بسمه تعالی

پیکربندی امن پروتکل SSL/TLS بر روی وب‌سرور IIS

(جهت رمزنگاری ارتباطات)

شمارهٔ مستند ..... APA-AMIRKABIR- 1395-1-29
تاریخ نگارش ..... ۲۹ فروردین‌ماه ۱۳۹۵
نسخهٔ نگارش ۲,۰

نگارش: مرکز پژوهشی آپا – دانشگاه صنعتی امیرکبیر
http://apa.aut.ac.ir

فهرست مطالب

۱ مقدمه

پروتکل‌های SSL و TLS جهت امن کردن ارتباط میان کاربر و سرور از طریق تصدیق هویت، رمزنگاری و صحت، طراحی و پیاده‌سازی شده است. جهت امن کردن داده‌ها این پروتکل‌ها از cipher suite هایی استفاده می‌شود. هر cipher suite ترکیبی از الگوریتم‌های تصدیق اصالت، رمزنگاری و کد تصدیق هویت پیغام (MAC) است. در زمان پیکربندی TLS/SSL باید تنظیمات به‌درستی انجام شده و cipher suite های امن مورد استفاده قرار گیرد. برخی از مهم‌ترین این تنظیمات شامل غیرفعال کردن SSL 2.0 و SSL 3.0، غیرفعال کردن TLS 1.0 Compression و cipher suite های ناامن و استفاده از آخرین نسخه‌ی نرم‌افزارهاست. پیکربندی ارائه شده بر روی سروری با مشخصات زیر انجام شده است.

نام نرم‌افزار	نسخه‌ی مورد استفاده
سیستم‌عامل	Windows 7 64 bit Ultimate
وب سرور	IIS 7.5

ذکر این نکته لازم است که در ابتدا باید تمامی ماژول‌های وب سرور IIS (در Turn Windows feature On or Off) فعال گردد.

۲ ارزیابی وضعیت فعلی سرویس دهنده

برای ارزیابی وضعیت امنیتی SSL/TLS در سرویس دهنده خود از سرویس زیر استفاده نمایید:

https://sslcheck.certcc.ir/

پس از انجام موارد امنیتی زیر مجدداً با استفاده از آدرس فوق سرویس خود را پویش کنید تا از برطرف شدن مشکلات مطمئن شوید.

