به نام خدا

پیکربندی امن

Apache Tomcat 7

مرکز مدیریت راهبردی افتا

SCWS- Apache-Tomcat-7

فروردین ۹۶
نسخه ۱,۰

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 Apache Tomcat 7 است. در این سند مقادیر و تنظیمات امن برای سیاست‌های پیکربندی محصول مذکور ارائه شده است. مخاطب با استفاده از این سند توانایی پیاده‌سازی تنظیمات ارائه شده را خواهد داشت.

این سند توسط شرکت "فناوران توسعه امن ناجی" و به درخواست و تحت نظارت مرکز مدیریت راهبردی افتا تهیه گردیده است و از تلاش کارشناسان آن شرکت صمیمانه قدردانی می‌گردد. 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 Apache Tomcat 7 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 پیاده-سازی الزام توسط مدیر سامانه ارائه شده است.

تنظیمات

SCWS-1: حذف منابع غیراصلی

SCWS-1-1: حذف فایل‌ها و دایرکتوری‌های غیراصلی

شرح اجمالی:

در هنگام فرآیند نصب و راه‌اندازی، ممکن است برنامه‌های کاربردی نمونه، مستندات و دایرکتوری‌های غیر ضروری نصب شوند و هرگز مورد استفاده قرار نگیرند.

نحوه پیاده‌سازی:

به منظور حذف منابع غیراصلی موارد زیر را اجرا نمایید:

۱. نتیجه دستورات زیر باید بدون خروجی باشد:

```
$ rm -rf $CATALINA_HOME/webapps/js-examples \
        $CATALINA_HOME/webapps/servlet-example \
        $CATALINA_HOME/webapps/webdav \
        $CATALINA_HOME/webapps/tomcat-docs \
        $CATALINA_HOME/webapps/balancer \
        $CATALINA_HOME/webapps/ROOT/admin
\$CATALINA_HOME/webapps/examples
```

در صورت عدم استفاده از نرم‌افزار مدیریت، منابع ذیل نیز حذف گردد:

```
$ rm –rf $CATALINA_HOME/server/webapps/host-manager \
      $CATALINA_HOME/server/webapps/manager \
      $CATALINA_HOME/conf/Catalina/localhost/host-manager.xml \
      $CATALINA_HOME/conf/Catalina/localhost/manager.xml
```

SCWS-1-2: غیرفعال نمودن Connectorهای بلااستفاده

شرح اجمالی:

هنگامی که Tomcat به صورت پیش‌فرض نصب می‌گردد، به منظور راحتی در نصب، تنظیمات پیش‌فرض شامل Connectorها را نیز می‌شوند. لذا بهتر است این Connectorها حذف شده و تنها Connectorهای مورد نیاز فعال گردند.

نحوه پیاده‌سازی:

با اجرای دستور زیر میتوان پیکربندی connectorها را فهمید و تنها connectorها مورد نیاز را فعال باقی گذاشت.

```
$grep “Connector” $CATALINA_HOME/conf/server.xml
```

به منظور غیرفعال نمودن Connectorهای بلااستفاده موارد زیر را اجرا نمایید:

۱. در $CATALINA_HOME/conf/server.xml، Connectorهای بلااستفاده را حذف و یا کامنت نمایید.

به عنوان مثال، به منظور غیرفعال نمودن یک نمونه از HTTP Connector، مقادیر ذیل را حذف نمایید:

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
 ...
 connectionTimeout="60000"/>
```

SCWS-2: محدود کردن افشاء اطلاعات مربوط به پلتفرم سرور

با جلوگیری از نشت اطلاعات مربوط به پلتفرم سرور، تشخیص آسیب پذیری‌های متناسب بپلتفرم برای مهاجمان سخت‌تر می‌گردد.

SCWS-2-1: تغییر محتویات فایل server.info

شرح اجمالی:

Server.info شامل نام معرفی مشخصات سرویس نرم‌افزار است. این اطلاعات مربوط به سیستم به کاربران Tomcat و یا کاربران نهایی‌که به سرور متصل می‌شوند و از سرویس وب استفاده می‌کنند، نمایش داده می‌شود.

نحوه پیاده‌سازی:

برای تغییر نام و مشخصات پلت‌فرم سرور که به کاربران متصل به وب سرور Tomcat نمایش داده می‌شود، مراحل زیر انجام گیرد:

۱. استخراج فایل ServerInfo.properties از فایل catalina.jar

```
$ cd $CATALINA_HOME/lib
$ jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

۲. به دایرکتوری util که ایجاد شده بود بروید:

```
cd org/apache/catalina/util
```

۳. ServerInfo.properties را در یک ویرایشگر باز نمایید.

۴. در اینجا می‌توانید ویژگی های server.info را در فایل ServerInfo.properties، ویرایش کنید.

```
server.info=<SomeWebServer>
```

۵. catalina.jar را با فایل تغییر یافته ServerInfo.properties بروز نمایید.

```
$ jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

SCWS-2-2: تغییر بنر فایل server.number

شرح اجمالی:

server.number نشان دهنده و شامل نسخه خاصی از Tomcat است که در حال اجرا می‌باشد. این مقدار به کاربران Tomcat متصل به سرور نمایش داده می‌شود.

نحوه پیاده‌سازی:

برای تغییر عنوان نسخه سرور که به کاربران متصل به سرور نمایش داده می‌شود، مراحل زیر انجام گیرد:

۱. استخراج فایل ServerInfo.properties از فایلcatalina.jar

```
$ cd $CATALINA_HOME/lib
$ jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

۲. به دایرکتوری util که ایجاد شده بود بروید:

```
cd org/apache/catalina/util
```

۳. ServerInfo.properties را در یک ویرایشگر باز نمایید.

۴. بروز رسانی ویژگی server.number : در اینجا میتوانید نسخه تامکت را ویرایش کنید.

```
server.info=< someversion >
```

