

## Zgłoszenie błędu nr: 1.1

### Tytuł błędu:

Formularz kontaktowy przepuszcza niepoprawne dane (brak walidacji pól)

### Opis błędu:

Formularz kontaktowy na stronie umożliwia przesłanie wiadomości mimo wprowadzenia **niepoprawnych i niepełnych danych** we wszystkich polach, w tym:

- Imię i nazwisko: tylko jeden znak (.)
- Adres e-mail: bardzo krótki (a@b.pl)
- Temat: puste pole
- Wiadomość: pojedynczy znak (.)

Brakuje walidacji poprawności danych użytkownika, co może prowadzić do:

- nadużyć (spam, boty),
- błędów po stronie administratora (brak możliwości kontaktu),
- negatywnego odbioru przez użytkownika (strona wygląda nieprofesjonalnie).

### Kroki do odtworzenia:

1. Przejdź na stronę formularza kontaktowego.
2. Wprowadź dane:
  - Imię i nazwisko: .
  - Adres e-mail: a@b.pl
  - Temat: (pozostaw puste)
  - Wiadomość: .
  - Zaznacz checkbox z zgodą marketingową
3. Kliknij „Wyślij”.
4. Formularz zostaje przesłany bez jakiegokolwiek błędu lub ostrzeżenia.

### **Oczekiwane zachowanie:**

Formularz powinien uniemożliwić przesłanie wiadomości, jeśli:

- Imię i nazwisko zawiera mniej niż 2 znaki i/lub nie są to litery alfabetu,
- Adres e-mail jest podejrzanie krótki (np. jeden znak przed i po „@”),
- Temat jest pusty (jeśli wymagany),
- Treść wiadomości ma mniej niż np. 10 znaków i nie zawiera sensownej treści.

Dodatkowo warto:

- Zablokować znaki interpunkcyjne jako jedyne znaki w polu,
- Wymusić poprawny format każdego pola.

### **Rekomendacja:**

➡ Wprowadzić walidację front-endową i back-endową:

- Imię i nazwisko: min. 2 znaki, tylko litery (opcjonalnie z myślnikiem),
- E-mail: sprawdzenie długości przed @ i po @, użycie regex,
- Temat i wiadomość: wymagane pola z min. liczbą znaków (np. 10),
- Odrzucić pola zawierające tylko znaki interpunkcyjne.

➡ Dodać CAPTCHA / honeypot jako zabezpieczenie przed spamem.

➡ W przypadku błędu – pokazać informację w UI (np. na czerwono pod polem).

### **Załączniki:**

- Zrzut ekranu wypełnionego formularza
- Link do formularza kontaktowego (należy podać)

IMIĘ I NAZWISKO

ja

ADRES E-MAIL

a@b.pl

TEMAT

x

WIADOMOŚĆ (OPCJONALNE)

x



WYRAŻAM ZGODĘ NA PRZESYŁANIE NA PODANY PRZEZE MNIE ADRES E-MAIL INFORMACJI HANDLOWYCH W CELU MARKETINGU BEZPOŚREDNIEGO PRODUKTÓW ORAZ USŁUG ROBERT BOSOWSKI POROLEX-PLUS Z SIEDZIBĄ W TARNOWIE PRZY WYKORZYSTANIU TELEKOMUNIKACYJNYCH URZĄDZEŃ KOŃCOWYCH I/LUB AUTOMATYCZNYCH SYSTEMÓW WYWOŁUJĄCYCH.

Wyślij

Twoja wiadomość została wysłana. Dziękujemy!

## Zgłoszenie błędu nr: 1.2

### Tytuł błędu:

Panel logowania WordPressa dostępny publicznie bez ograniczeń dostępu

### Opis błędu:

Panel logowania WordPressa ([wp-login.php](https://porolex.pl/wp-login.php)) jest dostępny publicznie pod adresem:

 <https://porolex.pl/wp-login.php>

Dostęp do tego panelu nie jest w żaden sposób ograniczony – każdy użytkownik (w tym boty i potencjalni atakujący) może wejść na stronę logowania i próbować:

- zgadywać dane logowania (brute-force),
- testować różne hasła,
- sprawdzać istnienie kont,
- rozpoznać, że strona działa na WordPressie (co zwiększa ryzyko ataku ukierunkowanego).

