پیکربندی امن

Microsoft IIS 8.0

مرکز مدیریت راهبردی افتا

SCWS-MS-IIS-8.0-0.0

اسفند ۹۵

فهرست

پیش‌گفتار

مرکز مدیریت راهبردی افتا[1] به منظور ساماندهی امنیت تجهیزات در حوزه فاوا[2]، پروژه «پیکربندی امن محصولات IT در کشور» را آغاز نموده است. یکی از گام‌های اساسی در این پروژه ارائه چک‌لیست و راهنمای پیکربندی امن برای محصولات IT می‌باشد. ارائه چک‌لیست برای محصولات داخلی بر عهده تولیدکننده محصول می‌باشد. تولید کننده ملزم است، چک‌لیست خود را در غالب ارائه شده از سمت مرکز افتا ارائه دهد. چک‌لیست‌های ارائه شده، توسط مرکز افتا مورد ارزیابی قرار گرفته و منتشر می‌گردد. سازمان‌های دولتی ملزم به استفاده از چک لیست‌های مذکور برای محصولات در حال استفاده خود هستند. همچنین سازمان‌های دولتی موظفند قبل از استفاده از محصولات IT، آن‌را مطابق چک‌لیست امنیتی مورد تایید مرکز افتا پیکربندی نمایند.

توجه به این نکته حائز اهمیت می‌باشد که چک‌لیست‌های ارائه شده، یک امنیت سطح پایه برای محصول ایجاد می‌نماید و سازمان‌ها ملزم هستند که برای رسیدن به سطح امنیت مورد نیاز خود، پس از اجرای مدیریت ریسک[3]، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

[1] امنیت فضای تولید و تبادل اطلاعات
[2] فناوری اطلاعات و ارتباطات
[3] Risk management

مقدمه

این سند، راهنمایی برای پیکربندی امن Microsoft IIS 8 است. در این سند مقادیر و تنظیمات مناسب برای امن سازی سیاست‌ها و پیکربندهای محصول یاد شده ارائه شده است. مدیر سامانه با استفاده از این سند می‌تواند تنظیمات ارائه شده را پیاده سازی نماید.

مرکز مدیریت راهبردی افتا ضمن استقبال از نظرات کارشناسان و متخصصان این حوزه برای غنای بیشتر این سند و دیگر اسناد مقاوم سازی، آمادگی دریافت پیشنهادات سازنده از طریق آدرس پست الکترونیکی Hardening@aftasec.ir را اعلام می‌دارد.

در ادامه، تنظیمات مورد نیاز برای پیکربندی امن Microsoft IIS 8 آمده است. در این سند هر تنظیم با یک نام لاتین و شماره مختص آن آورده شده است. برای هر الزام دو بخش شرح اجمالی و نحوه پیاده‌سازی ارائه شده است. در بخش شرح اجمالی، توضیحی مختصر از ماهیت الزام بیان گردیده و در بخش نحوه پیاده‌سازی نیز، راهنمایی برای پیاده‌سازی الزام توسط مدیر سامانه ارائه شده است.

جدول ۱: گروه‌بندی و اختصارسازی نام برای محصولات IT

محصولات IT	
نام گروه	شماره گروه
نرم افزار آنتی ویروس	AV
سرویس‌دهنده نرم‌افزارهای کاربردی[۴]	AS
احراز اصالت[۵]	AU
اتوماسیون	AT
نرم‌افزار مدیریت پیکربندی[۶]	CM
سیستم مدیریت پایگاه داده	DB
نرم‌افزار کاربردی رومیزی[۷]	DA
سرویس گیرنده رومیزی[۸]	DC
سرویس دایرکتوری[۹]	DS
DNS سرور	DN
ایمیل سرور	ES
نرم‌افزار کاربردی سازمانی[۱۰]	EA
دیوار آتش[۱۱]	FI
تجهیزات قابل حمل[۱۲]	HD
مدیریت هویت[۱۳]	IM
سیستم تشخیص نفوذ[۱۴]	ID

[۴] Application Server
[۵] Authentication
[۶] Configuration Management System
[۷] Desktop Application
[۸] Desktop Client
[۹] Directory Service
[۱۰] Enterprise Application
[۱۱] Firewall
[۱۲] Handheld Device
[۱۳] Identity Management
[۱۴] Intrusion Detection System

محصولات IT	
نام گروه	شماره گروه
سرویس‌دهنده ایمیل[۱۵]	MS
راهکارهای موبایلی[۱۶]	MO
مسیریاب شبکه[۱۷]	RO
سوئیچ شبکه	SW
سیستم عامل	OS
تجهیزات جانبی[۱۸]	PD
سرویس دهنده[۱۹]	SR
نرم‌افزار مجازی‌سازی[۲۰]	VI
مرورگر وب	WB
سرویس‌دهنده وب	WS

[۱۵] Mail Server
[۱۶] Mobile Solution
[۱۷] Network Router
[۱۸] Peripheral Device
[۱۹] Server
[۲۰] Virtualization Software

تنظیمات

SCWS-1: پیکربندی اولیه

SCWS-1-1: اطمینان یافتن از اینکه محتویات وب بر روی پارتیشن غیر سیستمی باشد

شرح اجمالی:

نحوه پیاده‌سازی:

دستور زیر برای اطمینان یافتن از اینکه دایرکتوری مجازی بر روی درایو سیستمی نگاشت نشده باشد، اجرا گردد:

```
%systemroot%\system32\inetsrv\appcmd  list  vdir
```

محتوی وب را از مسیر C:\inetpub\wwwroot\ باز کنید.

محتوی را به یک پوشه محدود و اختصاصی وب بر روی درایو غیر سیستمی مانند D:\webroot کپی یا انتقال دهید.

نگاشت مسیرها در هر برنامه یا دایرکتوری مجازی با مسیر جدید تغییر دهید.

اصلاحیه:

برای تغییر نگاشت در برنامه‌ای به نام app1 که در Default Web Site قرار دارد، IIS Manager باز شود.

۱. Server node باز شود.
۲. Sites باز شود.
۳. Default Web Site باز گردد.
۴. بر روی برنامه app1 کلیک گردد.
۵. در Actions pane، گزینه Basic Settings انتخاب گردد.
۶. در جعبه متن مسیر فیزیکی، مسیر جدید برنامه، به عنوان مثال به صورت زیر D:\wwwroot\app1 تایپ گردد.

SCWS-1-2: اطمینان یافتن از 'host headers' برروی تمامی سایت‌ها قرار دارد

شرح اجمالی:

نحوه پیاده‌سازی:

دستور زیر باید برای تشخیص سایت‌هایی که هدر میزبان مورد نیاز در آنها پیکربندی نشده است، اجرا گردد:

```
%systemroot%\system32\inetsrv\appcmd  list sites
```

تمامی سایت‌ها باید مانند زیر لیست شوند:

SITE "Default Web Site" (id:1,bindings:http/*:80:test.com,state:Started)

SITE "badsite" (id:3,bindings:http/*:80:,state:Started)

برای تمامی سایت‌های غیرSSL، اطمینان حاصل شود که IP:port:host به سه تائی که دارای یک نام میزبان می‌باشد، انقیاد شود. برای مثال، اولین سایت Default Web Site با توجه به توصیه‌های داده شده پیکربندی شده است test.com. هدر میزبان دارد ولی در badsite هدر میزبان پیکربندی نشده است. همانگونه که دیده می‌شود 80: * را نشان می‌دهد بدین معنی که همه IPها قبل پورت ۸۰، هدر میزبان ندارند.

لیستی از تمامی سایت‌ها با استفاده از دستور appcmd.exe بدست آورید.

```
%systemroot%\system32\inetsrv\appcmd list sites
```

اصلاحیه:

IIS Manager را به منظور پیکربندی هدر میزبان برای سایت Default Web Site به صورت زیر اجرا نمائید.

۱. IIS Manager باز شود.
۲. در Connections pane expand گزینه Sites node و Default Web Site انتخاب گردد.
۳. در Actions pane گزینه Bindings کلیک شود.
۴. در جعبه متن Site Bindings، هدرهای میزبان مورد دلخواه که باید پیکربندی شوند انتخاب شود، به عنوان مثال در اینجا پورت ۸۰ می باشد.
۵. گزینه Edit کلیک گردد.
۶. در زیر نام میزبان، sites FQDN ، از قبیل <www.examplesite.com> وارد شود.
۷. سپس گزینه OK و بعد Close کلیک گردد.

SCWS-1-3: اطمینان یافتن از غیرفعال بودن 'directory browsing'

شرح اجمالی:

این ویژگی مشخص می‌کند که امکان مرور دایرکتوری ها وجود دارد یا خیر. اگر این گزینه فعال باشد فهرست تمام فایل‌ها و زیرپوشه ها توسط مرورگر قابل مشاهده خواهد بود.

نحوه پیاده‌سازی:

با دستور زیر می‌توان از غیرفعال بودن Directory Browsing بر روی سطح سرور اطمینان حاصل کرد:

```
%systemroot%\system32\inetsrv\appcmd list config /section:directoryBrowse
```

در صورتی‌که سرور مطابق توصیه‌ها پیکربندی شده باشد، پاسخ زیر نمایش داده خواهد شد:

```
<system.webServer>
<directoryBrowse enabled="false" />
<system.webServer>
```

اصلاحیه:

Directory Browsing را می‌توان با استفاده از UI با اجرای appcmd.exe و ویرایش فایل‌های پیکربندی به‌طور مستقیم، یا از طریق اسکریپت‌های WMI تنظیم نمود. برای غیرفعال ساختن Directory Browsing با استفاده از دستور appcmd.exe می‌توان گام‌های زیر را انجام داد:

```
%systemroot%\system32\inetsrv\appcmd set config /section:directoryBrowse /enabled:false
```

SCWS-1-4: اطمینان یافتن از پیکربندی 'application pool identity' برای تمامی application poolها

شرح اجمالی:

نحوه پیاده‌سازی:

برای بررسی پیکربندی صحیح application pools باید با استفاده از IIS Manager، ApplicationPoolIdentity را اجرا کرد:

۱. IIS Manager باز شود.
۲. گزینه Application Pools زیر بخش machine node باز گردد و Application Pool بررسی شود.
۳. بر روی گزینه Application Pool راست کلیک کرده و Advanced Settings انتخاب گردد.

۴. زیر بخش Process Model، گزینه Identity option قرار دارد و اطمینان حاصل شود که ApplicationPoolIdentity تنظیم شده باشد.

این پیکربندی در همان فایل applicationHost.config برای سایت‌های وبی و دایرکتوری‌های مجازی/ برنامه در بخش آخر فایل با تگ < location path="path/to/resource " > ذخیره می‌شود.

