عنوان: **یافتن اکشن متدهای Post ایی در ASP.NET MVC که فیلتر CSRF ندارند**
نویسنده: وحید نصیری
تاریخ: ۱۳۹۲/۱۲/۰۸ ۰:۱۰
آدرس: www.dotnettips.info
گروه‌ها: MVC, Security

روش مرسوم مقابله با حملات CSRF در ASP.NET MVC، استفاده از فیلتر امنیتی ValidateAntiForgeryToken بر روی اکشن متدهایی از نوع Post است و سپس فراخوانی Html.AntiForgeryToken در View متناظر.
با بالا رفتن تعداد اکشن متدهای یک پروژه، ممکن است استفاده از ValidateAntiForgeryToken فراموش شود. در ادامه مثالی را ملاحظه می‌کنید که یک پروژه‌ی ASP.NET MVC را جهت یافتن اکشن متدهای Post ایی که فیلتر ValidateAntiForgeryToken ندارند، اسکن می‌کند:

```
using System;
using System.Linq;
using System.Reflection;
// Add a ref. to \Program Files\Microsoft ASP.NET\ASP.NET MVC 4\Assemblies\System.Web.Mvc.dll
using System.Web.Mvc;
// Add a ref. to System.Web
using System.Web.UI;

namespace FindOutputCaches
{
    class Program
    {
        static void Main(string[] args)
        {
            var path = @"D:\path\bin\site.dll";
            var asmTarget = Assembly.LoadFrom(path);

            checkCsrfTokens(asmTarget);

            Console.WriteLine("Press a key...");
            Console.Read();
        }


        private static void checkCsrfTokens(Assembly asmTarget)
        {
            // یافتن کلیه کنترلرها
            var controllers = asmTarget.GetTypes()
                                       .Where(type => typeof(IController).IsAssignableFrom(type) &&
                                                      !type.Name.StartsWith("T4MVC"))
                                       .ToList();

            foreach (var controller in controllers)
            {
                // یافتن کلیه اکشن متدهای کنترلر جاری
                var actionMethods = controller.GetMethods(BindingFlags.Public | BindingFlags.Instance |
BindingFlags.DeclaredOnly)
                                              .Where(method =>
typeof(ActionResult).IsAssignableFrom(method.ReturnType))
                                              .ToList();

                foreach (var method in actionMethods)
                {
                    var httpPostAttributes = method.GetCustomAttributes(typeof(HttpPostAttribute),
true);
                    if (httpPostAttributes == null || !httpPostAttributes.Any())
                        continue;

                    var csrfTokens =
method.GetCustomAttributes(typeof(ValidateAntiForgeryTokenAttribute), true);
                    if (csrfTokens == null || !csrfTokens.Any())
                    {
                        Console.WriteLine("Detected [HttpPost] without [ValidateAntiForgeryToken] in:\n
{0}-->{1}",
                                          controller.FullName, method.Name);
                    }
                }
            }
        }
    }
}
```

ابتدا مسیر اسمبلی کامپایل شده پروژه ASP.NET MVC که حاوی کنترلرهای برنامه است، باید مشخص گردد.
سپس در این اسمبلی، کلیه نوع‌های تعریف شده، یافت گردیده و آن‌هایی که پیاده سازی کننده IController هستند (یعنی کلاس‌های کنترلر واقعی برنامه)، جدا خواهند شد.
در ادامه در این کنترلرها، متدهایی را بررسی خواهیم کرد که دارای خروجی از نوع ActionResult باشند (فقط اکشن متدها مدنظر هستند). اگر این اکشن متد یافت شده دارای ویژگی HttpPost بود و همچنین ValidateAntiForgeryToken نداشت، یعنی یک مشکل امنیتی که باید برطرف شود.