



Bezpieczeństwo sieciowe
2021/2022

Raport aplikacji

Implementacja dowolnej aplikacji nastawionej na
bezpieczeństwo przechowywania/przesyłania danych

Jaworski Mateusz, Igor Ślusarski
Edukacja Techniczno-Informatyczna
05.01.2022r.

dr. inż. Krzysztof Bzowski

1. Cel i opis projektu

Celem projektu było utworzenie aplikacji webowej nastawionej na bezpieczeństwo przesyłania/przechowywania danych użytkownika z wykorzystaniem nowoczesnych technologii i metod. Aplikacja została stworzona w języku PHP w oparciu o framework CodeIgniter 3 z następującymi funkcjonalnościami:

- logowanie użytkownika
- rejestracja użytkownika
- wylogowanie użytkownika
- panel użytkownika z logami prób logowań

W celu zabezpieczenia danych użytkownika podczas przechowywania w bazie danych MySQL wykorzystano standardowe szyfrowanie w języku PHP z algorytmem bcrypt (*password_hash*, *password_verify*) - kod PIN do zalogowania. Do przechowywania po stronie serwera danych o zalogowanym użytkowniku wykorzystano system sesji w języku PHP.

Podczas procesu rejestracji/logowania wykorzystano weryfikację dwuetapową 2FA (*Google Authenticator*) przy pomocy biblioteki *GoogleAuthentication* dostępnej w PHP. Po pomyślnej rejestracji na stronie wyświetlany jest kod oraz QR CODE, który należy wkleić/zeskanować w aplikacji na urządzeniu mobilnym aby móc generować czasowe kody autoryzacji służące do późniejszego logowania. Podczas logowania użytkownik jest zmuszony do wpisania kodu 2FA z aplikacji mobilnej.

