IIS'de HTTP Güvenlik Başlıklarını Ekleme

(+) Bu belge birebir denenmiştir ve başarıyla uygulanmıştır.

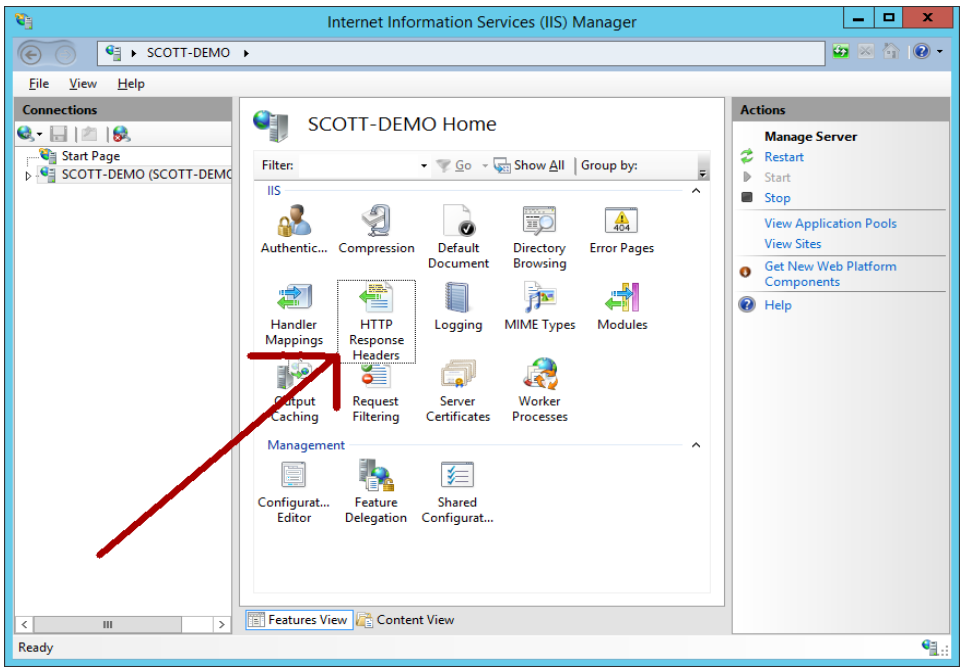
Gereksinimler

Windows Server 2008 R2 Sanal Makinası

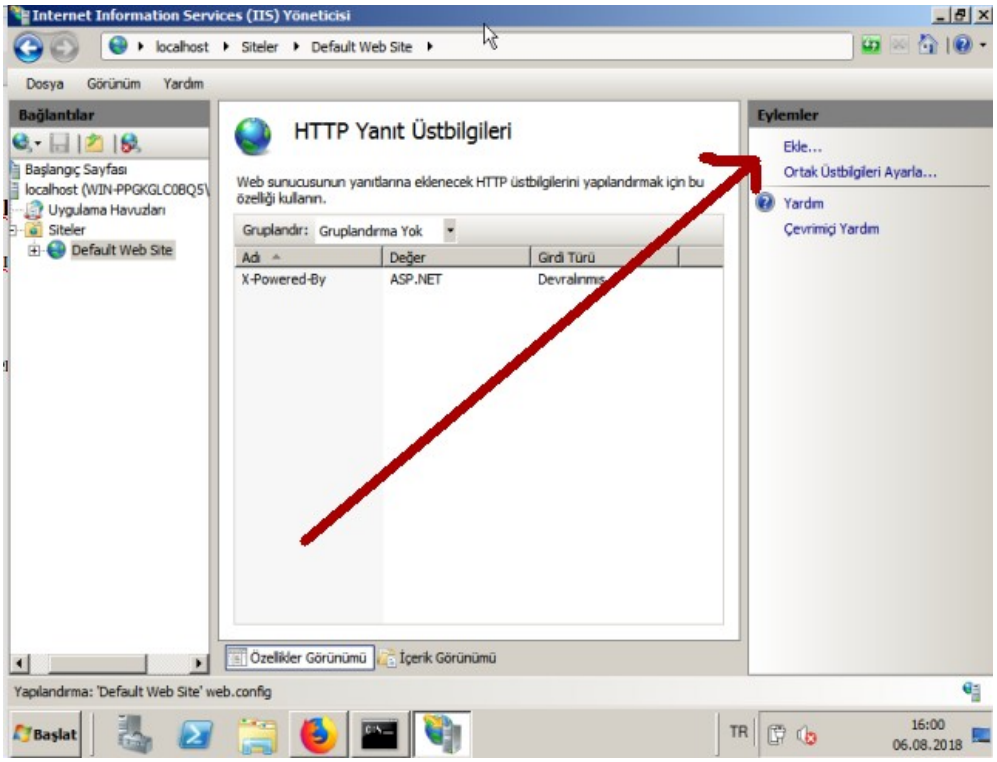
Belli başlı http güvenlik başlıkları vardır. Bunlar arasında

```
Content-Security-Policy          // Yeni tarayıcılar için XSS önleyici header
X-XSS-Protection                 // Eski tarayıcılar için XSS önleyici header
X-Frame-Options                  // Clickjacking önleyici header
X-Content-Type-Options           // Sunucudan gelen dosyayı belirtilen uzantıyla
                                 // çalıştırma kısıtı
Referrer-Policy                  // Referer request header'ını denetim altına
                                 // alarak Open redirect sonucu phising'i önler,
                                 // ayrıca kaynak siteden gelen parametrelerin
                                 // aktarımı sonucu kullanıcının gizliliğini ihlal
                                 // etmeyi engeller.
Set-cookie                       // Ortaya çıkabilecek olası zafiyetlere karşı
                                 // (örn; xss'e karşı) çerez güvenliğini sağlar
                                 // ve çerezin üçüncü parti sunuculara gidişini
                                 // önler.
Strict-Transport-Security        // Hem http hem de https kullanan web uygula-
                                 // maları için sslstrip saldırılarını önler. Erişim
                                 // http ise http, https ise https üzerinden akar.
                                 // Https ken http üzerinden akmaz. Engellenir.
```

