Dokumentacja techniczna
Kalkulator CVSS 4.0

Autorzy:

Miłosz Brzeziński, Michał Duszyński, Bartosz Barwiński, Adam Kądziela, Bartłomiej Kowalewski

1. Wstęp

Projekt „Kalkulator CVSS 4.0” powstał jako część projektu zespołowego realizowanego w ramach studiów na Politechnice Wrocławskiej, na kierunku Cyberbezpieczeństwo (specjalność CBS). Celem przedsięwzięcia było stworzenie w pełni funkcjonalnej aplikacji webowej, umożliwiającej obliczanie wskaźników podatności zgodnie z najnowszą wersją standardu CVSS (Common Vulnerability Scoring System) w wersji 4.0.

Aplikacja pozwala użytkownikowi w intuicyjny sposób wprowadzić zestaw metryk opisujących podatność i uzyskać automatycznie obliczony wynik, uwzględniający komponenty takie jak Base Score, Threat Score czy Environmental Score. System zapewnia dynamiczne przeliczanie wyników w czasie rzeczywistym oraz przejrzystą wizualizację wpływu poszczególnych metryk.

Projekt skierowany jest przede wszystkim do specjalistów ds. bezpieczeństwa IT, takich jak analitycy SOC, pentesterzy czy audytorzy, którzy chcą szybko i precyzyjnie ocenić potencjalne zagrożenia. Jednocześnie aplikacja może służyć jako narzędzie dydaktyczne dla studentów kierunków technicznych, uczących się analizy ryzyka w kontekście podatności systemów informatycznych.

2. CVSS 4.0

Standard CVSS 4.0, opracowany przez organizację FIRST, dostarcza ujednoliconą metodę ilościowej oceny podatności w trzech następujących po sobie etapach obliczeniowych. Na początku użytkownik przypisuje wartości metryk podstawowych (Base Metrics), które definiują charakterystykę ataku i jego wpływ na system. Metryki te obejmują zarówno parametry określające wektor ataku – na przykład stopień skomplikowania, wymagane uprawnienia i udział użytkownika – jak i oddziaływanie na poufność, integralność oraz dostępność zasobów w „systemie pierwotnym” oraz w systemach zależnych. Wynik tej fazy, nazywany Base Score, jest wyliczany zgodnie z formule zawartą w specyfikacji, przy uwzględnieniu wpływu zmiany zakresu (Scope) działania podatności.

Kolejnym krokiem jest korekta Base Score przy użyciu metryki Exploit Maturity z grupy Threat Metrics. Ta metryka ocenia dostępność i dojrzałość istniejących exploitów, co pozwala podkreślić przypadki, w których zagrożenie jest realne i aktualnie wykorzystywane. W efekcie powstaje Threat Score, który – w zależności od wartości Exploit Maturity – może podnieść lub obniżyć ocenę wyjściową.

Ostatnia faza obejmuje tzw. Environmental Metrics, służące do adaptacji wyniku do specyfiki danego środowiska. Pozwalają one na zmianę wag wpływu poszczególnych parametrów (np. zwiększenie znaczenia poufności w środowisku przetwarzającym wrażliwe dane) oraz nadpisanie wybranych metryk podstawowych własnymi wartościami. Po ponownym obliczeniu modyfikowanych wskaźników uzyskujemy końcowy Environmental Score, precyzyjnie odzwierciedlający realne ryzyko w warunkach konkretnej organizacji.

Ostatecznym rezultatem pracy kalkulatora są trzy odrębne oceny w skali od 0.0 do 10.0 – Base Score, Threat Score i Environmental Score – wraz z przypisanym poziomem ryzyka (np. Low, Medium, High, Critical). Szczegółowe opisy parametrów, pełne wzory obliczeniowe oraz zasady zaokrągleń można znaleźć w oficjalnej specyfikacji CVSS 4.0, dostępnej pod adresem: https://www.first.org/cvss/v4-0/specification-document

3. Metryki

Metryki CVSS to zestandaryzowane parametry, które służą do ilościowej oceny podatności systemów informatycznych. Każda metryka opisuje jeden z aspektów podatności – zarówno pod kątem jej wykorzystania przez potencjalnego atakującego (np. poziom uprawnień wymaganych do przeprowadzenia ataku), jak i jej wpływu na system (np. utrata poufności, integralności lub dostępności). Wersja 4.0 systemu CVSS wprowadza dodatkowe udoskonalenia, takie jak oddzielne uwzględnienie wpływu na systemy zależne, lepsze odwzorowanie kontekstu środowiskowego oraz możliwość rozbudowania oceny o dodatkowe czynniki zarządcze.