۵. catalina.jar را با فایل تغییر یافته ServerInfo.properties بروز نمایید.

```
$ jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

SCWS-2-3: تغییر بنر server.built Data

شرح اجمالی:

server.built Date نشان دهنده تاریخی می‌باشد که Tomcat کامپایل و پکیج شده است. این مقدار به کاربران Tomcat متصل به سرور نمایش داده می‌شود.

نحوه پیاده‌سازی:

برای تغییر عنوان نسخه سرور که به کاربران متصل به سرور نمایش داده می‌شود، مراحل زیر انجام گیرد:

۱. استخراج فایل ServerInfo.properties از فایل catalina.jar:

```
$ cd $CATALINA_HOME/lib
$ jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

۲. به دایرکتوری util که ایجاد شده بود بروید:

```
$ cd org/apache/Catalina/util
```

۳. ServerInfo.properties را در یک ویرایشگر باز نمایید.

۴. ویژگی server.info را در فایل ServerInfo.properties. بروز نمایید.

```
server.built=
```

۵. catalina.jar را با فایل تغییر یافته ServerInfo.properties بروز نمایید.

```
$ jar uf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

SCWS-2-4: غیر فعال نمودن X-Powered-By از هدر HTTP و تغییر نام سرور برای تمام اتصالات

شرح اجمالی:

اگر آپاچی Tomcat تنظیمات xpoweredBy را از طریق سربرگ XPoweredby- HTTP نمایان می‌سازد، توصیه می‌گردد که این مقدار false شود. به‌طور پیش‌فرض مشخصات سرور در سربرگ HTTP و تحت پوشش آپاچی Tomcat ارسال می‌شود.

نحوه پیاده‌سازی:

به منظور جلوگیری از معرفی وجود سرور Tomcat به وسیله X-Powered HTTP Header، مراحل زیر انجام گیرد:

۱. اضافه کردن ویژگی xpoweredBy به هر Connector مشخص شده در $CATALINA_HOME/conf/server.xml و تنظیم مقدار xpoweredBy به false .

```
<Connector
 ...
xpoweredBy="false" />
```

روش دیگر، اطمینان حاصل کنید که ویژگی xpoweredBy برای هر Connector مشخص شده در $CATALINA_HOME/conf/server.xml وجود ندارد.

۲. در $CATALINA_HOME/conf/server.xml مشخصات سرور را برای هر Connector خاص اضافه کنید و مقدار مشخصه سرور را به هر چیزی به جز یک رشته خالی تغییر دهید.

SCWS-2-5: غیر فعال نمودن Stack Traces کاربر

شرح اجمالی:

هنگامی که خطای runtime در طی پردازش درخواست‌ها رخ می‌دهد، Apache Tomcat، اطلاعات debugging را به درخواست کننده نمایش می‌دهد. لذا توصیه می‌گردد که این اطلاعات debug به درخواست کننده و کاربران ارائه نشود و کاربران نباید به جزییات خطا اطلاع داشته باشند.

نحوه پیاده‌سازی:

برای جلوگیری از نمایش اطلاعات خطاهای debug به درخواست کننده در سرور Tomcat، مراحل زیر انجام گیرد:

۱. یک صفحه وب که حاوی پیامی مخصوص است که هنگام مواجهه با یک خطای اجرا است باید نمایش داده شود را ایجاد کنید. برای مثال این صفحه در error.jsp/ واقع گردد.
۲. یک عامل child، <error-page> به <web-app> ، در CATALINA_HOME/conf/web.xml $file. اضافه نمایید.
۳. یک عامل child،<exception-type> به عامل مربوط به <error-page> اضافه نمایید. مقدار عامل مربوط به <exception-type> را به java.lang.Throwable تغییر دهید.
۴. عامل، <location>، به عامل <error-page> اضافه نمایید. مقدار <location> به محل صفحه ایجاد شده در خط ۱ تغییر دهید.

نتایج حاصله مشابه ذیل خواهد بود:

```
<error-page>
  <exception-type>java.lang.Throwable</exception-type>
  <location>/error.jsp</location>
</error-page>
```

SCWS-2-6: خاموش کردن TRACE

شرح اجمالی:

دستورالعمل HTTP TRACE اطلاعات debugging و تشخیصی را برای یک درخواست معین فراهم می‌نماید.

نحوه پیاده‌سازی:

برای جلوگیری از پذیرش درخواست TRACE در Tomcat موارد زیر انجام گیرد:

۱. مشخصه allowTrace در $CATALINA_HOME/conf/server.xml به false تغییر پیدا کند.

```
<Connector ... allowTrace="false" />
```

اطمینان از عدم وجود مشخصه allowTrace برای هر اتصال در $CATALINA_HOME/conf/server.xml

SCWS-3: محافظت از پورت Shutdown

Tomcat درخواست‌های Shutdown را روی tcp و پورت ۸۰۰۵ شنود می‌نماید. با اتصال به این پورت و ارسال فرمان SHUTDOWN، تمام برنامه‌های کاربردی در Tomcat خاموش (halt) می‌گردند.

SCWS-3-1: نامعین کردن مقدار Shutdown

شرح اجمالی:

Tomcat درخواست‌های Shutdown را روی tcp و پورت 8005 دریافت می‌نماید. با اتصال به این پورت و ارسال دستور SHUTDOWN، تمام برنامه‌های کاربردی در Tomcat متوقف می‌گردند. در ضمن پورت Shutdown بر روی شبکه قرار نمی‌گیرد، بلکه محدود به اینترفیس loopback است. لذا توصیه می‌گردد که یک مقدار غیر ثابت برای ویژگی Shutdown در $CATALINA_HOME/conf/server.xml تعیین گردد.

نحوه پیاده‌سازی:

برای تنظیم یک مقدار غیر قطعی برای مشخصه Shutdown، موارد زیر انجام گیرد:

۱. به‌روز رسانی مشخصه Shutdown در $CATALINA_HOME/conf/server.xml به‌صورت زیر انجام می‌پذیرد:

```
<Server port="8005" shutdown="NONDETERMINISTICVALUE">
```

نکته: NONDETERMINISTICVALUE باید با عبارتی از کاراکترهای تصادفی جایگزین گردد.

SCWS-3-2: غیرفعال نمودن پورت Shutdown

شرح اجمالی:

Tomcat درخواست‌های Shutdown را روی tcp و پورت 8005 شنود می‌نماید. با اتصال به این پورت و ارسال دستور SHUTDOWN، تمام برنامه‌های کاربردی در Tomcat متوقف می‌گردند. در ضمن پورت Shutdown بر روی شبکه قرار نمی‌گیرد، بلکه محدود به اینترفیس loopback است. لذا توصیه می‌گردد که یک مقدار غیر ثابت برای ویژگی shutdown در $CATALINA_HOME/conf/server.xml تعیین گردد. در صورتی که این عملکرد مورد استفاده قرار نمی‌گیرد، توصیه می‌شود که پورت shutdown از غیرفعال شود.

نحوه پیاده‌سازی:

برای غیر فعال کردن پورت Shutdown موارد زیر انجام گیرد:

۱. در فایل $CATALINA_HOME/conf/server.xml پورت به ۱- تنظیم شود.

```
<Server port="-1" shutdown="SHUTDOWN">
```

SCWS-4: محافظت از تنظیمات Tomcat

درصورت عدم پیکربندی امن تنظیمات Tomcat، امنیت پروسس‌ها و داده‌های وابسته و یا مربوط به Tomcat ممکن است به خطر بیافتند.

SCWS-4-1: محدود نمودن دسترسی به $CATALINA_HOME

شرح اجمالی:

$CATALINA_HOME یک متغیر محیطی است که مسیر دایرکتوری ریشه Tomcat را نگهداری می‌نماید. به منظور حفاظت از فایل‌های کتابخانه‌ای و باینری Tomcat، می‌بایست به منظور جلوگیری از دسترسی و تغییر غیرمجاز آن، اقدامات حفاظتی لازم را به عمل آورد. توصیه می‌شود که مالکیت $CATALINA_HOME به Tomcat_admin:Tomcat داده شود. همچنین توصیه می‌شود تا بر روی $CATALINA_HOME، از خواندن، نوشتن و اجرای فایل برای تمامی کاربران (o-rwx) و از دسترسی نوشتن برای گروه (g-w) جلوگیری بعمل آید.

نحوه پیاده‌سازی:

مراحل زیر توصیه می‌گردد:

۱. تنظیم مالکیت $CATALINA_HOME به tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown Tomcat_admin.Tomcat $CATALINA_HOME
# chmod g-w,o-rwx $CATALINA_HOME
```

SCWS-4-2: محدود نمودن دسترسی $CATALINA_BASE

شرح اجمالی:

$CATALINA_BASE یک متغیر محیطی است که نشان دهنده دایرکتوری است که دارای بیشترین مسیرهای وابسته است. $CATALINA_BASE معمولا زمانی که چند نسخه Tomcat همزمان با هم در حال اجرا باشند، استفاده می‌شود. به منظور جلوگیری از تغییر غیر مجاز فایل‌های کتابخانه‌ای و باینری Tomcat، می‌بایست از این متغیر محافظت نمود. توصیه می‌شود که مالکیت $CATALINA_BASE به Tomcat_admin:Tomcat داده شود. همچنین توصیه می‌شود تا بر روی $CATALINA_BASE، از خواندن، نوشتن و اجرای فایل برای تمامی کاربران (o-rwx) و از دسترسی نوشتن برای گروه (g-w) جلوگیری بعمل آید.

نحوه پیاده‌سازی:

مراحل زیر توصیه می‌گردد:

۱. تنظیم مالکیت $CATALINA_BASE به tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown Tomcat_admin.Tomcat $CATALINA_BASE
 # chmod g-w,o-rwx $CATALINA_BASE
```

SCWS-4-3: محدود نمودن دسترسی به دایرکتوری پیکربندی Tomcat

شرح اجمالی:

دایرکتوری /$CATALINA_HOME/conf حاوی فایل‌های پیکربندی Tomcat می‌باشد. توصیه می‌شود که مالکیت این دایرکتوری به کاربر Tomcat_admin:Tomcat داده شود. همچنین توصیه می‌شود تا بر روی این دایرکتوری، از خواندن، نوشتن و اجرای فایل برای تمامی کاربران (o-rwx) و از دسترسی نوشتن برای گروه (g-w) جلوگیری بعمل آید.

نحوه پیاده‌سازی:

به منظور محدود نمودن دسترسی به دایرکتوری پیکربندی Tomcat مراحل زیر انجام گیرد:

۱. تنظیم مالکیت /$CATALINA_HOME/conf به tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown Tomcat_admin:Tomcat $CATALINA_HOME/conf
# chmod g-w,o-rwx $CATALINA_HOME/conf
```

SCWS-4-4: محدودیت در دسترسی به دایرکتوری لاگ‌ها در Tomcat

شرح اجمالی:

دایرکتوری /$CATALINA_HOME/logs حاوی فایل‌های لاگ Tomcat است. توصیه می‌شود که مالکیت این دایرکتوری به کاربر Tomcat_admin:Tomcat داده شود. همچنین توصیه می‌شود تا بر روی این دایرکتوری، از خواندن، نوشتن و اجرای فایل برای تمامی کاربران (o-rwx) جلوگیری بعمل آید.

باید از دسترسی به این دایرکتوری توسط کاربران داخلی برای تغیرات سهوی و یا عمدی جلوگیری به عمل آید.