۳ موارد پیشنهادی برای ارتقای امنیت

۳-۱ اضافه کردن زوج کلید معتبر به وب سرور

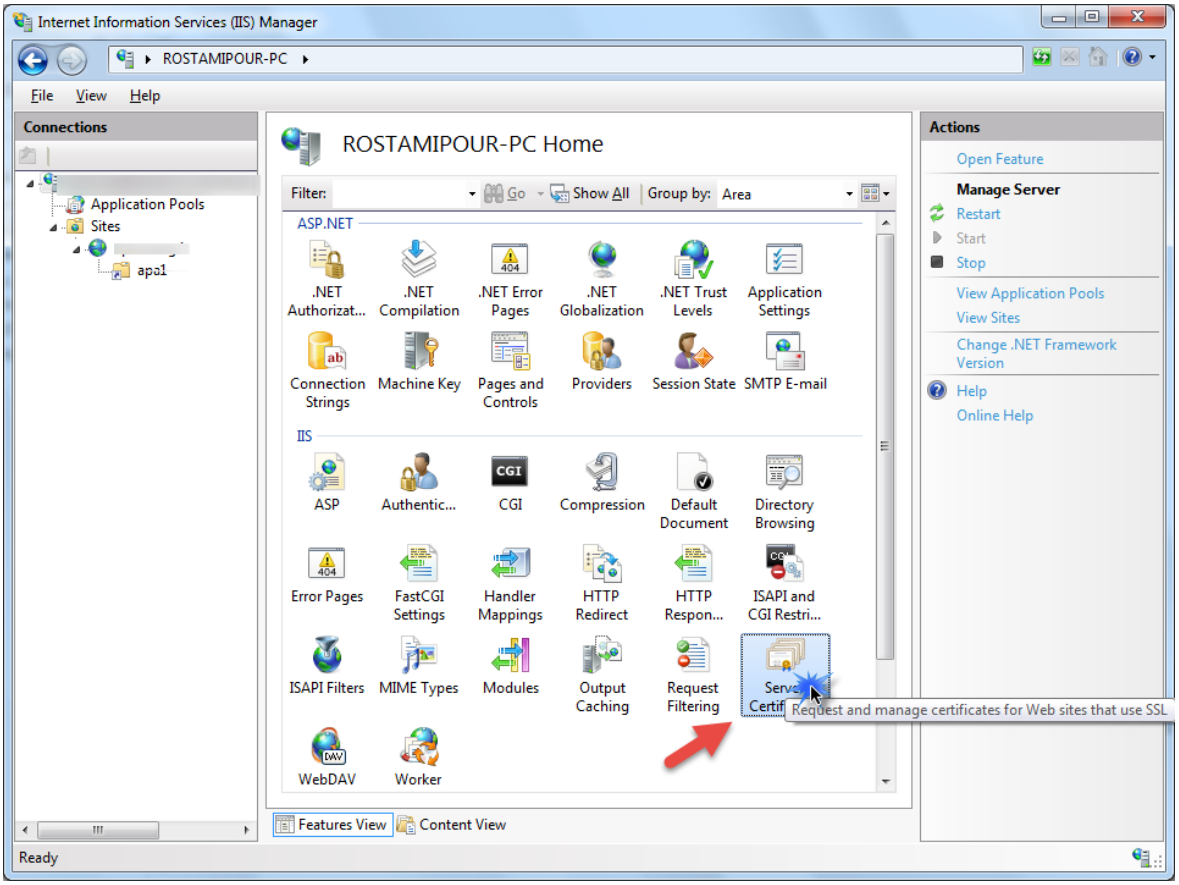
جهت امن‌سازی ارتباط از طریق SSL/TLS یکی از موارد استفاده از زوج کلید خصوصی و عمومی معتبر است. جهت انجام این امر باید روند زیر دنبال گردد.

پس از دریافت زوج کلید از یک CA معتبر به همراه کلید عمومی CA باید با استفاده از دستور openssl زیر هر سه کلید را به یک کلید با فرمت pfx تبدیل کرد. (private.key نام فایل حاوی کلید خصوصی، Certificate.crt نام فایل حاوی کلید عمومی و Intermediate_CA.crt فایل حاوی کلید عمومی CA هستند.)

```
openssl pkcs12 -export -out certificate.pfx -inkey private.key -in Certificate.crt -certfile Intermediate_CA.crt
```

پس از وارد کردن این دستور یک کلمه‌عبور از کاربر دریافت می‌شود. سپس فایل خروجی (certificate.pfx) باید در وب سرور IIS اضافه شود. مراحل زیر باید جهت انجام این امر صورت پذیرد:

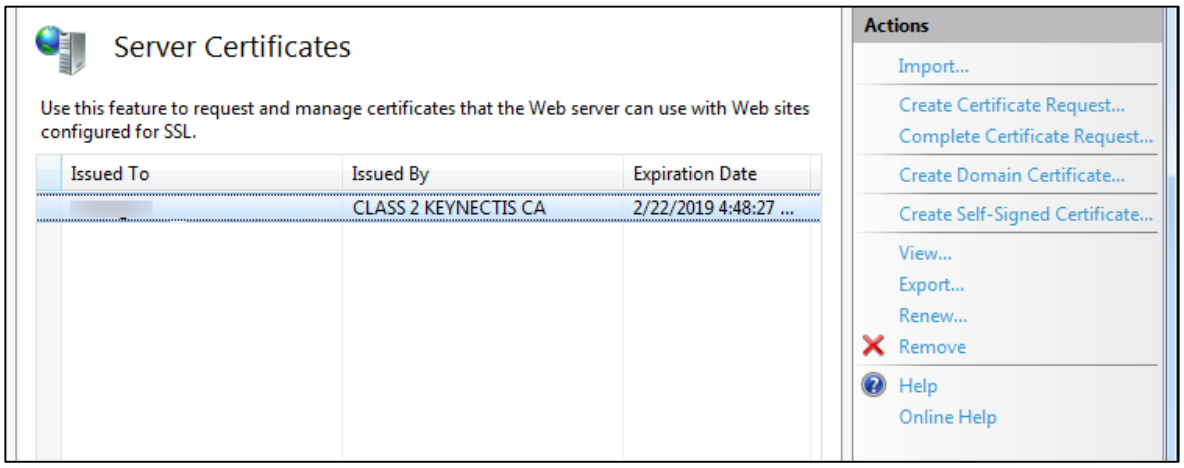
۱. باید پس از بازکردن IIS Manager بر روی Server Certificate از پنجره‌ی Home کلیک کرد.