### Kroki do odtworzenia:

1. Otwórz dowolną przeglądarkę internetową.
2. Wejdź na adres: <https://porolex.pl/wp-login.php>
3. Pojawia się panel logowania WordPressa.

### Oczekiwane zachowanie:

Panel logowania WordPressa powinien być **niewidoczny lub ograniczony** dla nieautoryzowanych użytkowników – np. dostęp tylko z określonego adresu IP lub za pomocą dodatkowego hasła.

### Rekomendacje:

- ➡ Zmienić domyślny adres logowania za pomocą wtyczki, np. **WPS Hide Login**
- ➡ Dodać **uwierzytelnianie podstawowe (basic auth)** na [/wp-login.php](#) i [/wp-admin](#)
- ➡ Ograniczyć dostęp do panelu logowania wg IP w [.htaccess](#)
- ➡ Zastosować **ochronę przed brute-force** (np. przez Wordfence, iThemes Security)
- ➡ Włączyć **uwierzytelnianie dwuskładnikowe (2FA)**
- ➡ Monitorować logi serwera pod kątem podejrzanych prób logowania

### Poziom zagrożenia:

**Wysoki** – podatność na automatyczne ataki typu brute-force i ujawnienie używanej technologii



Nazwa użytkownika lub adres e-mail

Hasło



☐ Zapamiętaj mnie

Zaloguj się

Nie pamiętasz hasła?

← [Przejdź do Porolex – producent rolet i żaluzji](#)

[Polityka prywatności](#)



Polski



Zmień

## Zgłoszenie błędu nr: 1.3

### Tytuł błędu:

Publiczny dostęp do pliku **readme.html** ujawniającego wersję WordPressa

### Opis błędu:

Plik **readme.html**, będący częścią domyślnej instalacji WordPressa, jest dostępny publicznie pod adresem:

 <https://porolex.pl/readme.html>

Plik ten:

- ujawnia wersję WordPressa, np. *WordPress 6.4.3*,
- może zostać wykorzystany przez osoby niepowołane do sprawdzenia znanych luk bezpieczeństwa,
- nie stanowi bezpośredniego zagrożenia, ale ułatwia analizę podatności.



### Kroki do odtworzenia:

1. Otwórz przeglądarkę internetową.
2. Przejdź do adresu: <https://porolex.pl/readme.html>
3. Pojawia się strona z informacją o wersji WordPressa.

### Oczekiwane zachowanie:

Dostęp do pliku **readme.html** powinien być **całkowicie zablokowany (błąd 403)** lub plik powinien zostać **usunięty z serwera**.

### Rekomendacje:

-  **Usuń plik **readme.html**** z katalogu głównego (np. przez FTP lub menedżera plików).
-  **Zablokuj dostęp do pliku** na poziomie serwera:

## .htaccess (Apache):

```
<Files "readme.html">  
Order allow,deny  
Deny from all  
</Files>
```

## nginx:

```
location = /readme.html {  
deny all;  
}
```



## Poziom zagrożenia:

● **Średni** – nie umożliwia bezpośredniego ataku, ale zwiększa ryzyko ataku ukierunkowanego na znaną wersję WordPressa.



Semantic Personal Publishing Platform

### First Things First

Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I am proud to be a part of. Thousands of hours have gone into WordPress, and we are dedicated to making it better every day. Thank you for making it part of your world.

— Matt Mullenweg

### Installation: Famous 5-minute install

1. Unzip the package in an empty directory and upload everything.
2. Open [wp-admin/install.php](#) in your browser. It will take you through the process to set up a wp-config.php file with your database connection details.
  1. If for some reason this does not work, do not worry. It may not work on all web hosts. Open up wp-config-sample.php with a text editor like WordPad or similar and fill in your database connection details.
  2. Save the file as wp-config.php and upload it.
  3. Open [wp-admin/install.php](#) in your browser.
3. Once the configuration file is set up, the installer will set up the tables needed for your site. If there is an error, double check your wp-config.php file, and try again. If it fails again, please go to the [WordPress support forums](#) with as much data as you can gather.
4. **If you did not enter a password, note the password given to you.** If you did not provide a username, it will be admin.
5. The installer should then send you to the [login page](#). Sign in with the username and password you chose during the installation. If a password was generated for you, you can then click on "Profile" to change the password.