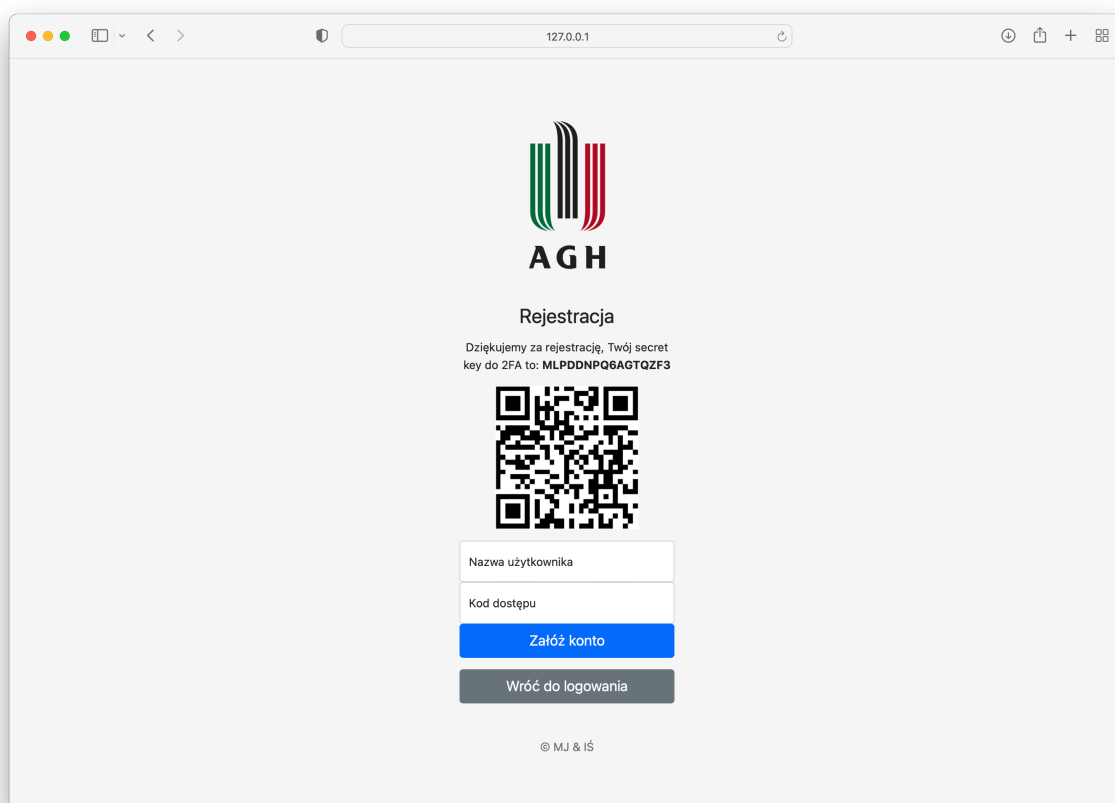
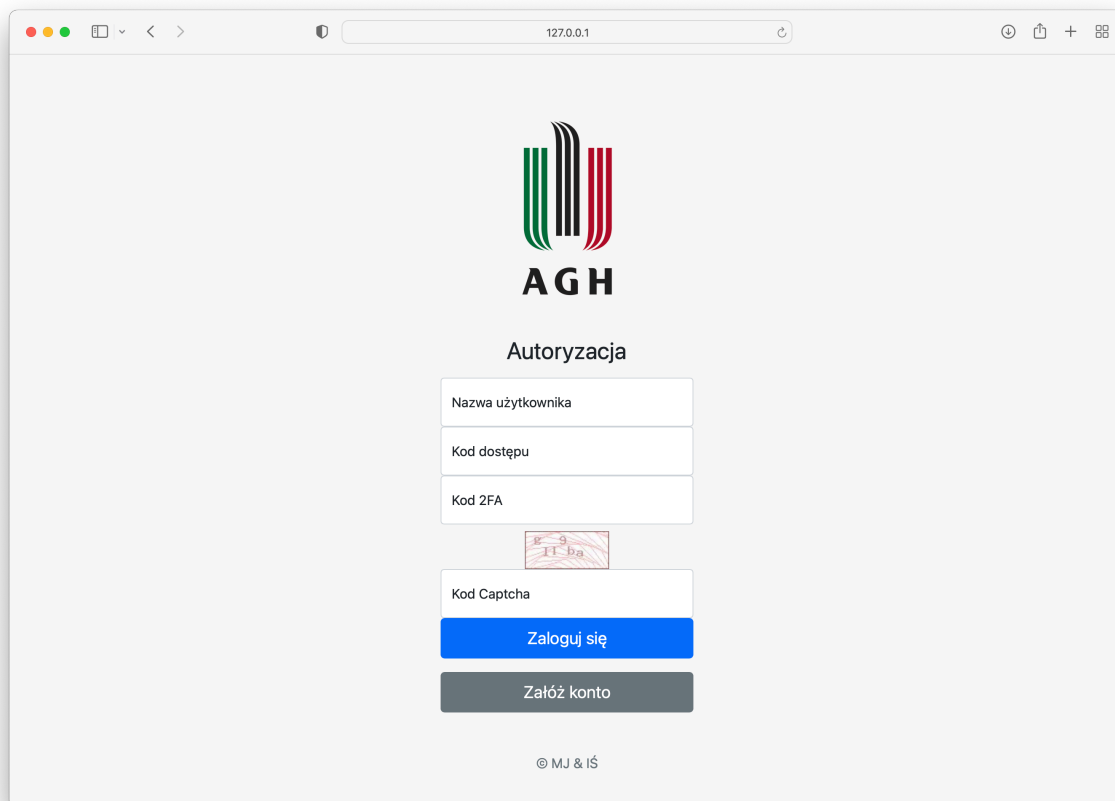
Dodatkowo, podczas logowania użytkownika wymagany jest do przepisania 6 znakowy kod CAPTCHA, który zabezpiecza proces logowania przez automatycznymi botami. Kod CAPTCHA jest generowany przy każdym odświeżeniu strony, następnie zapisywany w sesji i generowany plik graficzny z „nieczytelny” kodem (przykładowa grafika poniżej).

