

# Secure Notes Application

311192 Ciszewski Jakub

# Moduł Uwierzytelniania

- Walidacja danych wejściowych
- Sprawdzanie siły hasła dla użytkownika ma podstawie wyrażeń regularnych i entropii
- Ograniczone informacje o błędach (Tylko walidacja i błąd niepowodzenia logowania)
- Przechowywanie hasła z wykorzystaniem soli
- Kontrola dostępu użytkownika do zasobów
- Zbieranie informacji dotyczących prób dostępu do konta z dostępem dla użytkownika
- Aktywacja konta z linku / restart z linku (Wyświetlane w konsoli)
- Ograniczona liczba prób logowania (Po przekroczeniu blokada 2h)
- Honeypots w formularzach rejestracji

# Możliwości modułu notatek dla użytkownika

- Walidacja danych
- Możliwość wyświetlania notatek tylko dla zalogowanych użytkowników
- Udostępnianie dostępu do notatek dla użytkowników
- Szyfrowanie notatek (dowolne hasło z wskaźnikiem siły, AES-CBC)
- Sanityzacja treści notatek
- Możliwość dodawania zdjęć i linków

# Elementy dodatkowe

- Formularze zabezpieczone CSRF
- Honeypots
- CSP
- Wyłączenie nagłówka server
- Dokeryzacja środowiska docker-compose build/up
- https

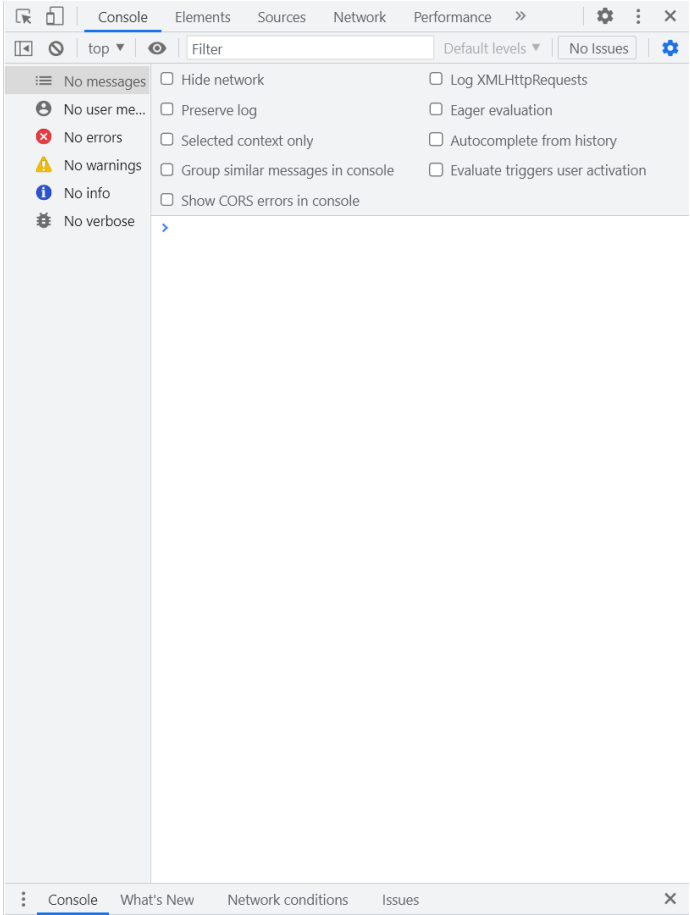
# Przewodnik

## Main Page

- [Main](#)
- [Login](#)
- [Register](#)

### PUBLIC NOTES:

- Title: mobile-cashdesk-pipeline  
Author: Admin  
Link: [Link](#)
- Title: mobile-cashdesk-pipeline  
Author: Admin  
Link: [Link](#)



# Kreacja konta i aktywacja

- Wypełnij formularz rejestracji i doklej link do adresu strony link ważny jest przez 2 godziny

## Register

- [Main](#)
- [Login](#)
- [Register](#)

