

شاید شما هم قصد داشته باشید تا از برخی درخواست ها به وب سایت یا اپلیکیشن خود ممانعت عمل بیاورید. نظیر درخواست های SQL Injection یا برخی Query String های خاص یا برخی درخواست های مزاحم.

یکی از مزاحمت هایی که گریبانگیر وب سایت هاست، Bot های متفاوتی است که برای کپی اطلاعات، درج کامنت به صورت خودکار و مواردی از این دست، به آنها مراجعه میکنند. شاید در نگاه اول بد نباشد که این Bot ها به سراغ وب سایت ما بیایند و باعث افزایش تعداد ویزیت سایتمان شوند؛ ولی ضررهای ناشی از کپی و سرقت مطالب سایت، آنهم با سرعت بالا، بیشتر از منافع ناشی از بالا رفتن رنک سایت است. به طور مثال همین سایت NET Tips دارای تعداد زیادی مقالات مفید است که افراد متعددی در نگارش و تهیه آنها زحمت کشیده اند، یا وب سایتی برای جلب اعتماد مشتریان جهت درج اطلاعاتشان و یا آگهی هایشان زحمت زیادی کشیده است، Bot های آماده ی زیادی وجود دارد که با چند دقیقه صرف وقت جهت تنظیم شدن آماده میشوند تا مطالب را طبق ساختار تعیین شده، مورد به مورد کپی کنند.

برای خلاصی از این موارد روش های متعددی وجود دارد که از جمله آنها می توان به تنظیمات فایل htaccess در وب سرورهایی نظیر Apache و یا web.config در IIS اشاره کرد. در این مقاله این امکان را با IIS مرور میکنیم و برای فعال سازی آن کافی است در:

IIS 7.5 و بالاتر، همراه با انتخاب Request Filtering در مراحل نصب IIS

IIS 7.0 پس از نصب بسته آپدیت [Microsoft Knowledge Base Article 957508](https://support.microsoft.com/kb/957508).

IIS 6.0 با نصب URLScan 3.0

در بخش <system.webServer> و سپس <security>، تگ requestFiltering را استفاده کنیم، در این تگ دستورالعمل های ویژه ی پالایشگر درخواست ها را مینویسیم (filteringRules) هر دستورالعمل پالایش دارای خصیصه های (Attributes) زیر است:

denyUnescapedPercent

مقدار Boolean و انتخابی

اگر برابر با true تنظیم گردد، درخواست هایی که دارای کاراکتر "درصد" (%) هستند و به وسیله escape character ها پوشش داده نشده باشند، رد می شوند. (جهت جلوگیری از حملات XSS و...) مقدار پیش فرض true است.

name

عنوان دستورالعمل.

مقدار پیش فرض نداشته و درج کردن آن اجباری است.

scanAllRaw

مقدار Boolean و انتخابی

اگر برابر با true تنظیم گردد، پالایشگر درخواست ها موظف است تا با بررسی متن header های درخواست، در صورت یافتن یکی از واژه هایی که در خصیصه denyStrings ذکر کرده اید، درخواست را رد کند. مقدار پیش فرض false است.

scanQueryString

مقدار Boolean و انتخابی

اگر برابر با true تنظیم گردد، پالایشگر درخواستها موظف است تا Query string را بررسی کند تا در صورتی که یکی از واژه‌های درج شده در خصیصه denyStrings را بیابد، درخواست را رد کند.

اگر خصیصه‌ی unescapeQueryString از تگ < requestFiltering > برابر با true باشد، query string دوبار بررسی می‌شود: یکبار متن query string برای یافتن عبارات ممنوعه و بار دیگر برای یافتن کاراکترهای بدون پوشش scaped. مقدار پیشفرض false است.

scanUrl

مقدار Boolean و انتخابی

اگر برابر با true تنظیم گردد، پالایشگر درخواستها URL را برای یافتن واژه‌های ممنوعه‌ی ذکر شده در خصیصه denyStrings بررسی می‌نماید. مقدار پیش فرض false است.