شکل ۱: نمایی از IIS Manager و انتخاب Server Certificate

۲. سپس از منوی Action باید گزینه import انتخاب شود.

۳. سپس باید مسیر فایل کلید تولید شده در مرحله‌ی قبل را در بخش Certificate file وارد کرده و کلمه‌عبور وارد شده نیز در بخش password وارد شود.

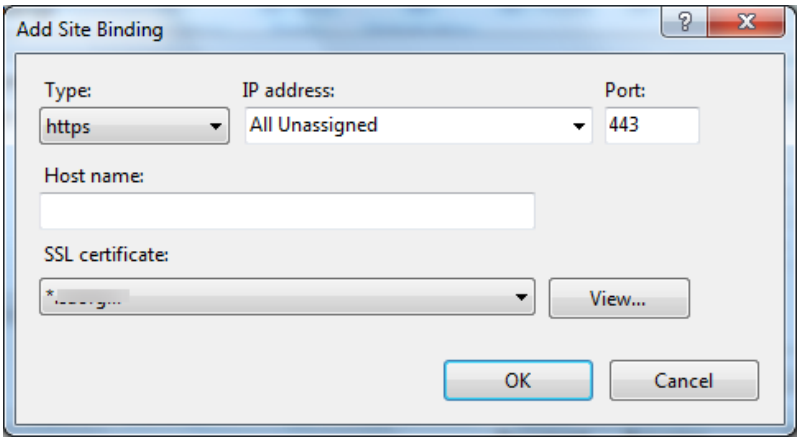


شکل ۲: نمایی از کلید اضافه شده به سرور

٤. در مرحله بعد باید از بخش sites بر روی نام سایت مورد نظر کلیک کرده و سپس گزینه‌ی Binding از منوی Action را انتخاب کرد.

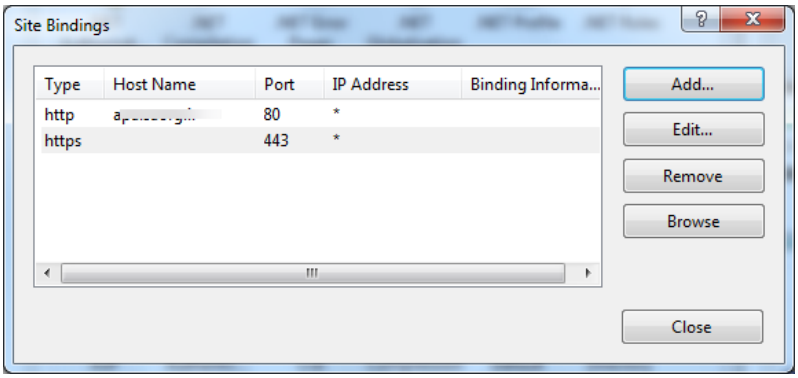
٥. سپس بر روی گزینه‌ی add در پنجره‌ی باز شده کلیک شود.

٦. در پنجره‌ی باز شده باید type به https تغییر یابد. سپس از منوی SSL Certificate نام certificate اضافه شده در مراحل قبل را انتخاب کرد.



شکل ۳: نمایی از اضافه کردن کلید به سرور

۷. در نهایت با کلیک بر روی OK زوج کلیدها بر روی سرور فعال می‌گردند.



