Architektura bezpiecznych aplikacji internetowych na platformie Java Enterprise Edition.

Jakub Grabowski

Warszawa, 2008-01-08

Agenda

1. Teza
2. Bezpieczeństwo aplikacji internetowych
   - Usługi bezpieczeństwa
   - Problemy bezpieczeństwa
3. Architektura bezpieczeństwa platformy Java Enterprise Edition
4. Propozycja rozwiązania problemów bezpieczeństwa

Teza

- Realizacja bezpiecznej aplikacji internetowej opartej na bazie danych wymaga zastosowania warstwy pośredniej odpowiadającej za bezpieczeństwo.

Bezpieczeństwo aplikacji internetowych

- Duża popularność „zachęca” potencjalnych intruzów
- Większość problemów jest niezależna od języka programowania, czy platformy
- Bardzo szerokie zagadnienie
- Pareto☺

Pożądane cechy bezpiecznej aplikacji internetowej

- Zabezpieczenie przed nieautoryzowanym dostępem do funkcji aplikacji i dostępnych z jej poziomu danych
- Niezaprzeczalność, czyli zapewnienie, że użytkownik nie może wyprzeć się operacji, którą wykonał
- Zabezpieczenie przed zmniejszeniem parametrów jakości obsługi (*Quality of Service*) w wyniku różnego rodzaju ataków
- *Łatwość zarządzania i administracji*
- *Wygodna obsługa*

Usługi bezpieczeństwa

- Uwierzytelnienie
- Autoryzacja / sterowanie dostępem
- Integralność danych
- Poufność / prywatność danych
- Niezaprzeczalność
- *Jakość obsługi*
- *Audyt*

Najważniejsze problemy bezpieczeństwa aplikacji internetowych (1/2)

- Skrypty międzyserwisowe (Cross Site Scripting - XSS)
- Wstrzykiwanie złośliwego kodu (Injection Flaws)
- Złośliwe wykonywanie plików (Malicious File Execution)
- Niezabezpieczone bezpośrednie odwołanie do obiektu (Insecure Direct Object Reference)
- Fałszowanie żądań (Cross Site Request Forgery)

Najważniejsze problemy bezpieczeństwa aplikacji internetowych (2/2)

- Wyciek informacji i niepoprawna obsługa błędów (Information Leakage and Improper Error Handling)
- Niepoprawna obsługa uwierzytelnienia i sesji (Broken Authentication and Session Management)
- Błędy szyfrowania wrażliwych danych (Insecure Cryptographic Storage)
- Niezabezpieczona wymiana informacji (Insecure Communications)
- Brak zabezpieczenia dostępu poprzez URL (Failure to Restrict URL Access)

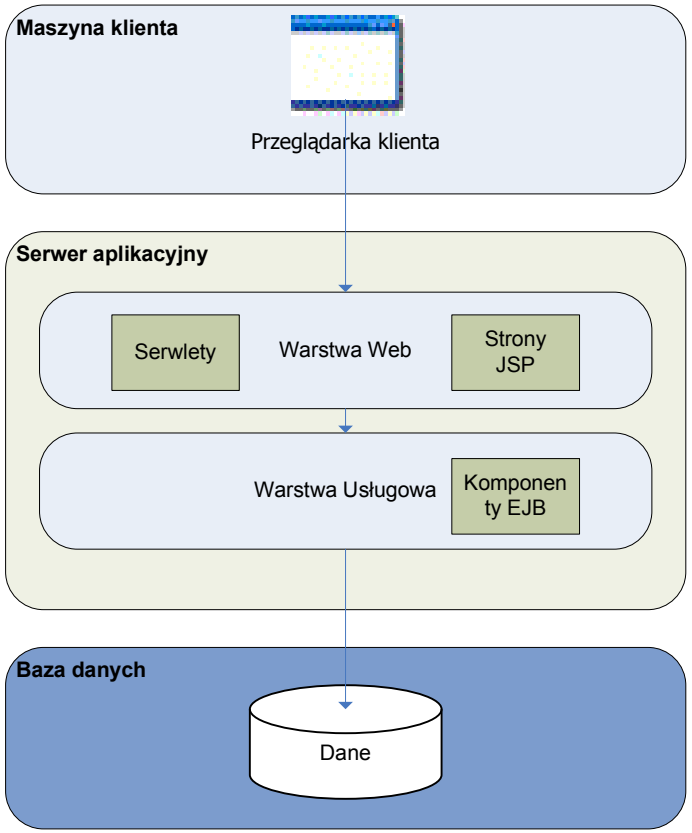
Mechanizmy bezpieczeństwa platformy Java

- Separacja poprzez maszynę wirtualną
- Bezpieczeństwo języka
- JAAS
- Java GSS-API
- JCE
- JSSE
- SASL

Sposoby wyrażania wymagań bezpieczeństwa na platformie Java EE

- Deklaratywne
- Programowe
- Adnotacje

Architektura aplikacji internetowej Java EE



Warstwowy model bezpieczeństwa Java EE

- Warstwa aplikacji (*application layer*)
- Warstwa transportowa (*transport layer*)
- Warstwa komunikatów (*message layer*)

Proponowane rozwiązania problemów (1/5)

- Skrypty międzyserwisowe
  - Walidacja danych wejściowych
  - Kodowanie danych wyjściowych
- Wstrzykiwanie złośliwego kodu
  - Walidacja danych wejściowych
  - Użycie szkieletu ORM
  - Poprawna obsługa błędów
  - Odpowiednie uprawnienia dostępu do bazy danych

Proponowane rozwiązania problemów (2/5)

- Złośliwe wykonywanie plików
  - Odwołanie do plików poprzez identyfikator
  - Walidacja danych wejściowych
- Niezabezpieczone bezpośrednie odwołanie do obiektu
  - Ograniczanie zestawu zwracanych danych
  - Autoryzacja dostępu

Proponowane rozwiązania problemów (3/5)

- Fałszowanie żądań
  - Użycie metody POST przy pobieraniu danych od użytkownika
  - SSL
  - Zabezpieczenie przed atakami XSS
- Wyciek informacji i niepoprawna obsługa błędów
  - Globalna obsługa wyjątków
  - Ograniczenie szczegółowości komunikatów błędów zwracanych użytkownikom

Proponowane rozwiązania problemów (4/5)

- Niepoprawna obsługa uwierzytelnienia i sesji
  - Wykorzystanie wbudowanego mechanizmu obsługi sesji
  - SSL
  - Dostępność przycisku Logout
  - Wygasanie sesji
  - Losowe hasła e-mail

Proponowane rozwiązania problemów (5/5)

- Błędy szyfrowania wrażliwych danych
  - Skróty haseł użytkowników
  - Odpowiednie prawa dostępu w systemie operacyjnym
- Niezabezpieczona wymiana informacji
  - SSL
- Brak zabezpieczenia dostępu poprzez URL
  - Autoryzacja

Dziękuję za uwagę

…Czekam na pytania