برای بررسی هر Application Pool جدید، از ApplicationPoolIdentity استفاده می‌گردد، با اجرای دستور زیر می‌توان اطمینان حاصل کرد که پیش فرض Application Pool به ApplicationPoolIdentity تغییر یافته باشد.

```
%systemroot%\system32\inetsrv\appcmd list config /section:applicationPools
```

اصلاحیه:

برای تغییر دادن پیش فرض به ApplicationPoolIdentity در واسط گرافیکی IIS Manager به صورت زیر باید عمل کرد:

۱. واسط گرافیکی کاربر IIS Manager باز شود.
۲. در پنل connections، server node را باز کرده و Application Pools را کلیک کنید.
۳. در صفحه Application Pools، گزینه DefaultAppPool را انتخاب و سپس Advanced Settings را از پنل Actions کلیک کنید.
۴. برای انتخاب Identity property بر روی دکمه '...' کلیک کرده تا کادر تبادلی Application Pool Identity باز گردد
۵. گزینه از لیست انتخاب نموده یا یک کاربر برنامه ایجاد شده برای این منظور وارد کنید.
۶. در نهایت IIS را دوباره راه‌اندازی نمائید.

برای تغییر ApplicationPool به ApplicationPoolIdentity با استفاده از appcmd.exe، دستور زیر را اجرا کنید:

```
%systemroot%\system32\inetsrv\appcmd set config /section:applicationPools  /[name='<your apppool>'].processModel.identityType:ApplicationPoolIdentity
```

SCWS-1-5: اطمینان یافتن از تنظیم 'unique application pools' برای سایت‌ها

شرح اجمالی:

نحوه پیاده‌سازی:

با استفاده از دستور زیر می‌توان لیستی از برنامه‌های پیکربندی شده که دارای سایت هستند را مشاهده نمود که تحت application pool اجرا می‌شوند:

```
%systemroot%\system32\inetsrv\appcmd list app
```

خروجی این فایل مشابه زیر است:

```
APP "Default Web Site/" (applicationPool:DefaultAppPool)
```

دستور بالا را به منظور اطمینان از اینکه application pool منحصربفرد برای هر سایت لیست شده تخصیص یافته باید اجرا کرد.

اصلاحیه:

۱. IIS Manager باز شود.
۲. Sites node زیر بخش machine node باز گردد.
۳. Site مورد نظری که باید تغییر کند.
۴. در پنل Actions pane، گزینه Basic Settings انتخاب شود.
۵. جعبه کنار Application Pool انتخاب شود.
۶. Application Pool دلخواه انتخاب
۷. دکمه OK کلیک کردد.

SCWS-1-6: اطمینان یافتن از پیکربندی برای تشخیص کاربرگمنام

شرح اجمالی:

نحوه پیاده‌سازی:

فایل applicationHost.config را پیدا و باز کنید و بررسی شود که مشخصات username در تگ anonymousAuthentication به رشته خالی تنظیم شده باشد.

```
<system.webServer>
<security>
<authentication>
<anonymousAuthentication userName="" />
</authentication>
</security>
</system.webServer>
```

این پیکربندی در فایل applicationHost.config برای وب‌سایت‌ها و دایرکتوری‌های مجازی/ برنامه ذخیره می‌شود که این پیکربندی در تگ‌های <location path="path/to/resource”> آخر فایل قرار دارد.

اصلاحیه:

برای تشخیص کاربر گمنام باید Application Pool Identity توسط واسط کاربر گرافیکی IIS Manager و با استفاده از دستورات AppCmd.exe تنظیم شود.

بنابراین مراحل زیر برای انجام کار انجام گردد.

۱. IIS Manager GUI را باز نموده و سرور ، سایت یا برنامه دلخواه انتخاب
۲. در Features View بر روی آیکون Authentication دابل کلیک کرده
۳. گزینه Anonymous Authentication و در پنل Actions، Edit انتخاب شود.
۴. در پنجره مدل Application pool identity انتخاب و سپس OK کلیک کردد.

با استفاده از AppCmd.exe برای پیکربندی anonymousAuthentication بر روی سطح سرور دستوری مانند زیر اجرا گردد:

```
%systemroot%\system32\inetsrv\appcmd set config -section:anonymousAuthentication
/username:"" –password
```

SCWS-2: پیکربندی Authentication و Authorization

SCWS-2-1: اطمینان یافتن از تنظیم دسترسی محدود به 'global authorization rule'

شرح اجمالی:

نحوه پیاده‌سازی:

۱. قانون تفحیض اختیار در سطح وب سایت یا برنامه کاربردی به صورت زیر پیکربندی می‌شود:
۲. ابتدا به IIS Manager باید متصل شد.
۳. سایت یا برنامه کاربردی جایی که تفحیض اختیار باید پیکربندی شود را انتخاب کنید.
۴. Authorization Rules را انتخاب و قوانین پیکربندی اضافه شده را بررسی کنید.

برای بررسی قانون تفحیض اختیار که دسترسی برای هیچ کاربر به استثناء گروه Administrators را نمی‌دهد، فایل web.config را باز کرده که باید برای سایت/ برنامه کاربردی پیکربندی شده به صورت زیر باشد:

```
<configuration>
<system.webServer>
<security>
<authorization>
<remove users="*" roles="" verbs="" />
<add accessType="Allow" roles="administrators" />
</authorization>
</security>
</system.webServer>
</configuration>
```

اصلاحیه:

برای پیکربندی URL Authorization در سطح سرور با استفاده از IIS Manager مراحل زیر را باید انجام داد:

۱. در ابتدا باید به IIS Manager متصل گردید.
۲. سرور را انتخاب نمود.
۳. Authorization Rules را انتخاب کنید.
۴. قانون"Allow All Users" را باید حذف کرد.
۵. بر روی Add Allow Rule کلیک کرده
۶. دسترسی به گروه کاربر یا نقش‌هایی که دارای اختیاراتی بر روی وب‌سایت‌ها و برنامه‌های کاربردی (مانند گروه Administrators) دارند را باید اجازه داد.

SCWS-2-2: اطمینان یافتن از دسترسی محدود به ویژگی‌های حساس سایت تنها برای کارهای اساسی احرازهویت شده

شرح اجمالی:

نحوه پیاده‌سازی:

برای بررسی اینکه ماژول تفحیض اختیار برای سایت دلخواه فعال شده است باید فایل web.config را باز کرده و بخش تگ‌های <authentication> را بررسی کرده که دارای یک مد تعریف شده باشد. برای نمونه، در مثال زیر Forms Authentication پیکربندی شده، کوکی‌ها مورد استفاده قرار می‌گیرند و SSL مورد نیاز است.

```
<system.web>
<authentication>
<forms cookieless="UseCookies" requireSSL="true" />
</authentication>
</system.web>
```

اصلاحیه:

برای پیکربندی ماژول احرازهویت برای بار اول، هر سازوکاری باید به طور کامل قبل از استفاده پیکربندی شوند.

فعال سازی احرازهویت می‌تواند با استفاده از واسط کاربری اجرا شود. برای بررسی سازوکار احرازهویت برای محتوی حساس با استفاده از واسط گرافیکی IIS Manager به صورت زیر باید عمل کرد:

۱. IIS Manager را باز کرده و سطح محتوی حساس را بیاورید.
۲. در Features View بر روی Authentication دابل کلیک کنید.
۳. بر روی صفحه Authentication اطمینان حاصل شود که ماژول احرازهویت فعال است، درحالیکه احرازهویت گمنام فعال می‌باشد.
۴. در صورت نیاز، ماژول احرازهویت دلخواه را انتخاب، سپس در پنل Actions، گزینه Enable فعال شود.

SCWS-2-3: اطمینان یافتن از استفاده از SSL در 'forms authentication'

شرح اجمالی:

نحوه پیاده‌سازی:

برای بررسی این‌که سایت، برنامه کاربردی یا محتوی مورد نظر در احرازهویت به SSL نیاز دارد باید، فایل web.config را باز کرد و باید تگ < forms requireSSL="true" /> فعال باشد.

```
<system.web>
<authentication>
<forms requireSSL="true" />
</authentication>
</system.web>
```

اصلاحیه:

۱. IIS Manager را باز کنید.
۲. در Features View، بر روی Authentication دابل کلیک کنید.
۳. در صفحه Authentication، Forms Authentication را انتخاب کنید.

۴. در پنل Actions، گزینه Edit کلیک کنید.
۵. کادر Requires SSL را در تنظیمات کوکی را بررسی و OK را کلیک کنید.

SCWS-2-4: اطمینان یافتن از استفاده از کوکی در 'forms authentication'

شرح اجمالی:

نحوه پیاده‌سازی:

فایل web.config را باز کرده و از وجود تگ <forms cookieless="UseCookies" /> اطمینان حاصل کنید.

```
<system.web>
<authentication>
<forms cookieles
s="UseCookies" requireSSL="true" timeout="30" />
</authentication>
</system.web>
```

اصلاحیه:

۱. IIS Manager را باز کنید.
۲. در Features View، بر روی Authentication دابل کلیک کنید.
۳. در صفحه Authentication، Forms Authentication را انتخاب کنید.
۴. در پنل Actions، گزینه Edit را کلیک کنید.
۵. در قسمت Cookie settings، آیتم Use cookies from the Mode dropdown را انتخاب کنید.

SCWS-2-5: اطمینان یافتن از پیکربندی 'cookie protection mode' برای 'forms authentication'

شرح اجمالی:

نحوه پیاده‌سازی:

فایل web.config را باز کرده و از وجود تگ </ protection="All" /> < اطمینان حاصل کنید.

```
<system.web>
<authentication>
<forms cookieless="UseCookies" protection="All" />
</authentication>
</system.web>
```

ویژگی protection="All" در فایل مذکور تنها در صورتی که مد حفاظتی کوکی به مقداری متفاوت تنظیم شده باشد نشان داده خواهد شد که باید به مقدار Encryption and validation تغییر یابد. برعکس، خط protection="All" می‌تواند در فایل web.config به طور دستی اضافه گردد.

اصلاحیه:

۱. IIS Manager را باز کنید.
۲. در Features View، بر روی Authentication دابل کلیک کنید.
۳. در صفحه Authentication، Forms Authentication را انتخاب کنید.
۴. در پنل Actions، گزینه Edit کلیک کنید.
۵. در قسمت Cookie settings، بررسی گردد که مد حفاظتی به Encryption and validation تنظیم شده باشد.

