

Dawid Kowalski

ZABEZPIECZENIE FORMULARZY

DOKUMENTACJA FORMSEC

DOKUMENTACJA PROJEKTU

OPIS PROJEKTU

NAZWA PROJEKTU
FORMSEC

PACKAGIST
KOWALSKIDAWID/FORMSEC

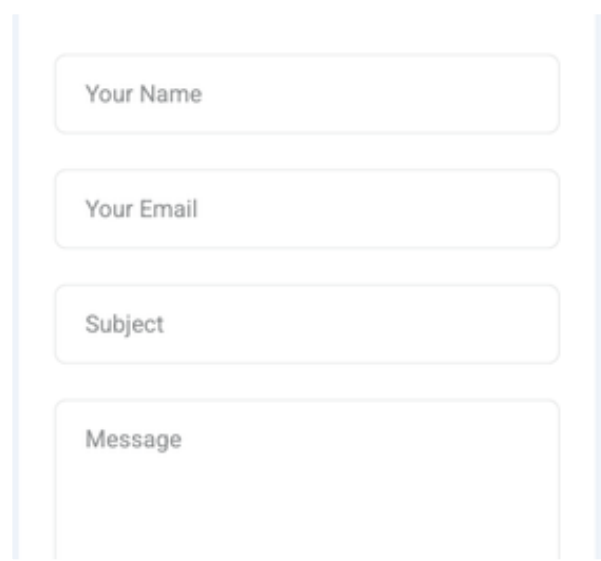
TECHNOLOGIA
PHP 5.6 LUB NOWSZA

GITHUB
KOWALSKIDAWID/FORMSEC

OPIS PROJEKTU

Biblioteka pozwala na zabezpieczenie formularzy na stronie internetowej stworzonej w języku PHP. Może być dodany na stronie dowolnej wielkości skierowanej na rynek polskijęzyczny.

Na podstawie treści, adresu email i adresu IP weryfikuje jej bezpieczeństwo oraz to czy została przesłana przez człowieka lub przez skrypty.



WYMAGANIA TECHNICZNE

- Zainstalowane PHP w wersji 5.6 lub nowsze.
- 50MB wolnego miejsca na dysku
- Otwarte port wychodzące **43**, **80**, oraz **443**

GDZIE WYKORZYSTAĆ

DODAJ DO:

- Formularz kontaktowy - niebezpieczna wiadomość nie dociera do obsługującego
- Formularz komentarzy - zmniejsz czas potrzebny na moderację
- Inne formularza - dodatek to reCAPTCHA

NIE DODAWAJ DO:

- formularzy do zgłaszania nadużyć lub błędów aplikacji
- formularzy przyjmujących treści języku rosyjskim, ukraińskim i innych zawierających cyrylicę

PRZYKŁAD WDROŻENIA



01

STRONA FIRMOWA

Zastosowanie biblioteki zabezpieczającej formularze pozwoliło skutecznie zablokować spam w formularzu kontaktowym, poprawiając jakość zgłoszeń i zwiększając zaufanie klientów.

02

PROJEKT SPOŁECZNY

Formularze zgłoszeniowe do wydarzeń i sekcja komentarzy zostały zabezpieczone przed botami. Zmniejszyło to liczbę fałszywych zapisów i umożliwiło bezpieczną komunikację uczestników.

03

PORTAL INFORMACYJNY

Wdrożenie biblioteki pozwoliło chronić formularze opinii i zgłoszeń od czytelników, eliminując masowe ataki spamowe i poprawiając jakość oraz wiarygodność przesyłanych treści.

KORZYŚCI I ZAGROŻENIA

KORZYŚCI

Wdrożenie biblioteki znacząco podnosi poziom bezpieczeństwa i jakości danych, poprawiając komfort użytkownika.

