

# IIS Web.config Temel Düzeyde Sıkılaştırma Ayarları

Github kullanıcısı marchbarry'den web.config için temel bazı güvenlik sıkılaştırmaları aşağıda verilmiştir. Bu sıkılaştırmaların toplamı web.config'e konarak temel düzeyde bir IIS sunucu sıkılaştırması yapılabilir.

## A. Web.config Sıkılaştırma Ayarları

### i) Disable tracing

```
<system.web>
  <trace enabled="false" />
</system.web>
```

### ii) Prevent applications running if debug=true

(\* Note: It can only be in machine level, not at the application level (i.e. can only be in Machine.Config, not Web.Config)

```
<system.web>
  <deployment retail="true"/>
</system.web>
```

### iii) Disable debug

```
<system.web>
  <compilation debug="false"/>
</system.web>
```

### iv) Rename the cookie to something more obscure ASP.NET\_SessionId

```
<system.web>
  <sessionState cookieName="s" />
</system.web>
```

### v) Disable ASP.NET version HTTP header

```
<system.web>
  <httpRuntime enableVersionHeader="false" />
</system.web>
```

### vi) Secure cookies on HTTPS deployments

```
<system.web>
  <httpCookies httpOnlyCookies="false" requireSSL="false" />
</system.web>
```

### vii) Remove unwanted http headers

```
<system.webServer>
  <httpProtocol>
    <customHeaders>
```

```

    <remove name="Server" />
    <remove name="X-Powered-By" />
    <remove name="X-AspNet-Version" />
    <remove name="X-AspNetMvc-Version" />
  </customHeaders>
</httpProtocol>
</system.webServer>

```

### viii) Configure custom error handlers for specific HTTP error codes

```

<system.webServer>
  <httpErrors errorMode="Custom">
    <remove statusCode="502" subStatusCode="-1" />
    <remove statusCode="501" subStatusCode="-1" />
    <remove statusCode="500" subStatusCode="-1" />
    <remove statusCode="412" subStatusCode="-1" />
    <remove statusCode="406" subStatusCode="-1" />
    <remove statusCode="405" subStatusCode="-1" />
    <remove statusCode="404" subStatusCode="-1" />
    <remove statusCode="403" subStatusCode="-1" />
    <remove statusCode="401" subStatusCode="-1" />
    <remove statusCode="400" subStatusCode="-1" />

    <error statusCode="400" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="401" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="402" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="403" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="404" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="405" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="406" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="412" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="500" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="501" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
    <error statusCode="502" subStatusCode="-1" path="/error-handler.aspx"
      prefixLanguageFilePath="" responseMode="ExecuteURL" />
  </httpErrors>
</system.webServer>

```

## ix) Remove unwanted modules to reduce your attack surface

```
<system.webServer>
<handlers>
  <remove name="TraceHandler-Integrated-4.0" />
  <remove name="TraceHandler-Integrated" />
  <remove name="AssemblyResourceLoader-Integrated-4.0" />
  <remove name="AssemblyResourceLoader-Integrated" />
  <remove name="WebAdminHandler-Integrated-4.0" />
  <remove name="WebAdminHandler-Integrated" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-2.0-64" />
  <remove name="svc-ISAPI-4.0_32bit" />
  <remove name="ScriptHandlerFactoryAppServices-Integrated-4.0" />
  <remove name="ScriptResourceIntegrated-4.0" />
  <remove name="svc-ISAPI-4.0_64bit" />
  <remove name="svc-Integrated-4.0" />
  <remove name="vbhtml-ISAPI-4.0_32bit" />
  <remove name="vbhtml-ISAPI-4.0_64bit" />
  <remove name="vbhtml-Integrated-4.0" />
  <remove name="vbhtml-ISAPI-4.0_32bit" />
  <remove name="vbhtml-ISAPI-4.0_64bit" />
  <remove name="vbhtml-Integrated-4.0" />
  <remove name="xamlx-ISAPI-4.0_32bit" />
  <remove name="xamlx-ISAPI-4.0_64bit" />
  <remove name="xamlx-Integrated-4.0" />
  <remove name="xoml-ISAPI-4.0_32bit" />
  <remove name="xoml-ISAPI-4.0_64bit" />
  <remove name="xoml-Integrated-4.0" />
  <remove name="HttpRemotingHandlerFactory-rem-Integrated-4.0" />
  <remove name="HttpRemotingHandlerFactory-rem-ISAPI-2.0" />
  <remove name="rules-ISAPI-4.0_32bit" />
  <remove name="rules-Integrated-4.0" />
  <remove name="HttpRemotingHandlerFactory-soap-Integrated" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-2.0" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-4.0_64bit" />
  <remove name="HttpRemotingHandlerFactory-soap-Integrated-4.0" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-4.0_32bit" />
  <remove name="rules-ISAPI-4.0_64bit" />
  <remove name="HttpRemotingHandlerFactory-rem-ISAPI-2.0-64" />
  <remove name="HttpRemotingHandlerFactory-rem-Integrated" />
  <remove name="HttpRemotingHandlerFactory-rem-ISAPI-4.0_32bit" />
  <remove name="HttpRemotingHandlerFactory-rem-ISAPI-4.0_64bit" />
  <remove name="AXD-ISAPI-2.0-64" />
  <remove name="cshtml-ISAPI-4.0_64bit" />
  <remove name="cshtml-Integrated-4.0" />
  <remove name="cshtml-Integrated-4.0" />
  <remove name="cshtml-ISAPI-4.0_32bit" />
  <remove name="cshtml-ISAPI-4.0_64bit" />
  <remove name="cshtml-ISAPI-4.0_32bit" />
  <remove name="AXD-ISAPI-4.0_64bit" />
  <remove name="AXD-ISAPI-2.0" />
  <remove name="AXD-ISAPI-4.0_32bit" />
```

```
<remove name="PageHandlerFactory-ISAPI-2.0-64" />
<remove name="PageHandlerFactory-ISAPI-2.0" />
<remove name="PageHandlerFactory-ISAPI-4.0_64bit" />
<remove name="PageHandlerFactory-ISAPI-4.0_32bit" />
<remove name="aspq-ISAPI-4.0_64bit" />
<remove name="aspq-Integrated-4.0" />
<remove name="WebServiceHandlerFactory-ISAPI-2.0" />
<remove name="aspq-ISAPI-4.0_32bit" />
<remove name="WebServiceHandlerFactory-Integrated-4.0" />
<remove name="WebServiceHandlerFactory-Integrated" />
<remove name="SimpleHandlerFactory-ISAPI-4.0_64bit" />
<remove name="SimpleHandlerFactory-Integrated-4.0" />
<remove name="SimpleHandlerFactory-Integrated" />
<remove name="SimpleHandlerFactory-ISAPI-2.0" />
<remove name="SimpleHandlerFactory-ISAPI-2.0-64" />
<remove name="WebServiceHandlerFactory-ISAPI-4.0_32bit" />
<remove name="WebServiceHandlerFactory-ISAPI-4.0_64bit" />
<remove name="WebServiceHandlerFactory-ISAPI-2.0-64" />
<remove name="SimpleHandlerFactory-ISAPI-4.0_32bit" />
<remove name="ISAPI-dll" />
<remove name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" />
<remove name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" />
<remove name="OPTIONSVerbHandler" />
<remove name="TRACEVerbHandler" />
</handlers>
</system.webServer>
```

#### **x) Restrict which HTTP verbs your application will work with**

```
<system.webServer>
<security>
<requestFiltering allowHighBitCharacters="false">
<verbs allowUnlisted="false">
<add verb="GET" allowed="true" />
<add verb="POST" allowed="true" />
</verbs>
</requestFiltering>
</security>
</system.webServer>
```

#### **xi) Also install IIS Managed “Remove Server Headers” Module**

*(\*) Not: Kurulum ve konfigürasyon hakkında uygulamalı ayrıntılı bilgi için bkz. Paketleme için Gözden Geçirilecekler / İnternette Edinilmiş Kıymetli Bilgiler / Sıkılaştırmalar / IIS Fingerprinting Engelleme Ayarı # Ekstra.*

Official Github Website:

<https://github.com/pingfu/iis-remove-server-headers>

Download Links:

<https://github.com/pingfu/iis-remove-server-headers#download>

Configuration Steps:

<https://github.com/pingfu/iis-remove-server-headers#configure-iis>

## B. Web.config Sıkılaştırma Ayarları Birleştirilmiş Hali

Web.config temel güvenlik sıkılaşturmalarının tamamı birleştirildiğinde aşağıdaki gibi bir dosya içeriği oluşur:

Web.config:

```
<system.web>

  <!-- -->
  <trace enabled="false" />

  <!-- Sadece Machine.Config'e Konabilir. Web.Config'de
  geçersizdir ve problemler doğurabilir. Bu satırın
  Web.Config'de kullanılması daha sonraları ilave olarak
  kullanılacak Ekstra Modüller vs..'ler dolayısıyla IIS
  sunucunun sürekli 500 Internal Error vermesine sebebiyet
  verebilir. Örn; IIS Remove Server Headers (by PingFu)
  modülünü IIS sunucuya yüklediğinde bu satırın sürekli
  500 Internal Error verdirmesi gibi. Bu satır Web.Config'ten
  kaldırıldığında sorun gitmiştir. Aynı şekilde bu satır
  Machine.Config'e konulduğunda olması gerektiği gibi yine
  sunucu sorunsuzca yanıtlarını dönebilmiştir.
  <deployment retail="true"/>
  -->

  <!-- -->
  <compilation debug="false" />

  <!-- -->
  <sessionState cookieName="s" />

  <!-- -->
  <httpRuntime enableVersionHeader="false" />

  <!-- -->
  <httpCookies httpOnlyCookies="false" requireSSL="false" />

</system.web>

<system.webServer>

  <!-- -->
```

```
<httpProtocol>
  <customHeaders>
    <!--
      IIS Remove Server Headers Modülü şu
      başlıkları otomatize bir şekilde kaldırır:

      Server
      X-Powered-By
      X-AspNet-Version
      X-AspNetMvc-Version

      Dolayısıyla aşağıdaki konfigürasyon ayarlarına
      ihtiyaç yoktur.
```

```
    <remove name="Server" />
    <remove name="X-AspNet-Version" />
    <remove name="X-AspNetMvc-Version" />
```

