June 2022

Ні

Ні

Редагувати

Розбан

Показано від 1 до 10 з 12 значень

<

1

2

>

Адміністративна панель / IP Бани

Бан IP адрес

IP Адреса:

Причина:

Перенаправлення на сторінку / сайт:

URL перенаправлення:

Бан

# 11. Особливості



## **Захист SQLi**

Захист від ін'єкцій SQL (SQLi) і вразливостей XSS (міжсайтові сценарії).

## **Захист проксі**

Захист від відвідувачів проксі, VPN та TOR або так званих людей, що ховаються за проксі.

## **Інтеграція DNSBL**

Інтеграція з однією з кращих баз даних спаму (DNSBL) для захисту вашого веб-сайту від псевдо-відвідувачів.

## **Захист від ботів та сканерів**

Блокує ботів та сканери, котрі забирають пропускну здатність вашого веб-сайту. Перевірка ботів пошукової системи, котрі відвідують ваш веб-сайт, дійсні вони або підроблені боти.

## **Інтелектуальне розпізнавання шаблонів**

Виявляє невідомі і нульові атаки, а алгоритми промислової міцності виявляють відомі хакерські атаки.



# 12. Всі функції

## Журнали загроз (логи)

Кожна загроза і атака реєструється в базі даних.

## Автобан

Функція, яка автоматично блокує зловмисників.

## Захист від фейкових ботів

Перевірка ботів пошукової системи, які відвідують ваш веб-сайт, істинні вони чи підроблені боти.

## Захист від ботів і сканерів

Блокує ботів і сканери, які забивають пропускну здатність вашого веб-сайту.

## Інтелектуальне розпізнавання шаблонів

Виявляє невідомі і нульові атаки.

## Алгоритми промислової міцності

Виявляє відомі хакерські атаки.

## Фільтрування поганих слів

Захисний модуль, який фільтрує нецензурні слова, погані слова, погані посилання, погані пропозиції та інший поганий вміст в режимі реального часу.

## Система заборони

Допомагає блокувати і направляти відвідувачів/користувачів (IP-адреси), країни, діапазони IP, операційні системи, браузер, постачальників послуг Інтернету (ISP) і рефералів.

## Виявлення Adblocker

Виявляє і блокує відвідувачів, що використовують Adblockers, щоб приховати рекламу на веб-сайті.

## Інтеграція DNSBL

Інтеграція з однією з кращих баз даних спаму (DNSBL) для захисту вашого веб-сайту від псевдо-відвідувачів.

## Санітарія вхідних даних

Модуль захисту, який автоматично дезінфікує всі вхідні та вихідні запити і відповіді.

## Захист проксі

Захист від відвідувачів проксі, VPN і TOR або так званих людей, котрі ховаються за проксі.

## Захист SQLi

Захист від ін'єкцій SQL (SQLi) і вразливостей XSS (міжсайтові сценарії).

## Захист від спаму

Захист від спамерів і спам-ботів, котрі направлені на ваш веб-сайт.

## Analytics

Відслідковуйте та аналізуйте, як люди використовують ваш веб-сайт.

## Перевірка заголовків

Заголовки відповідей кожного відвідувача будуть перевірятися, якщо є підозрілі предмети, їх доступ до веб-сайту буде обмежено.

## Інформаційна панель зі статистикою

На інформаційній панелі ви можете перевірити статистику відносно захисту вашого веб-сайту.

## Сканування всіх запитів в режимі реального часу

GET, POST та інші типи даних.

## Перевірка конфігурації PHP

Перевірте поточну конфігурацію PHP на наявність потенційних недоліків безпеки.

## Сповіщення електронною поштою

Ви отримаєте сповіщення електронною поштою, коли буде виявлена атака або загроза.

## Детальні журнали

Журнали містять багато інформації про загрозу/атаку, а саме браузер, операційна система, країна, місто, агент користувача, розташування на мапі та інша корисна інформація.

## Білий список IP і файлів

Список IP-адрес і файлів, які програма проігнорує і не заблокує.

## Редактор .htaccess

Відредагуйте файл .htaccess безпосередньо з панелі адміністратора, не потрібно відкривати його в будь-якому зовнішньому редакторі.

## Прямий трафік

Спостерігайте за відвідувачами в режимі реального часу, коли вони взаємодіють з вашим веб-сайтом.

## Моніторинг помилок

Корисний інструмент, який відображає всі зареєстровані помилки вашого веб-сайту.

## Інформація про сайт

Сторінка з величезною кількістю інформації і статистики про ваш веб-сайт. Сценарій дуже легкий і не сповільнює час завантаження веб-сайту.

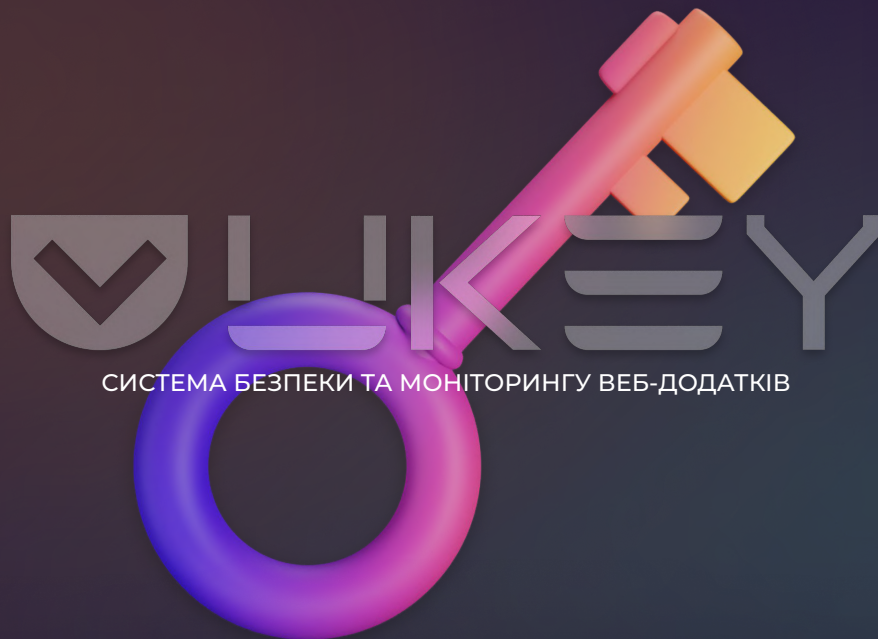
## Пошук IP

Ви можете досліджувати IP-адресу та перевірити його наявність в базі даних сценарію.

## Корисні інструменти

Колекція інструментів, таких як .htaccess Editor, Hash Generator та інші.





СИСТЕМА БЕЗПЕКИ ТА МОНІТОРИНГУ ВЕБ-ДОДАТКІВ