GLÓWNE ZALETY

- Ochrona przed spamem i botami – zmniejsza ilość niepożądanych zgłoszeń.
- Poprawa jakości danych – trafiają tylko wartościowe, prawdziwe zgłoszenia.
- Zwiększenie bezpieczeństwa – ogranicza ryzyko ataków typu injection i phishing.
- Lepsze doświadczenie użytkownika – nowoczesne zabezpieczenia działają dyskretnie.

ZAGROŻENIA

Pomimo licznych korzyści, biblioteka może być dodatkową przyczyną awarii oraz nieaktualizowana przepuszczać spam.

GLÓWNE WADY

- Nieaktualizowana biblioteka – może stać się podatna na nowe metody ataku.
- Fałszywe alarmy – czasem blokowane są poprawne zgłoszenia (false positives).
- Zależność od zewnętrznych usług (np. RIPE Database) – ryzyko awarii lub zmian w polityce prywatności.



Advantage



Disadvantage



DOKUMENTACJA PROJEKTU

SPOSÓB UŻYCIA

01 INSTALACJA COMPOSER

Bibliotekę można zainstalować za pomocą narzędzia composer. Composer to narzędzie służące do zarządzania zależnościami projektów PHP

```
php -r "copy('https://getcomposer.org/installer', 'composer-setup.php');"
php composer-setup.php
php -r "unlink('composer-setup.php');"
sudo mv composer.phar /usr/local/bin/composer
```

```
bash-3.2$ php -r "copy('https://getcomposer.org/installer', 'composer-setup.php');"
bash-3.2$ php composer-setup.php
All settings correct for using Composer
Downloading...

Composer (version 2.8.9) successfully installed to: /Users/dawidkowalski/formsec/composer.phar
Use it: php composer.phar

bash-3.2$ php -r "unlink('composer-setup.php');"
bash-3.2$ ls
composer.phar
bash-3.2$
```

```
bash-3.2$ composer require kowalskidawid/formsec
Composer could not detect the root package (user/nowa-strona) version, defaulting to 1.0.0
./composer.json has been updated
Composer could not detect the root package (user/nowa-strona) version, defaulting to 1.0.0
Running composer update kowalskidawid/formsec
Loading composer repositories with package information
Updating dependencies
Lock file operations: 1 install, 0 updates, 0 removals
  - Locking kowalskidawid/formsec (v0.0.3)
Writing lock file
Installing dependencies from lock file (including require-dev)
Package operations: 1 install, 0 updates, 0 removals
  - Installing kowalskidawid/formsec (v0.0.3): Extracting archive
Generating autoload files
No security vulnerability advisories found.
Using version ^0.0.3 for kowalskidawid/formsec
bash-3.2$
```

02 INSTALACJA BIBLIOTEKI

Po zainstalowaniu programu composer możesz zainstalować bibliotekę do swojej strony

```
composer init
composer require kowalskidawid/formsec
```

03 ZABEZPIECZENIE FORMULARZA

Po zainstalowaniu biblioteki można skorzystać z klasy FormSec\Checker, przekazać w konstruktorze: treść, adres email, oraz tablicę ze ścieżkami do plików. Po wywołaniu Checker::check() sprawdzisz liczbę punktów za pomocą Checker::getScore()

```
public function send(Request $request)
{
    $message = [
        'email' => $request->post( key: 'email'),
        'content' => $request->post( key: 'content'),
        'ip_address' => $request->post( key: 'ip_address'),
        'source_ip' => $request->ip(),
    ];
    $formCheck = new Checker();
    $formCheck->check($message['content'], $message['email'], $message['ip_address']);
    $score = $formCheck->getScore();
    if ($score > 60) {
        Message::create($message);
        return redirect()->route( route: 'contact')
            ->withSuccess('Dziękujemy za wiadomość! Odpowiemy najszybciej jak to możliwe.');
```