شکل ٤: نمایی از نتیجه‌ی نهایی تنظیمات کلید

۳-۲ تنظیم الگوریتم‌های قدرتمند و Forward secrecy

یکی از مهم‌ترین بخش‌های مربوط به پیکربندی SSL/TLS غیرفعال کردن الگوریتم‌های آسیب‌پذیر و CipherSiuteها به نحوی است که ضمن برآورده کردن امنیت، Forward secrecy نیز فعال گردد.

برای غیرفعال کردن تنظیم الگوریتم‌های ضعیف و آسیب پذیر بر روی وب سرور IIS، باید با استفاده از تعریف registryKey جدید در مسیر زیر از RegisteryEditor استفاده کرد:

HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\

به عنوان نمونه برای غیر فعال کردن SSL 2.0 باید در ابتدا یک کلید با نام پروتکل (در اینجا SSL 2.0) در مسیر بالا ایجاد شود. سپس در هر یک از زیر کلیدهای مربوط به سرور یک DWORD جدید با نام ‘Enabled’ و مقدار 0 تعریف شود. جهت حذف پروتکل‌های آسیب‌پذیر باید این فرآیند برای هر یک از موارد زیر انجام شود.

۱. غیرفعال کردن PCT 1.0
۲. غیرفعال کردن SSL 2.0
۳. غیرفعال کردن SSL 3.0

جهت فعال‌سازی پروتکل‌های قدرتمند بر روی سرور باید پروتکل‌های زیر فعال گردند.

۱. فعال کردن TLS 1.0
۲. فعال کردن TLS 1.1
۳. فعال کردن TLS 1.2

برای فعال کردن این پروتکل‌ها باید مشابه قبل بعد از ایجاد کلید و زیر کلید مقدار به ’Enabled‘ جای 0 به 0xffffffff مقداردهی شود. اما باید یک زیر کلید با نام ’DisabledByDefault‘ و مقدار 0 نیز ایجاد گردد. جهت پیکربندی راحت‌تر می‌توان از دستورات powershell زیر استفاده کرد. این دستورات به‌راحتی تمامی این بخش‌ها را انجام خواهند داد.

```
# Copyright 2014, Alexander Hass

# http://www.hass.de/content/setup-your-iis-ssl-perfect-forward-secrecy-and-tls-12

# Version 1.4

# - RC4 has been disabled.

# Version 1.3

# - MD5 has been disabled.

# Version 1.2

# - Re-factored code style and output

# Version 1.1

# - SSLv3 has been disabled. (Poodle attack protection)


Write-Host 'Configuring IIS with SSL/TLS Deployment Best Practices...'

Write-Host '-------------------------------------------------------------------------------'


# Disable Multi-Protocol Unified Hello

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Server' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Server' -name Enabled -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'Multi-Protocol Unified Hello has been disabled.'


# Disable PCT 1.0

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server' -name Enabled -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'PCT 1.0 has been disabled.'


# Disable SSL 2.0 (PCI Compliance)

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server' -name Enabled -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'SSL 2.0 has been disabled.'


# NOTE: If you disable SSL 3.0 the you may lock out some people still using

# Windows XP with IE6/7. Without SSL 3.0 enabled, there is no protocol available

# for these people to fall back. Safer shopping certifications may require that

# you disable SSLv3.
```

```
#

# Disable SSL 3.0 (PCI Compliance) and enable "Poodle" protection

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server' -name Enabled -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'SSL 3.0 has been disabled.'


# Add and Enable TLS 1.0 for client and server SCHANNEL communications

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -name 'Enabled' -value '0xffffffff' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'TLS 1.0 has been enabled.'


# Add and Enable TLS 1.1 for client and server SCHANNEL communications

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -Force | Out-Null

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -name 'Enabled' -value '0xffffffff' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client' -name 'Enabled' -value 1 -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'TLS 1.1 has been enabled.'


# Add and Enable TLS 1.2 for client and server SCHANNEL communications

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Force | Out-Null

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -name 'Enabled' -value '0xffffffff' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -name 'Enabled' -value 1 -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' -name 'DisabledByDefault' -value 0 -PropertyType 'DWord' -Force | Out-Null

Write-Host 'TLS 1.2 has been enabled.'
```

همچنین جهت تنظیم cipher Suite های قدرتمند و Forward secrecy می‌توان از دستورات زیر استفاده کرد.