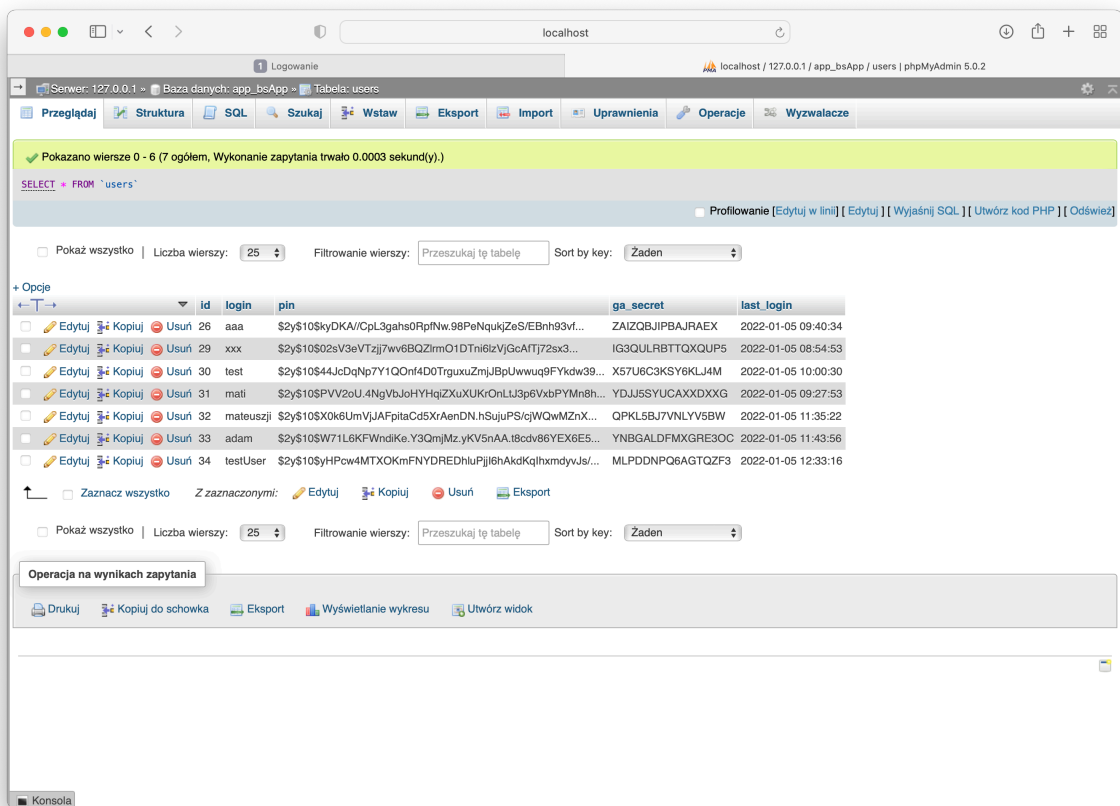
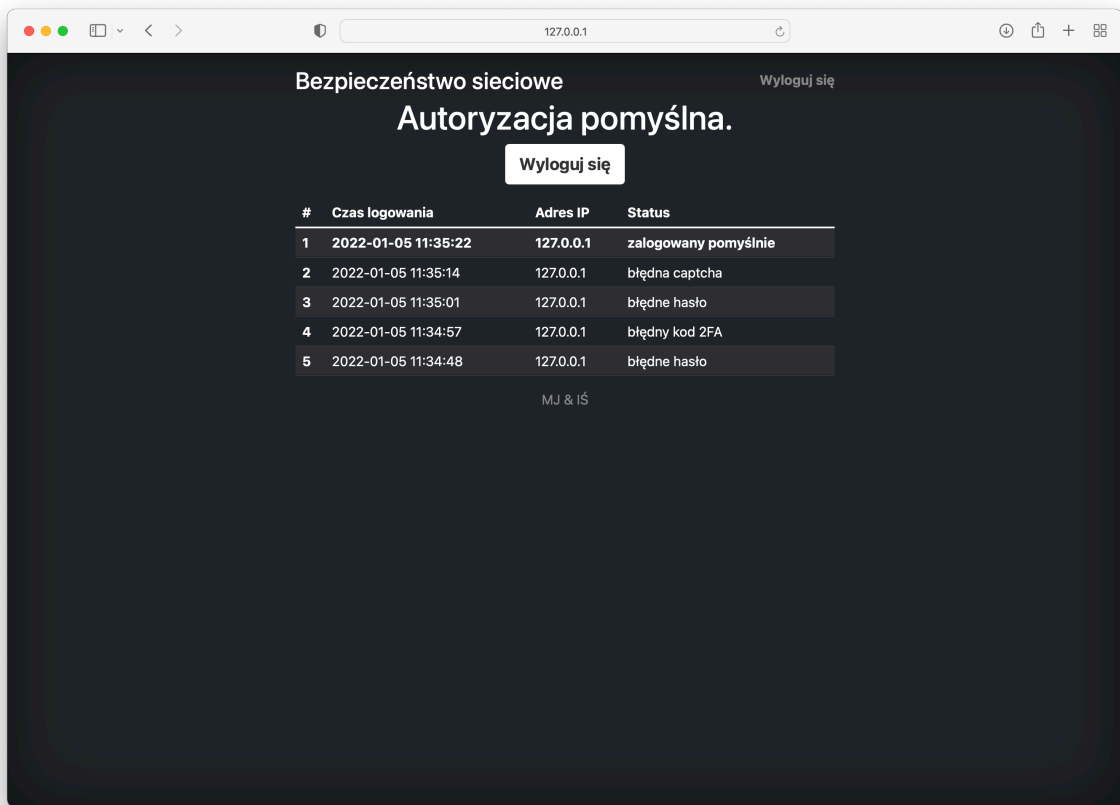
Podczas prawidłowej próby logowania została zaimplementowana również weryfikacja ilości błędnych prób logowania (niewłaściwe hasło). W przypadku trzykrotnego wprowadzenia złego hasła/PINu podczas logowania w przeciągu 15 minut konto zostaje tymczasowo zablokowane w celu zabezpieczenia przed atakami.

