

Autentykacja, Autoryzacja Moduły i Handlery HTTP

ASP.NET

Wiktor Zychla

Uniwersytet Wrocławski

Instytut Informatyki

22 listopad 2005

Handlers HTTP

- żądanie HTTP skierowane do serwera IIS w pierwszej kolejności determinuje filtr ISAPI, który ma je obsłużyć (dla plików ASP.NET tym filtrem jest `aspnet_isapi.dll`)
- ASP.NET w pewnym sensie powtarza ten proces - poszukiwany jest Handler HTTP, który ma obsłużyć konkretne rozszerzenie pliku. Na przykład pliki `*.aspx` obsługiwane są przez filtr `PageHandlerFactory`, a pliki `*.asmx` przez `WebServiceHandlerFactory`.
- za pomocą tej techniki można dodać obsługę własnego rozszerzenia plików i logikę ich obsługi

Handlers HTTP

Aby zaimplementować handler, należy napisać klasę implementującą interfejs `IHttpHandler`. Aby handler poprawnie zadziałał, należy:

- związać wybrane rozszerzenie z filtrem `aspnet_isapi.dll`
- dodać sekcję `httpHandlers` do pliku `web.config`

Moduły HTTP

Cykl obsługi żądania HTTP obejmuje następujące zdarzenia.

1. BeginRequest, AuthenticateRequest, AuthorizeRequest
2. AcquireRequestState, ResolveRequestCache
3. konstruktor strony
4. PreRequestHandlerExecute
5. Page.Init, Page.Load
6. PostRequestHandlerExecute
7. ReleaseRequestState, UpdateRequestCache
8. EndRequest
9. PreSendRequestHeaders, PreSendRequestContent

Dodanie własnej logiki do tego cyklu możliwe jest dzięki modułom HTTP.

Moduły HTTP

Aby zaimplementować moduł, należy napisać klasę implementującą interfejs `IHttpModule`. Aby moduł poprawnie zadziałał, należy:

- związać wybrane rozszerzenie z filtrem `aspnet_isapi.dll`
- dodać sekcję `httpHandlers` do pliku `web.config`

Moduły i Handlery HTTP

DEMO...

Autentykacja a autoryzacja

- Autentykacja to proces identyfikacji użytkownika
- Autoryzacja to nadawanie (lub nie) zidentyfikowanemu użytkownikowi dostępu do pewnych zasobów

Dostępne sposoby autentykacji to:

- Brak
- Custom
- Windows
- Forms
- Passport

Autentykacja Custom

- dane o użytkowniku przechowywane na przykład w sesji lub zaszyfrowanym `QueryString`
- często to jedyna możliwość, na przykład w aplikacjach WAP

Autentykacja Windows

Oznacza uwierzytelnianie użytkowników aplikacji internetowej w systemie operacyjnym lub domenie Active Directory.

Dostępne tryby uwierzytelniania:

- podstawowe
- szyfrowane
- zintegrowane (Kerberos)

Kontekst autentykacji może zezwalać na wcielanie tożsamości (impersonation).

Autentykacja Forms

Oznacza delegowanie własnego formularza do przeprowadzenia autentykacji. Informacja o tożsamości przechowywana jest w ciasteczku.

Własny moduł autentykacji

Zalety:

- mniejsza podatność na standardowe ataki
- łatwiej tworzyć własne obiekty `IIIdentity` i `IPrincipal`

Wady:

- część ważnych funkcji wspomagających ma status `internal` w `System.Web.*`, co utrudnia na przykład poprawną autoryzację

Autoryzacja

- zasoby autoryzuje się dokonując odpowiednich wpisów do sekcji `authorization` w `web.config`
- dostępne ustawienia to `deny` i `allow`
- w ustawieniach określa się użytkowników (`users`) lub role (`roles`)
- Ustawienia selektywne możliwe są dzięki dodatkowym sekcjom `location`

Autentykacja, autoryzacja

DEMO...