نحوه پیاده‌سازی:

به منظور محدود نمودن دسترسی به فایل لاگ Tomcat مراحل زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/logs/ به tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه

```
# chown tomcat_admin:tomcat $CATALINA_HOME/logs
# chmod o-rwx $CATALINA_HOME/logs
```

SCWS-4-5: محدودیت در دسترسی به پوشه‌های موقت Tomcat

شرح اجمالی:

دایرکتوری $CATALINA_HOME/temp/ در Tomcat برای باقی ماندن اطلاعات موقت روی دیسک استفاده شده است. توصیه می‌شود که مالکیت این دایرکتوری به کاربر tomcat_admin:tomcat داده شود. همچنین توصیه می‌شود تا بر ر وی این دایرکتوری، از خواندن، نوشتن و اجرای فایل برای تمامی کاربران (o-rwx) جلوگیری بعمل آید.

نحوه پیاده‌سازی:

به منظور محدودیت در دسترسی به پوشه‌های لاگ Tomcat موارد زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/logs به tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه

```
# chown tomcat_admin:tomcat $CATALINA_HOME/temp
# chmod o-rwx $CATALINA_HOME/temp
```

SCWS-4-6: محدود نمودن دسترسی به دایرکتوری باینری Tomcat

شرح اجمالی:

دایرکتوری /$CATALINA_HOME/bin در Tomcat شامل تعدادی دستور اجرایی است که بخشی از Tomcat run-time محسوب می‌گردد. توصیه می‌شود که مالکیت این دایرکتوری به کاربر tomcat_admin:tomcat اختصاص داده شود. همچنین توصیه می‌شود از خواندن، نوشتن و اجرای فایل $CATALINA_HOME توسط تمامی کاربران(o-rwx) و از دسترسی نوشتن برای صاحبان گروه (g-w) جلوگیری شود.

نحوه پیاده‌سازی:

به منظور محدودیت در دسترسی به پوشه‌های لاگ Tomcat موارد زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/logs به tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/bin
# chmod g-w,o-rwx $CATALINA_HOME/bin
```

SCWS-4-7: محدودیت در دسترسی به دایرکتوری اپلیکیشن وب Tomcat

شرح اجمالی:

دایرکتوری $CATALINA_HOME/webapps حاوی برنامه‌های کاربردی تحت وبی است که از طریق نصب کردن Tomcat نصب می‌گردد. توصیه می‌شود که مالکیت این دایرکتوری به کاربر tomcat_admin:tomcat اختصاص داده شود. همچنین توصیه می‌شود از خواندن، نوشتن و اجرای فایل $CATALINA_HOME/webapps توسط تمامی کاربران(o-rwx) و از دسترسی نوشتن برای صاحبان گروه (g-w) جلوگیری شود.

نحوه پیاده‌سازی:

به منظور محدودیت در دسترسی به پوشه‌های لاگ Tomcat موارد زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/webapps/ به tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/webapps
# chmod g-w,o-rwx $CATALINA_HOME/webapps
```

SCWS-4-8: محدود نمودن دسترسی به catalina.policy در Tomcat

شرح اجمالی:

فایل catalina.policy برای پیکربندی سیاست‌های امنیتی Tomcat استفاده می‌شود. توصیه می‌شود که با اعطای مجوزهای مناسب از تغییرات غیر مجاز و دسترسی به این فایل محافظت گردد.

نحوه پیاده‌سازی:

به منظور محدود نمودن دسترسی به $CATALINA_HOME/conf/catalina.policy در Tomcat موارد زیر انجام گیرد:

۱. مالک و گروه مالک را که شامل $CATALINA_HOME/ می‌شود را به کاربر tomcat_admin:tomcat، تنظیم نمایید.

```
# chmod 770 $CATALINA_HOME/conf/catalina.policy
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/catalina.policy
```

SCWS-4-9: محدود نمودن دسترسی به catalina.properties در Tomcat

شرح اجمالی:

Catalina.properties یک فایل با ویژگی‌های جاوا است که شامل تنظیماتی برای اطلاعات class loaderو لیست بسته‌های امنیتی و ویژگی عملکردی است. توصیه می‌شود که با اعطای مجوزهای مناسب از دسترسی به این فایل و تغییرات غیر مجاز محافظت گردد.

نحوه پیاده‌سازی:

به منظور محدود نمودن دسترسی به catalina.policy موارد زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/conf/catalina.policy به tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/catalina.properties
# chmod g-w,o-rwx $CATALINA_HOME/conf/catalina.properties
```

SCWS-4-10: محدود نمودن دسترسی به context.xml در Tomcat

شرح اجمالی:

فایل context.xml توسط همه برنامه‌های کاربردی وب بارگذاری می‌گردد و با تنظیمات پیکربندی معینی تنظیم می‌گردد. توصیه می‌شود که با اعطای مجوزهای مناسب از دسترسی به این فایل و تغییرات غیر مجاز محافظت گردد.

نحوه پیاده‌سازی:

به منظور محدود نمودن دسترسی به context.xml موارد زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/conf/context.xml به کاربر tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/context.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/context.xml
```

SCWS-4-11: محدود نمودن دسترسی به logging.properties در Tomcat

شرح اجمالی:

Logging.properties فایلی در Tomcat است که پیکربندی Logging را مشخص می‌نماید. توصیه می‌شود که با اعطای مجوزهای مناسب از دسترسی به این فایل و تغییرات غیر مجاز محافظت گردد.

نحوه پیاده‌سازی:

برای محدود کردن دسترسی به logging.properties موارد زیر باید انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/conf/logging.properties به کاربر tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/logging.properties
# chmod g-w,o-rwx $CATALINA_HOME/conf/logging.properties
```

SCWS-4-12: محدود نمودن دسترسی به server.xml در Tomcat

شرح اجمالی:

Server.xml حاوی پیکربندی‌ها و تعاریفTomcat Servlet می‌باشد. توصیه می‌شود که با اعطای مجوزهای مناسب از دسترسی به این فایل و تغییرات غیر مجاز محافظت گردد.

نحوه پیاده‌سازی:

به منظور محدود نمودن دسترسی به server.xml موارد زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/conf/server.xml به کاربر tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/server.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/server.xml
```

SCWS-4-13: محدود نمودن دسترسی به Tomcat-users.xml در Tomcat

شرح اجمالی:

Tomcat-users.xml حاوی اطلاعات احراز هویت برای برنامه‌های کاربردی Tomcat است. توصیه می‌شود که با اعطای مجوزهای مناسب از دسترسی به این فایل و تغییرات غیر مجاز محافظت گردد.