Username

Leon

Email

leon@leon.pl

Password

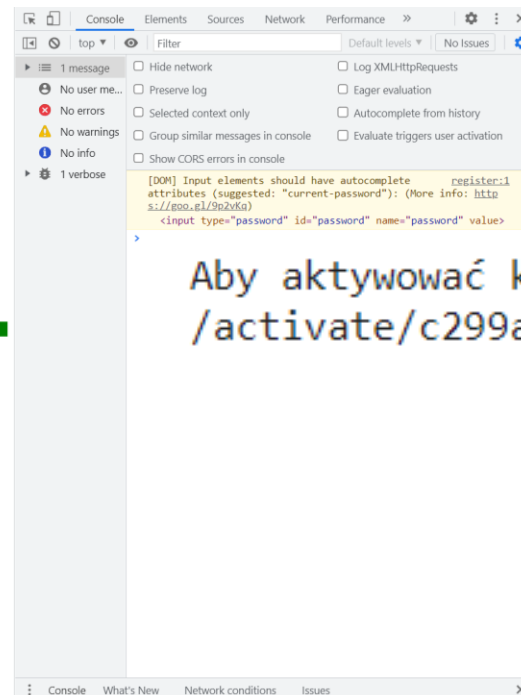
\*\*\*\*\*

Password Strength Checker

Strong

Entropy : 63 < 50

Create



Aby aktywować konto wejdź na link:  
/activate/c299a823-0fb0-44b1-bd74-a60208fcd663

[register:36](#)

# Resetowanie hasła

- Wypełnij formularz prośby o reset hasła wejdź na link z konsoli – link ważny 2 godziny
- Podaj nowe hasło

## Restore password

- [Main](#)
- [Login](#)
- [Register](#)

Email

Aby aktywować konto wejdź na link: [restore-passwd:38](#)  
[/reset\\_passwd/cf3f9536-f114-44b6-af2e-8c93bd078a72](#)

**Reset your password**

- [Main](#)
- [Login](#)
- [Register](#)

Password

Password Strength Checker

Entropy: 77 < 50

Aby zamknąć pełny ekran, naciśnij F11

Console

1 message

[DOM] Input elements should have autocomplete attributes (suggested: "new-password"): (More info: https://goo.gl/3p2v5a)

```
<input type="password" id="password" name="password" value=">
```

# Dodawanie notatki

- Wpisz wypełnij formularz
- Dodaj użytkowników do wglądu
- Odszyfruj notatkę

### Create note

- Welcome, Leon
- [Main](#)
- [Create notes](#)
- [Logout](#)

Note name

Note Dozwolone elementy: {"a" z "href", "p", "div", "i", "b", "em", "blockquote", "tr", "strong", "br", "ul", "ol", "li", "quote", "code", "img" z "src", "h1", "h2", "h3", "h4", "h5"}

```
<h1>h1</h1>
<h2>h2</h2>
<h3>h3</h3>
<h4>h4</h4>
<h5>h5</h5>


<a href="https://github.com/ciszeusj/SecureNotesApplication">GIT</a>

<script>
  alert("Hello! I am an alert box!!");
</script>
```

Password (could be empty)

\*\*\*

Password Strength Checker

**Weak**

Should be public

☐

### Decode note:

- Welcome, Leon
- [Main](#)
- [Create notes](#)
- [Logout](#)

Note password

Granted Access:

- Admin

Add player:

Username

Title:

mobile-cashdesk-pipeline

- Welcome, Leon
- [Main](#)
- [Create notes](#)
- [Logout](#)

Author:

Leon


h1

h2

h3

h4

h5





# Informacje o dostępie do konta

- Użytkownik widzi kiedy i z jakiego ip wykonywane były akcje związane z jego kontem

## Login logs

- Wellcome, Leon
- [Main](#)
- [Create notes](#)
- [Logout](#)
- [Logs](#)

LOGS:

- Ip: 192.168.4.1  
Operation: activate  
Result: SUCCESS  
Date: Tue Jan 03 12:18:38 UTC 2023
- Ip: 192.168.4.1  
Operation: login  
Result: SUCCESS  
Date: Tue Jan 03 12:18:49 UTC 2023
- Ip: 192.168.4.1  
Operation: Reset\_passwd\_request  
Result: REQUESTED  
Date: Tue Jan 03 12:21:40 UTC 2023
- Ip: 192.168.4.1  
Operation: reset\_passwd  
Result: SUCCESS  
Date: Tue Jan 03 12:23:41 UTC 2023
- Ip: 192.168.4.1  
Operation: login  
Result: SUCCESS  
Date: Tue Jan 03 12:23:51 UTC 2023

# Bibliografia

- <https://www.baeldung.com/security-spring>
- <https://owasp.org/www-project-java-html-sanitizer/>
- <https://www.baeldung.com/csrf-thymeleaf-with-spring-security>
- <https://stackoverflow.com/questions/55722738/how-can-i-remove-server-header-in-nginx-docker-container>
- <https://www.baeldung.com/spring-security-block-brute-force-authentication-attempts>