SCWS-2-6: اطمینان یافتن از پیکربندی لایه انتقال امنیتی برای 'basic authentication'

شرح اجمالی:

نحوه پیاده‌سازی:

هنگامی‌که لایه انتقال امنیتی پیکربندی می‌شود، دسترسی به سایت‌ها یا برنامه‌کاربردی تنها از طریق آدرس https:// میسر خواهد بود. تلاش برای بارگذاری سایت یا برنامه از طریق http:// باید درخواست با شکست مواجه شده و IIS دستور خطای ۴۰۳,۴ – Forbidden را نشان دهد.

اصلاحیه:

برای محافظت از احرازهویت اصلی در لایه امنیتی انتقال باید:

۱. IIS Manager باز شود.
۲. پنل Connections در سمت چپ، سرور مورد نظر را برای پیکربندی انتخاب شود.
۳. در پنل Connections، سرور و سپس Sites را باز کرده و سایت مورد نظر را انتخاب کنید.
۴. در پنل Actions، گزینه Bindings کلیک کرده، پنجره Site Bindings ظاهر می‌شود.
۵. در صورتی که HTTPS binding قابل دسترس باشد، Close کلیک و "To require SSL" بررسی شود.
۶. اگر HTTPS binding غیرقابل رویت باشد مراحل زیر باید اجرا شود:

برای اضافه کردن HTTPS binding

۱. در کادر محاوره‌ای Site Bindings، دکمه Add کلیک، کادر Add Site Binding ظاهر می‌شود.
۲. زیر Type، https را انتخاب کنید.
۳. زیر SSL certificate، .۵۰۹X certificate را انتخاب کنید.
۴. دکمه OK و سپس close کلیک گردد.

برای فعال سازی SSl

۱. در Features View، بر روی SSL Settings دابل کلیک کنید.
۲. در صفحه SSL Settings، گزینه Require SSL را انتخاب کنید.
۳. در پنل Actions، Apply کلیک شود.

SCWS-2-7: اطمینان یافتن از عدم تنظیم 'passwordFormat' به clear

شرح اجمالی:

نحوه پیاده‌سازی:

فایل پیکربندی برای برنامه کاربردی پیکربندی شده باز شده تا بررسی شود که credentials element وجود ندارد.

```
<configuration>
<system.web>
<authentication mode="Forms">
<forms name="SampleApp" loginUrl="/login.aspx">
<credentials passwordFormat="SHA1">
<user
name="UserName1"
password="SHA1EncryptedPassword1"/>
<user
name="UserName2"
password="SHA1EncryptedPassword2"/>
</credentials>
</forms>
</authentication>
</system.web>
</configuration>
```

اصلاحیه:

مد احرازهویت در machine.config، web.config در سطح root یا web.config در سطح برنامه کاربردی قابل پیکربندی است:

۱. فایل پیکربندی در مکانی که اعتبارات ذخیره می‌شوند را باز کنید.
۲. آیتم <credentials> را پیدا کنید.
۳. در صورت وجود، اطمینان حاصل شود که passwordFormat به مقدار Clear تنظیم نشده باشد.
۴. سپس passwordFormat به SHA۱ تغییر یابد.
۵. کلمات عبور متن واضح باید با نسخه مناسب درهم‌سازی شده جایگزین شوند.

SCWS-2-8: اطمینان یافتن از عدم ذخیره اعتبارات در فایل‌های پیکربندی

شرح اجمالی:

نحوه پیاده‌سازی:

فایل پیکربندی برنامه کاربردی باز شود و بررسی گردد که credentials element وجود نداشته باشد.

```
<configuration>
<system.web>
<authentication mode="Forms">
<forms name="SampleApp" loginUrl="/login.aspx">
</forms>
</authentication>
</system.web>
</configuration>
```

مد احرازهویت در machine.config، web.config در سطح root یا web.config در سطح برنامه کاربردی قابل پیکربندی است:

۱. فایل پیکربندی در مکانی که اعتبارات ذخیره می‌شوند را باز کنید.
۲. آیتم <credentials> را پیدا کنید.
۳. در صورت وجود، این بخش باید حذف شود.

این عمل باعث می‌شود تمامی مراجع کاربران ذخیره شده را در فایل‌های پیکربندی حذف نماید.

SCWS-3: پیشنهادات پیکربندی ASP.NET

SCWS-3-1: اطمینان یافتن از تنظیمات 'deployment method retail'

شرح اجمالی:

نحوه پیاده‌سازی:

بعد از دوباره راه‌اندازی مجدد IIS، فایل machine.config را باز کرده و بررسی کنید که < deployment retail="true" /> به True تنظیم شده باشد.

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

اصلاحیه::

۱. فایل machine.config را باز کرده و در بخش systemroot%\Microsoft.NET\Framework<bitness (if not the ٪ 32 bit)>\<framework version>\CONFIG
۲. خط < deployment retail="true" > در داخل بخش <system.web> اضافه گردد.
۳. اگر سیستم‌ها ۶۴ بیتی باشد مشابه بالا انجام می‌شود در فایل machine.config :

%systemroot%\Microsoft.NET\Framework<bitness (if not the 32 bit)>\<framework version>\CONFIG

SCWS-3-2: اطمینان یافتن از غیرفعال بودن 'debug'

شرح اجمالی:

این ویژگی مشخص می‌کند که اطلاعات Debug به سمت کاربر مجدد ارسال می‌شود. زمانی که این ویژگی فعال باشد کاربران می‌توانند اطلاعات غیرضروری مربوط به Debug را مشاهده کنند.

نحوه پیاده‌سازی:

فایل web.config که مربوط به سرور و یا برنامه کاربردی مورد نظر برای پیکربندی است را باز کنید. به بخش <compilation debug> رفته و و بررسی کنید که به false تنظیم شده باشد.

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

اصلاحیه:

برای تغییر این پیکربندی باید:

۱. IIS Manager را باز کرده و سرور، سایت یا برنامه مورد نظر را پیدا کنید.
۲. در Features View، .NET Compilation را دابل کلیک نمائید.
۳. بر روی صفحه .NET Compilation، در بخش Behavior، اطمینان حاصل کنید که فیلد Debug به False تنظیم شده باشد.
۴. سپس، Apply در پنل Actions را کلیک کنید.

SCWS-3-3: اطمینان یافتن از عدم غیرفعال شدن پیغام‌های سفارشی خطاها

شرح اجمالی:

این ویژگی مشخص می‌کند که پیام‌های خطا به مرورگر کاربر ارسال گردد. تغییر این ویژگی از مقدار پیش‌فرض به مقدار جدید مانع شناسایی پیام‌های خطا توسط پویشگرها می‌شود.

نحوه پیاده‌سازی:

فایل web.config را باز کرده و بررسی کنید که تگ‌های <customErrors mode="RemoteOnly”> یا <customErrors mode="On” /> تعریف شده باشد.

اصلاحیه:

احتمالا customErrors برای یک سرور، سایت یا برنامه کاربردی با استفاده از IIS Manager و توسط دستورات AppCmd.exe در پنجره خط فرمان تنظیم شده باشد. برای اعمال تنظیمات customErrors به مد RemoteOnly یا On برای وب‌سایت به صورت زیر است:

۱. IIS Manager GUI را باز کرده و سایت مورد نظر را کلیک کرده
۲. در Features View، آیکون .NET Error Pages را پیدا و دابل کلییک نمائید
۳. در پنل Actions، گزینه Edit Feature Settings را کلیک کرده
۴. در کادر محاوره ای On یا Remote Only برای مد تنظیمات انتخاب نمائید
۵. در نهایت OK را کلیک کنید.

SCWS-3-4: اطمینان یافتن از پنهان بودن جزئیات خطاهای IIS HTTP از نمایش راه دور

شرح اجمالی:

نحوه پیاده‌سازی:

خصیصه errorMode در فایل پیکربندی Web.config در آیتم <httpErrors> از بخش <system.webServer> تنظیم می‌شود. فایل مذکور را باز کرده و بررسی گردد که errorMode به DetailedLocalOnly یا Custom تنظیم شده باشد.

```
<system.web>
<system.webServer>
<httpErrors errorMode="DetailedLocalOnly">
</httpErrors>
</system.webServer>
```

مراحل زیر نحوه اعمال تنظیمات خصیصه errorMode به DetailedLocalOnly یا Custom را نشان می‌دهد:

۱. IIS Manager GUI را با مجوز Administrative باز کنید.
۲. در پنل Connections، سرور و سپس Sites folder را باز کنید.
۳. وب‌سایت یا برنامه کاربردی مورد نظر جهت پیکربندی انتخاب کنید.
۴. در Features View، Error Pages را از پنل Actions انتخاب و Open Feature انتخاب نمائید.

۵. در پنل Actions، گزینه Edit Feature Settings را کلیک کنید.

در کادر محاوره ای Edit Error Pages Settings زیر بخش Error Responses، Custom error pages یا Detailed errors for local requests و custom error pages for remote requests را انتخاب کنید.

در نهایت OK را کلیک و از کادر محاوره‌ای Edit Error Pages Settings خارج شوید.

SCWS-3-5: اطمینان یافتن از غیرفعال بودن ASP.NET stack tracing

شرح اجمالی:

نحوه پیاده‌سازی:

پیگیری[۲۱] در چندین سطوح مختلف قابل پیکربندی است:

۱. Machine.config
۲. Root-level web.config
۳. Application-level web.config
۴. Virtual or physical directory-level web.config
۵. Individual ASP.Net page level

```
Trace="false"
```

در فایل پیکربندی web.config برای برنامه کاربردی، اطمینان حاصل شود که پیگیری مانند زیر غیرفعال باشد:

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

[۲۱] Tracing

اصلاحیه:

۱. اطمینان حاصل شود که در فایل machine.config، تگ <deployment retail="true" /> فعال باشد.
۲. تمامی خصیصه‌های مرجع به پیگیری ASP.NET با استفاده از حذف پیگیری و خصیصه‌های فعال پیگیری، حذف کنید.

در هر صفحه:

حذف مرجع:

```
Trace="false"
```

برای هر برنامه کاربردی:

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

SCWS-3-6: اطمینان یافتن از پیکربندی مد 'httpcookie' برای وضعیت نشست

شرح اجمالی:

نحوه پیاده‌سازی:

فایل پیکربندی web.config برای سایت یا برنامه کاربردی را باز کرده و بررسی کنید که تگ sessionState برای استفاده از کوکی‌ها تنظیم شده باشد.

```
<system.web>
<sessionState cookieless="UseCookies" />
</system.web>
```

اصلاحیه:

مراحل زیر برای تنظیم خصیصه cookieless از نود sessionState برای استفاده از UseCookies به صورت زیر است:

۱. IIS Manager را باز کرده و سرور، سایت یا برنامه کاربردی دلخواه را انتخاب کنید.
۲. در Features View بر روی آیکون Session State دابل کلیک کنید.
۳. در بخش Cookie Settings از گزینه‌ها Use Cookies انتخاب گردد.
۴. در پنل Actions دکمه Apply کلیک کنید.