نحوه پیاده‌سازی:

به منظور محدود نمودن دسترسی به Tomcat-users.xml موارد زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/conf/Tomcat-users.xml به کاربر tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه

۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/Tomcat-users.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/Tomcat-users.xml
```

SCWS-4-14: محدود نمودن دسترسی به web.xml در Tomcat

شرح اجمالی:

Web.xml فایلی از تنظیمات پیکربندی Tomcat است که تنظیمات پیکربندی نرم افزار در آن ذخیره می‌گردد. توصیه می‌شود که با اعطای مجوزهای مناسب از دسترسی به این فایل و تغییرات غیر مجاز محافظت گردد.

نحوه پیاده‌سازی:

به منظور محدود نمودن دسترسی به web.xml موارد زیر انجام گیرد:

۱. تنظیم مالکیت $CATALINA_HOME/conf/web.xml به کاربر tomcat_admin:tomcat
۲. حذف مجوزهای خواندن، نوشتن و اجرا برای همه
۳. حذف مجوزهای نوشتن، برای گروه.

```
# chown tomcat_admin:tomcat $CATALINA_HOME/conf/web.xml
# chmod g-w,o-rwx $CATALINA_HOME/conf/web.xml
```

SCWS-5: پیکربندی حوزه‌ها

Tomcat realm پایگاه داده‌ای از نام‌های کاربری و کلمات عبور است که به منظور شناسایی کاربران معتبر برنامه‌های کاربردی وب مورد استفاده قرار می‌گیرد.

SCWS-5-1: استفاده از حوزه‌های امن

شرح اجمالی:

Realm پایگاه داده‌ای از نام‌های کاربری و کلمات عبور است که به منظور شناسایی کاربران معتبر برنامه‌های کاربردی وب مورد استفاده قرار می‌گیرد. لازم است نسبت به بازبینی پیکربندی‌های Realmها را برای حصول اطمینان از اینکهTomcat نسبت به موارد JDBCRealm، UserDatabaseRealm یا JAASRealm پیکربندی نشده است، اقدام شود. به خصوص که Tomcat نباید از MemoryRealm استفاده کند.

نحوه پیاده‌سازی:

تنظیمات Realm className در $CATALINA_HOME/conf/server.xml به یکی از Realmهای مناسب تنظیم گردد.

SCWS-5-2: استفاده از lockout Realms

شرح اجمالی:

Lockout Wrap، به Realm استاندارد، قابلیت قفل نمودن یک حساب کاربری پس از چند بار ورود ناموفق را اضافه می‌نماید.

نحوه پیاده‌سازی:

یک فایل Lockout که شامل موارد استاندارد می‌شود، مانند مثال زیر ایجاد نمایید:

```
<Realm className="org.apache.catalina.realm.LockOutRealm"
failureCount="3" lockOutTime="600" cacheSize="1000"
cacheRemovalWarningTime="3600">
      <Realm
className="org.apache.catalina.realm.DataSourceRealm"
dataSourceName=... />
</Realm>
```

SCWS-6: امنیت اتصال (Connector Security)

امنیت ارتباطات Tomcatتضمین می‌نماید که برنامه‌های کاربردی ایجاد شده در Tomcat، در سطح قابل قبولی از امنیت قرار دارند. موارد زیر امنیت ارتباط را تضمین می‌کنند:

SCWS-6-1: تنظیم احراز هویت Client-cert

شرح اجمالی:

احراز هویت Client-cert ملزم می‌دارد که هر کاربر جهت ارتباط با ب سرور دارای گواهینامه‌ای برای احراز هویت باشد. این مورد احراز هویت قدرتمندتری نسبت به رمز عبور به شمار می‌آید زیرا لازم می‌دارد که کاربر دارای مجوزی باشد و تنها دانستن رمز عبور کافی نمی‌باشد.

نحوه پیاده‌سازی:

در عامل اتصال، می‌بایست پارامتر clientAuth مقدار true داشته باشد.

```
<-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector
    port="8443" minProcessors="5" maxProcessors="75"
    enableLookups="true" disableUploadTimeout="true"
    acceptCount="100" debug="0" scheme="https" secure="true";
    clientAuth="true" sslProtocol="TLS"/>
```

SCWS-6-2: اطمینان از True بودن مقدار SSLEnable برای اتصالات حساس

شرح اجمالی:

در صورتی که برای Connector خاصی SSL فعال باشد، می‌بایست مقادیر SSLEnable را نیز تنظیم نمود. توصیه می‌گردد SSL برای هر Connector که اطلاعات حساس مانند احراز هویت و اطلاعات شخصی را ارسال و دریافت می‌کند، استفاده گردد.

نحوه پیاده‌سازی:

می‌بایست برای هر اتصالی که اطلاعات حساس را ارسال و دریافت می‌کند مقدار SSLEnable در server.xml، True گردد:

```
<Connector
  …
  SSLEnabled="true"
  …
/>
```

SCWS-6-3: اطمینان از تنظیم دقیق طرح (scheme)

شرح اجمالی:

ویژگی scheme به منظور جهت نشان دادن اینکه کدام یک از Schemeها توسط درخواست کنندگان request.getScheme()، مورد استفاده قرار می‌گیرد. لذا می‌بایست از اینکه ویژگی scheme برای Connectorهایی که بر روی HTTP در حال کار هستند معادل http قرار داده شود، اطمینان حاصل نمود. همچنین مطمئن شوید که ویژگی scheme برای Connectorهایی که بر روی HTTPS در حال کار هستند نیز معادل https قرار داده شود.

نحوه پیاده‌سازی:

می‌بایست در server.xml، برای Connectorهایی که روی بستر HTTP فعالیت می‌کنند ویژگی scheme به http و برای Connectorهایی که روی بستر HTTPS فعالیت می‌کنند ویژگی scheme به https، پیکربندی گردند.