این دستورات نیز بخش cipher مسیر زیر از RegisteryKey را تغییر می‌دهند.

```
# Re-create the ciphers key.
New-Item 'HKLM:SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers' -Force | Out-Null

# Disable insecure/weak ciphers.
$insecureCiphers = @(
  'DES 56/56',
  'NULL',
  'RC2 128/128',
  'RC2 40/128',
  'RC2 56/128',
  'RC4 40/128',
  'RC4 56/128',
  'RC4 64/128',
  'RC4 128/128'
)
Foreach ($insecureCipher in $insecureCiphers) {
  $key = (Get-Item HKLM:\).OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers',
$true).CreateSubKey($insecureCipher)
  $key.SetValue('Enabled', 0, 'DWord')
  $key.close()
  Write-Host "Weak cipher $insecureCipher has been disabled."
}

# Enable new secure ciphers.
# - RC4: It is recommended to disable RC4, but you may lock out WinXP/IE8 if you enforce this. This is a requirement for FIPS 140-2.
# - 3DES: It is recommended to disable these in near future.
$secureCiphers = @(
  'AES 128/128',
  'AES 256/256',
  'Triple DES 168/168'
)
Foreach ($secureCipher in $secureCiphers) {
  $key = (Get-Item HKLM:\).OpenSubKey('SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers',
$true).CreateSubKey($secureCipher)
  New-ItemProperty -path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\$secureCipher" -
name 'Enabled' -value '0xffffffff' -PropertyType 'DWord' -Force | Out-Null
  $key.close()
  Write-Host "Strong cipher $secureCipher has been enabled."
}

# Set hashes configuration.
New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5' -Force | Out-Null
```

```
New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5' -name Enabled -value 0 -PropertyType 'DWord' -Force | Out-Null


New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA' -name Enabled -value '0xffffffff' -PropertyType 'DWord' -Force | Out-Null


# Set KeyExchangeAlgorithms configuration.

New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman' -name Enabled -value '0xffffffff' -PropertyType 'DWord' -Force | Out-Null


New-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS' -Force | Out-Null

New-ItemProperty -path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS' -name Enabled -value '0xffffffff' -PropertyType 'DWord' -Force | Out-Null


# Set cipher suites order as secure as possible (Enables Perfect Forward Secrecy).

$cipherSuitesOrder = @(

  'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521',

  'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384',

  'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256',

  'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521',

  'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384',

  'TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256',

  'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521',

  'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521',

  'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384',

  'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256',

  'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384',

  'TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256',

  'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521',

  'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384',

  'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521',

  'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384',

  'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256',

  'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521',

  'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384',

  'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521',

  'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384',

  'TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256',

  'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521',
```

```
  'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384',
  'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256',
  'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521',
  'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384',
  'TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256',
  'TLS_DHE_DSS_WITH_AES_256_CBC_SHA256',
  'TLS_DHE_DSS_WITH_AES_256_CBC_SHA',
  'TLS_DHE_DSS_WITH_AES_128_CBC_SHA256',
  'TLS_DHE_DSS_WITH_AES_128_CBC_SHA',
  'TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA',
  'TLS_RSA_WITH_AES_256_CBC_SHA256',
  'TLS_RSA_WITH_AES_256_CBC_SHA',
  'TLS_RSA_WITH_AES_128_CBC_SHA256',
  'TLS_RSA_WITH_AES_128_CBC_SHA'
)
$cipherSuitesAsString = [string]::join(',', $cipherSuitesOrder)
New-ItemProperty -path 'HKLM:\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002' -name 'Functions' -
value $cipherSuitesAsString -PropertyType 'String' -Force | Out-Null


Write-Host '------------------------------------------------------------------------------'
Write-Host 'NOTE: After the system has been rebooted you can verify your server'
Write-Host '      configuration at https://www.ssllabs.com/ssltest/'
Write-Host "------------------------------------------------------------------------------`n"


Write-Host -ForegroundColor Red 'A computer restart is required to apply settings. Restart computer now?'
Restart-Computer -Force -Confirm
```

این دستورات با قرار گرفتن در یک اسکریپت با فرمت ps1 بر روی سیستم‌عامل‌های ویندوز قابل اجرا هستند.