با استفاده از AppCmd.exe برای پیکربندی sessionState در سطح سرور، دستوری مانند زیر اجرا گردد:

```
%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:sessionState
/cookieless:UseCookies /cookieName:ASP.NET_SessionID /timeout:20
```

هنگامی که از Appcmd.exe برای پیکربندی <sessionstate> در سطح global استفاده می‌شود، commit:WEBROOT / باید در فایل پیکربندی لحاظ شود. بنابراین این تغییرات در root فایل web.config اعمال می‌شود.

SCWS-3-7: اطمینان یافتن از تنظیم 'cookies' به خصیصه HttpOnly

شرح اجمالی:

نحوه پیاده‌سازی:

بعد از راه‌اندازی دوباره IIS، در صورتی‌که فایل web.config برنامه کاربردی باز شود، کوکی‌ها با httpOnly فعال خواهند شد. برای اطمینان لازم است ویژگی httpOnlyCookies به true تنظیم گردد:

< httpCookies httpOnlyCookies="true" />

اصلاحیه:

۱. فایل پیکربندی web.config را باز کنید.
۲. تگ <httpCookies httpOnlyCookies="true" /> داخل <system.web> به صورت مقابل اضافه شود:

```
<configuration>
<system.web>
<httpCookies httpOnlyCookies="true" />
</system.web>
```

SCWS-3-8: اطمینان یافتن از پیکربندی 'MachineKey validation method - .Net.3.5'

شرح اجمالی:

نحوه پیاده‌سازی:

برای بررسی متد اعتبار سنجی Machine Key با استفاده IIS Manager به صورت زیر می توان انجام داد:

۱. IIS Manager را باز کرده و در سطحی که پیکربندی شده بود، WEBROOT یا سرور، به همان قسمت بروید.
۲. در features view، بر روی Machine Key دابل کلیک کرده
۳. در صفحه Machine Key، بررسی شود که برای متد اعتبارسنجی، SHA۱ انتخاب شده باشد.

اصلاحیه:

تنظیمات رمزنگاری Machine key با استفاده از UI و با اجرای appcmd.exe با ویرایش فایل‌های پیکربندی انجام می‌گیرد:

```
%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:machineKey
/validation:SHA1
```

SCWS-3-9: اطمینان یافتن از پیکربندی 'MachineKey validation method - .Net.4.5'

شرح اجمالی:

نحوه پیاده‌سازی:

برای بررسی متد اعتبار سنجی Machine Key با استفاده IIS Manager به صورت زیر می توان انجام داد:

۱. IIS Manager ر اباز کرده و در سطحی که پیکربندی شده بود، WEBROOT یا سرور
۲. در features view، بر روی Machine Key دابل کلیک کرده
۳. در صفحه Machine Key، بررسی شود که برای متد اعتبارسنجی، HMACSHA256 انتخاب شده باشد.

اصلاحیه:

تنظیمات رمزنگاری Machine key با استفاده از UI و با اجرای appcmd.exe با ویرایش فایل‌های پیکربندی انجام می‌گیرد:

```
%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:machineKey
/validation:HMACSHA256
```

SCWS-3-10: اطمینان یافتن از پیکربندی global .NET Trust Level

شرح اجمالی:

نحوه پیاده‌سازی:

برای بررسی global .NET Trust Level با استفاده IIS Manager به صورت زیر می توان انجام داد:

۱. IIS Manager را باز کرده و در سطحی که پیکربندی شده بود، به عنوان مثال سرور، به همان قسمت بروید.
۲. در features view، بر روی .NET Trust Levels دابل کلیک کرده
۳. در صفحه .NET Trust Levels، بررسی شود که Medium (web_mediumtrust.config) انتخاب شده باشد.

اصلاحیه:

تنظیمات رمزنگاری Trust level با استفاده از UI و با اجرای appcmd.exe با ویرایش فایل‌های پیکربندی انجام می‌گیرد.
برای تنظیم .Net Trust Level به Medium در سطح سرور به صورت زیر است:

```
%systemroot%\system32\inetsrv\appcmd set config /commit:WEBROOT /section:trust
/level:Medium
```

نکته:

به طور پیش‌فرض، برنامه‌های کاربردی وب ASP.NET تحت تنظیمات اطمینان کامل اجرا می‌شوند.

SCWS-3-11: اطمینان یافتن از قفل کردن 'encryption providers'

نحوه پیاده‌سازی:

برای تایید اینکه مجوزها از بین رفته‌اند:

۱. GUID ماشین را از بخش مقدار رجیستری "MachineGuid" در کلید رجیستری زیر بدست آورید:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography
```

۲. سپس از طریق cmd دستور icacls را اجرا کنید و مطمئن شوید که BUILTIN\IIS_IUSRS(R) از بین رفته است:

```
icacls
%ALLUSERSPROFILE%\Microsoft\Crypto\RSA\MachineKeys\76944fb33636aeddb9590521c2e8815a_<M
achineGUID>
```

اصلاحیه:

از بین بردن دسترسی به iisWasKey می‌تواند از طریق اجرای دستور aspnet_regiis.exe اجرا شود که نحوه‌ی اجرای آن بصورت زیر است و به نسخه‌ی .NET. استفاده شده وابسته است:

```
%systemroot%\Microsoft.NET\Framework<bitness (if not the 32 bit)>\<framework
version>\aspnet_regiis.exe -pr iisWasKey IIS_IUSRS
```

برای از بین بردن دسترسی خواندن به گروه امنیتی IIS_IUSRS در سیستمی که از .NET Framework v2.0 استفاده می‌کند:

یک cmd با دسترسی بالا باز کنید.

دستور aspnet_regiis.exe زیر را اجرا کنید:

```
%systemroot%\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -pr iisWasKey
IIS_IUSRS
```

و اگر ازسیستم ۶۴ بیت استفاده می‌کنید، دستور زیر را هم اجرا کنید:

```
%systemroot%\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis.exe -pr iisWasKey
IIS_IUSRS
```

نکته: یک نسخه‌ی واحد از aspnet_regiis.exe شامل هر نسخه ای از .NET Framework می‌شود. بدلیل اینکه هر نسخه از ابزار تنها بر روی نسخه‌ی .NET Framework مرتبط با خودش اعمال می‌شود، مطمئن شوید که از نسخه‌ی صحیح برای ابزار استفاده می‌کنید.

SCWS-4: فیلتر درخواست و سایر ماژول‌های محدود سازی

SCWS-4-1: اطمینان یافتن ازپیکربندی 'maxAllowedContentLength'

نحوه پیاده‌سازی:

در زمان تجاوز از مقدار تعیین شده برای فیلتر کردن درخواست، IIS یک کد وضعیت 404.13 را ارسال می‌کند.

برای تایید دستی تغییر، فایل web.config وبسایت و یا برنامه که در آن فیلتر درخواست، ست شده است را باز کنید و مطمئن شوید که مقدار تعریف شده برای maxAllowedContentLength همان مقدار تعیین شده است. مثال زیر یک نمونه ی 28.6 مگابایتی را نشان می‌دهد:

```
<configuration>
<system.webServer>
<security>
<requestFiltering>
<requestLimits
maxAllowedContentLength="30000000" />
</requestFiltering>
</security>
</system.webServer>
</configuration>
```

اصلاحیه:

فیلتر درخواست MaxAllowedContentLength ممکن است برای یک سرور، وبسایت و یا برنامه ای که از رابط گرافیکی IIS Manager استفاده می‌کند، از طریق دستور AppCmd.exe در یک پنجره command-line تنظیم شود و/یا مستقیما از طریق ویرایش فایل‌های config انجام پذیرد. برای تنظیم از طریق رابط گرافیکی IIS Manager:

۱. IIS Maneger را باز کنید.
۲. در پنل connections بر روی سرور، سایت، برنامه و یا دایرکتوری جهت تنظیم، کلیک کنید.
۳. در پنل Home، روی Request Filtering کلیک کنید.
۴. روی Edit Feature Settings در پنل Actions کلیک کنید.

۵. در بخش Requst Limits، حداکثر مقدار محتوا در واحد بایت را که به برنامه‌ها اجازه می‌دهد عملکرد مورد نظر خود را بازیابی کنند، وارد کنید. مثلا ۳۰۰۰۰۰۰۰(حدودا ۲۸,۶ مگابایت).

۶. برای ست کردن این فیلتر درخواست، از طریق دستور AppCmd.exe، دستور زیر را در یک cmd با دسترسی بالا اجرا کنید:

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/requestLimits.maxAllowedContentLength:30000000
```

SCWS-4-2: اطمینان یافتن از پیکربندی 'maxURL request filter'

نحوه پیاده‌سازی:

IIS یک کد وضعیت 404.14 در زمانیکه URL درخواست شده بدلیل تجاوز از حد تعیین شده در فیلتر، رد شده باشد، ارسال می‌کند.

برای تایید دستی تغییر، فایل web.config را برای وبسایت یا برنامه ای که در آن فیلتر درخواست، ست شده است را باز کنید. مقدار تعیین شده برای maxURL را تایید کنید.

```
<configuration>
<system.webServer>
<security>
<requestFiltering>
<requestLimits
maxURL="4096" />
</requestFiltering>
</security>
</system.webServer>
</configuration>
```

اصلاحیه:

فیلتر درخواست MaxURL ممکن است برای یک سرور، وبسایت و یا برنامه ای که از رابط گرافیکی IIS Manager استفاده می‌کند، از طریق دستورات AppCmd.exe در یک پنجره command-line و/یا مستقیما با ویرایش فایل‌های config انجام می‌پذیرد. برای تنظیم از طریق رابط گرافیکی IIS Manager:

۱. IIS Manager را باز کنید.
۲. در پنل Connections، بر روی Connection، سایت، برنامه و یا دایرکتوری که باید تنظیم شود، کلیک کنید.
۳. در پنل Home بر روی فیلترینگ درخواست، کلیک کنید
۴. در پنل Actions بر روی Edit Feature Settings کلیک کنید.
۵. در بخش Requst Limits، حداکثر مقدار محتوا در واحد بایت را که از طریق برنامه‌های تحت وب تست شده است را وارد کنید.