Not: X-Powered-By başlığı Windows Server sürümüne göre modül olsa bile ona rağmen gelebilmekteymiş. O nedenle eğer X-Powered-By engellenememişse aşağıdakini ilave etmemiz gerekirmiş:

```
    -->
    <remove name="X-Powered-By" />
  </customHeaders>
</httpProtocol>
```

```
<!-- -->
<httpErrors errorMode="Custom">
  <remove statusCode="502" subStatusCode="-1" />
  <remove statusCode="501" subStatusCode="-1" />
  <remove statusCode="500" subStatusCode="-1" />
  <remove statusCode="412" subStatusCode="-1" />
  <remove statusCode="406" subStatusCode="-1" />
  <remove statusCode="405" subStatusCode="-1" />
  <remove statusCode="404" subStatusCode="-1" />
  <remove statusCode="403" subStatusCode="-1" />
  <remove statusCode="401" subStatusCode="-1" />
  <remove statusCode="400" subStatusCode="-1" />

  <error statusCode="400" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="401" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="402" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="403" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="404" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="405" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="406" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
<error statusCode="412" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
<error statusCode="500" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
<error statusCode="501" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
<error statusCode="502" subStatusCode="-1" path="/error-handler.aspx"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
</httpErrors>
```

```
<!-- -->
```

```
<handlers>
```

```
<remove name="TraceHandler-Integrated-4.0" />
<remove name="TraceHandler-Integrated" />
<remove name="AssemblyResourceLoader-Integrated-4.0" />
<remove name="AssemblyResourceLoader-Integrated" />
<remove name="WebAdminHandler-Integrated-4.0" />
<remove name="WebAdminHandler-Integrated" />
<remove name="HttpRemotingHandlerFactory-soap-ISAPI-2.0-64" />
<remove name="svc-ISAPI-4.0_32bit" />
<remove name="ScriptHandlerFactoryAppServices-Integrated-4.0" />
<remove name="ScriptResourceIntegrated-4.0" />
<remove name="svc-ISAPI-4.0_64bit" />
<remove name="svc-Integrated-4.0" />
<remove name="vbhtm-ISAPI-4.0_32bit" />
<remove name="vbhtm-ISAPI-4.0_64bit" />
<remove name="vbhtm-Integrated-4.0" />
<remove name="vbhtml-ISAPI-4.0_32bit" />
<remove name="vbhtml-ISAPI-4.0_64bit" />
<remove name="vbhtml-Integrated-4.0" />
<remove name="xamlx-ISAPI-4.0_32bit" />
<remove name="xamlx-ISAPI-4.0_64bit" />
<remove name="xamlx-Integrated-4.0" />
<remove name="xoml-ISAPI-4.0_32bit" />
<remove name="xoml-ISAPI-4.0_64bit" />
<remove name="xoml-Integrated-4.0" />
<remove name="HttpRemotingHandlerFactory-rem-Integrated-4.0" />
<remove name="HttpRemotingHandlerFactory-rem-ISAPI-2.0" />
<remove name="rules-ISAPI-4.0_32bit" />
<remove name="rules-Integrated-4.0" />
<remove name="HttpRemotingHandlerFactory-soap-Integrated" />
<remove name="HttpRemotingHandlerFactory-soap-ISAPI-2.0" />
<remove name="HttpRemotingHandlerFactory-soap-ISAPI-4.0_64bit" />
<remove name="HttpRemotingHandlerFactory-soap-Integrated-4.0" />
<remove name="HttpRemotingHandlerFactory-soap-ISAPI-4.0_32bit" />
<remove name="rules-ISAPI-4.0_64bit" />
<remove name="HttpRemotingHandlerFactory-rem-ISAPI-2.0-64" />
<remove name="HttpRemotingHandlerFactory-rem-Integrated" />
<remove name="HttpRemotingHandlerFactory-rem-ISAPI-4.0_32bit" />
<remove name="HttpRemotingHandlerFactory-rem-ISAPI-4.0_64bit" />
```

```
<remove name="AXD-ISAPI-2.0-64" />
<remove name="cshtml-ISAPI-4.0_64bit" />
<remove name="cshtml-Integrated-4.0" />
<remove name="cshtm-Integrated-4.0" />
<remove name="cshtml-ISAPI-4.0_32bit" />
<remove name="cshtm-ISAPI-4.0_64bit" />
<remove name="cshtm-ISAPI-4.0_32bit" />
<remove name="AXD-ISAPI-4.0_64bit" />
<remove name="AXD-ISAPI-2.0" />
<remove name="AXD-ISAPI-4.0_32bit" />
<remove name="PageHandlerFactory-ISAPI-2.0-64" />
<remove name="PageHandlerFactory-ISAPI-2.0" />
<remove name="PageHandlerFactory-ISAPI-4.0_64bit" />
<remove name="PageHandlerFactory-ISAPI-4.0_32bit" />
<remove name="aspq-ISAPI-4.0_64bit" />
<remove name="aspq-Integrated-4.0" />
<remove name="WebServiceHandlerFactory-ISAPI-2.0" />
<remove name="aspq-ISAPI-4.0_32bit" />
<remove name="WebServiceHandlerFactory-Integrated-4.0" />
<remove name="WebServiceHandlerFactory-Integrated" />
<remove name="SimpleHandlerFactory-ISAPI-4.0_64bit" />
<remove name="SimpleHandlerFactory-Integrated-4.0" />
<remove name="SimpleHandlerFactory-Integrated" />
<remove name="SimpleHandlerFactory-ISAPI-2.0" />
<remove name="SimpleHandlerFactory-ISAPI-2.0-64" />
<remove name="WebServiceHandlerFactory-ISAPI-4.0_32bit" />
<remove name="WebServiceHandlerFactory-ISAPI-4.0_64bit" />
<remove name="WebServiceHandlerFactory-ISAPI-2.0-64" />
<remove name="SimpleHandlerFactory-ISAPI-4.0_32bit" />
<remove name="ISAPI-dll" />
<remove name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" />
<remove name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" />
<remove name="OPTIONSVerbHandler" />
<remove name="TRACEVerbHandler" />
</handlers>
```

```
<!-- -->
```

```
<security>
```

```
<requestFiltering allowHighBitCharacters="false">
```

```
<verbs allowUnlisted="false">
```

```
<add verb="GET" allowed="true" />
```

```
<add verb="POST" allowed="true" />
```

```
</verbs>
```

```
</requestFiltering>
```

```
</security>
```

```
</system.webServer>
```



Web.config'i destekleyici unsur olan IIS Remove Server Headers modülü ise IIS sunucuya kurulduğunda ve gerekli yapılandırma ayarları yapıldığında IIS sunucunun döneceği http yanıtlarında şu http başlıkları gönderimi (bilgi ifşaları) engellenmiş olur:

Server  
X-Powered-By  
X-AspNet-Version  
X-AspNetMvc-Version

IIS Remove Server Headers Kurulumu;

(\*) Uygulama başlığı altında kurulumu, konfigürasyonu ve çalışıyor mu testi gösterilmiştir.

- Adım I : RemoveServerHeader Modülü kurulur. Sonra sistem yeniden başlatılır.  
Adım II : Ardından IIS Manager açılır ve Server level'da olan (yani application level'da olan değil, Server level'da olan) Modules'e girilir.  
Adım III : Add Managed Module.. seçeneğine tıklanır.  
Adım IV : Modül ismi olarak keyfi bir (tanımlayıcı) ifade girilir. Modül türü olarak da Windows Server 2008 R2'ye exe'siyle kurduğumuz modül seçilerek konur.  
Adım V : Windows Server 2008 R2 sonrası windows server'larda default olarak kurulu gelmeyen ISAPI Filters built-in özelliği ilgili sürümde yüklenmelidir: Add Roles and Features Wizard -> Server Roles -> Web Server (IIS) -> Web Server -> Application Development -> + ISAPI Filters && + ISAPI Extensions  
(optional) Böylece IIS bilgi ifşası sunan http yanıtlarının gönderimi engellenmiş olacaktır.

Not:

Eğer X-Powered-By halen gelirse ki muhtemel gelecektir (çünkü Windows Server sürümden sürüme modülün davranışı uyumluluk dolayısıyla farklılık arz edebilmekteymiş), bu durumda web.config'e sadece şunu ilave etmek yeterliymiş:

web.config

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <remove name="X-Powered-By" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

Böylece tüm başlıklar kapatılabilir.

## Uygulama

(+) Birebir Windows Server 2008 R2 sanal makinesinde denenmiştir ve başarıyla uygulanmıştır.

a) Windows Server 2008 R2’de IIS Web.Config Sıkılaştırmalarının Birleştirilmesi

Bilgisayarında yüklü Windows Server 2008 R2 sanal makinasında IIS web.config dosyasına konulmuş ve sorunsuz IIS restart’lanarak kullanılabilmiş sıkılaştırmalar:

C:\inetpub\www\:

```
aspnet_client\  
iisstart.htm  
web.config  
welcome.png  
hataGosterim.htm      // 404 sayfası amacıyla oluşturulmuş custom error sayfası
```