```
<Connector
  …
  scheme="https"
  …
 />
```

SCWS-6-4: اطمینان از اینکه secure بر روی مقدار True و فقط برای اتصالات SSL-Enabled تنظیم شده است.

شرح اجمالی:

ویژگی secure به منظور انتقال وضعیت‌های امنیتی Connector به برنامه‌هایی که از طریق Connector عمل می‌نمایند، مورد استفاده قرار می‌گیرد. این ویژگی معمولا با فراخوانی request.isSecure() به دست می‌آید. لذا مطمئن شوید که مقدار secure برای اتصالاتی که SSLEnable مقدار True دارد، برابر True باشد.

نحوه پیاده‌سازی:

برای هر Connector تعریف شده در server.xml، مقدار secure برای Connectorهایی که SSLEnable مقدار True دارد، برابر True تنظیم گردد. همچنین مقدار secure برای Connectorهایی که SSLEnable مقدار False دارد، برابر False تنظیم گردد.

```
<Connector SSLEnabled="true"
    …
    secure="true"
    …
/>
```

SCWS-6-5: اطمینان از تنظیم TLS در پروتکل SSL برای اتصالات امن

شرح اجمالی:

تنظیمات sslProtocol پروتکل Tomcatای که برای محافظت از ترافیک به کار می‌رود را شناسایی می‌کند. لذا توصیه می‌شود که ویژگی sslProtocol بر روی TLS تنظیم شود.

نحوه پیاده‌سازی:

در server.xml، برای همه اتصالاتی که SSLEngine مقدار on دارد می‌بایست sslProtocol به TLS تنظیم شود.

```
<Connector
  …
  sslProtocol="TLS"
  …
/>
```

SCWS-7: ایجاد و حفاظت از لاگ‌ها

فعال نمودن قالبیت لاگ‌گیری و اطمینان از اینکه لاگ‌ها بطور کامل محافظت می‌شوند.

SCWS-7-1: نرم‌افزار مخصوص لاگ‌گیری

شرح اجمالی:

به‌طور پیش‌فرض java.util.logging در هر VM تنها برای یک وب قابل پیکربندی است. برای غلبه بر این محدودیت در Tomcat، پیاده‌سازی JULI (Java Util Logging Implementation) به‌عنوان یک پوشش برای java.util.logging صورت می‌گیرد. همچنین JULI قابلیت‌های اضافی را فراهم می‌کند. لذا شما می‌توانید هر برنامه تحت وب را با خصیصه‌های لاگ‌گیری متفاوتی تنظیم نمایید.

نحوه پیاده‌سازی:

یک فایل logging.properties ایجاد نموده و در آدرس دایرکتوری WEB-INF\classes را قرار دهید.

توجه: به‌طور پیش‌فرض آدرس فایل logging.properties در مسیر $CATALINA_HOME\conf می‌باشد.

SCWS-7-2: تعیین فایل مدیریت کننده در logging.properties

شرح اجمالی:

Handlerها مکانی را که لاگ‌ها به آنجا ارسال می‌گردند را مشخص می‌نمایند. کنسول مدیریت کننده لاگ‌ها را به کنسول جاوا ارسال می‌کند و فایل مدیریت کننده آن‌ها را در یک فایل قرار می‌دهد.

نحوه پیاده‌سازی:

اگر کدهای زیر در logging.properties وجود ندارد، آن‌ها را اضافه نمایید.

```
handlers=org.apache.juli.FileHandler, java.util.logging.ConsoleHandler
```

از خاموش نبودن قابلیت لاگ‌گیری مطمئن شوید و سطح لاگ‌گیری را همانند زیر به سطح مورد نظر خود تنظیم نمایید.

```
org.apache.juli.FileHandler.level=FINEST
```

SCWS-7-3: اطمینان از تنظیم صحیح className در context.xml

شرح اجمالی:

از تنظیم مقدار ویژگی className معادل AccessLogValve اطمینان حاصل نمایید. ویژگی className تعیین کننده دسترسی به log valve است که جهت لاگ‌برداری مورد استفاده قرار می‌گیرد.

نحوه پیاده‌سازی:

اگر جمله زیر در فایل $CATALINA_BASE\webapps\<app name>\METAINF\context.xml وجود نداشت، آن را اضافه نمایید.

```
<Valve
className="org.apache.catalina.valves.AccessLogValve"
directory="$CATALINA_HOME/logs/"
 prefix="access_log"
fileDateFormat="yyyy-MM-dd.HH"
suffix=".log"
pattern="%t %H cookie:%{SESSIONID}c request:%{SESSIONID}r %m %U %s %q %r"
/>
```

SCWS-7-4: اطمینان از امن بودن آدرس در context.xml

شرح اجمالی:

از ویژگی دایرکتوری این است که محل ذخیره‌سازی لاگ‌ها را به Tomcat بیان میکند. توصیه می‌گردد که موقعیت مشخص شده توسط ویژگی دایرکتوری تحت اقدامات امنیتی قرار گیرد.

نحوه پیاده‌سازی:

موارد زیر را انجام دهید:

۱. اگر جمله زیر در فایل $CATALINA_BASE\webapps\<app-name>\METAINF\context.xml وجود نداشت، آن را اضافه نمایید.

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="$CATALINA_HOME/logs/"
prefix="access_log" fileDateFormat="yyyy-MM-dd.HH" suffix=".log" pattern="%t %H
cookie:%{SESSIONID}c request:%{SESSIONID}r %m %U %s %q %r"
/>
```