W standardzie CVSS v4.0 metryki dzielą się na cztery grupy:

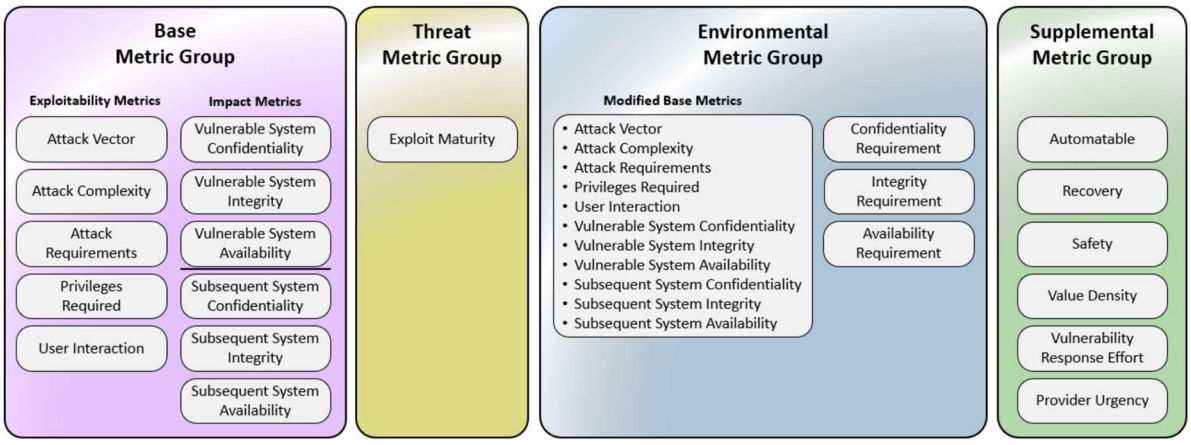
Base Metric Group – metryki podstawowe opisujące podatność w sposób niezależny od kontekstu, obejmujące zarówno trudność wykorzystania podatności (np. Attack Vector, Privileges Required), jak i jej wpływ (np. Confidentiality, Integrity, Availability).

Threat Metric Group – obejmuje metrykę **Exploit Maturity**, która służy do określenia poziomu zaawansowania i dostępności technik wykorzystywania danej podatności w praktyce (np. czy exploit jest już publicznie dostępny).

Environmental Metric Group – pozwala na dostosowanie wyniku do specyfiki środowiska, w którym dana podatność występuje, m.in. poprzez zmianę wag metryk wpływu (np. wymagania poufności) oraz modyfikację wybranych metryk podstawowych.

Supplemental Metric Group – grupa dodatkowa, zawiera metryki wspomagające decyzje zarządcze, takie jak: wpływ na bezpieczeństwo, wysiłek związany z naprawą czy pilność reakcji dostawcy. Nie wpływa na liczbowy wynik końcowy.

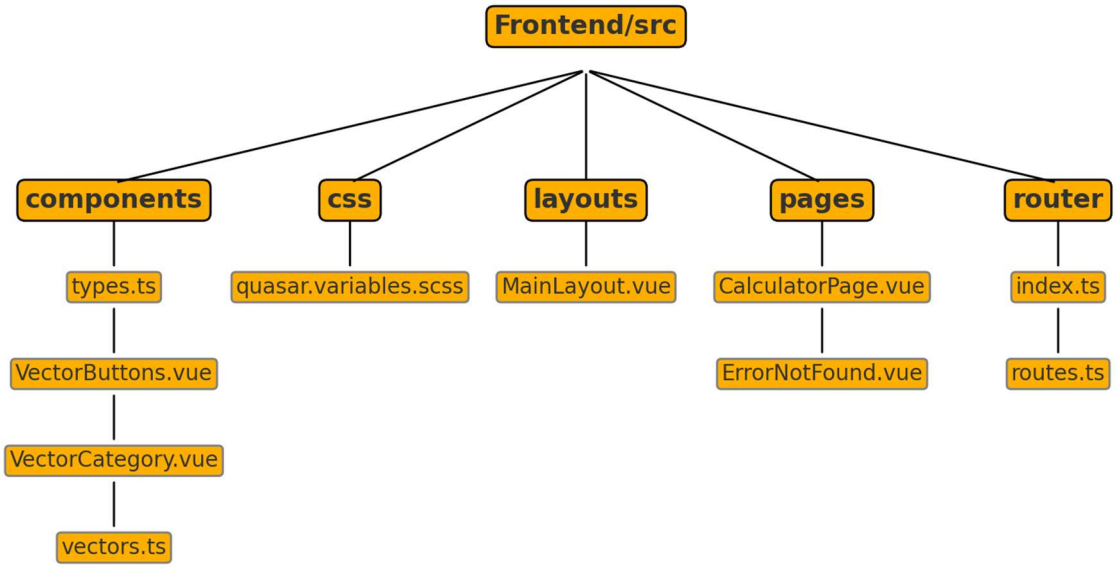
Poniżej załączono grafikę przedstawiającą pełny podział metryk CVSS 4.0 zgodnie z dokumentacją:



Rys.1 Podział metryk CVSS 4.0
Źródło: https://www.first.org/cvss/v4-0/specification-document

4. Architektura projektu

Projekt został stworzony jako interfejs użytkownika działający w przeglądarce, zbudowany w oparciu o Vue. Interfejs został podzielony na komponenty, takie jak przyciski *VectorButtons.vue* i kategorie wektorów *VectorCategory.vue*, które trafiają do głównej strony kalkulatora – *CalculatorPage.vue*. Całość zbudowana w oparciu o *MainLayout.vue*, zapewniający spójne nagłówki, menu boczne i stopkę, a także style oparte na zestawie zmiennych pliku *quasar.variables.scss*. Całość została postawiona na usłudze nginx działającej na prywatnym serwerze. Poniższy diagram ilustruje główną strukturę katalogów.



Rys. 2 Diagram struktury najważniejszych katalogów i plików.

4.1 Szczegółowy opis plików i ich głównej zawartości

components/types.ts

Scentralizowane definicje interfejsów używanych w całym UI.

Typy*:*

VectorButtonsType – opis pojedynczego przycisku

VectorCategoryType – grupa przycisków

ModelMapType – mapa aktualnych wyborów użytkownika do kolejnych metryk.

components/vectors.ts

Opis wszystkich możliwych metryk CVSS 4.0 oraz funkcja łączenia wyborów.

Tablice stałe:

exploitability_metrics

vulnerable_system_impact_metrics

subsequent_system_impact_metrics

supplemental_metrics

exploitability_metrics_env

vulnerable_system_impact_metrics_env

subsequent_system_impact_metrics_env

environmental_security_requirements

threat_metrics

ModelMapType2Vector(model: ModelMapType): string

Buduje ciąg wektora CVSS (np. "AV:N/AC:L/PR:N/UI:R/S:C/...")

components/VectorButtons.vue

Tworzy jeden przycisk wyboru metryki. Emituje *update:modelValue* przy kliknięciu.

Props:

vectorButtons: VectorButtonsType

modelValue: string

components/VectorCategory.vue

Grupuje zestaw przycisków dla jednej kategorii metryk. Iteruje po *category.buttons*, grupuje *VectorButtons*.vue, aktualizuje *modelMap*.

Props:

vectorCategory: VectorCategoryType

Model:

modelMap: ModelMapType

css/quasar.variables.scss

Zawiera globalne zmienne SCSS dla motywu Quasar.

Zawartość:

Kolory*: $primary, $secondary, $accent, $dark, $dark-page, $positive, $negative, $info, $warning*

layouts/MainLayout.vue

Zawiera główny szkielet aplikacji (layout), stosowany dla strony.

pages/CalculatorPage.vue

Tworzenie interaktywnej strony kalkulatora CVSS.

pages/ErrorNotFound.vue

Fallback 404 dla wszystkich nieznanych ścieżek.

router/index.ts oraz router/routes.ts

Konfiguracja Vue Router i definicje tras

5. Przepływ danych (Data Flow)

1) Użytkownik wybiera opcje metryk na *CalculatorPage.vue*.
2) Komponenty *VectorCategory.vue* → *VectorButtons.vue* modyfikują *modelMap*.
3) Computed w *CalculatorPage.vue* wywołuje:
   a) *ModelMapType2Vector(modelMap)*
   b) *pandatixCvss.calculate(vectorString)*
4) Wynik (*BaseScore*, *EnvScore*) trafia do zmiennych.
5) Widok aktualizuje tabele.
6) Eksport PDF – przycisk zbiera aktualny stan i przekazuje do *pdfmake*.

6. Źródła

https://github.com/finczli/CVSS-v4.0-calculator

https://www.first.org/cvss/v4-0/specification-document