NEW MEDIA & COMMUNICATION TECHNOLOGY

ASP.NET MVC Labo Week 10

Doelstelling:

- Opzetten basis security voor de webapplicaties
- Voorkomen van tampering parameters
- Voorkomen van overposting

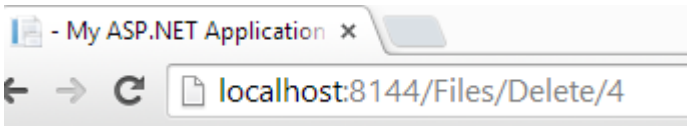
Voor u start met dit labo moet u eerst de twee vorige weken afgewerkt hebben !!!

Tampering

Een veel gemaakte fout is het niet voorzien dat gebruikers URL's kunnen tamperen (wijzigen) door bijvoorbeeld andere waarden in de URL te gebruiken dan deze die de applicatie er plaatst. Dit kan er voor zorgen dat je toegang krijgt tot pagina's of files die niet voor u zijn. Dit is ook zo bij ons NMCT dropbox opgave. In de onderstaande oefening gaan we dit probert

Verwijderen files

Test eerst zelf uit of je door het "tamperen" van de URL files kan verwijderen waar u geen rechten voor hebt als ingelogde gebruiker. Wijzig het id van de file in een id waar je GEEN toegang tot hebt. U zou toch de vraag moeten krijgen om deze file te verwijderen. Dit mag niet.

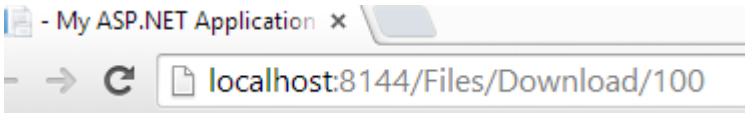


Hoe kunnen we dit nu oplossen? Eerst en vooral mogen files enkel verwijderd worden door de persoon die deze heeft geüpload. Voor we het verwijderen starten zullen we volgende zaken moeten doen in de actionmethod:

1) Een "FileRegistration" object ophalen voor het opgegeven ID
2) Kijken of de username in het "FileRegistration" object overeen komt met de ingelogde gebruiker
3) Indien deze niet hetzelfde zijn moet er een foutmelding verschijnen want de ingelogde persoon heeft geen toegang om de file te verwijderen.
4) Indien de username hetzelfde is als de ingelogde gebruiker mag de file worden verwijderd.

Downloaden files

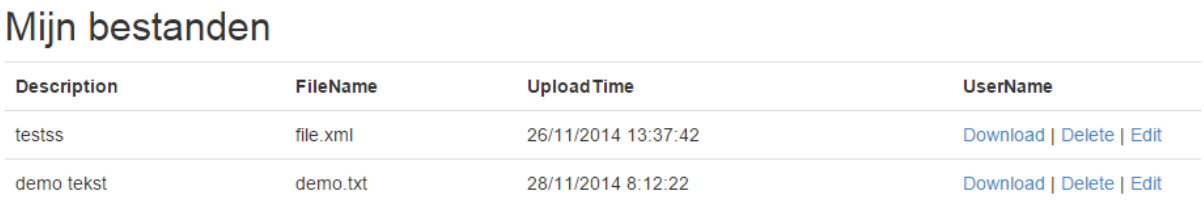
Dit is het zelfde principe als bij het verwijderen van files. Test zelf uit of je door het "tamperen" van de URL files kan downloaden waar je geen rechten voor hebt. U zal zelf de url moeten intikken in de browser en het ID (onderstaande voorbeeld 100) wijzigen.



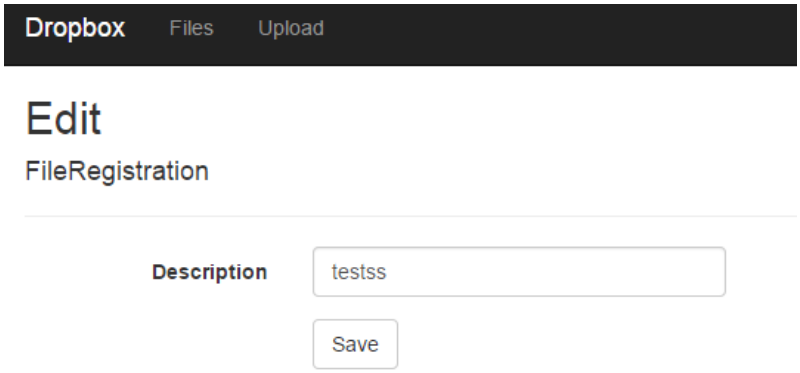
Normaal gezien kan je alle files downloaden. Ook deze waar u eigenlijk geen rechten voor hebt. Wijzig de actionmethod voor het downloaden zodat enkel de mensen die de file mogen downloaden dit kunnen doen. Welke stappen moet je hiervoor ondernemen ? Hoe kan je weten wie welke file mag downloaden. Probeer dit zelfstandig op te lossen en toon uw oplossing aan de docent.

Uitbreiding wijzigen van description

Maak een kleine uitbreiding in de applicatie. Zorg ervoor dat bij “Mijn Bestanden” er een “Edit” knop is.



Na het kiezen van “Edit” moet je de “Description” kunnen wijzigen.



U zou instaat moeten zijn om dit volledig zelf te implementeren**. Tip: U zal wel een SQL Update query moeten schrijven!**

Opgepast:

- Zorg er ook voor dat enkel de persoon die het bestand heeft geüpload de omschrijving kan wijzigen. Andere personen mogen dit NIET kunnen.
- Ga ook overposting tegen. Hoe kan je voorkomen dat de velden FileName,UploadTime en UserName NIET gewijzigd worden door overposting ?

Laat uw oplossing controleren door de docent !