برای ست کردن این فیلتر درخواست از طریق یک دستور AppCmd.exe، دستورات زیر را در یک cmd با دسترسی بالا اجرا کنید:

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/requestLimits.maxURL:4096
```

نکته: زمانیکه درخواست فیلترینگ بر روی یک سیستم نصب شده باشد، مقدار پیش فرض بصورت "maxURL="4096 می‌باشد.

SCWS-4-3: اطمینان یافتن از پیکربندی 'MaxQueryString request filter'

نحوه پیاده‌سازی:

اگر یک درخواست، بدلیل تجاوز از حد تعیین شده در درخواست فیلتر maxQueryString یک کد وضعیت 404.15 در فایل لاگ IIS، درج می‌شود.

برای تایید دستی تغییر، فایل web.config را برای وبسایت و یا برنامه ای که فیلتر برای آن ست شده است را باز کنید. مطئن شوید که مقدار تعریف شده برای maxQueryString همان مقدار تعیین شده است.

```
<configuration>
<system.webServer>
<security>
<requestFiltering>
<requestLimits
maxQueryString="2048" />
</requestFiltering>
</security>
</system.webServer>
</configuration>
```

اصلاحیه:

فیلتر درخواست MaxQueryString می‌تواند برای یک سرور، وبسایت و یا برنامه ای که از رابط گرافیکی IIS Manager استفاده می‌کند، می‌تواند از طریق دستورات AppCmd.exe در یک پنجره ی command-line و/یا مستقیما از طریق ویرایش فایل config انجام پذیرد.

برای تنظیم از طریق رابط گرافیکی IIS Manager:

۱. IIS Manager را باز کنید.
۲. در پنل connections به قسمت connection، سایت، برنامه یا دایرکتوری برای تنظیم بروید.
۳. در پنل Home، روی Request Filtering کلیک کنید
۴. بر روی Edit Feature Settings در پنل Actions کلیک کنید.
۵. در بخش Request Limits، با استفاده از یک دستور، AppCmd.exe دستور زیر را یک command prompt اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/requestLimits.maxQueryString:2048
```

نکته: وقتی Request filtering روی یک سیستم نصب شد، مقدار پیش فرض بصورت maxQueryString=”2048” می‌باشد.

SCWS-4-4: اطمینان یافتن از عدم مجوز کارکترهای غیر اسکی در URLها

نحوه پیاده‌سازی:

اگر یک درخواست بدلیل اینکه شامل کارکتر high-bit باشد، یک کد 404.12 در فایل لاگ IIS درج می‌شود.

برای تایید دستی تغییر، فایل web.config را برای وبسایت و یا برنامه ای که فیلتر درخواست برای آن ست شده بود را باز کنید. مطمئن شوید که مقدار تعریف شده برای فیلتر false می‌باشد. به صورت زیر:

```
<configuration>
<system.webServer>
<security>
<requestFiltering
allowHighBitCharacters="false">
</requestFiltering>
</security>
</system.webServer>
</configuration>
```

اصلاحیه:

فیلتر درخواست AllowHighBitCharacters می‌تواند برای یک سرور، وبسایت و یا برنامه ای که از واسط گرافیکی IIS Manager استفاده می‌کند و از طریق دستورات AppCmd.exe در پنجره command-line و یا مستقیما از طریق ویرایش فایل config انجام می‌پذیرد. برای تنظیم از طریق رابط گرافیکی IIS Manager:

۱. IIS Manager را باز کنید.
۲. در پنل connection، به قسمت connection، سایت یا دایرکتوری برای تنظیم بروید.
۳. در پنل Home، روی Request Filtering کلیک کنید.
۴. روی Edit Feature Settings در پنل Actions کلیک کنید.

۵. در بخش General، Allow High-bit characters را uncheck کنید.

نکته: اجازه ندادن به کارکترهای اسکی high-bit در URL ممکن است بر روی عملکرد سایت‌هایی که نیاز به پشتیبانی از زبان‌های بین المللی دارند، اثر منفی داشته باشد.

برای تنظیم این فیلتر درخواست، از طریق دستور AppCmd.exe، دستور زیر را در یک command prompt با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/allowHighBitCharacters:false
```

نکته: وقتی که Request Filtering روی سیستم نصب باشد، حالت طبیعی اینست که کارکترهای high-bit در URI مجاز باشد.

SCWS-4-5: اطمینان یافتن از رد درخواست‌های Double-Encoded

نحوه پیاده‌سازی:

اگر یک درخواست، به این دلیل که شامل یک درخواست double-encoded باشد، یک کد 404.11 برای وضعیت HTTP در فایل لاگ IIS درج می‌شود.

برای تایید دستی تغییر، فایل web.config را برای وبسایت و یا برنامه ای که فیلتر درخواست برای آن ست شده بود را باز کنید. مطمئن شوید که مقدار تعریف شده برای allowDoubleEscaping برابر false می‌باشد:

```
<configuration>
<system.webServer>
<security>
<requestFiltering
allowDoubleEscaping="false">
</requestFiltering>
</security>
</system.webServer>
</configuration>
```

اصلاحیه:

فیلتر درخواست allowDoubleEscaping می‌تواند برای یک سرور، وبسایت و یا برنامه ای که از رابط گرافیکی IIS Manager استفاده می کند و از طریق دستورات AppCmd.exe در یک پنجره command-line و/یا مستقیما از طریق ویرایش فایل config انجام پذیرد. برای config از طریق رابط گرافیکی IIS Manager:

۱. IIS Manager را باز کنید.
۲. در پنل connection، به قسمت connection، سایت یا دایرکتوری برای تنظیم بروید.
۳. در پنل Home، روی Request Filtering کلیک کنید.
۴. روی Edit Feature Settings در پنل Actions کلیک کنید.
۵. در بخش General، Allow double escaping را uncheck کنید.

اگر نام یک فایل در یک URL شامل "+" باشد، آنگاه allowDoubleEscaping می‌بایست برابر true ست شود تا عملکرد درست اجرا شود.

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/allowDoubleEscaping:false
```

برای تنظیم این فیلتر درخواست، از طریق دستور AppCmd.exe، دستور زیر را در یک command prompt با دسترسی بالا اجرا کنید.

SCWS-4-6: اطمینان یافتن از غیرفعال بودن 'HTTP Trace Method'

نحوه پیاده‌سازی:

IIS یک خطای HTTP 404.6 را در زمانیکه فیلتر درخواست یک درخواست HTTP را بلاک می‌کند به کلاینت ارسال می‌کند.

برای تایید دستی تغییر، فایل web.config را برای وبسایت و یا برنامه ای که فیلتر درخواست برای آن ست شده بود را باز کنید و تنظیمات زیر را تایید کنید:

```
<configuration> <system.webServer> <security> <requestFiltering> <verbs> <add verb="TRACE"
allowed="false" /> </verbs> </requestFiltering> </security> </system.webServer> </configuration>
```

اصلاحیه:

۱. IIS Manager را باز کنید.
۲. در پنل connection، به قسمت connection، سایت یا دایرکتوری برای تنظیم بروید.
۳. در پنل Home، روی Request Filtering کلیک کنید.
۴. در پنل Request Filtering روی سربرگ HTTP Verbs کلیک کرده و سپس روی Deny Verb در پنل Actions کلیک کنید.
۵. در کادر محاوره ای Deny Verb، TRACE را وارد کنید و سپس روی OK کلیک کنید.

برای تنظیم این فیلتر درخواست، از طریق دستور AppCmd.exe، دستور زیر را در یک command prompt با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/+verbs.[verb='TRACE',allowed='false']
```

نکته: TRACE verb بصورت پیش فرض، فیلتر نمی‌شود.

SCWS-4-7: اطمینان یافتن از عدم مجوز به Unlisted File Extension

نحوه پیاده‌سازی:

وقتی IIS یک درخواست را بر اساس فرمت یک فایل فیلتر می‌کند، کد خطای درج شد معادل 404.7 می‌باشد.

برای تایید دستی تغییر، فایل web.config را برای وبسایت و یا برنامه ای که فیلتر درخواست برای آن ست شده بود را باز کنید. مطمئن شویدکه <fileExtensionsaAllowUnlisted="false">. تنظیمات web.config زیر تمامی درخواست-های فایل‌هایی که فرمت .asp, .aspx, .html ندارند را فیلتر می‌کند.

```
<configuration>
<system.webServer>
<security>
<requestFiltering>
<fileExtensions allowUnlisted="false">
<add fileExtension=".asp" allowed="true" />
<add fileExtension=".aspx" allowed="true" />
<add fileExtension=".html" allowed="true" />
</fileExtensions>
</requestFiltering>
</security>
</system.webServer>
</configuration>
```

اصلاحیه:

فیلتر درخواست allowUnlisted می‌تواند برای یک سرور، وبسایت و یا برنامه ای که از رابط گرافیکی IIS Manager استفاده می کند و از طریق دستورات AppCmd.exe در یک پنجره command-line و/یا مستقیما از طریق ویرایش فایل config انجام پذیرد. برای config از طریق رابط گرافیکی IIS Manager:

۱. IIS Manager را باز کنید.
۲. در پنل connection، به قسمت connection، سایت یا دایرکتوری برای تنظیم بروید.
۳. در پنل Home، روی Request Filtering کلیک کنید.
۴. روی Edit Feature Settings در پنل Actions کلیک کنید.
۵. در بخش General، Allow unlisted file name extensions را از حالت انتخاب خارج کنید.

برای تنظیم این فیلتر درخواست، از طریق دستور AppCmd.exe، دستور زیر را در یک command prompt با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd set config /section:requestfiltering
/fileExtensions.allowunlisted:false
```

نکته: تنظیمات پیش‌فرض فیلتر درخواست تمامی درخواست‌های Unlisted file extenstions را مجاز می‌داند.

SCWS-4-8: اطمینان یافتن از عدم اعطای مجوز Handler برای Write and Script/Execute

نحوه پیاده‌سازی:

فایل ApplicationHost.config در %systemroot%\system32\inetsrv\config را باز کنید. بخش <handlers> را پیدا کرده و تایید کنید که ویژگی accessPolicy وقتیکه Script یا Execute وجود دارند، شامل Write نمی‌شود. مثال زیر یک نمونه‌ی قابل قبول است:

```
<system.webserver> <handlers accessPolicy="Read, Script"> </handlers> </system.webserver>
```

اصلاحیه:

ویژگی accessPolicy در بخش <handlers> هم در ApplicationHost.config و هم در web.config نباید دسترسی write داشته باشند، وقتی که Script یا Execute وجود داشته باشند. برای حل این مسئله برای یک وب سرور، ویژگی بخش <handlers> در فایل ApplicationHost.config برای یک سرور باید بصورت دستی ویرایش شود. برای ویرایش فایل ApplicationHost.config از طریق Notepad، مراحل زیر را اجرا کنید:

۱. Notepad را بصورت Administator اجرا کنید.
۲. ApplicationHost.config در %systemroot%\system32\inetsrv\config را باز کنید.
۳. ویژگی accessPolicy در بخش <handlers> را ویرایش کنید بطوریکه با وجود Script یا Execute، دسترسی Write وجود نداشته باشد.