web.config:

```
<?xml version="1.0" encoding="utf-8" ?>  
<configuration>  
<system.web>  
  
<!-- -->  
<trace enabled="false" />  
  
<!-- Sadece Machine.Config’e Konabilir. Web.Config’de  
geçersizdir ve problemler doğurabilir. Bu satırın  
Web.Config’de kullanılması daha sonraları ilave olarak  
kullanılacak Ekstra Modüller vs..’ler dolayısıyla IIS  
sunucunun sürekli 500 Internal Error vermesine sebebiyet  
verebilir. Örn; IIS Remove Server Headers (by PingFu)  
modülünü IIS sunucuya yüklediğinde bu satırın sürekli  
500 Internal Error verdirmesi gibi. Bu satır Web.Config’ten  
kaldırıldığında sorun gitmiştir. Aynı şekilde bu satır  
Machine.Config’e konulduğunda olması gerektiği gibi yine  
sunucu sorunsuzca yanıtlarını dönebilmiştir.  
<deployment retail="true"/>  
-->  
  
<!-- -->  
<compilation debug="false" />  
  
<!-- -->  
<sessionState cookieName="s" />  
  
<!-- -->  
<httpRuntime enableVersionHeader="false" />  
  
<!-- -->  
<httpCookies httpOnlyCookies="false" requireSSL="false" />
```

```
</system.web>
```

```
<system.webServer>
```

```
<!-- -->
```

```
<httpProtocol>
```

```
<customHeaders>
```

```
<remove name="Server" />
```

```
<remove name="X-Powered-By" />
```

```
<remove name="X-AspNet-Version" />
```

```
</customHeaders>
```

```
</httpProtocol>
```

```
<!-- -->
```

```
<httpErrors errorMode="Custom">
```

```
<remove statusCode="502" subStatusCode="-1" />
```

```
<remove statusCode="501" subStatusCode="-1" />
```

```
<remove statusCode="500" subStatusCode="-1" />
```

```
<remove statusCode="412" subStatusCode="-1" />
```

```
<remove statusCode="406" subStatusCode="-1" />
```

```
<remove statusCode="405" subStatusCode="-1" />
```

```
<remove statusCode="404" subStatusCode="-1" />
```

```
<remove statusCode="403" subStatusCode="-1" />
```

```
<remove statusCode="401" subStatusCode="-1" />
```

```
<remove statusCode="400" subStatusCode="-1" />
```

```
<error statusCode="400" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="401" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="402" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="403" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="404" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="405" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="406" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="412" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="500" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="501" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
<error statusCode="502" subStatusCode="-1" path="/hataGosterim.htm"  
  prefixLanguageFilePath="" responseMode="ExecuteURL" />
```

```
</httpErrors>
```

```
<!-- -->
```

```
<handlers>
  <remove name="TraceHandler-Integrated-4.0" />
  <remove name="TraceHandler-Integrated" />
  <remove name="AssemblyResourceLoader-Integrated-4.0" />
  <remove name="AssemblyResourceLoader-Integrated" />
  <remove name="WebAdminHandler-Integrated-4.0" />
  <remove name="WebAdminHandler-Integrated" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-2.0-64" />
  <remove name="svc-ISAPI-4.0_32bit" />
  <remove name="ScriptHandlerFactoryAppServices-Integrated-4.0" />
  <remove name="ScriptResourceIntegrated-4.0" />
  <remove name="svc-ISAPI-4.0_64bit" />
  <remove name="svc-Integrated-4.0" />
  <remove name="vbhtm-ISAPI-4.0_32bit" />
  <remove name="vbhtm-ISAPI-4.0_64bit" />
  <remove name="vbhtm-Integrated-4.0" />
  <remove name="vbhtml-ISAPI-4.0_32bit" />
  <remove name="vbhtml-ISAPI-4.0_64bit" />
  <remove name="vbhtml-Integrated-4.0" />
  <remove name="xamlx-ISAPI-4.0_32bit" />
  <remove name="xamlx-ISAPI-4.0_64bit" />
  <remove name="xamlx-Integrated-4.0" />
  <remove name="xoml-ISAPI-4.0_32bit" />
  <remove name="xoml-ISAPI-4.0_64bit" />
  <remove name="xoml-Integrated-4.0" />
  <remove name="HttpRemotingHandlerFactory-rem-Integrated-4.0" />
  <remove name="HttpRemotingHandlerFactory-rem-ISAPI-2.0" />
  <remove name="rules-ISAPI-4.0_32bit" />
  <remove name="rules-Integrated-4.0" />
  <remove name="HttpRemotingHandlerFactory-soap-Integrated" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-2.0" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-4.0_64bit" />
  <remove name="HttpRemotingHandlerFactory-soap-Integrated-4.0" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-4.0_32bit" />
  <remove name="rules-ISAPI-4.0_64bit" />
  <remove name="HttpRemotingHandlerFactory-rem-ISAPI-2.0-64" />
  <remove name="HttpRemotingHandlerFactory-rem-Integrated" />
  <remove name="HttpRemotingHandlerFactory-rem-ISAPI-4.0_32bit" />
  <remove name="HttpRemotingHandlerFactory-rem-ISAPI-4.0_64bit" />
  <remove name="AXD-ISAPI-2.0-64" />
  <remove name="cshtml-ISAPI-4.0_64bit" />
  <remove name="cshtml-Integrated-4.0" />
  <remove name="cshtm-Integrated-4.0" />
  <remove name="cshtml-ISAPI-4.0_32bit" />
  <remove name="cshtm-ISAPI-4.0_64bit" />
  <remove name="cshtm-ISAPI-4.0_32bit" />
  <remove name="AXD-ISAPI-4.0_64bit" />
  <remove name="AXD-ISAPI-2.0" />
  <remove name="AXD-ISAPI-4.0_32bit" />
  <remove name="PageHandlerFactory-ISAPI-2.0-64" />
  <remove name="PageHandlerFactory-ISAPI-2.0" />
  <remove name="PageHandlerFactory-ISAPI-4.0_64bit" />
```

```

<remove name="PageHandlerFactory-ISAPI-4.0_32bit" />
<remove name="aspq-ISAPI-4.0_64bit" />
<remove name="aspq-Integrated-4.0" />
<remove name="WebServiceHandlerFactory-ISAPI-2.0" />
<remove name="aspq-ISAPI-4.0_32bit" />
<remove name="WebServiceHandlerFactory-Integrated-4.0" />
<remove name="WebServiceHandlerFactory-Integrated" />
<remove name="SimpleHandlerFactory-ISAPI-4.0_64bit" />
<remove name="SimpleHandlerFactory-Integrated-4.0" />
<remove name="SimpleHandlerFactory-Integrated" />
<remove name="SimpleHandlerFactory-ISAPI-2.0" />
<remove name="SimpleHandlerFactory-ISAPI-2.0-64" />
<remove name="WebServiceHandlerFactory-ISAPI-4.0_32bit" />
<remove name="WebServiceHandlerFactory-ISAPI-4.0_64bit" />
<remove name="WebServiceHandlerFactory-ISAPI-2.0-64" />
<remove name="SimpleHandlerFactory-ISAPI-4.0_32bit" />
<remove name="ISAPI-dll" />
<remove name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" />
<remove name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" />
<remove name="OPTIONSVerbHandler" />
<remove name="TRACEVerbHandler" />
</handlers>

<!-- -->
<security>
  <requestFiltering allowHighBitCharacters="false">
    <verbs allowUnlisted="false">
      <add verb="GET" allowed="true" />
      <add verb="POST" allowed="true" />
    </verbs>
  </requestFiltering>
</security>

</system.webServer>

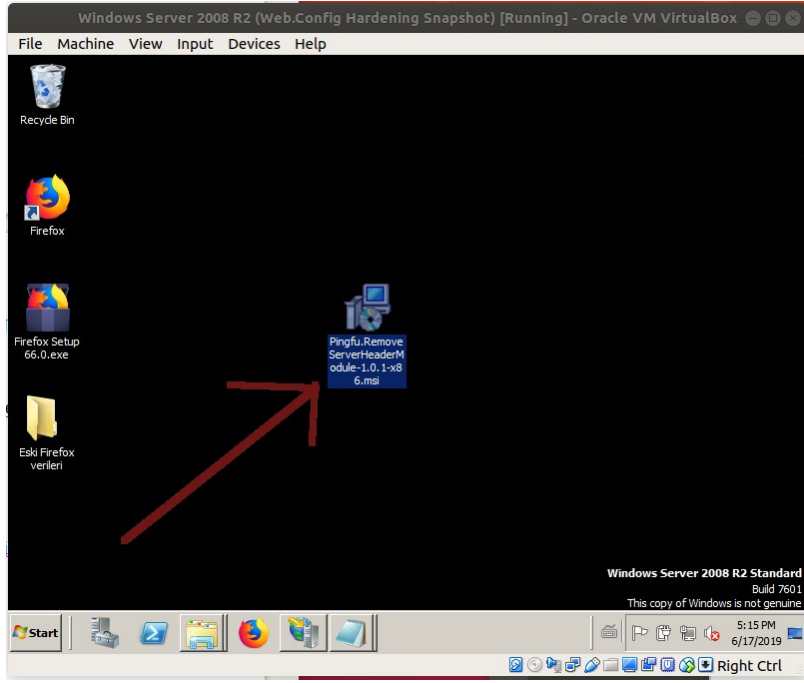
</configuration>

```

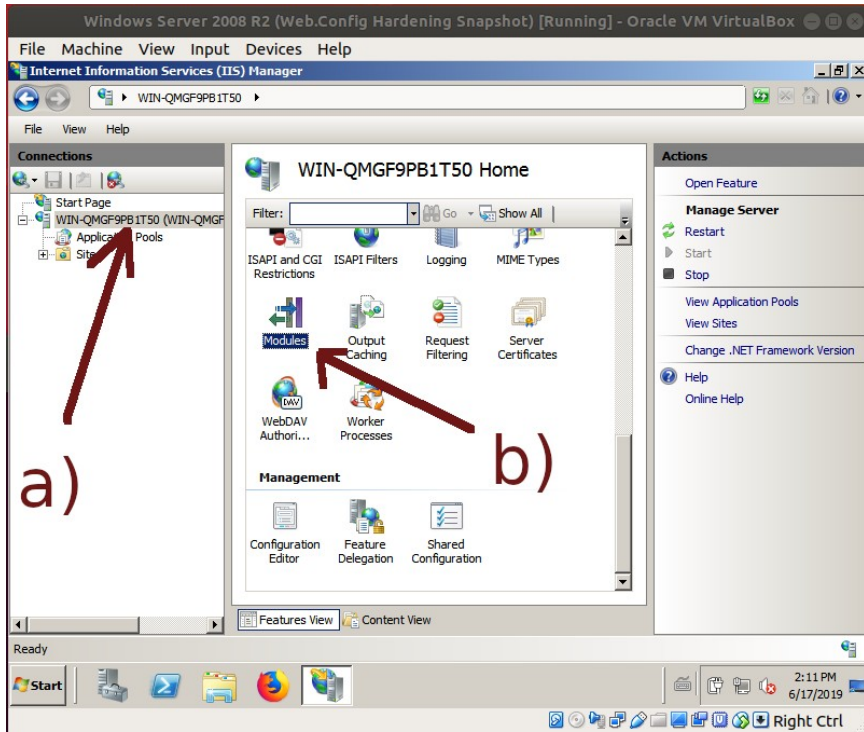
## **b) Windows Server 2008 R2'ye IIS Managed Module'ü Remove Server Headers Kurma**

IIS'in resmi olarak destek verdiği ve kabul ettiği (üçüncü taraf olmayan) modül IIS Remove Server Headers kurulumu ve konfigürasyonu ile Server, X-Powered-By, X-AspNet-Version, X-AspNetMvc-Version başlıklarının istemcilere gönderimini engelleyelim.

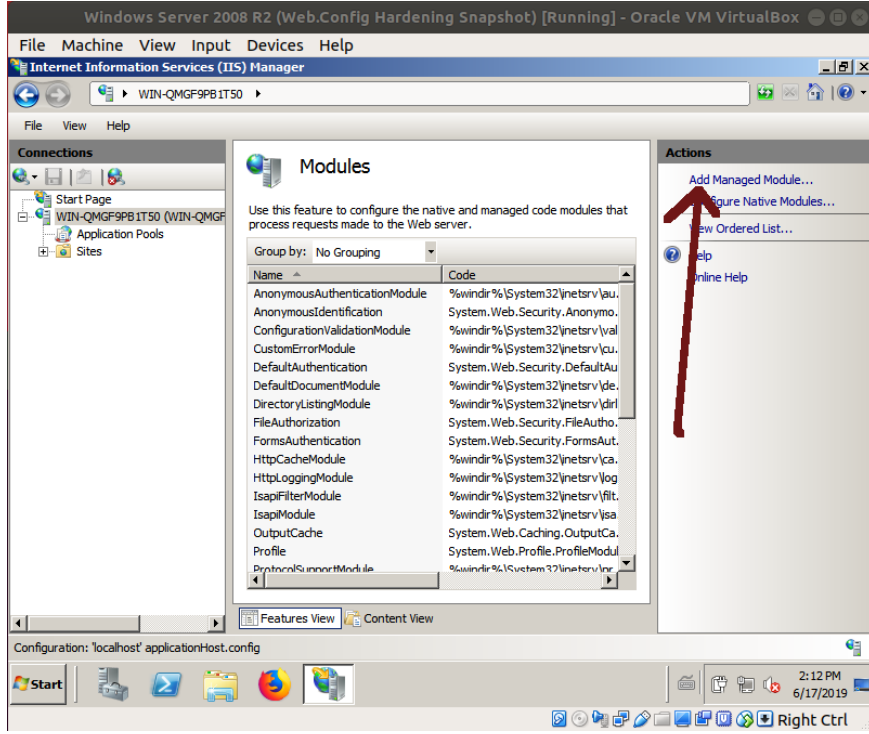
Adım I: RemoveServerHeader Modülü kurulur ve sonra sistem restart'lanır.



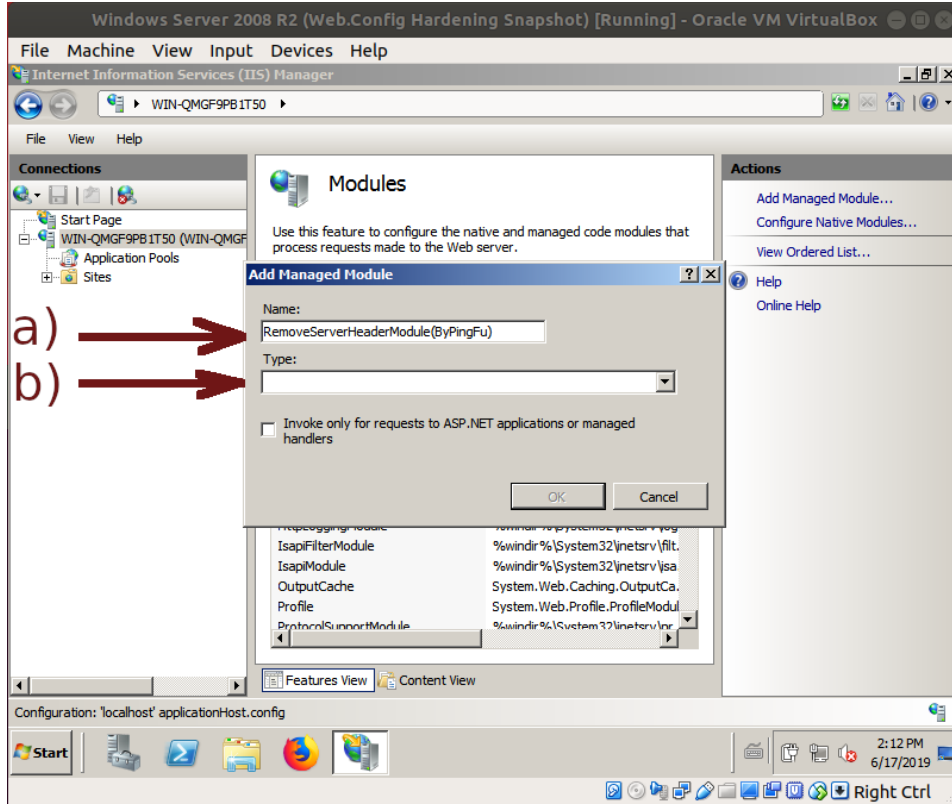
Adım II: Ardından IIS Manager açılır ve Server level'da olan (yani application level'da olan değil, Server level'da olan) Modules'e girilir.