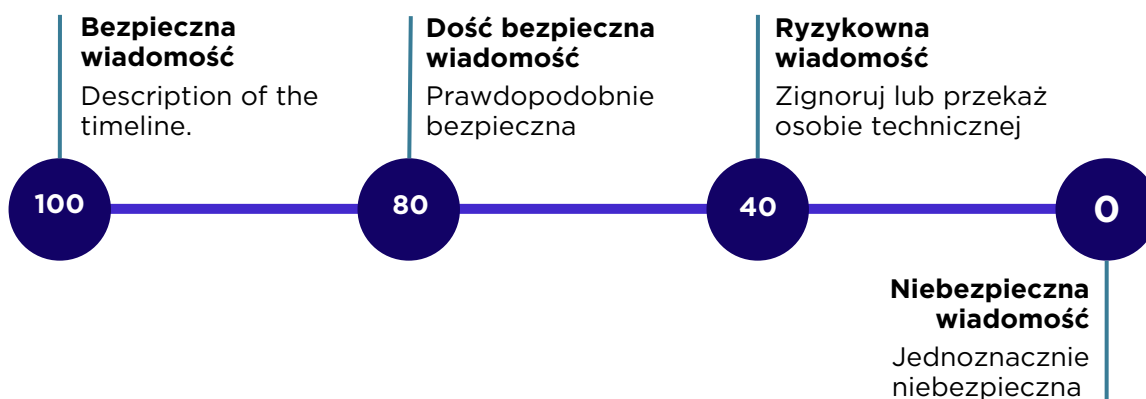
SYSTEM PUNKTACJI

ZASADA DZIAŁANIA

Klasa szuka elementów wskazujących że wiadomość może nie być przesłana przez człowieka. Na podstawie składowych wiadomości jak IP z serwera czy treść wyglądającą na niebezpieczną obniżana jest końcowa ocena.

Wiadomość oceniana jest w skali od 0 do 100, gdzie 100 to zwykły użytkownik.

SKALA PUNKTOWA



OCENINE ELEMENTY

Blokowanie proxy

Wykrywanie darmowych oraz komercyjnych rozwiązań proxy używanych przez boty

Blokowanie VPN

Wykrywanie publicznych oraz komercyjnych rozwiązań VPN używanych przez boty

Weryfikacja domen

90% domen użytych w atakach rejestrowana jest do 3 miesięcy przed jej użyciem.

Monitorowanie CERT

Sprawdzamy treść i nadawcę pod kątem ostrzeżeń CERT Polska

Analiza treści

Weryfikacja treści pod kątem ataków XSS, złośliwych linków oraz języka

Antywirus

Weryfikacja bezpieczeństwa załączników za pomocą integracji z VirusTotal

MOŻLIWE PROBLEMY I BŁĘDY

PRZYCZYNY

biblioteka opiera się o komunikację z zewnętrznymi serwisami na portach 43, 80, 443 oraz wykorzystuje dysk do tymczasowego przechowywania tych informacji. W przypadku problemów sprawdź uprawnienia katalogów, zaporę sieciową, DNS oraz konfigurację php jeżeli została zmieniona.

PRZYKŁADY

file could not be downloaded

Biblioteka używa `file_get_content` do pobierania aktualnych informacji. sprawdź czy `allow_url_fopen` jest włączone

Failed to open stream : No such file or directory

Sprawdź czy katalog `vendor` ma uprawnienia do odczytu oraz czy użytkownik jest w prawidłowej grupie

open_basedir restriction in effect

Upewnij się, że katalog `vendor` mieści się w ścieżce dozwolonej przez `open_basedir` lub tymczasowo wyłącz `open_basedir`

Connection timed out

Biblioteka łączy się z zewnętrznymi systematami, sprawdź czy port 43 oraz port 80 i 443 nie jest blokowany przez firewall

php_network_getaddresses: getaddrinfo failed

Sprawdź konfigurację DNS w pliku `/etc/resolv.conf` lub dodaj zewnętrzny serwer DNS

FORMSEC
-
**ZABEZPIECZENIE
FORMULARZY**

formsec.pl