برای تنظیم این فیلتر درخواست، از طریق دستور AppCmd.exe، دستور زیر را در یک command prompt با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd set config /section:handlers /accessPolicy:Read,Script
```

نکته: این تنظیمات نمی‌تواند از طریق IIS Manager انجام پذیرد.

نکته: تنظیم پیش‌فرض accesspolicy بصورت Read,Script می‌باشد.

SCWS-4-9: اطمینان یافتن از تنظیم 'notListedIsapisAllowed' به false

نحوه پیاده‌سازی:

فایل applicationHost.config در %systemroot%\system32\inetsrv\config را باز کنید. تایید کنید که ویژگی notListedIsapisAllowed در مولفه‌ی <isapiCgiRestriction> برابر false تنظیم شده است.

```
<system.webServer> <security> <isapiCgiRestriction notListedIsapisAllowed="false">
</isapiCgiRestriction> </security> </system.webServer>
```

اصلاحیه:

برای تنظیم ویژگی notListedIsapisAllowed برابر false از طریق IIS Manager:

۱. IIS Manager را بصورت Administrator اجرا کنید.
۲. در پنل Connections و در قسمت چپ، سرور را جهت تنظیم انتخاب کنید.
۳. در قسمت Features View، ISAPI و CGI Restrictions را انتخاب کنید. در پنل Actions، Open Feature را انتخاب کنید.
۴. در پنل Actions، Edit Feature Settings را انتخاب کنید.
۵. در کادر تنظیمات Edit ISAPI and CGI Restrictions، اگر گزینه‌ی Allow unspecified ISAPI modules، انتخاب شده است، آن را از حالت انتخاب خارج کنید.
۶. OK را کلیک کنید.

برای تنظیم این فیلتر درخواست، از طریق دستور AppCmd.exe، دستور زیر را در یک command prompt با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd.exe set config -
section:system.webServer/security/isapiCgiRestriction /notListedIsapisAllowed:false
```

نکته: مقدار پیش‌فرض برای notListedIsapisAllowed برابر false می‌باشد.

SCWS-4-10: اطمینان یافتن از تنظیم 'notListedCgisAllowed' به false

نحوه پیاده‌سازی:

فایل applicationHost.config را باز کنید و تایید کنید که ویژگی notListedCgisAllowed در مولفه‌ی <isapiCgiRestriction> برابر false تنظیم شده است.

```
<system.webServer> <security> <isapiCgiRestriction notListedCgisAllowed="false">
</isapiCgiRestriction> </security> </system.webServer>
```

اصلاحیه:

برای تنظیم ویژگی notListedCgisAllowed برابر false از طریق IIS Manager:

۱. IIS Manager را بصورت Administrator اجرا کنید.
۲. در پنل Connections و در قسمت چپ، سرور را جهت تنظیم انتخاب کنید.
۳. در قسمت Features View، ISAPI و CGI Restrictions را انتخاب کنید. در پنل Actions، Open Feature را انتخاب کنید.
۴. در پنل Actions، Edit Feature Settings را انتخاب کنید.
۵. در کادر تنظیمات Edit ISAPI and CGI Restrictions، اگر گزینه‌ی Allow unspecified CGI modules، انتخاب شده است، آن را از حالت انتخاب خارج کنید.
۶. OK را کلیک کنید.

برای تنظیم این فیلتر درخواست، از طریق دستور AppCmd.exe، دستور زیر را در یک command prompt با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd.exe set config -
section:system.webServer/security/isapiCgiRestriction /notListedCgisAllowed:false
```

نکته: مقدار پیش‌فرض برای notListedCgisAllowed برابر false می‌باشد.

SCWS-4-11: اطمینان یافتن از فعال بودن 'Dynamic IP Address Restrictions'

نحوه پیاده‌سازی:

به تعداد دفعات لازم به سرور متصل شوید تا محدودیت IP بر اساس تنظیمات وارد شده تریگر شود.

اصلاحیه:

۱. IIS Manager را باز کنید.
۲. ویژگی IP Address and Domain Restrictions را باز کنید.
۳. Edit Dynamic Restrictions Settings را کلیک کنید.
۴. گزینه‌های "رد آدرس IP بر اساس تعداد درخواست‌های همزمان" و "رد آدرس IP بر اساس تعداد درخواست-های یک بازه‌ی زمانی" را انتخاب کنید. هر دوی این مقادیر هم بر اساس نیاز شما قابل انتخاب هستند.

مقدار پیش‌فرض:

بصورت پیش‌فرض، محدودیت‌های IP های داینامیک، فعال نیستند.

SCWS-5: پیشنهادات لاگ گرفتن IIS

این قسمت شامل پیشنهاداتی مرتبط با لاگ گیری IIS که در بخش تنظیمات ابتدایی پوشش داده نشده اند، می-شود.

SCWS-5-1: اطمینان یافتن از جابجائی مکان لاگ وب Default IIS

نحوه پیاده‌سازی:

برای تایید اینکه لاگ‌های وب در مکان جدیدی درج شده اند، Windows Explorer را باز کنید و به مسیری که تعیین شده بود، بروید. بسته به اینکه لاگ‌گیری چگونه تنظیم شده باشد، می‌تواند:

۱. یک فولدر شامل فایل‌های log.
۲. فایل های log. در مسیر روت دایرکتوری مشخص شده باشد.

اصلاحیه:

تغییر مکان پیش‌فرض می‌تواند بسادگی از طریق ویژگی‌های لاگ‌گیری در رابط گرافیکی IIS Manager یا AppCmd.exe انجام گیرد. برای تغییر مکان لاگ‌گیری به D:\LogFiles از طریق AppCmd.exe:

```
%systemroot%\system32\inetsrv\appcmd set config -section:sites -
siteDefaults.logfile.directory:"D:\LogFiles"
```

تغییر مکان پیش‌فرض فایل‌های لاگ به یک درایو غیر سیستمی و یا پارتیشنی جدا از محل اجرا برنامه کاربردی تحت وب و/یا سرویس محتوا، ارجحیت دارد. همچنین، مجوزهای NTFS فولدر می‌بایست تا حد ممکن محدود شود. معمولا ادمین‌ها و سیستم، تنها هویت‌هایی هستند که به دسترسی احتیاج دارند.

بدلیل اینکه لاگ‌های استاندارد IIS می‌تواند از طریق IIS Manager منتقل و ویرایش شود، ابزارهای مدیریتی جانبی نیز برای مدیریت لاگ‌های تولید شده توسط سایر ویژگی‌های IIS نیز نیاز است مانند فیلترینگ درخواست و لاگ‌گیری پیشرفته‌ی IIS. این افزونه‌ها می‌توانند از طریق Web Platform Installer و یا از سایت Microsoft دریافت شود. محل لاگ‌گیری HTTPErr می‌تواند با اضافه کردن یک کلید رجیستری، تغییر کند.

نکته: محل پیش‌فرض برای لاگ‌های وب در %SystemDrive%\inetpub\logs\LogFiles IIS8 می‌باشد.

SCWS-5-2: اطمینان یافتن از فعال بودن لاگ‌گیری از Advanced IIS

نحوه پیاده‌سازی:

به محل ذخیره‌سازی لاگ‌های پیشرفته بروید و تایید کنید که فایل‌های log. تولید شده‌اند. در نظر داشته باشید که لاگ‌ها بعد از مدت زمانی در دیسک نوشته می‌شوند. آنها می‌توانند فورا در دایرکتوری تعریف شده نوشته شوند، اگر در تعریف لاگ، گزینه‌های انتشار بلادرنگ رویدادها و نوشتن در دیسک انتخاب شده باشند.

اصلاحیه:

لاگ‌گیری پیشرفته‌ی IIS می‌تواند برای سرور، وبسایت و دایرکتوری در IIS Manager تنظیم شود. برای فعال سازی لاگ‌گیری پیشرفته از طریق رابط کاربر:

۱. IIS Manager را باز کنید.
۲. در پنل connection روی server کلیک کنید.
۳. روی آیکون Advance Logging در صفحه‌ی اصلی کلیک کنید.
۴. در پنل Actions گزینه‌ی Enable Advanced Logging را فعال کنید.

فیلدهایی که قرار است از آنها لاگ گرفته شود، می‌بایست از طریق Edit Logging Fields action تنظیم شوند. همچنین بر اساس استاندارد فایل‌های لاگ IIS، محل ذخیره سازی آنها می‌بایست تغییر کند.

نکته: ممکن است ملاحظات امنیتی بسته به حدود تنظیمات وجود داشته باشد. لاگ‌گیری پیشرفته به نصب از طریق Web Platform Installer نیاز دارد.

نکته: لاگ‌گیری پیشرفته‌ی IIS بصورت پیش‌فرض فعال نمی‌باشد.

SCWS-5-3: اطمینان یافتن از فعال بودن 'ETW Logging'

نحوه پیاده‌سازی:

با استفاده از تحلیلگر پیام، کوئری برای Microsoft-Windows-IIS-Logging را تنظیم کنید. تایید کنید که داده‌های لاگ را بصورت زنده از طریق دسترسی به وبسایت می‌توانید مشاهده کنید.

اصلاحیه:

برای تنظیم لاگ‌گیری ETW:

۱. IIS Manager را باز کنید.

۲. Server و یا سایت را برای فعالسازی ETW انتخاب کنید.
۳. Logging را انتخاب کنید.
۴. مطمئن شوید که فرمت فایل لاگ W3C می‌باشد.
۵. گزینه‌های log file و رویداد ETW را انتخاب کنید.
۶. تنظیمات را ذخیره کنید.

SCWS-6: درخواست‌های FTP

این قسمت شامل تنظیمات حساس برای اجرا پروتکل انتقال فایل می‌باشد.

SCWS-6-1: اطمینان یافتن از رمزگذاری درخواست‌های FTP

نحوه پیاده‌سازی:

سایت FTP می‌بایست از FTP-S استفاده کند. این موضوع را با استفاده از یک کلاینت FTP که FTP-S را پشتیبانی نمی‌کند و یا برای پشتیبانی از FTP-S تنظیم نشده است، تست کنید. اگر راه‌اندازی موفقیت آمیز بود، درخواست، رد می‌شود. متقابلا، یک cmd در سرور باز کنید و ftp localhost را در آن وارد کنید. پس از وارد کردن نام کاربری و رمز عبور، سرور می‌بایست یک پیغام Access is Denied برگرداند.

اصلاحیه:

برای امن‌سازی یک سایت FTP از طریق گواهینامه SSL، ابتدا می‌بایست یک گواهینامه روی سیستم نصب شود. سیستم‌های تولید همیشه می‌بایست از یک گواهینامه شخص ثالث از یک ریشه‌ی معتبر مانند VeriSign استفاده کنند. زمانیکه گواهینامه برای استفاده در IIS نصب شد، مراحل زیر را برای تنظیم سایت FTP برای پشتیبانی از SSL انجام دهید:

۱. IIS Manager را باز کنید، سرور FTP را باز کنید و تنظیمات FTP SSL را در پنل Features View انتخاب کنید.
۲. در لیست گواهینامه‌های SSL، گواهی X.509 را انتخاب کنید.
۳. در بخش SSL Policy، گزینه‌ی Require SSL Connections را انتخاب کنید.
۴. در پنل Actions روی Apply کلیک کنید.

نکته: بصورت پیش‌فرض SSL بر روی سایت‌های FTP فعال نیست.

SCWS-6-2: اطمینان یافتن از فعال بودن محدودیت تلاش‌ها در FTP Logon

نحوه پیاده‌سازی:

به سرور FTP و با استفاده از حساب کاربری administrator متصل شوید و یک رمز عبور نامعتبر وارد کنید. تایید کنید که پس از ماکسیمم دفعات مجاز برای لاگین کردن، پیغام "Connection closed by remote host" را در زمان اتصال به FTP دریافت می‌کنید.

اصلاحیه:

۱. IIS Manager را باز کنید
۲. در سطح سرور، ویژگی FTP Logon Attempt Restriction را باز کنید.
۳. Enable FTP Logon Attempt Restrictions را انتخاب کنید و ماکسیمم تعداد تلاش ناموفق و بازه‌ی زمانی را مشخص کنید. گزینه‌ی رد کردن آدرس‌های IP بر اساس تعداد تلاش‌های ناموفق را فعال کنید.
۴. روی Apply کلیک کنید.

مقدار پیش فرض:

بصورت پیش‌فرض وقتی که FTP نصب شده باشد، این ویژگی فعال نیست.

SCWS-7: رمزنگاری انتقال

این بخش شامل پیشنهاداتی برای تنظیم پروتکل IIS و مجموعه‌های رمزنگاری می‌شود.

SCWS-7-1: اطمینان یافتن از پیکربندی تنظیمات HSTS Header

نحوه پیاده‌سازی:

ماکسیمم زمان پیشنهادی ۸ دقیقه (۴۸۰ ثانیه) و یا بیشتر می‌باشد. هر مقداری بیشتر از صفر قابل قبول است. مراحل زیر را در IIS Manager اجرا کنید تا هدرهای تنظیم شده برای سرور را ببینید:

۱. IIS Manager را باز کنید.
۲. درپنل Connections، سرور خود را انتخاب کنید.
۳. در پنل Features View، روی HTTP Response Headers دابل کلیک کنید.
۴. تایید کنید که یک ورودی بنام Strict-Transport-Security وجود دارد.
۵. روی Strict-Transport-Security دابل کلیک کنید و مطمئن شوید که:

Value: box contains any value greater than 0

۶. روی OK کلیک کنید.

مراحل زیر را در IIS Manager اجرا کنید تا هدرهای تنظیم شده برای وبسایت را ببینید:

۱. IIS Manager را باز کنید.
۲. در پنل Connections، از لیست درختی Website را انتخاب کنید.
۳. در پنل Features View روی هدر HTTP Response کلیک کنید.
۴. تایید کنید که یک ورودی بنام Strict-Transport-Security وجود دارد.
۵. روی Strict-Transport-Security دابل کلیک کنید و تایید کنید که:

Value: box contains any value greater than 0

۶. روی OK کلیک کنید.

اصلاحیه:

هر مقدار بیشتر از صفر این پیشنهاد را برآورده می‌کند. مثال زیر مشخصا مربوط به ۸ دقیقه می‌باشد اما می‌تواند با توجه به نیاز شما تنظیم شود.

برای تنظیم هدر HTTP در سطح سرور با استفاده از دستور AppCmd.exe، دستورات زیر را در یک cmd با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpProtocol
/+"customHeaders.[name='Strict-Transport-Security',value='max-age=480']"
```