gibi header'lar mevcuttur. Bu http güvenlik başlıklarının http response'da yer alabilmesi için IIS panelindeki HTTP Response Headers seçeneğine tıklanır.



Gelen ekrandaki Add (Ekle) linkine tıklanır.

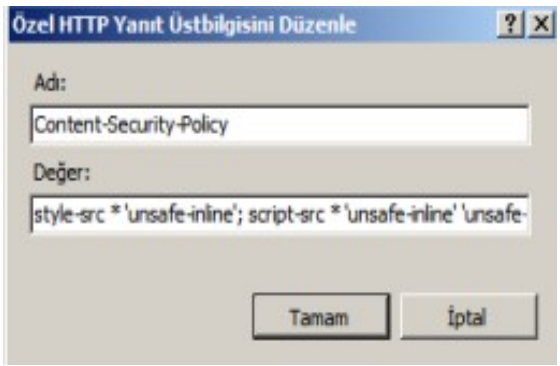


Not: Görüldüğü üzere http response header'ları arasında X-Powered-By header'ı mevcuttur. Bu belgede bu header'ın yanına başka header'lar da ekleyeceğiz.

Ardından http güvenlik başlıkları aşağıdaki gibi eklenir:

a) Content-Security-Policy

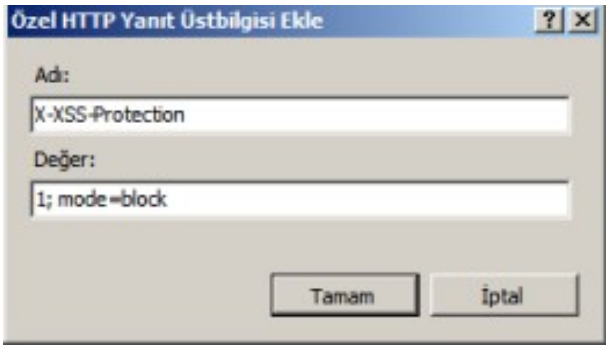
Name: Content-Security-Policy
Value: style-src * 'unsafe-inline'; script-src * 'unsafe-inline' 'unsafe-eval'; img-src *; connect-src: *; frame-src: *; object-src: *



Content-Security-Policy

b) X-XSS-Protection

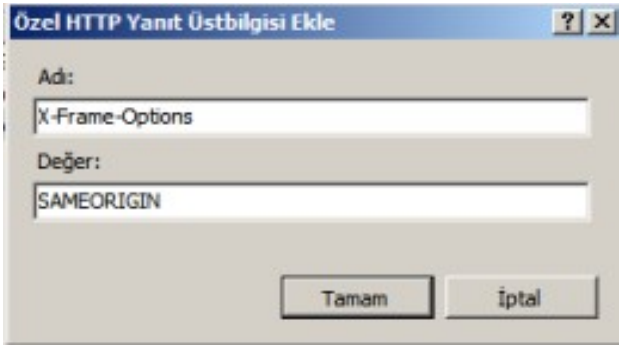
Name: X-XSS-Protection
Value: 1; mode=block