چند مثال:

مثال 1: در این مثال عنوان User-Agent هایی را که در موارد متعدد برای وب سایت هایی که روی آنها کار می‌کردم مزاحمت ایجاد میکردند را پالایش میکنیم. (لیست این Bot ها آپدیت میشود)

```
<requestFiltering>
  <filteringRules>
    <filteringRule name="BlockSearchEngines" scanUrl="false" scanQueryString="false">
      <scanHeaders>
        <clear />
        <add requestHeader="User-Agent" />
      </scanHeaders>
      <appliesTo>
        <clear />
      </appliesTo>
      <denyStrings>
        <clear />
        <add string="Python Urllib" />
        <add string="WGet" />
        <add string="Apache HttpClient" />
        <add string="Unknown Bot" />
        <add string="Yandex Spider" />
        <add string="libwww-perl" />
        <add string="Nutch" />
        <add string="DotBot" />
        <add string="CCBot" />
        <add string="Majestic 12 Bot" />
        <add string="Java" />
        <add string="Link Checker" />
        <add string="Baiduspider" />
        <add string="Exabot" />
        <add string="PHP" />
      </denyStrings>
    </filteringRule>
  </filteringRules>
</requestFiltering>
```

مثال 2: ممانعت از SQL Injection

```
<requestFiltering>
  <filteringRules>
    <filteringRule name="SQLInjection" scanUrl="false" scanQueryString="true">
      <appliesTo>
        <clear />
        <add fileExtension=".asp" />
        <add fileExtension=".aspx" />
        <add fileExtension=".php" />
      </appliesTo>
      <denyStrings>
        <clear />
        <add string="--" />
        <add string=";" />
      </denyStrings>
    </filteringRule>
  </filteringRules>
</requestFiltering>
```

```

        <add string="*" />
        <add string="@" />
        <add string="char" />
        <add string="alter" />
        <add string="begin" />
        <add string="cast" />
        <add string="create" />
        <add string="cursor" />
        <add string="declare" />
        <add string="delete" />
        <add string="drop" />
        <add string="end" />
        <add string="exec" />
        <add string="fetch" />
        <add string="insert" />
        <add string="kill" />
        <add string="open" />
        <add string="select" />
        <add string="sys" />
        <add string="table" />
        <add string="update" />
    </denyStrings>
    <scanHeaders>
        <clear />
    </scanHeaders>
</filteringRule>
</filteringRules>
</requestFiltering>

```

مثال 3: ممانعت از درخواست انواع خاصی از فایل ها

```

<requestFiltering>
    <filteringRules>
        <filteringRule name="Block Image Leeching" scanUrl="false" scanQueryString="false"
scanAllRaw="false">
            <scanHeaders>
                <add requestHeader="User-agent" />
            </scanHeaders>
            <appliesTo>
                <add fileExtension=".zip" />
                <add fileExtension=".rar" />
                <add fileExtension=".exe" />
            </appliesTo>
            <denyStrings>
                <add string="leech-bot" />
            </denyStrings>
        </filteringRule>
    </filteringRules>
</requestFiltering>

```

[اطلاعات بیشتر در وب سایت رسمی IIS](#)

نظرات خوانندگان

نویسنده: امین مصباحی
تاریخ: ۱۳۹۳/۰۲/۰۶ ۶:۳۰

تکمیلی 1: AhrefsBot هم از جمله ی Bot های مزاحم است، لذا:

```
</ "add string="AhrefsBot">
```

نویسنده: وحید نصیری
تاریخ: ۱۳۹۳/۰۲/۰۶ ۹:۳۵

لیست User-Agent هایی است که من در این سایت بستم تا امروز (از لاگ های خطای برنامه استخراج شدند):
[bots.txt](#)

نویسنده: مهدیار
تاریخ: ۱۳۹۴/۰۴/۰۸ ۱۶:۴۲

در لیست bots.txt یکی از بوت های درج شده huawei است که باعث می شود گوشی های huawei نتوانند سایت را باز کنند.

نویسنده: علی یگانه مقدم
تاریخ: ۱۳۹۴/۰۴/۰۸ ۱۷:۲۴

مدتی است برای سایت جاری این مشکل رفع شده است.

نویسنده: مهدیار
تاریخ: ۱۳۹۴/۰۴/۰۸ ۱۷:۳۷

ما این مشکل رو داخل سایت خودمون داشتیم . گفتم اطلاع بدم بقیه دوستان هم مطلع بشن از فایل بوت حذفش کنند.