برای تنظیم هدر HTTP و قراردادن زیردامنه‌ها در سطح سرور با استفاده از دستور AppCmd.exe دستورات زیر را در یک cmd با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpProtocol
/+"customHeaders.[name='Strict-Transport-Security',value='max-age=480; includeSubDomains']"
```

برای تنظیم هدر HTTP در سطح Website با استفاده از دستور AppCmd.exe دستورات زیر را در یک cmd با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpProtocol
/+"customHeaders.[name='Strict-Transport-Security',value='max-age=480']"
```

برای تنظیم هدر HTTP و قراردادن زیردامنه‌ها در سطح وبسایت با استفاده از دستور AppCmd.exe دستورات زیر را در یک cmd با دسترسی بالا اجرا کنید.

```
%systemroot%\system32\inetsrv\appcmd.exe set config "Website" -
section:system.webServer/httpProtocol /+"customHeaders.[name='Strict-Transport-
Security',value='max-age=480; includeSubDomains']"
```

SCWS-7-2: اطمینان یافتن از غیرفعال بودن SSLv2

نحوه پیاده‌سازی:

مراحل زیر را انجام دهید تا مطمئن شوید، SSL2.0 غیرفعال است.

۱. اگر کلید زیر وجود نداشته باشد، SSL 2.0 غیرفعال است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0
```

۲. مطمئن شوید که کلید زیر بر روی صفر تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server\Enabled
```

اصلاحیه:

مراحل زیر را انجام دهید تا SSL2.0 را غیرفعال کنید:

۱. اگر کلید زیر موجود نباشد، SSL2.0 غیرفعال است. شمامی‌توانید کلید را حذف کنید تا پروتکل را غیرفعال کنید. اگر کلید را حذف کردید، مرحله ۲ الزامی نیست.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0
```

۲. اگر کلید وجود دارد، آن را روی صفر تنظیم کنید.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server\Enabled
```

مقدار پیش‌فرض:

فعال

SCWS-7-3: اطمینان یافتن از پیکربندی تنظیمات SSLv3

نحوه پیاده‌سازی:

مرحله زیر را انجام دهید تا مطمئن شوید SSL3.0 غیرفعال است.

۱. مطمئن شوید که کلید زیر برابر صفر تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server\Enabled
```

اصلاحیه:

مرحله زیر را انجام دهید تا SSL3.0 را غیرفعال کنید:

۱. کلید زیر را برابر صفر قرار دهید.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server\Enabled
```

مقدار پیش‌فرض:

فعال

SCWS-7-4: اطمینان یافتن از غیرفعال بودن TLS 1.0

نحوه پیاده‌سازی:

لوکیشن رجیستری‌های زیر را بازبینی کنید تا مشخص شود که TLS 1.0 همانطور که باید، تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled
```

اصلاحیه:

لوکیشن رجیستری‌های زیر را تنظیم کنید تا TLS1.0 را غیرفعال کنید. Enabled را برابر صفر قرار دهید.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled
```

SCWS-7-5: اطمینان یافتن از غیرفعال بودن TLS 1.1

نحوه پیاده‌سازی:

لوکیشن رجیستری‌های زیر را بازبینی کنید تا مطمئن شوید که TLS 1.1 فعال است.

تنظیمات فعالسازی: Enabled برابر ۱.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\Enabled
```

اصلاحیه:

لوکیشن رجیستری زیر را تنظیم کنید تا TLS 1.1 را فعال کنید. Enabled را برابر ۱ قرار دهید.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\Enabled
```

SCWS-7-6: اطیمان یافتن از فعال بودن TLS 1.2

نحوه پیاده‌سازی:

مراحل زیر را انجام دهید تا تایید کنید که TLS 1.2 فعال شده است.

۱. مطمئن شوید که کلید زیر وجود ندارد. اگر وجود دارد به مرحله ۲ بروید.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\
```

۲. مطمئن شوید که کلید زیر بر روی 0xFFFFFFFF تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Server\Enabled
```

اصلاحیه:

مراحل زیر را انجام دهید تا TLS 1.2 را فعال کنید:

۱. بررسی کنید که کلید زیر وجود دارد. اگر وجود ندارد، TLS 1.2 بصورت پیش‌فرض فعال شده است. اگر وجود دارد، می‌توانید آن را حذف کنید یا به مرحله ۲ بروید.
۲. اگر کلید وجود دارد، کلید زیر را برابر 0xFFFFFFFF تنظیم کنید.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\
```

SCWS-7-7: اطمینان یافتن از غیرفعال بودن NULL Cipher Suites

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Server\Enabled
```

نحوه پیاده‌سازی:

برای تایید اینکه سایفر NULL غیر فعال شده است، مطمئن شویدکه مراحل زیر وجود ندارد و یا آن را برابر صفر قرار دهید:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL\Enabled
```

اصلاحیه:

برای غیرفعال کردن سایفر NULL، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر صفر تنظیم شده است.

