عنوان: **کنترل عمومی فایل‌های آپلودی در ASP.NET MVC**
نویسنده: وحید نصیری
تاریخ: ۱۳۹۱/۰۹/۰۹ ۱۳:۲
آدرس: www.dotnettips.info
برچسب‌ها: MVC, Security

در مطلب « محدود کردن کاربرها به آپلود فایل‌هایی خاص در ASP.NET MVC » تصمیم گیری بر اساس یک لیست سفید صورت می‌گیرد. برای مثال کاربران فقط قرار است تصویرهایی از نوع png یا jpg را ارسال کنند. اکنون نیاز است حالت کلی‌تری را درنظر بگیریم که کاربر قرار است هر نوع فایل دلخواهی را ارسال کند. در اینجا نباید امکان آپلود هر نوع فایلی، خصوصا فایل‌های اجرایی ASP.NET یا هر نوع موتور اجرایی دیگری که ممکن است روی سرور نصب باشد (مثلا PHP)، وجود داشته باشد. برای این منظور فیلتر دیگری به نام AllowUploadSafeFiles طراحی شده است که سورس آن‌را در ذیل مشاهده می‌کنید:

```
using System;
using System.Linq;
using System.Collections.Generic;
using System.IO;
using System.Web.Mvc;

namespace SecurityModule
{
    [AttributeUsage(AttributeTargets.Method, AllowMultiple = false)]
    public sealed class AllowUploadSafeFilesAttribute : ActionFilterAttribute
    {
        static readonly IList<string> ExtToFilter = new List<string> {
            ".aspx", ".asax", ".asp", ".ashx", ".asmx", ".axd", ".master", ".svc", ".php" ,
            ".php3" , ".php4", ".ph3", ".ph4", ".php4", ".ph5", ".sphp", ".cfm", ".ps", ".stm",
            ".htaccess", ".htpasswd", ".php5", ".phtml", ".cgi", ".pl", ".plx", ".py", ".rb", ".sh",
".jsp",
            ".cshtml", ".vbhtml", ".swf" , ".xap", ".asptxt"
        };

        static readonly IList<string> NameToFilter = new List<string> {
           "web.config" , "htaccess" , "htpasswd", "web~1.con"
        };

        static bool canUpload(string fileName)
        {
            if (string.IsNullOrWhiteSpace(fileName))
                return false;

            fileName = fileName.ToLowerInvariant();
            var name = Path.GetFileName(fileName);
            var ext = Path.GetExtension(fileName);

            if (string.IsNullOrWhiteSpace(name))
                throw new InvalidOperationException("Uploaded file should have a name.");

            return !ExtToFilter.Contains(ext) &&
                   !NameToFilter.Contains(name) &&
                   !NameToFilter.Contains(ext) &&
                   //for "file.asp;.jpg" files
                   ExtToFilter.All(item => !name.Contains(item));
        }

        public override void OnActionExecuting(ActionExecutingContext filterContext)
        {
            var files = filterContext.HttpContext.Request.Files;
            foreach (string file in files)
            {
                var postedFile = files[file];
                if (postedFile == null || postedFile.ContentLength == 0) continue;

                if (!canUpload(postedFile.FileName))
                    throw new InvalidOperationException(string.Format("You are not allowed to upload
{0} file.", Path.GetFileName(postedFile.FileName)));
            }

            base.OnActionExecuting(filterContext);
        }
    }
}
```

در این فیلتر، یک سری پسوند خطرناک مانند aspx، asp و امثال آن فیلتر می‌شوند و اجازه آپلود نخواهند یافت. همچنین فایل‌هایی

مانند web.config یا نام داسی آن معادل web~1.con نیز فرصت آپلود نخواهد یافت.

استفاده از این فیلتر سفارشی به نحو زیر است:

```
[AllowUploadSafeFiles]
public ActionResult UploadFile(HttpPostedFileBase file)
```