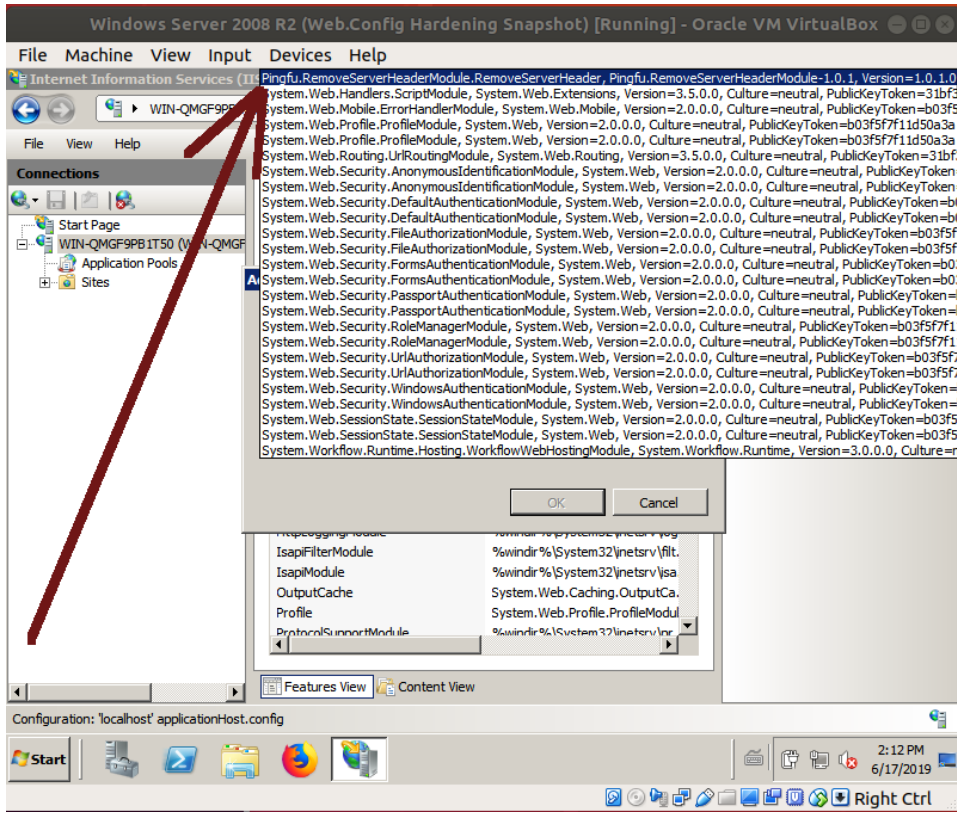
Adım III: Add Managed Module.. seçeneğine tıklanır.



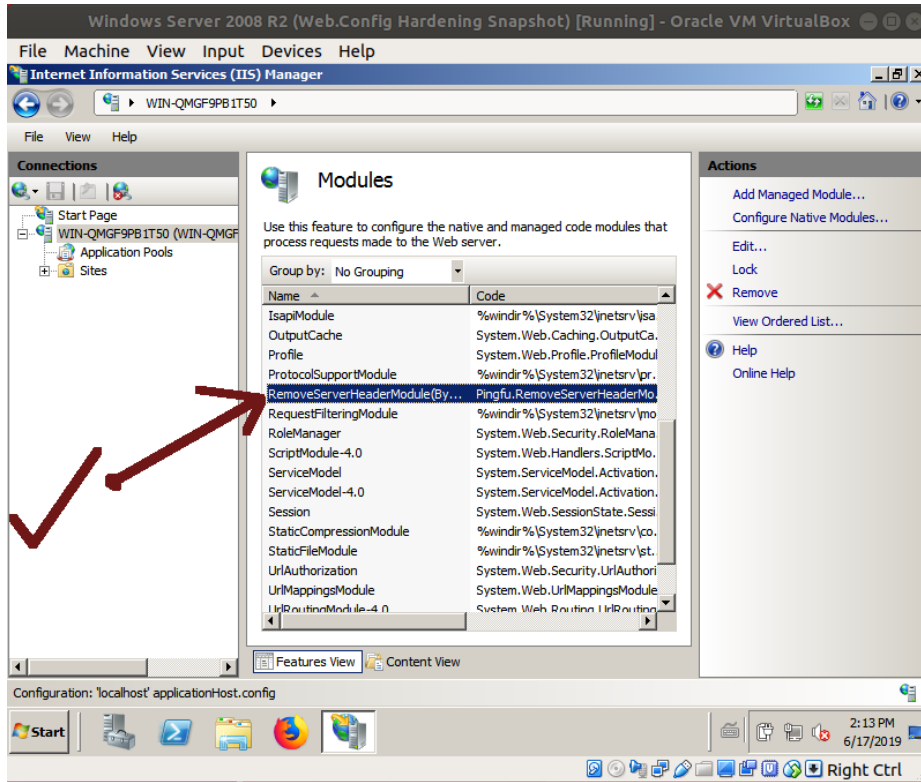
Adım IV: Modül ismi olarak keyfi bir (tanımlayıcı) ifade girilir. Modül türü olarak da Windows Server 2008 R2'ye exe'siyle kurduğumuz modül seçilerek konur.



(Keyfi / Tanımlayıcı Modül İsmi Girilir )

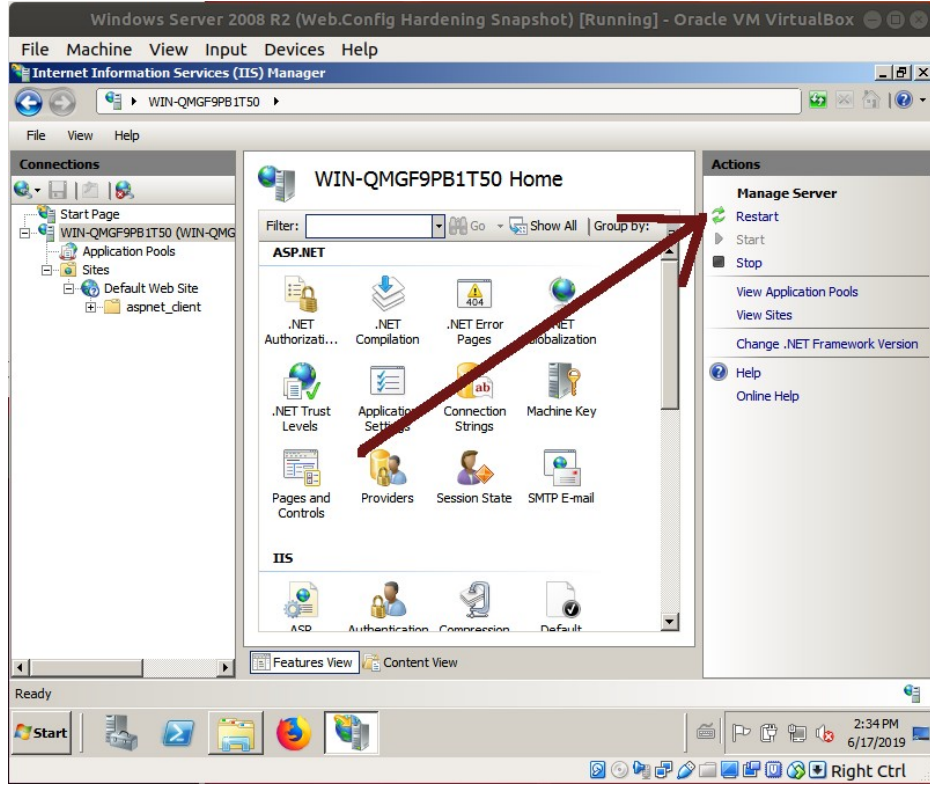


( Windows Server 2008 R2'ye exe'siyle yüklenen modül seçilir )



( Windows Server 2008'e Kurulan Modül IIS Manager'dan IIS'e Eklenir )





( IIS sunucu restart'lanır ve eklenen modül böylece etkin hale gelir )

NOT 1:

Eğer halen X-Powered-By geliyorsa ufak bir elle müdahale yapmak ve web.config içerisinde şunu ilave etmek yeterlidir:

web.config

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <remove name="X-Powered-By" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

Böylece şu başlıkların tamamının dışarıyı çıkışı engellenecektir

Server  
X-Powered-By  
X-AspNet-Version  
**X-AspNetMvc-Version**

NOT 2:

IIS Managed Remove Server Headers Modülünün Uyumluluğu Hk.

(\*) Windows Server 2012 ve sonrasına hitap eden bu ilave adım Ekstra başlığı altında uygulamalı olarak gösterilmiştir.

IIS Remove Server Headers modülü .NET 2.0 ile çalıştığından .NET 2.0'ı içeren .NET 3.5 feature'unun Windows Server 2012 ve sonrasında IIS'e feature olarak eklenmesi gerekmektedir. Çünkü Windows Server 2012 ve sonrasında hazır kurulu gelen .NET framework versiyonu artık .NET 4.5 sürüm framework'tür. Ayrıca Windows Server 2012 ve sonrasında IIS Remove Server Headers modülünün ihtiyaç duyduğu ISAPI Filters ve ISAPI Extensions feature'ları Windows Server 2008 ve öncesinde default kuruluyken sonrasında kurulu olarak gelmediğinden ilave feature olarak eklenmeleri gerekmektedir.

Server Manager

Roles and Features

Web Server (IIS)

Application Development

.NET 3.5 Extensibility	(*) Gerekli
.NET 4.0 Extensibility	(*) <i>Seçime Bağlı (optional)</i>
ASP	(*) Gerekli
ASP.NET 3.5	(*) Gerekli
ASP.NET 4.5	(*) <i>Seçime Bağlı (optional)</i>
ISAPI Extensions	(*) Gerekli
ISAPI Filters	(*) Gerekli

[!] Uyarı:

Bu yüklemeler için Windows Server Kurulum DVD'si takılmalıdır ve IIS feature eklemeleri sırasında kurulum kaynak dosyası yolu için DVD'nin takılı olduğu sürücü ve akabinde \sources\sxs\ dizin yolu gösterilmelidir. Ancak bu sayede, kurulum başarıyla tamamlanabilecektir.

Kurulum sonrası IIS Remove Headers modülünü IIS panele ekleme işlemi sorunsuzca gerçekleşip modül, bilgi ifşası sunan sunucu başlıklarının gönderimini engelleyebilecektir.