X-XSS-Protection

c) X-Frame-Options

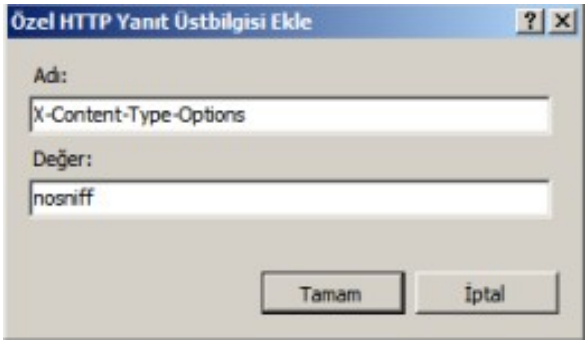
Name: X-Frame-Options
Value: SAMEORIGIN



X-Frame-Options

d) X-Content-Type-Options

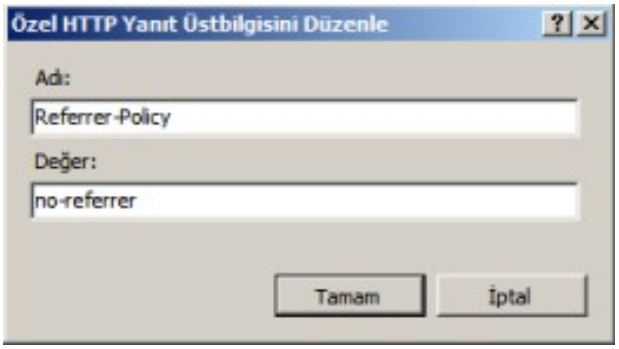
Name: X-Content-Type-Options
Value: nosniff



X-Content-Type-Options

e) Referrer-Policy

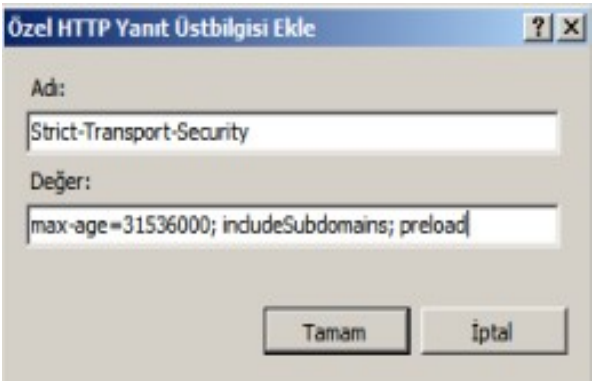
Name: Referrer-Policy
Value: no-referrer



Referrer-Policy

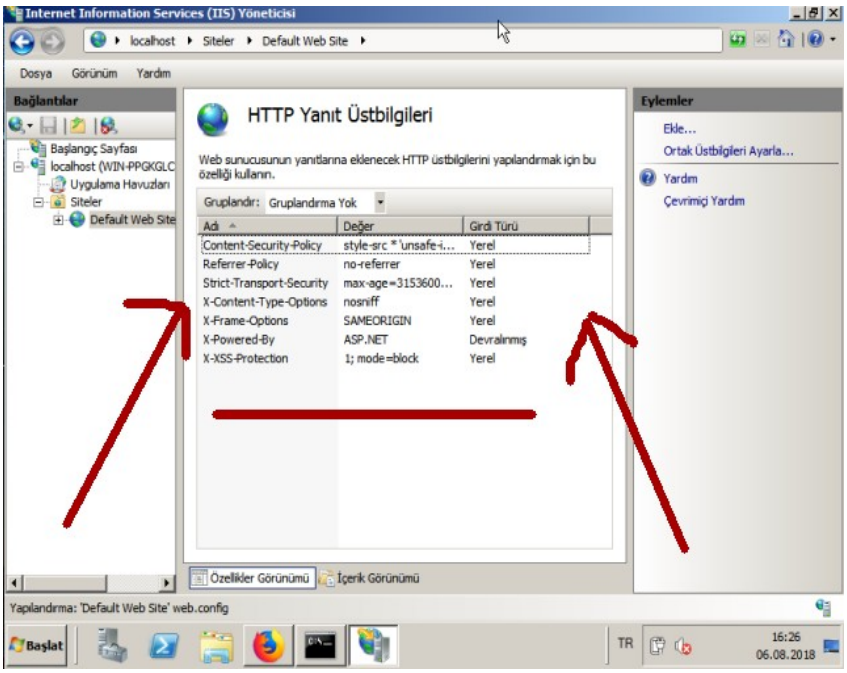
f) Strict-Transport-Security

Name: Strict-Transport-Security
Value: max-age=31536000; includeSubdomains; preload



Strict-Transport-Security

Son durum şu şekilde olur:



Ardından IIS sunucu restart'lanır ve işlem tamamlanır.

IIS sunucunun http yanıtlarında http güvenlik başlıklarını gönderip göndermediğini test edecek olursak;

Ubuntu 14.04 LTS Terminal:

> telnet 172.16.3.107 80 // Windows Server 2008 R2 Sanal Makina IP'si
Trying 172.16.3.107...
Connected to 172.16.3.107.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Fri, 16 Feb 2018 13:23:58 GMT
Accept-Ranges: bytes
ETag: "175fbb6629a7d31:0"
Server: IIS/7.5
X-Powered-By: ASP.NET
Content-Security-Policy: style-src * 'unsafe-inline'; script-src * 'unsafe-inline' 'unsafe-eval'; img-src *; connect-src: *; frame-src: *; object-src: *
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Date: Mon, 06 Aug 2018 13:24:11 GMT
Connection: close

Connection closed by foreign host.

görüldüğü üzere http güvenlik başlıkları sorunsuzca http yanıtıyla beraber gelmiştir.

Kaynak:

https://scotthelme.co.uk/hardening-your-http-response-headers/