۳-۳ به‌روزرسانی نرم‌افزارها و نسخه‌ها

یکی از توصیه‌های مهم درزمینه‌ی پیکربندی امن SSL/TLS به روزبودن نسخه‌ی وب سرور و نصب آخرین وصله‌های امنیتی بر روی آن است.

۳-٤ فعال کردنOCSP Stapling

روشی برای بالا بردن سرعت در چک کردن لیست ابطال کلید برای گواهی است. با استفاده از OCSP Stapling نیاز نیست که سرویس گیرنده درخواستی را به سرور OCSP بدهد و با استفاده از اطلاعات مهیا شده همراه گواهی، می‌تواند از باطل نبودن گواهی اطمینان حاصل کند.

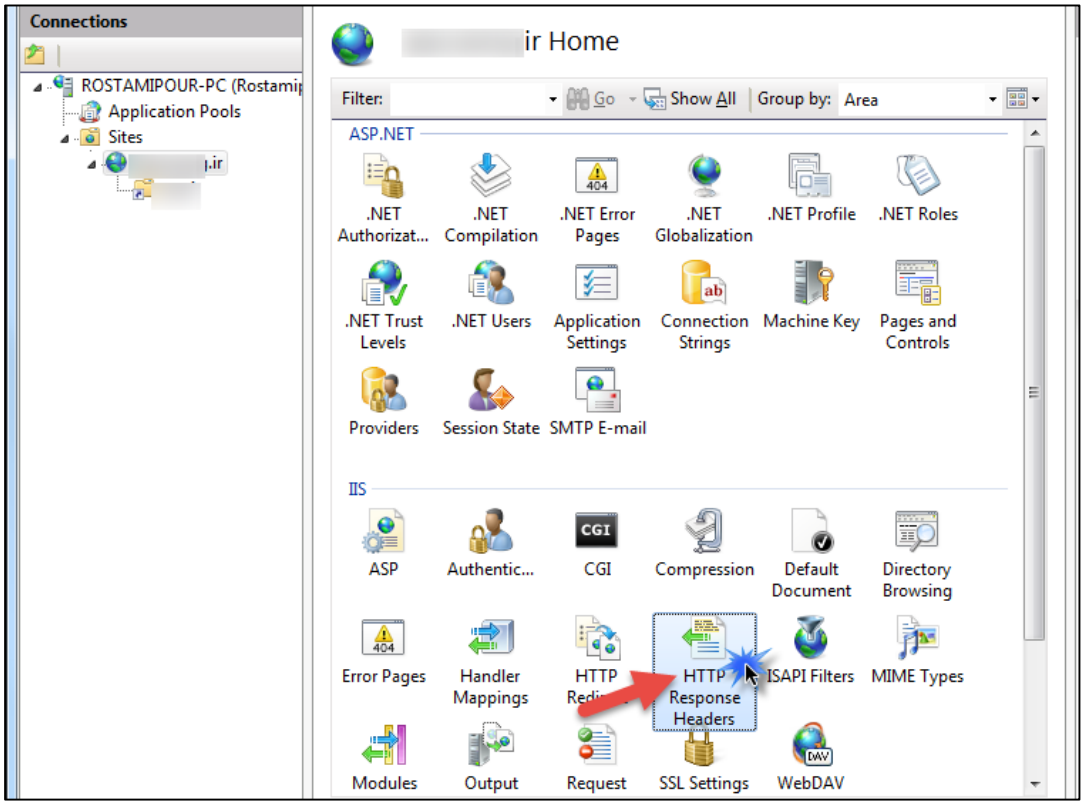
در بسیاری از موارد، با اضافه کردن زوج کلیدهای تولید شده توسط CAها به سرور، این قابلیت به خودی خود فعال می‌گردد. اما برای فعال کردن آن در نسخه‌های بالای وب سرور IIS می‌توان مراحل زیر را انجام داد:

۱. باید پس از بازکردن IIS Manager بر روی نام وب سایتی که نیاز است که OCSP بر روی فعال گردد، کلیک کرد.
۲. سپس از منوی Action باید بر روی گزینه Binding کلیک کرد.
۳. پس از انتخاب ورودی که مربوط https است، باید بر روی گزینه‌ی edit کلیک کرد.
٤. در نهایت باید گزینه‌ی Require Server Name Indication غیر فعال گردد.

۳-٥ فعال کردن HSTS

HTTP Strict Transport Security یک بهبود امنیتی برای برنامه‌های تحت وبی است که از پروتکل HTTPS استفاده می‌کنند. وجود این مکانیسم باعث جلوگیری از Downgrade Attack و Cookie Hijacking می‌شود. این قابلیت همچنین مرورگر را ملزم می‌کند که حتماً از پروتکل HTTPS برای ارتباط با سرور استفاده کند. برای فعال‌سازی این قابلیت می‌توان به‌صورت زیر عمل کرد.

۱. باید در ابتدا بر روی ماژول HTTP Response Headers کلیک کرد.



شکل ۵: انتخاب گزینه‌ی HTTP Response Headers

۲. سپس در منوی Action از منوی سمت راست پنجره‌ی باز شده باید گزینه Add را انتخاب کرد.

۳. سپس در بخش نام Strict-Transport-Security و در بخش value باید max-age=31536000; includeSubDomains قرار داده شود.

علاوه بر آن باید اجبار الزام کاربر به استفاده از HTTPS نیز انجام شود. جهت انجام این امر می‌تواند خطوط زیر را در فایل web.config سایت مورد نظر قرار داد.

در ابتدا باید با استفاده از دستور زیر ماژول headers را فعال کرد:

```
<httpErrors lockAttributes="allowAbsolutePathsWhenDelegated,defaultPath" errorMode="Custom">
        <error statusCode="403" subStatusCode="4" path="https://XXX" responseMode="Redirect" />
</httpErrors>
```

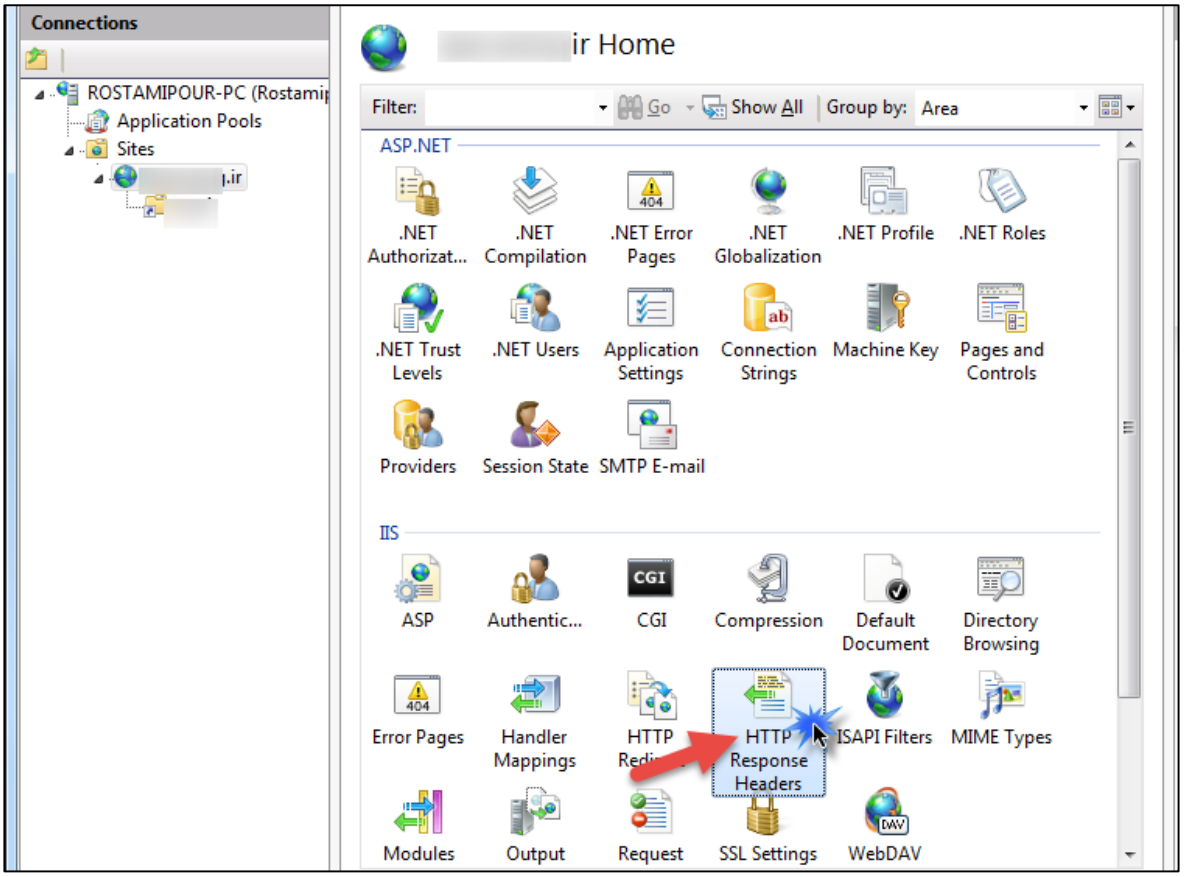
یکی دیگر از راه‌های ممکن برای انجام این امر استفاده از UrlRewrite است که به صورت کامل در لینک زیر روش انجام آن، شرح داده شده است.