### c) Windows Server 2008 R2'de Web.Config Sıkılaştırmalarının ve IIS Remove Server Headers Modülünün Etkin Olup Olmadığını Test Etme

i) Test 1: Custom Error Sayfası hataGosterim.htm Çalışıyor mu Testi

Olmayan bir web sayfasına erişmeye çalıştığımızda 404 Not Found varsayılan hata sayfası mı dönecek yoksa IIS web.config'te belirttiğimiz hataGosterim.htm web sayfası mı ekrana verilecek testi;

Ubuntu 18.04 LTS Terminal (Var Olan Sayfa Talep Etme ve Gelen Yanıt) :

```
> telnet 172.16.3.113 80
GET / HTTP/1.0
Host: 172.16.3.113
```

// Anasayfa Talep Edilir

Çıktı:  
HTTP/1.1 200 OK // Ve sorun yok yanıtı gelir.  
Content-Type: text/html  
Last-Modified: Tue, 19 Mar 2019 13:50:27 GMT  
Accept-Ranges: bytes  
ETag: "d1d742b55aded41:0"  
Date: Tue, 18 Jun 2019 02:33:36 GMT  
Connection: close  
Content-Length: 18

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
<!--
body {
    color:#000000;
...

```

Ubuntu 18.04 LTS Terminal (Var Olmayan Sayfa Talep Etme ve Gelen Yanıt):

```
> telnet 172.16.3.113 80
GET /abdfdfdfd HTTP/1.0 // Var Olmayan Bir Sayfa Talep Edilir
Host: 172.16.3.113
```

Çıktı:  
HTTP/1.1 200 OK // Ve sorun yok yanıtı gelir. Fakat  
Content-Type: text/html // Custom Error Sayfasıyla.  
Last-Modified: Tue, 19 Mar 2019 13:50:27 GMT  
Accept-Ranges: bytes  
ETag: "d1d742b55aded41:0"  
Date: Tue, 18 Jun 2019 02:40:27 GMT  
Connection: close  
Content-Length: 18  
**400 Bad Request...** // Custom Error Sayfası (hataGos  
Connection closed by foreign host. // terim.htm) İçeriği

Sonuç olarak Web.config'teki eklenen

```
<httpErrors errorMode="Custom">
...
<error statusCode="404" subStatusCode="-1" path="/hataGosterim.htm"
prefixLanguageFilePath="" responseMode="ExecuteURL" />
...
</httpErrors>
```

satırları çalıştığından dolayı olmayan bir sayfayı istediğimizde 404 Not Found standard hata sayfası gelmeliyken bizim sunucuda tanımladığımız custom hata sayfası hataGosterim.htm ekrana gelmiştir.

## ii) Test 2: İzinli Tanımlaması Yapılmamış HEAD Talebi Halen Yapılabiliyor mu Testi

Telnet ile HEAD talebi yaptığımızda sunucu web.config'te belirttiğimiz izinli http talep listesinde olmayan HEAD talebine karşılık olumlu yanıt mı dönecek yoksa olumsuz yanıt mı dönecek testi aşağıda verilmiştir:

Ubuntu 18.04 LTS Terminal (İzinliler Listesine Konmamış Talep Türüyle Http Talep Yapma) :

```
> telnet 172.16.3.113 80
HEAD / HTTP/1.0
Host: 172.16.3.113
```

// Anasayfaya HTTP HEAD Talebi yapılır

```
Çıktı:
Trying 172.16.3.113...
Connected to 172.16.3.113.
Escape character is '^]'.
HEAD / HTTP/1.0
Host: 172.16.3.113
```

```
HTTP/1.1 404 Not Found
Content-Length: 0
Date: Tue, 18 Jun 2019 03:05:17 GMT
Connection: close
Connection closed by foreign host.
```

// Metod Çalışmaz ve Sunucudan  
// Olumsuz Yanıt Gelir.

Sonuç olarak Web.config'teki eklenen

```
<security>
  <requestFiltering allowHighBitCharacters="false">
    <verbs allowUnlisted="false">
      <add verb="GET" allowed="true" />
      <add verb="POST" allowed="true" />
    </verbs>
  </requestFiltering>
</security>
```

satırları çalıştığından dolayı izin verilmemiş http talebi HEAD yapıldığında sunucu olması gerektiği gibi olumlu değil olumsuz yanıt dönmüştür.

## iii) Test 3: IIS Remove Server Headers Modülü Sunucu Bilgi İfşası Yapan Başlıkları Engellemekte mi Testi

IIS Managed Modülü IIS Remove Server Headers ile IIS sunucunun döndüğü yanıtlardaki bilgi ifşalarının önüne geçilip geçilmediği testi aşağıda verilmiştir:

Ubuntu 18.04 LTS Terminal ( MODÜL ÖNCESİ ):

```
> telnet 172.16.3.113 80
HEAD / HTTP/1.0
```

```
Çıktı:
HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT
Accept-Ranges: bytes
Etag: "43acgjr0874933dafwq"
Server: IIS/7.5
X-Powered-By: ASP.NET
Date: Mon, 17 Jun 2019, 21:22:36 GMT
Connection: close
Connection closed by foreign host.
```

Ubuntu 18.04 LTS Terminal ( MODÜL SONRASI ):

```
> telnet 172.16.3.113 80
HEAD / HTTP/1.0
```

```
Çıktı:
HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT
Accept-Ranges: bytes
Etag: "43acgjr0874933dafwq"
X-Powered-By: ASP.NET
Date: Mon, 17 Jun 2019, 21:22:36 GMT
Connection: close
Connection closed by foreign host.
```

// (-) Halen geliyor.

Bilgi ifşa eden başlıklardan sadece X-Powered-By kalmış. Bazı durumlarda X-Powered-By başlığı gelebilirmiş. Bu nedenle eğer IIS remove headers modülü kurulmasına rağmen halen X-Powered-By gelmekteyse web.config dosyasına

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <remove name="X-Powered-By" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
```

</configuration>

ayarlarını eklemek yeterlidir.

Ubuntu 18.04 LTS Terminal ( MODÜL SONRASI ve Web.Config İlave Ayarı SONRASI ):

```
> telnet 172.16.3.113 80
HEAD / HTTP/1.0
```

Çıktı:

HTTP/1.1 200 OK

Content-Length: 689

Content-Type: text/html

Last-Modified: Mon, 19 Nov 2018 23:23:51 GMT

Accept-Ranges: bytes

Etag: "43acgjr0874933dafwq"

// (+) Bilgi ifşa eden başlıklar

Date: Mon, 17 Jun 2019, 21:22:36 GMT

// kalkmıştır.

Connection: close

Connection closed by foreign host.

## Ekstra

(+) Birebir Windows Server 2012 R2 sanal makinesinde denenmiştir ve başarıyla uygulanmıştır.

a) Windows Server 2012 R2’de IIS Web.Config Sıkılaştırmalarının Birleştirilmesi

Bilgisayarında yüklü Windows Server 2012 R2 sanal makinasında IIS web.config dosyasına konulmuş ve sorunsuz IIS restart’lanarak kullanılabilmiş sıkılaştırmalar:

C:\inetpub\www\:

aspnet\_client\

iisstart.htm

web.config

iis-85.png

hataGosterim.htm // 404 sayfası amacıyla oluşturulmuş custom error sayfası

web.config:

```
<?xml version="1.0" encoding="utf-8" ?>
```

```
<configuration>
```

```
<system.web>
```

```
<!-- -->
```

```
<trace enabled="false" />
```

```
<!-- Sadece Machine.Config’e Konabilir. Web.Config’de  
geçersizdir ve problemler doğurabilir. Bu satırın
```

Web.Config’de kullanılması daha sonraları ilave olarak kullanılacak Ekstra Modüller vs..’ler dolayısıyla IIS sunucunun sürekli 500 Internal Error vermesine sebebiyet verebilir. Örn; IIS Remove Server Headers (by PingFu) modülünü IIS sunucuya yüklediğinde bu satırın sürekli 500 Internal Error verdirmesi gibi. Bu satır Web.Config’ten kaldırıldığında sorun gitmiştir. Aynı şekilde bu satır Machine.Config’e konulduğunda olması gerektiği gibi yine sunucu sorunsuzca yanıtlarını dönebilmiştir.

```
<deployment retail="true"/>
```

```
-->
```

```
<!-- -->
```

```
<compilation debug="false" />
```

```
<!-- -->
```

```
<sessionState cookieName="s" />
```

```
<!-- -->
```

```
<httpRuntime enableVersionHeader="false" />
```

```
<!-- -->
```

```
<httpCookies httpOnlyCookies="false" requireSSL="false" />
```

```
</system.web>
```

```
<system.webServer>
```

```
<!-- -->
```

```
<httpProtocol>
```

```
<customHeaders>
```

```
<!--
```

```
IIS Remove Server Headers Modülü şu başlıkları otomatize bir şekilde kaldırır:
```

```
Server
```

```
X-Powered-By
```

```
X-AspNet-Version
```

```
X-AspNetMvc-Version
```

```
Dolayısıyla aşağıdaki konfigürasyon ayarlarına ihtiyaç yoktur.
```

```
<remove name="Server" />
```

```
<remove name="X-AspNet-Version" />
```

```
<remove name="X-AspNetMvc-Version" />
```

```
Not: X-Powered-By başlığı Windows Server sürümüne göre modül olsa bile ona rağmen gelebilmekteymiş. O nedenle eğer X-Powered-By engellenememişse aşağıdakini ilave etmemiz gerekirmiş:
```

```
-->
```

```
<remove name="X-Powered-By" />
</customHeaders>
</httpProtocol>

<!-- -->
<httpErrors errorMode="Custom">
  <remove statusCode="502" subStatusCode="-1" />
  <remove statusCode="501" subStatusCode="-1" />
  <remove statusCode="500" subStatusCode="-1" />
  <remove statusCode="412" subStatusCode="-1" />
  <remove statusCode="406" subStatusCode="-1" />
  <remove statusCode="405" subStatusCode="-1" />
  <remove statusCode="404" subStatusCode="-1" />
  <remove statusCode="403" subStatusCode="-1" />
  <remove statusCode="401" subStatusCode="-1" />
  <remove statusCode="400" subStatusCode="-1" />

  <error statusCode="400" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="401" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="402" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="403" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="404" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="405" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="406" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="412" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="500" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="501" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
  <error statusCode="502" subStatusCode="-1" path="/hataGosterim.htm"
    prefixLanguageFilePath="" responseMode="ExecuteURL" />
</httpErrors>

<!-- -->
<handlers>
  <remove name="TraceHandler-Integrated-4.0" />
  <remove name="TraceHandler-Integrated" />
  <remove name="AssemblyResourceLoader-Integrated-4.0" />
  <remove name="AssemblyResourceLoader-Integrated" />
  <remove name="WebAdminHandler-Integrated-4.0" />
  <remove name="WebAdminHandler-Integrated" />
  <remove name="HttpRemotingHandlerFactory-soap-ISAPI-2.0-64" />
  <remove name="svc-ISAPI-4.0_32bit" />
  <remove name="ScriptHandlerFactoryAppServices-Integrated-4.0" />