۲. تنظیم آدرس مذکور به ویژگی‌های tomcat_admin:tomcat با مجوز o-rwx

```
# chown tomcat_admin:tomcat $CATALINA_HOME/logs
# chmod o-rwx $CATALINA_HOME/logs
```

SCWS-7-5: اطمینان از تنظیم صحیح الگو در context.xml

شرح اجمالی:

تنظیمات pattern به Tomcat اطلاع می‌دهد که چه اطلاعاتی باید ثبت و خیره شود. لذا حداقل اطلاعات کافی باید برای یک درخواست تشخیص هویت منحصر به فرد مانند: نوع درخواست، منشا درخواست و چه زمانی درخواست رخ داده بایستی لاگ و ذخیره شود، باشند. مطابق شرح زیر ثبت درخواست تاریخ و زمان (%t)، URL درخواستی (%U)، آدرس remote IP (%a)، آدرس IP محلی (%A)، ، متد درخواستی (%m)، پورت محلی (%p)، پرس و جوی string در صورت وجود (%q) و کد موقعیت پاسخ HTTP (%s) لاگ می‌شوند.

```
pattern="%t %U %a %A %m %p %q %s”
```

نحوه پیاده‌سازی:

۱. اگر جمله زیر در فایل CATALINA_BASE\webapps\<app name>\METAINF\context.xml وجود نداشت، آن را اضافه کنید.

```
<Valve
className="org.apache.catalina.valves.AccessLogValve"directory="$CATALINA_HOME/logs/"
```

```
prefix="access_log" fileDateFormat="yyyy-MM-dd.HH" suffix=".log"
pattern="%h %t %H cookie:%{SESSIONID}c request:%{SESSIONID}r %m %U %s
%q %r"
/>
```

SCWS-7-6: اطمینان از امن بودن دایرکتوری logging.properties

شرح اجمالی:

از ویژگی این دایرکتوری این است که محل ذخیره‌سازی لاگ‌ها را به Tomcat بیان می‌دارد. مقدار دایرکتوری باید مکان ایمنی با دسترسی محدود باشد.

نحوه پیاده‌سازی:

موارد زیر را انجام دهید:

۱. اگر جمله زیر در فایل logging.properties وجود نداشت، آن را اضافه کنید.

```
<application_name>.org.apache.juli.FileHandler.directory=<log_location>
<application_name>.org.apache.juli.FileHandler.prefix=<application_name>
```

۲. آدرس اشاره شده به ویژگی دایرکتوری به tomcat_admin:tomcat با مجوز o-rwx تنظیم گردد.

```
# chown tomcat_admin:tomcat <log_location>
# chmod o-rwx <log_location>
```

SCWS-7-7: تنظیم اندازه فایل لاگ

شرح اجمالی:

به طور پیش‌فرض، فایل logging.propeties هیچ محدودیت تعریف شده‌ای برای اندازه فایل log ندارد. لذا به صورت بالقوه مستعد یک حمله منع سرویس است زیرا ممکن است یک درایو یا پارتیشن حاوی فایل‌های log را پر کند.

نحوه پیاده‌سازی:

در فایل logging.properties عبارت زیر را وارد نمایید. این محدودیت با تعداد بایت‌ها مشخص می‌گردد.

```
java.util.logging.FileHandler.limit=10000
```

SCWS-8: پیکربندی سیاست Catalina

سیاست در پیکربندی Catalina بر این است که برنامه‌های تحت وب را از دسترسی محدود شده یا پکیج‌های ناشناخته‌ای که ممکن است برای برنامه مضر یا خطرناک باشد، محافظت می‌کند.

SCWS-8-1: محدودیت دسترسی زمان اجرا برای پکیج‌های حساس

شرح اجمالی:

Package.access دسترسی به پکیج‌های لیست شده را در زمان اجرا اعطا یا لغو می‌کند. توصیه می‌شود که دسترسی برنامه برای پکیج‌های معین محدود شود.

نحوه پیاده‌سازی:

$CATALINA_BASE/conf/catalina.properties را از طریق افزودن پکیج‌های مجاز به لیست package.access ویرایش نمایید.

```
package.access = sun.,org.apache.catalina.,org.apache.coyote.,org.apache.Tomcat.,
org.apache.jasper
```

SCWS-9: استقرار برنامه

با اجرای Tomcat توسط مدیر امنیت که در نصب و راه اندازی سامانه ها دید امنیتی را لحاظ میکند، برنامه‌ها در یک sandbox اجرا می‌شوند که می‌تواند از دسترسی کدهای مشکوک به فایل‌های سیستم‌فایل جلوگیری کند.

SCWS-9-1: شروع Tomcat با مدیریت امنیتی

شرح اجمالی:

برنامه را برای اجرا در یک sandbox با استفاده از مدیر امنیتی (Security Manager) پیکربندی نمایید. مدیر امنیتی محدود کننده کلاس‌هایی است که تامکت می‌تواند به آن دسترسی داشته باشد از این رو سرور شما را از اشتباهات، تروجان‌ها و کدهای مخرب محافظت می‌کند.

نحوه پیاده‌سازی:

سیاست‌های امنیتی پیاده‌سازی شده توسط مدیر امنیتی جاوا در فایل$CATALINA_HOME/conf/catalina.policy پیکربندی می‌شوند. به محض اینکه شما فایل catalina.policy را برای استفاده توسط یک مدیر امنیتی پیکربندی کنید، Tomcat توسط مدیر امنیتی با استفاده از گزینه‌ی security-- آغاز می‌شود.

```
$CATALINA_HOME/bin/catalina.sh start -security (Unix)
C:\> %CATALINA_HOME%\bin\catalina start -security (Windows)
```

SCWS-9-2: غیر فعال کردن خود استقراری برنامه‌ها

شرح اجمالی:

Auto deployment برنامه‌ها هنگامی که Tomcat در حال اجرا می‌باشد، فعال است. لذا توصیه می‌گردد این قابلیت غیرفعال گردد.

