

**Uniwersytet Dolnośląski DSW we Wrocławiu**  
**Wydział Studiów Stosowanych**  
**studia pierwszego stopnia**

Kierunek studiów: Informatyka

Zakres kształcenia: Inżynier aplikacji i systemów chmurowych

Jan Kowalski

**Tytuł Przykładowej Pracy Inżynierskiej**

Praca inżynierska  
napisana pod kierunkiem  
dr Imię Nazwisko

Wrocław 2026

# Spis treści

|                             |          |
|-----------------------------|----------|
| <b>Spis treści</b>          | <b>2</b> |
| <b>1 Wstęp</b>              | <b>3</b> |
| 1.1 Cel dokumentu . . . . . | 3        |
| <b>2 Opis problemu</b>      | <b>3</b> |
| 2.1 Zakres . . . . .        | 3        |
| <b>3 Podsumowanie</b>       | <b>3</b> |
| 3.1 Dalsze kroki . . . . .  | 3        |
| <b>Bibliografia</b>         | <b>4</b> |

# **1. Wstep**

Ten dokument jest przykładowym szkieletem pracy inżynierskiej.

## **1.1. Cel dokumentu**

Pokazanie minimalnej struktury oraz procesu kompilacji szablonu.

# **2. Opis problemu**

Rozdział opisuje kontekst, założenia i ograniczenia projektu.

## **2.1. Zakres**

Zakres obejmuje przygotowanie treści, bibliografii oraz poprawną kompilację PDF.

# **3. Podsumowanie**

Przykładowa praca pokazuje jak uruchomić build i dostosować metadane.

## **3.1. Dalsze kroki**

Skopiuj `metadata.yaml.example` do `metadata.yaml` i twórz własne rozdziały.

## Bibliografia

1. Cloudflare, *Cloudflare Web Application Firewall*, dostęp: <https://developers.cloudflare.com/waf/> (15.01.2026).
2. Cloudflare, *Rate Limiting Rules*, dostęp: <https://developers.cloudflare.com/waf/rate-limiting-rules/> (15.01.2026).
3. Cloudflare, *OWASP Core Ruleset Concepts*, dostęp: <https://developers.cloudflare.com/waf/managed-rules/reference/owasp-core-ruleset/concepts/> (15.01.2026).
4. Cloudflare, *Security Level*, dostęp: <https://developers.cloudflare.com/waf/tools/security-level/> (15.01.2026).
5. Cloudflare, *DDoS Protection*, dostęp: <https://developers.cloudflare.com/ddos-protection/> (15.01.2026).
6. Coraza WAF Project, *Coraza – repozytorium kodu źródłowego*, dostęp: <https://github.com/corazawaf/coraza> (15.01.2026).
7. Coraza WAF Project, *Coraza SPOA – repozytorium kodu źródłowego*, dostęp: <https://github.com/corazawaf/coraza-spoa> (15.01.2026).
8. DeepWiki, *Coraza SPOA: HAProxy Integration*, dostęp: <https://deepwiki.com/corazawaf/coraza-spoa/3.2-haproxy-integration> (15.01.2026).
9. HAProxy Technologies, *Custom Rules*, dostęp: <https://www.haproxy.com/documentation/haproxy-configuration-tutorials/proxying-essentials/custom-rules/> (15.01.2026).
10. HAProxy Technologies, *Four Examples of HAProxy Rate Limiting*, dostęp: <https://www.haproxy.com/blog/four-examples-of-haproxy-rate-limiting> (15.01.2026).
11. OWASP CRS Project, *Anomaly Scoring*, dostęp: [https://coreruleset.org/docs/2-how-crs-works/2-1-anomaly\\_scoring/](https://coreruleset.org/docs/2-how-crs-works/2-1-anomaly_scoring/) (15.01.2026).
12. OWASP CRS Project, *Paranoia Levels*, dostęp: [https://coreruleset.org/docs/2-how-crs-works/2-2-paranoia\\_levels/](https://coreruleset.org/docs/2-how-crs-works/2-2-paranoia_levels/) (15.01.2026).
13. OWASP CRS Project, *OWASP CRS – repozytorium kodu źródłowego*, dostęp: <https://github.com/coreruleset/coreruleset> (15.01.2026).
14. OWASP CRS Project, *Engine Integration Options*, dostęp: [https://coreruleset.org/docs/1-getting-started/1-4-engine\\_integration\\_options/](https://coreruleset.org/docs/1-getting-started/1-4-engine_integration_options/) (15.01.2026).
15. OWASP Foundation, *OWASP ModSecurity Core Rule Set*, dostęp: <https://owasp.org/www-project-modsecurity-core-rule-set/> (15.01.2026).
16. OWASP Foundation, *OWASP Coraza Web Application Firewall*, dostęp: <https://owasp.org/www-project-coraza-web-application-firewall/> (15.01.2026).