```



```
<remove name="ScriptResourceIntegrated-4.0" />
<remove name="svc-ISAPI-4.0_64bit" />
<remove name="svc-Integrated-4.0" />
<remove name="vbhtm-ISAPI-4.0_32bit" />
<remove name="vbhtm-ISAPI-4.0_64bit" />
<remove name="vbhtm-Integrated-4.0" />
<remove name="vbhtml-ISAPI-4.0_32bit" />
<remove name="vbhtml-ISAPI-4.0_64bit" />
<remove name="vbhtml-Integrated-4.0" />
<remove name="xamlx-ISAPI-4.0_32bit" />
<remove name="xamlx-ISAPI-4.0_64bit" />
<remove name="xamlx-Integrated-4.0" />
<remove name="xoml-ISAPI-4.0_32bit" />
<remove name="xoml-ISAPI-4.0_64bit" />
<remove name="xoml-Integrated-4.0" />
<remove name="HttpRemotingHandlerFactory-rem-Integrated-4.0" />
<remove name="HttpRemotingHandlerFactory-rem-ISAPI-2.0" />
<remove name="rules-ISAPI-4.0_32bit" />
<remove name="rules-Integrated-4.0" />
<remove name="HttpRemotingHandlerFactory-soap-Integrated" />
<remove name="HttpRemotingHandlerFactory-soap-ISAPI-2.0" />
<remove name="HttpRemotingHandlerFactory-soap-ISAPI-4.0_64bit" />
<remove name="HttpRemotingHandlerFactory-soap-Integrated-4.0" />
<remove name="HttpRemotingHandlerFactory-soap-ISAPI-4.0_32bit" />
<remove name="rules-ISAPI-4.0_64bit" />
<remove name="HttpRemotingHandlerFactory-rem-ISAPI-2.0-64" />
<remove name="HttpRemotingHandlerFactory-rem-Integrated" />
<remove name="HttpRemotingHandlerFactory-rem-ISAPI-4.0_32bit" />
<remove name="HttpRemotingHandlerFactory-rem-ISAPI-4.0_64bit" />
<remove name="AXD-ISAPI-2.0-64" />
<remove name="cshtml-ISAPI-4.0_64bit" />
<remove name="cshtml-Integrated-4.0" />
<remove name="cshtm-Integrated-4.0" />
<remove name="cshtml-ISAPI-4.0_32bit" />
<remove name="cshtm-ISAPI-4.0_64bit" />
<remove name="cshtm-ISAPI-4.0_32bit" />
<remove name="AXD-ISAPI-4.0_64bit" />
<remove name="AXD-ISAPI-2.0" />
<remove name="AXD-ISAPI-4.0_32bit" />
<remove name="PageHandlerFactory-ISAPI-2.0-64" />
<remove name="PageHandlerFactory-ISAPI-2.0" />
<remove name="PageHandlerFactory-ISAPI-4.0_64bit" />
<remove name="PageHandlerFactory-ISAPI-4.0_32bit" />
<remove name="aspq-ISAPI-4.0_64bit" />
<remove name="aspq-Integrated-4.0" />
<remove name="WebServiceHandlerFactory-ISAPI-2.0" />
<remove name="aspq-ISAPI-4.0_32bit" />
<remove name="WebServiceHandlerFactory-Integrated-4.0" />
<remove name="WebServiceHandlerFactory-Integrated" />
<remove name="SimpleHandlerFactory-ISAPI-4.0_64bit" />
<remove name="SimpleHandlerFactory-Integrated-4.0" />
<remove name="SimpleHandlerFactory-Integrated" />
```

```
<remove name="SimpleHandlerFactory-ISAPI-2.0" />
<remove name="SimpleHandlerFactory-ISAPI-2.0-64" />
<remove name="WebServiceHandlerFactory-ISAPI-4.0_32bit" />
<remove name="WebServiceHandlerFactory-ISAPI-4.0_64bit" />
<remove name="WebServiceHandlerFactory-ISAPI-2.0-64" />
<remove name="SimpleHandlerFactory-ISAPI-4.0_32bit" />
<remove name="ISAPI-dll" />
<remove name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" />
<remove name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" />
<remove name="OPTIONSVerbHandler" />
<remove name="TRACEVerbHandler" />
</handlers>

<!-- -->
<security>
  <requestFiltering allowHighBitCharacters="false">
    <verbs allowUnlisted="false">
      <add verb="GET" allowed="true" />
      <add verb="POST" allowed="true" />
    </verbs>
  </requestFiltering>
</security>

</system.webServer>

</configuration>
```

## b) Windows Server 2012 R2'ye IIS Managed Module'ü Remove Server Headers Kurma

IIS'in resmi olarak destek verdiği ve kabul ettiği (üçüncü taraf olmayan) modül IIS Remove Server Headers kurulumu ve konfigürasyonu ile Server, X-Powered-By, X-AspNet-Version, X-AspNetMvc-Version başlıklarının istemcilere gönderimini engelleyelim.

### IIS Managed Remove Server Headers Modülünün Uyumluluğu Hk.

---

(\* ) Windows Server 2012 ve sonraki sürümlere hitap etmektedir.

IIS Remove Server Headers modülü .NET 2.0 ile çalıştığından .NET 2.0'ı içeren .NET 3.5 feature'unun Windows Server 2012 ve sonrasında IIS'e feature olarak eklenmesi gerekmektedir. Çünkü Windows Server 2012 ve sonrasında hazır kurulu gelen .NET framework versiyonu .NET 4.5 tir ve .NET 3.5 seçime bağlı olarak sonradan eklenebilir halde hazır kurulu gelmemektedir. Ayrıca Windows Server 2012 ve sonrasında IIS Remove Server Headers modülünün ihtiyaç duyduğu ISAPI Filters ve ISAPI Extensions feature'ları Windows Server 2008 ve öncesinde default kuruluken sonrasında kurulu olarak gelmediğinden ilave feature olarak eklenmeleri gerekmektedir.

Server Manager

Roles and Features

Web Server (IIS)

Application Development

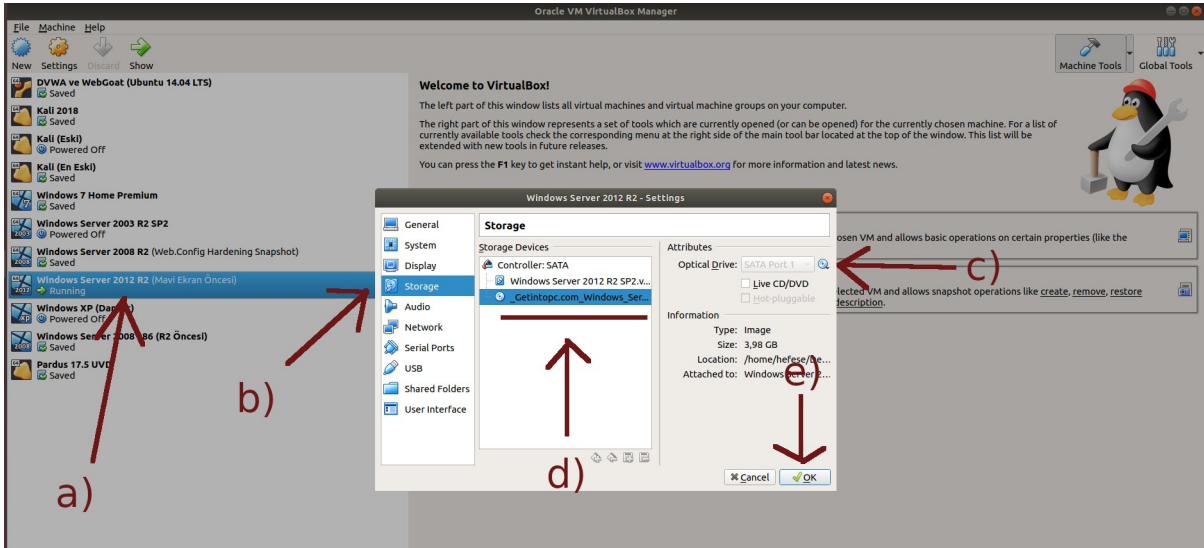
- + .NET 3.5 Extensibility (\*) Gerekli
- + .NET 4.0 Extensibility (\*) *Seçime Bağlı (optional)*
- + ASP (\*) Gerekli
- + ASP.NET 3.5 (\*) Gerekli
- + ASP.NET 4.5 (\*) *Seçime Bağlı (optional)*
- + ISAPI Extentions (\*) Gerekli
- + ISAPI Filters (\*) Gerekli

[!] Uyarı:

Bu yüklemeler için Windows Server Kurulum DVD'si takılmalıdır ve IIS feature eklemeleri sırasında kurulum kaynak dosyası yolu için DVD'nin takılı olduğu sürücü ve akabinde \sources\sxs\ dizini yolu gösterilmelidir. Ancak bu sayede, kurulum başarıyla tamamlanabilecektir.

Kurulum sonrası IIS Remove Headers modülünü IIS panele ekleme işlemi sorunsuzca gerçekleşip modül, bilgi ifşası sunan sunucu başlıklarının gönderimini engelleyebilecektir.

Adım I: RemoveServerHeader modülünün ihtiyaç duyduğu .net framework sürümü (ihtiyaç duyulan 2.0 sürümünü içerdiğinden 3.5 sürümü) ve ISAPI Filters feature'larını IIS'e yüklemek için Windows Server kurulum DVD'si takılır.



Ardından Server Manager açılır. Add Roles And Features'dan "Server Roles" penceresine gelindiğinde

Web Server (IIS) -> Web Server -> Application Development

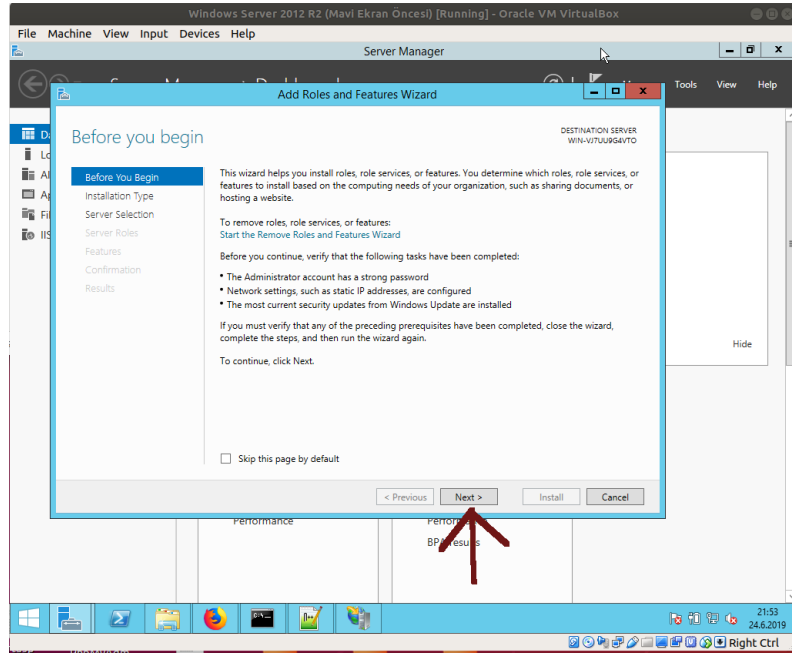
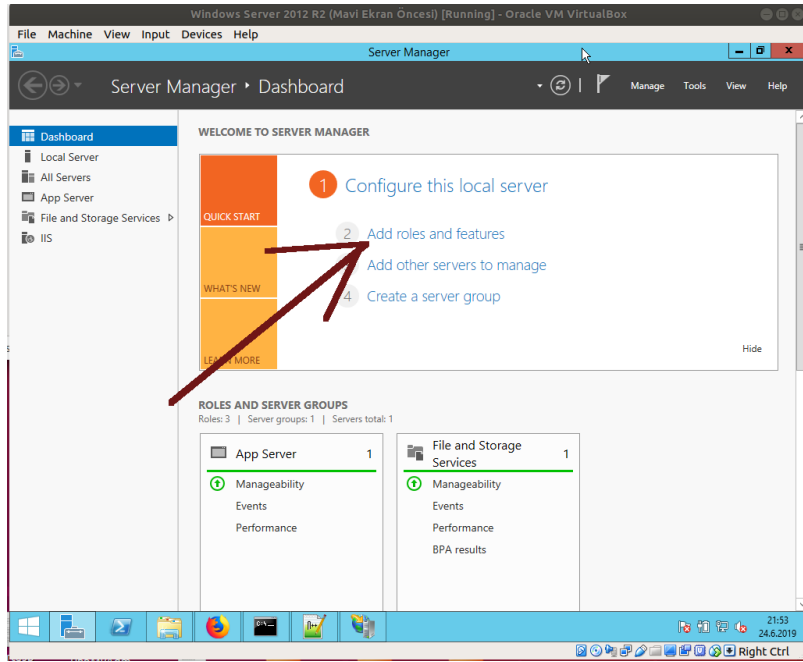
seçeneklerine gidilir ve