```
HKLM System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL\Enabled
```

SCWS-7-8: اطمینان یافتن از غیرفعال بودن DES Cipher Suite

نحوه پیاده‌سازی:

برای تایید اینکه DES 56/56 غیرفعال شده است، مطمئن شوید که کلید زیر وجود ندارد با برابر صفر تنظیم شده است:

اصلاحیه:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56
```

برای غیرفعال کردن DES 56/56، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر صفر تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56\Enabled
```

SCWS-7-9: اطمینان یافتن از غیرفعال بودن RC2 Cipher Suite

نحوه پیاده‌سازی:

برای تایید اینکه سایفر RC2 40/128 غیرفعال است، مطمئن شوید که کلید زیر وجود ندارد با برابر صفر تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128\Enabled
```

برای تایید اینکه سایفر RC2 56/128 غیرفعال است، مطمئن شوید که کلید زیر وجود ندارد با برابر صفر تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128\Enabled
```

اصلاحیه:

برای غیرفعال کردن RC2 40/128، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر صفر تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128\Enabled
```

برای غیرفعال کردن RC2 56/128، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر صفر تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128\Enabled
```

SCWS-7-10: اطمینان یافتن از RC4 Cipher Suites

نحوه‌ی پیاده‌سازی:

برای تایید اینکه سایفر RC4 40/128 غیرفعال است، مطمئن شوید که کلید زیر وجود ندارد با برابر صفر تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128\Enabled
```

برای تایید اینکه سایفر RC4 56/128 غیرفعال است، مطمئن شوید که کلید زیر وجود ندارد با برابر صفر تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128\Enabled
```

برای تایید اینکه سایفر RC4 64/128 غیرفعال است، مطمئن شوید که کلید زیر وجود ندارد با برابر صفر تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128\Enabled
```

برای تایید اینکه سایفر RC4 128/128 غیرفعال است، مطمئن شوید که کلید زیر وجود ندارد با برابر صفر تنظیم شده است:

اصلاحیه:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128\Enabled
```

برای غیرفعال کردن RC2 40/128، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر صفر تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128\Enabled
```

برای غیرفعال کردن RC2 56/128، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128\Enabled
```

صفر تنظیم شده است.

برای غیرفعال کردن RC2 64/128، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر صفر تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128\Enabled
```

برای غیرفعال کردن RC2 128/128، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر صفر تنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128\Enabled
```

SCWS-7-11: اطمینان یافتن از غیرفعال بودن Triple DES Cipher Suites

برای تایید اینکه سایفر Triple DES 168/168 غیرفعال است، مطمئن شوید که کلید زیر وجود ندارد با برابر 0xFFFFFFFF تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168\Enabled
```

اصلاحیه:

برای فعال کردن Triple DES 168/168، مطمئن شوید که کلید زیر وجود ندارد. اگر کلید وجود دارد، مطمئن شوید که برابر 0xFFFFFFFFتنظیم شده است.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168\Enabled
```

SCWS-7-12: اطمینان یافتن از پیکربندی AES 128/128 Cipher Suite

نحوه‌ی پیاده‌سازی:

برای تایید اینکه سایفر AES 128/128 فعال است، مطمئن شوید که کلید زیر وجود ندارد با برابر 0xFFFFFFFF تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128\Enabled
```

اصلاحیه:

برای فعالسازی AES 128/128، مطمئن شوید که کلید زیر برابر 0xFFFFFFFF ست شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128\Enabled
```

SCWS-7-13: اطمینان یافتن از فعال بودن AES 256/256 Cipher Suit

نحوه‌ی پیاده‌سازی:

برای تایید اینکه سایفر AES 256/256 فعال است:

۱. مطمئن شوید که کلید زیر وجود ندارد. اگر وجود دارد، می‌توانید آنرا حذف کنید و یا به مرحله ۲ بروید.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\
```

۲. اگر کلید زیر وجود دارد، مطمئن شوید که برابر 0xFFFFFFFF تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\Enabled
```

اصلاحیه:

برای فعالسازی سایفر AES 256/256:

۱. مطمئن شوید که کلید زیر وجود ندارد. اگر وجود دارد، می‌توانید آنرا حذف کنید و یا به مرحله ۲ بروید.

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\
```

۲. اگر کلید زیر وجود دارد، مطمئن شوید که برابر 0xFFFFFFFF تنظیم شده است:

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\Enabled
```

SCWS-7-14: اطمینان یافتن از پیکربندی TLS Cipher Suite ordering

نحوه‌ی پیاده‌سازی:

برای تایید اینکه ترتیب مجموعه سایفر صحیح است، مطمئن شویدکه کلید زیر برابر این مقادیر است:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

```
HKLM\System\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002\Functions
```

اصلاحیه:

برای مرتب کردن صحیح مجموعه سایفر، مطمئن شوید که کلید زیر برابر این مقادیر است:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

HKLM\System\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002\Functions

اثر:

ترتیب سایفرها مهم است چرا که می‌بایست امن‌ترین سایفرها در ابتدای لیست قرار گیرند و در زمان لازم روی سایفرهای ضعیف‌تر استفاده شوند.

جدول ممیزی

جدول ممیزی خلاصه‌ای از تمامی الزامات بیان شده در متن سند می‌باشد. قابل ذکر است که ستون‌های "وضعیت" و "قابلیت پیاده‌سازی" باید توسط ممیز و برای هر سیستم حاوی این برنامه تکمیل گردد. در ستون وضعیت، ممیز باید از عبارت‌های "قبول" و "رد" متناسب با وضعیت الزام در محصول مورد ارزیابی استفاده نماید. در ستون قابلیت پیاده‌سازی، ممیز باید قابلیت پیاده‌سازی الزام برای محصول مورد ارزیابی را با عبارات "دارد" و "ندارد" بیان نماید. در صورتی که الزامی برای محصول مذکور قابلیت پیاده‌سازی نداشته باشد، علت عدم قابلیت پیاده‌سازی آن باید در ذیل جدول توضیح داده شود.

شناسه	وضعیت	تنظیمات	قابلیت پیاده-سازی تنظیمات	مقدار پیش-فرض	مقدار مطلوب
SCWS-1		**پیکربندی اولیه**			
SCWS-1-1		اطمینان یافتن از اینکه محتویات وب بر روی پارتیشن غیر سیستمی باشد			
SCWS-1-2		اطمینان یافتن از 'host headers' برروی تمامی سایتها قرار دارد			
SCWS1-3		اطمینان یافتن از غیرفعال بودن 'directory browsing'			
SCWS-1-4		اطمینان یافتن از پیکربندی 'application pool identity' برای تمامی application pools			
SCWS-1-5		اطمینان یافتن از تنظیم 'unique application pools' برای سایتها			
SCWS-1-6		اطمینان یافتن از پیکربندی برای تشخیص کاربرگمنام			
SCWS-2		**پیکربندی Authentication و Authorization**			
SCWS-2-1		اطمینان یافتن از تنظیم دسترسی محدود به 'global authorization rule'			
SCWS-2-2		اطمینان یافتن از دسترسی محدود به ویژگیهای حساس سایت تنها برای کارهای اساسی احرازهویت شده			

SCWS-2-3		اطمینان یافتن از استفاده از SSL در 'forms authentication'			
SCWS-2-4		اطمینان یافتن از استفاده از کوکی در 'forms authentication'			
SCWS-2-5		اطمینان یافتن از پیکربندی 'cookie protection mode' برای 'forms authentication'			
SCWS-2-6		اطمینان یافتن از پیکربندی لایه انتقال امنیتی برای 'basic authentication'			
SCWS-2-7		اطمینان یافتن از عدم تنظیم 'passwordFormat' به clear			
SCWS-2-8		اطمینان یافتن از عدم ذخیره اعتبارات در فایلهای پیکربندی			
SCWS-3		**پیشنهادات پیکربندی ASP.NET**			
SCWS-3-1		اطمینان یافتن از تنظیمات 'deployment method retail'			
SCWS-3-2		اطمینان یافتن از غیرفعال بودن 'debug'			
SCWS-3-3		اطمینان یافتن از عدم غیرفعال شدن پیغامهای سفارشی خطاها			
SCWS-3-4		اطمینان یافتن از پنهان بودن جزئیات خطاهای IIS HTTP از نمایش راه دور			
SCWS-3-5		اطمینان یافتن از غیرفعال بودن ASP.NET stack tracing			
SCWS-3-6		اطمینان یافتن از پیکربندی مد 'httpcookie' برای وضعیت نشست			
SCWS-3-7		اطمینان یافتن از تنظیم 'cookies' به خصیصه HttpOnly			
SCWS-3-8		اطمینان یافتن از پیکربندی 'MachineKey validation method - .Net.3.5			
SCWS-3-9		اطمینان یافتن از پیکربندی 'MachineKey validation method - .Net.4.5			
SCWS-3-10		اطمینان یافتن از پیکربندی global .NET Trust Level			

SCWS-3-11		اطمینان یافتن از قفل کردن 'encryption providers'			
SCWS-4		**فیلتر درخواست و سایر ماژولهای محدود سازی**			
SCWS-4-1		اطمینان یافتن ازپیکربندی 'maxAllowedContentLength'			
SCWS-4-2		اطمینان یافتن از پیکربندی 'maxURL request filter'			
SCWS-4-3		اطمینان یافتن از پیکربندی 'MaxQueryString request filter'			
SCWS-4-3		اطمینان یافتن از عدم مجوز کارکترهای غیر اسکی درURL ها			
SCWS-4-5		اطمینان یافتن از رد درخواستهای-Double Encoded			
SCWS-4-6		اطمینان یافتن از غیرفعال بودن 'HTTP Trace Method'			
SCWS-4-7		اطمینان یافتن از عدم مجوز به Unlisted File Extension			
SCWS-4-8		اطمینان یافتن از عدم اعطای مجوز Handler برای Write and Script/Execute			
SCWS-4-9		اطمینان یافتن از تنظیم 'notListedIsapisAllowed'بهfalse’			
SCWS-4-10		اطمینان یافتن از تنظیم 'notListedCgisAllowed'بهfalse			
SCWS-4-11		اطمینان یافتن از فعال بودن 'Dynamic IP Address Restrictions'			
SCWS-5		**پیشنهادات لاگ گرفتن IIS**			
SCWS-5-1		اطمینان یافتن از جابجائی مکان لاگ وب Default IIS			
SCWS-5-2		اطمینان یافتن از فعال بودن لاگگیری از Advanced IIS			
SCWS-5-3		اطمینان یافتن از فعال بودن'ETW Logging'			
SCWS-6		**درخواستهایFTP**			
SCWS-6-1		اطمینان یافتن از رمزگذاری درخواستهایFTP			

SCWS-6-2		اطمینان یافتن از فعال بودن محدودیت تلاشها در FTP Logon			
SCWS-7		**رمزنگاری انتقال**			
SCWS-7-1		اطمینان یافتن از پیکربندی تنظیمات HSTS Header			
SCWS-7-2		اطمینان یافتن از غیرفعال بودنSSLv2			
SCWS-7-3		اطمینان یافتن از پیکربندی تنظیماتSSLv3			
SCWS-7-4		اطمینان یافتن از غیرفعال بودنTLS 1.0			
SCWS-7-5		اطمینان یافتن از غیرفعال بودن TLS ۱,۱			
SCWS-7-6		اطمینان یافتن از فعال بودن			
SCWS-7-7		اطمینان یافتن از غیرفعال بودن NULL Cipher Suites			
SCWS-7-8		اطمینان یافتن از غیرفعال بودن DES Cipher Suite			
SCWS-7-9		اطمینان یافتن از غیرفعال بودن RC2 Cipher Suite			
SCWS-7-10		اطمینان یافتن ازRC4 Cipher Suites			
SCWS-7-11		اطمینان یافتن از غیرفعال بودن Triple DES Cipher Suites			
SCWS-7-12		اطمینان یافتن از پیکربندی AES 128/128 Cipher Suite			
SCWS-7-13		اطمینان یافتن از فعال بودن AES 256/256 Cipher Suit			
SCWS-7-14		اطمینان یافتن از پیکربندی TLS Cipher Suite ordering			