Przy każdej próbie logowania (pomyślnej lub nie) do bazy danych zapisywane są logi zawierające adres IP, z którego nastąpiło logowanie, czas oraz status logowania (0 - *pomyślne*, 1 - *błędne hasło*, 2 - *błędny 2FA*, 3 - *błędna captcha*, 4 - *kilkukrotnie błędnie wprowadzone hasło*). Logi użytkownika są wyświetlane w panelu użytkownika po pomyślnej autoryzacji użytkownika.

Po wylogowaniu użytkownika zostaje natychmiastowo zniszczona sesja zawierająca dane o zalogowanym użytkowniku oraz przekierowuje ponownie na stronę logowania.

2. Zrzuty ekranu





localhost

Logowanie

localhost / 127.0.0.1 / app_bsApp / ci_sessions | phpMyAdmin 5.0.2

Serwer: 127.0.0.1 » Baza danych: app_bsApp » Tabela: ci_sessions

Przeglądaj Struktura SQL Szukaj Wstaw Eksport Import Uprawnienia Operacje Wyzwalacze

✓ Pokazano wiersze 0 - 23 (24 ogółem, Wykonanie zapytania trwało 0.0002 sekund(y).)

SELECT * FROM `ci_sessions`

Profilowanie [Edytuj w linii] [Edytuj] [Wyjaśnij SQL] [Utwórz kod PHP] [Odśwież]

☐ Pokaż wszystko | Liczba wierszy: 25 Filtrowanie wierszy: Przeszukaj tę tabelę Sort by key: Żaden