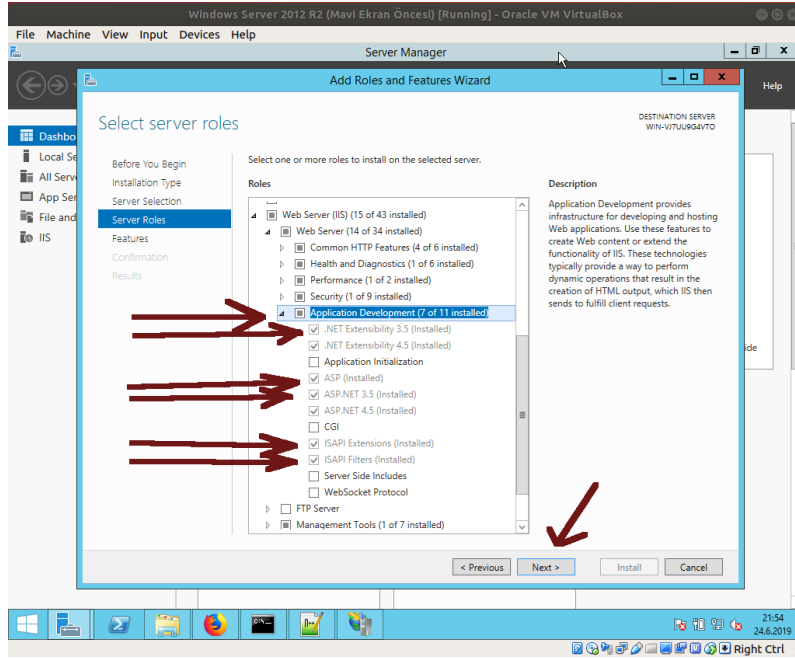
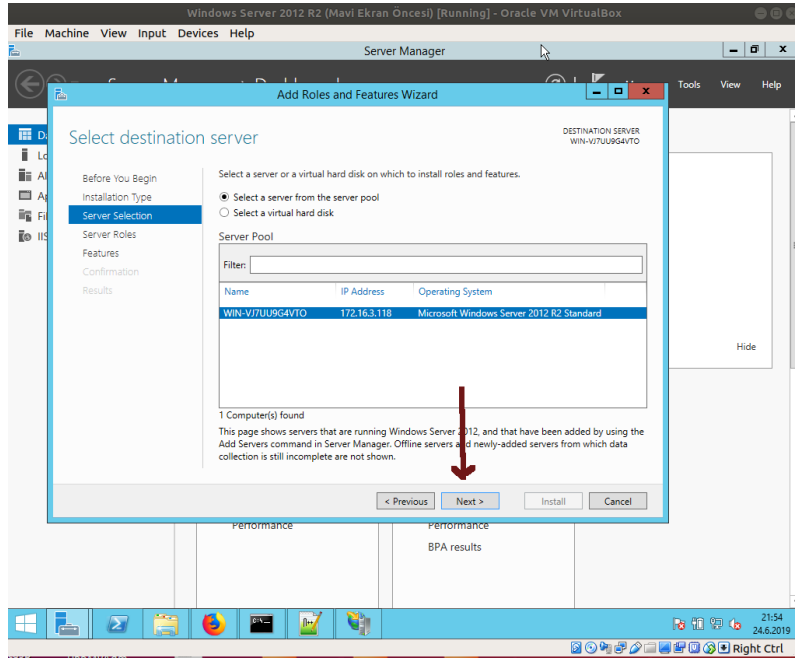
- .NET 3.5 Extensibility (\*) Gerekli
- .NET 4.0 Extensibility (\*) *Seçime Bağlı (optional)*
- ASP (\*) Gerekli
- ASP.NET 3.5 (\*) Gerekli
- ASP.NET 4.5 (\*) *Seçime Bağlı (optional)*
- ISAPI Extentions (\*) Gerekli

ISAPI Filters

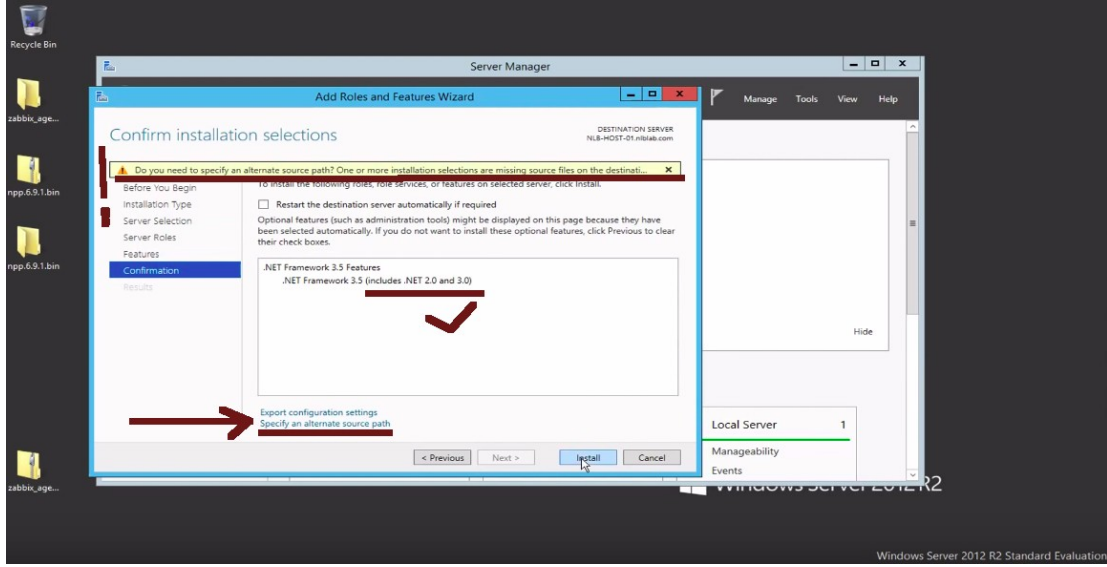
(\*) Gerekli

seçenekleri işaretlenir.





Ardından yüklenecekler listesi ekrana gelir. Bu ekranda bir uyarı görünecektir: "... One or more installation selections are missing source files on the destination...".



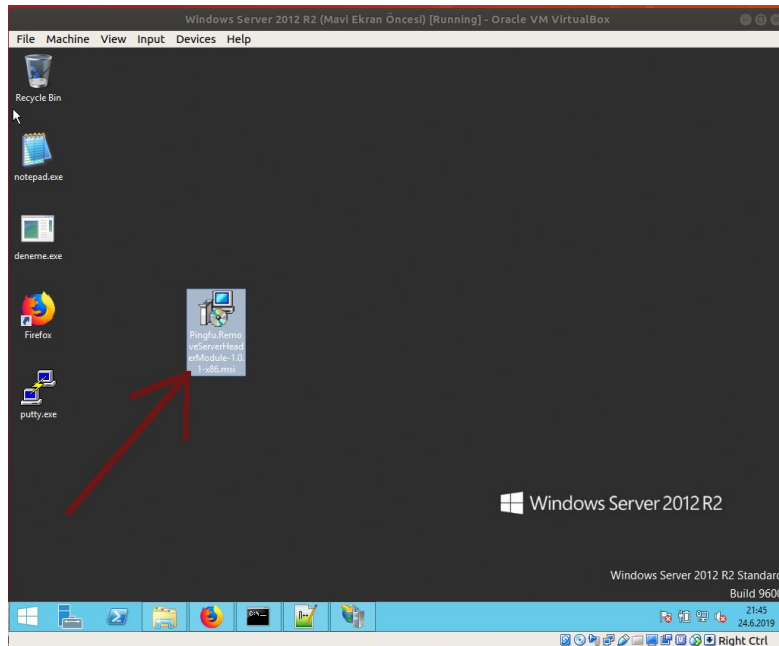
Bu ekranda yüklenecekler listesindeki bazı bileşenler (örn; .NET Framework 3.5) Windows Server kurulum DVD'sinin sources\sxs\ dizininde yer alan kurulum dosyalarına ihtiyaç duyarlar. Dolayısıyla ekrandaki "Specify an alternate source path" linkine tıklanıp gelen ekrandaki source path textbox'ına Windows Server kurulum DVD'si ve sources\sxs\ dizin yolu girilmelidir ve sonra kurulumla başlanmalıdır. Böylece yükleme sorunsuz gerçekleşecektir.

Kurulum Dosyaları Path'i (örn):

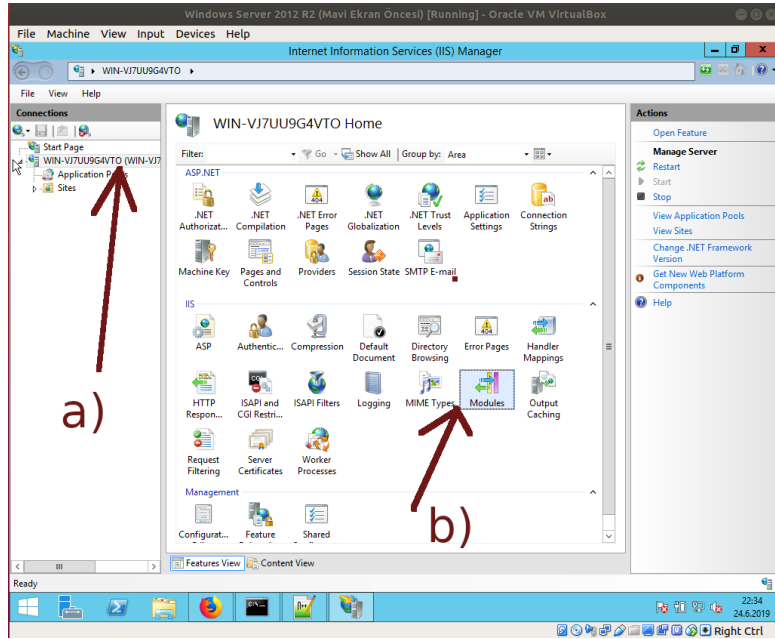
D:\sources\sxs\

// D sürücüsü DVD'nin Olduğu Sürücü

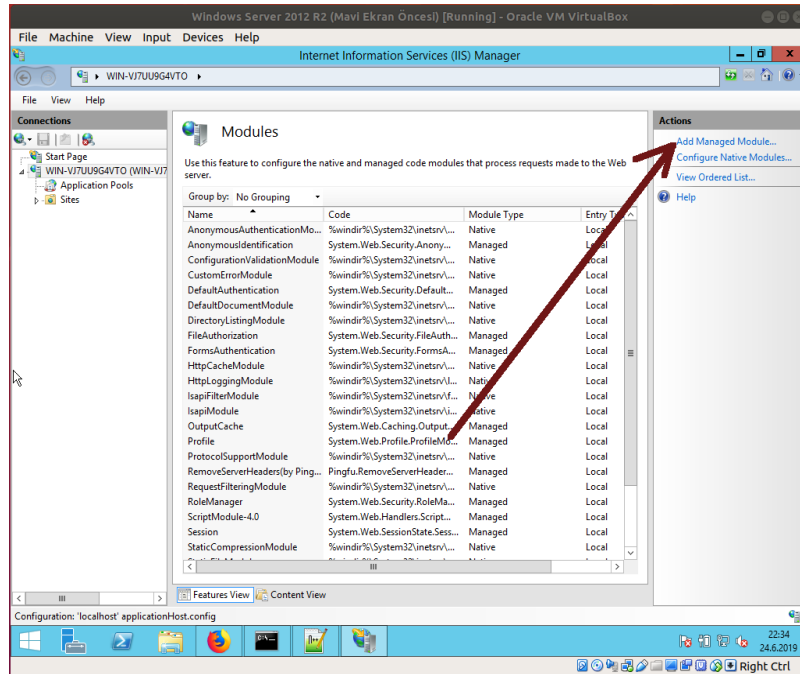
Adım II: RemoveServerHeader Modülü kurulum ve sonra sistem restart'lanır.