https://www.namecheap.com/support/knowledgebase/article.aspx/9595/0/http-to-https

۳-۶ فعال کردن HPKP

HTTP Public Key Pinning یک قابلیت است که به وب‌سایت‌هایی که از HTTPS استفاده می‌کنند اجازه می‌دهد تا نسبت به جعل هویت حمله‌کننده مقاوم باشند. بدین معنی که تنها CAهای معتبر، مجاز به امضای گواهی وب‌سایت می‌باشند. در غیر این صورت هر CA قرار گرفته در لیست مرورگر قادر به امضای گواهی خواهد بود. بنابراین امکان جعل هویت را از حمله‌کننده می‌گیرد. برای فعال‌سازی این قابلیت می‌توان به‌صورت زیر عمل کرد.

۱. باید در ابتدا بر روی ماژول HTTP Response Headers کلیک کرد.



شکل ۶: انتخاب گزینه‌ی HTTP Response Headers

۲. سپس در منوی Action از منوی سمت راست پنجره‌ی باز شده باید گزینه Add را انتخاب کرد.

۳. سپس در بخش نام Public-Key-Pins و در بخش value باید مقدار زیر قرار داده شود.

```
pin-sha256=”SPKI_digest#1"; pin-sha256="SPKI_digest#2"; max-age=31536000
```

هر کدام از SPKI digestهای مربوط به یک CA را می‌توان از طریق کپی کردن محتوای کلید عمومی با فرمت PEM در فیلد قرار داده شده در سایت زیر، محاسبه کرد.

https://projects.dm.id.lv/s/pkp-online/calculator.html

٤ مراجع

[1]. https://www.hass.de/content/setup-your-iis-ssl-perfect-forward-secrecy-and-tls-12

[2]. https://www.namecheap.com/support/knowledgebase/article.aspx/9597/0/hpkp

[3]. https://www.namecheap.com/support/knowledgebase/article.aspx/9595/0/http-to-https

[4]. https://www.namecheap.com/support/knowledgebase/article.aspx/9596/0/hsts

[5]. https://www.namecheap.com/support/knowledgebase/article.aspx/9602/0/ocsp

[6].http://serverfault.com/questions/114795/iis7-how-to-import-public-key-and-private-key-as-two-seperate-files

[7]. https://www.digicert.com/ssl-support/pfx-import-export-iis-7.htm