+ Opcje

		id	ip_address	timestamp	data				
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	1on3tuqduf17cc1j6v4d72jmk7htm8pj	127.0.0.1	1641381013	[BLOB - 67 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	383tvg4b68hpeeo88baap5j36ls2aj2h	127.0.0.1	1641382579	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	39tvmkv83m4tocmncs72n1lv146pcg9r	10.71.119.117	1641377206	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	3er9brihukgdtc9cejvuaop7d7r4mtl8	127.0.0.1	1641378885	[BLOB - 67 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	4fatt0b0djkeimn3d3npn7vpo2fbike	:::1	1641373222	[BLOB - 34 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	6mtj0brvb58j1us9jr9r4e1m1ks23nc	127.0.0.1	1641380513	[BLOB - 67 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	70pkaf1nfmkbl1fmltkq31pefarr	:::1	1641382586	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	7o5bcbdnq7v9abnauusbmmlne7s328hh	127.0.0.1	1641377669	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	aa2s0qg8uc2k1ke3c3v128gp0o9g1v1t	127.0.0.1	1641380206	[BLOB - 67 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	cn3mqpe2a51j6s1bbe7ms9v4gk016sf	127.0.0.1	1641378584	[BLOB - 67 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	cvb3ah3sfka3mor8qmv5to0l8gtv23s	:::1	1641377637	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	dgmegddueh5gjiu8sse28mds4262f02m	:::1	1641374264	[BLOB - 34 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	e65cagom6uncbjoko8m4vachmarld7rk	:::1	1641374576	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	er5dcgvuohla75mtkuqb8dgt3u70qsgq	127.0.0.1	1641382318	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	h6du64l9ihun7glp4bgvbmrv247p2kpi	:::1	1641373847	[BLOB - 34 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	h7ah19lndppe4l7lm1qc5ha0kett51	:::1	1641382457	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	ku7b0mes6gobq36aj29mh397ebum6552	127.0.0.1	1641378280	[BLOB - 67 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	l2j951iorr6ig5bb8tqhtl8jq4teaaq	:::1	1641375896	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	lvqlfllpok2sn3hrgdcdfhcae0bb5c5	127.0.0.1	1641377977	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	n8q1mivucbuqk82jnvsc94h469q51bfuq	:::1	1641374957	[BLOB - 55 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	paf1qd1ubqtho8fusq4m0lnmns920gtl	127.0.0.1	1641379422	[BLOB - 67 B]
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	q64suqapiq1mi94d1se0h1jdinntlb3	10.71.119.117	1641377206	[BLOB - 55 B]

Konsola

localhost

Logowanie

localhost / 127.0.0.1 / app_bsApp / logs | phpMyAdmin 5.0.2

Serwer: 127.0.0.1 » Baza danych: app_bsApp » Tabela: logs

Przeglądaj Struktura SQL Szukaj Wstaw Eksport Import Uprawnienia Operacje Wyzwalacze

✓ Pokazano wiersze 0 - 4 (5 ogółem, Wykonanie zapytania trwało 0.0003 sekund(y).)

SELECT * FROM `logs`

Profilowanie [Edytuj w linii] [Edytuj] [Wyjaśnij SQL] [Utwórz kod PHP] [Odśwież]

☐ Pokaż wszystko | Liczba wierszy: 25 Filtrowanie wierszy: Przeszukaj tę tabelę Sort by key: Żaden

+ Opcje

		id	user_id	ip	time	status				
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	23	32	127.0.0.1	2022-01-05 11:34:48	1
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	24	32	127.0.0.1	2022-01-05 11:34:57	2
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	25	32	127.0.0.1	2022-01-05 11:35:01	1
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	26	32	127.0.0.1	2022-01-05 11:35:14	3
<input type="checkbox"/>	Edytuj	<input type="checkbox"/>	Kopiuuj	<input type="checkbox"/>	Usuń	27	32	127.0.0.1	2022-01-05 11:35:22	0

☐ Zaznacz wszystko Z zaznaczonymi: Edytuj Kopiuuj Usuń Eksport

☐ Pokaż wszystko | Liczba wierszy: 25 Filtrowanie wierszy: Przeszukaj tę tabelę Sort by key: Żaden

Operacja na wynikach zapytania

Drukuj Kopiuuj do schowka Eksport Wyświetlanie wykresu Utwórz widok

Konsola