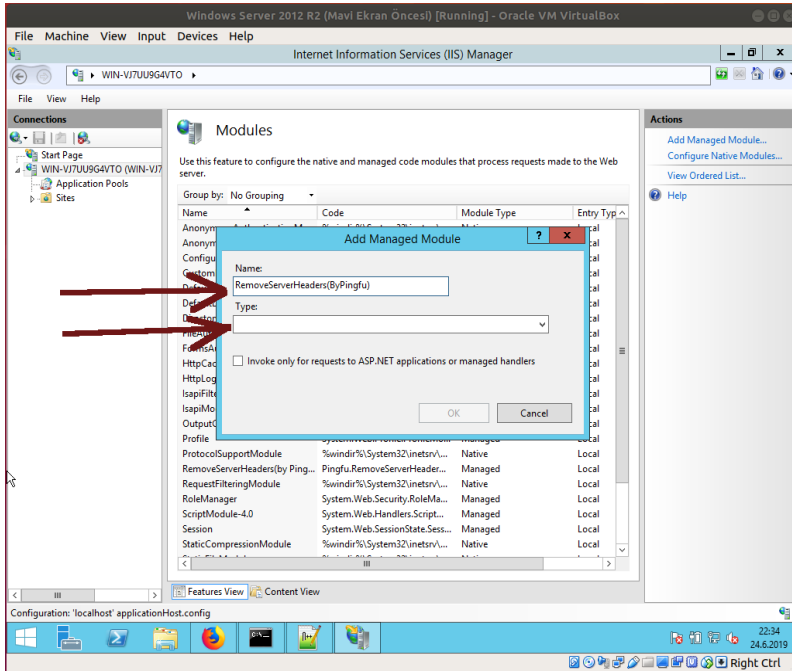
Adım III: Ardından IIS Manager açılır ve Server level'da olan (yani application level'da olan değil, Server level'da olan) Modules'e girilir.



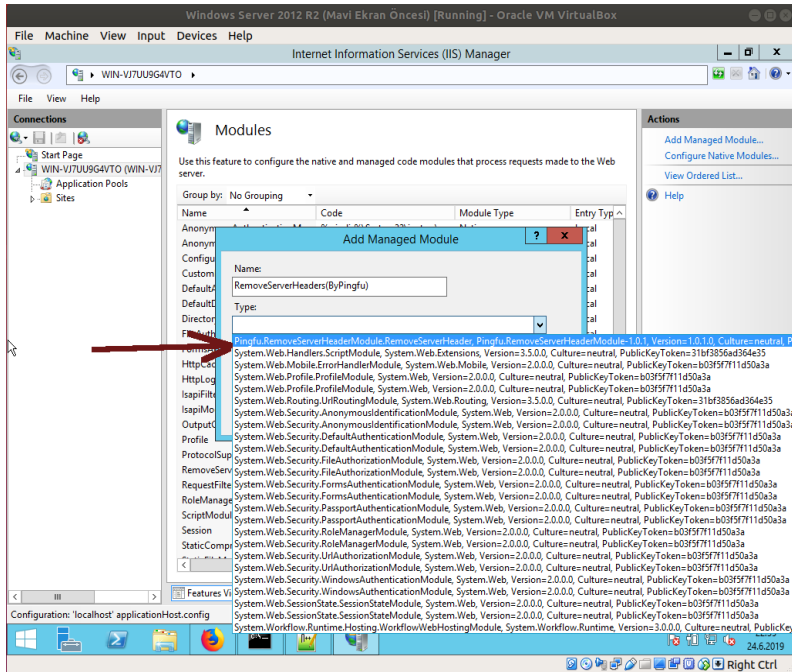
Adım IV: Add Managed Module.. seçeneğine tıklanır.



Adım V: Modül ismi olarak keyfi bir (tanımlayıcı) ifade girilir. Modül türü olarak da Windows Server 2012 R2'ye exe'siyle kurduğumuz modül seçilerek konur.

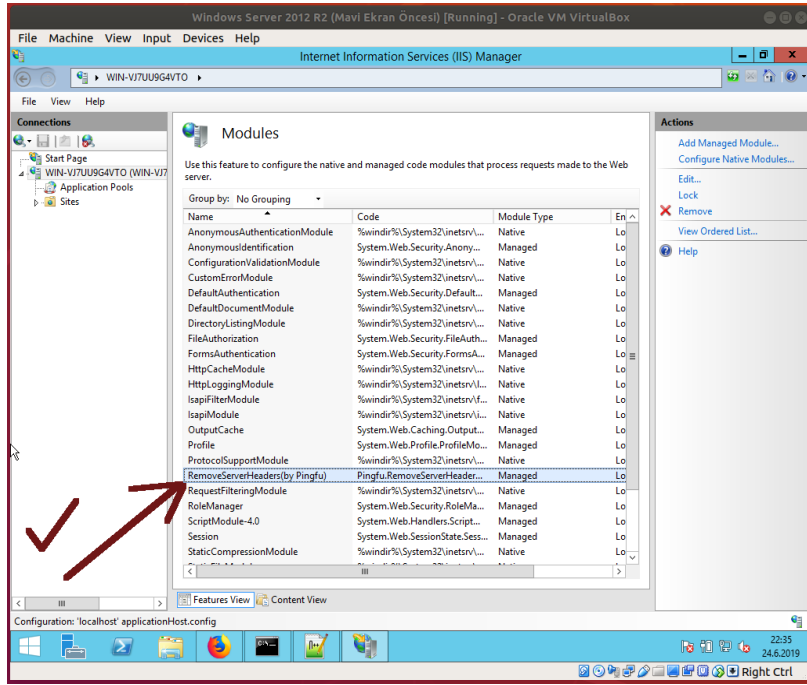


(Keyfi / Tanımlayıcı Modül İsmi Girilir)

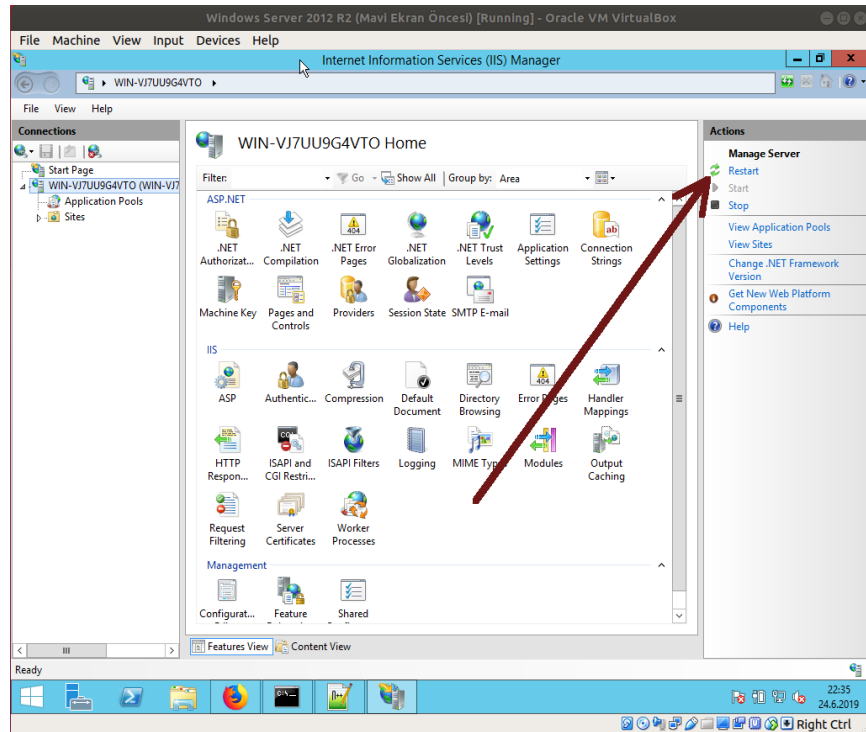


( Windows Server 2012 R2'ye exe'siyle yüklenen modül seçilir )





( Windows Server 2012'e Kurulan Modül IIS Manager'dan IIS'e Eklenir)



( IIS sunucu restart'lanır ve eklenen modül böylece etkin hale gelir )

NOT 1:

Eğer halen X-Powered-By geliyorsa ufak bir elle müdahale yapmak ve web.config içerisinde şunu ilave etmek yeterlidir:

web.config

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <remove name="X-Powered-By" />
      </customHeaders>
    </httpProtocol>
  </system.webServer>
</configuration>
```

Böylece şu başlıkların tamamının dışarıyı çıkışı engellenecektir.

```
Server
X-Powered-By
X-AspNet-Version
X-AspNetMvc-Version
```

NOT 2:

Windows server'dan gönderilen http paketlerinde X-Powered-By header'ı eğer hiç görünmüyorsa (yani IIS Remove Headers modülü yüklü değilken ve başka ekstra konfigürasyon ayarı yapmamışken buna rağmen görünmüyorsa) .NET Framework'ü yüklü değildir demektir. .NET 3.5 ve/veya .NET 4.0 framework feature'ları IIS rolü'ne kurulduğunda X-Powered-By başlığı görünecektir.

Ubuntu 18.04 LTS Terminal (Hedef Sunucuda .NET Framework **Yüklü Değilken**) :

```
> telnet 172.16.3.118 80                ( IP; Windows Server 2012 R2 Makinası )
Trying 172.16.3.118...
Connected to 172.16.3.118.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 701
Content-Type: text/html
Last-Modified: Tue, 13 Feb 2018 08:56:57 GMT
Accept-Ranges: bytes
ETag: "f0a2569aa8a4d31:0"
Server: IIS/8.5                          (*)
Date: Mon, 24 Jun 2019 18:25:23 GMT
Connection: close
```

Connection closed by foreign host.

Ubuntu 18.04 LTS Terminal (Hedef Sunucuda .NET Framework **Yüklemesi Sonrası**) :

```
> telnet 172.16.3.118 80 ( IP; Windows Server 2012 R2 Makinası )
Trying 172.16.3.118...
Connected to 172.16.3.118.
Escape character is '^]'.
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK
Content-Length: 701
Content-Type: text/html
Last-Modified: Tue, 13 Feb 2018 08:56:57 GMT
Accept-Ranges: bytes
ETag: "f0a2569aa8a4d31:0"
Server: IIS/8.5 (*)
X-Powered-By: ASP.NET (*)
Date: Mon, 24 Jun 2019 18:25:23 GMT
Connection: close
```

Connection closed by foreign host.

Dolayısıyla bunun akabinde (yani .NET Framework'ü varken) var olan ve görünen X-Powered-By'ı şimdi durdurmak için yukarıdaki not 1'de yer alan elle müdahalenin yapılması gerekecektir.

Kaynaklar:

<https://gist.github.com/marcbarry/47644b4a43fbfb63ef54>

<https://gist.github.com/marcbarry/56afe3c14318048427aa>

<https://github.com/pingfu/iis-remove-server-headers>

<https://www.devcurry.com/2010/11/using-deployment-retailtrue-attribute.html>

<https://docs.microsoft.com/en-us/iis/configuration/system.webserver/modules/add>

<https://docs.microsoft.com/tr-tr/dotnet/api/system.web.configuration.deploymentsection.retail?view=netframework-4.8>

<https://www.devcurry.com/2010/11/using-deployment-retailtrue-attribute.html>

<https://www.youtube.com/watch?v=yRNZ3zWOyNI>