

 **OWASP TOP 10** 

 **Nagłówki bezpieczeństwa HTTP** 

# OWASP TOP 10

- [OWASP](#) - Open Web Application Security Project
- Zadaniem OWASP jest popularyzacja wiedzy na temat bezpieczeństwa aplikacji webowych
- Co kilka lat publikuje listę najpoważniejszych zagrożeń dla aplikacji webowych
- Aktualna wersja: [OWASP Top 10 2021](#)
- Nowa wersja jest spodziewana w pierwszej połowie 2025 roku

# Nagłówki HTTP

# Nagłówek HTTP - Content Security Policy (CSP)

- [Content Security Policy](#) - polityka bezpieczeństwa treści
- Zabezpiecza przed atakami typu XSS (Cross-Site Scripting)
- Określa, jakie zasoby mogą być załadowane na stronie
- Jest wykorzystywany przez przeglądarkę
- Polityka działa w trybie *Allow-List*
- Przy budowaniu polityki można korzystać z trybu *Report-Only*

# Nagłówek HTTP - Access-Control-Allow-Origin (CORS)

- [Cross-Origin Resource Sharing](#) - Zasady udostępniania zasobów między różnymi domenami
- Określa, czy zasób może być udostępniany między różnymi domenami
- Wartość nagłówka może być ustawiona na konkretną domenę lub na znak \* dla wszystkich
- Nagłówek nie wspiera wyrażeń regularnych!

# Nagłówek HTTP - Cache-Control

- [Cache-Control](#) - określa, jak należy przechowywać dany zasób
- Pozwala na kontrolę ważności danego zasobu na poziomie:
  - aplikacji
  - przeglądarki
  - CDN - Content Delivery Network

# Plik *robots.txt*

- [robots.txt](#) - plik tekstowy, który określa, które zasoby mogą być indeksowane przez boty
- Jest dostępny w postaci pliku tekstowego pod adresem `https://[domain address]/robots.txt`
- Może też wskazywać na plik `sitemap.xml`