نحوه پیاده‌سازی:

در فایل $CATALINA_HOME/conf/server.xml مقدار autoDeploy را به false تغییر دهید.

```
autoDeploy="false"
```

SCWS-9-3: غیرفعال کردن استقرار در شروع برنامه‌ها

شرح اجمالی:

Tomcat امکان deployment خودکار برنامه‌ها را فراهم می‌کند. لذا توصیه می‌شود که این قابلیت غیرفعال گردد.

نحوه پیاده‌سازی:

در فایل $CATALINA_HOME/conf/server.xml مقدار deployOnStartup را به false تغییر دهید.

```
deployOnStartup="false"
```

SCWS-10: دیگر تنظیمات پیکربندی

ذخیره‌سازی محتوای وب در بخش جداگانه‌ای از فایل‌های سیستمی Tomcat بیاد انجام گیرد.

SCWS-10-1: اطمینان از قرارگیری دایرکتوری محتوای وب در بخش جداگانه‌ای از فایل‌های سیستمی Tomcat

شرح اجمالی:

محتوای وب را در بخش جداگانه‌ای از فایل‌های سیستمی Tomcat ذخیره می‌گردد.

نحوه پیاده‌سازی:

فایل‌های محتوای وب را به پارتیشن‌های جداگانه‌ای از فایل‌های سیستمی Tomcat انتقال دهید و همچنین پیکربندی خود را بروزرسانی نمایید.

SCWS-10-2: محدود نمودن دسترسی به دایرکتوری مدیریت وب

شرح اجمالی:

دسترسی به برنامه‌ی مدیریت وب را محدود نموده تا فقط افراد مجاز که نیازمند دسترسی هستند اجازه دسترسی را داشته باشند. باید به صفحات ادمین و پیکربندی برنامه وب فقط کاربر ادمین دسترسی داشته باشد.

نحوه پیاده‌سازی:

برای برنامه‌ی مدیریت، $CATALINA_HOME/conf/server.xml را ویرایش نموده و به‌صورت زیر آن را از حالت کامنت خارج نمایید:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="127\.0\.0\.1"/>
```

توجه: انتظار می‌رود ویژگی RemoteAddrValve به‌صورت یک regular expression باشد، بنابراین بازه‌ها و دیگر متا-کاراکترهای مربوط به regular expression باید در نظر گرفته نشوند.

SCWS-10-3: محدود سازی برنامه‌های مدیریتی

شرح اجمالی:

دسترسی به برنامه‌ی مدیریتی را محدود نموده تا فقط افراد مجاز که نیازمند دسترسی هستند اجازه دسترسی را داشته باشند.

نحوه پیاده‌سازی:

$CATALINA_BASE/conf/[enginename]/[hostname]/ manager.xmlرا برای برنامه‌ی مدیریتی اصلاح نموده و خطوط پر رنگ را اضافه نمایید:

```
<Context path="/manager" docBase="${catalina.home}/webapps/manager" debug="0"
privileged="true">
 <Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="127\.0\.0\.1"/>
<!-- Link to the user database we will get roles from -->
<ResourceLink name="users" global="UserDatabase"
type="org.apache.catalina.UserDatabase"/>
</Context>
```

افزودن هاست‌ها و جدا کردن بوسیله کاما امکان دسترسی به برنامه‌ی ادمین را فراهم می‌کند.

توجه: انتظار می‌رود ویژگی RemoteAddrValve به‌صورت یک regular expression باشد، بنابراین بازه‌ها و دیگر متا-کاراکترهای regular expression می‌بایست در نظر گرفته نشوند.

SCWS-10-4: هنگام دسترسی به برنامه‌ی مدیریتی، SSL را اجباری کنید.

شرح اجمالی:

هنگام دسترسی به برنامه مدیریت، به منظور اطمینان از مصون ماندن SSL، از ویژگی transport-guarantee استفاده نمایید.

نحوه پیاده‌سازی:

تنظیمات مربوط به $CATALINA_HOME/webapps/manager/WEB-INF/web.xml که در زیر نمایش داده شده است را انجام دهید.

```
<security-constraint>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL<</transport-guarantee>>
  <user-data-constraint>
 </security-constraint>
```

SCWS-10-5: تغییر نام برنامه مدیریت

شرح اجمالی:

برنامه‌ی مدیریت به مدیران اجازه می‌دهد تا از طریق یک رابط وب از راه دور Tomcat را مدیریت کنند. نام برنامه‌ی مدیریت و پورت های پیشفرض باید تغییر یابد تا مهاجمان و کدهای مخرب نتوانند به‌راحتی به آن دست یابند.

نحوه پیاده‌سازی:

موارد زیر را برای تغییر نام برنامه‌ی مدیریت انجام دهید:

۱. فایل XML برنامه‌ی مدیریت را تغییر نام دهید.

```
# mv $CATALINA_HOME/webapps/host-manager/manager.xml \
$CATALINA_HOME/webapps/host-manager/new-name.xml
```

۲. ویژگی docBase را در $CATALINA_HOME/webapps/host-manager/newname.xml به ${catalina.home}/webapps/new-name تغییر دهید.

۳. $CATALINA_HOME/webapps/manager را به $CATALINA_HOME/webapps/newname منتقل نمایید.

```
# mv $CATALINA_HOME/webapps/manager $CATALINA_HOME/webapps/new-name
```

SCWS-10-6: فعال نمودن محدودیت پذیرش servlet

شرح اجمالی:

STRICT_SERVLET_COMPLIANCE به چند روش بر رفتار و عملکرد Tomcat تاثیر می‌گذارد. لذا توصیه می‌شود مقدار STRICT_SERVLET_COMPLIANCE به true تنظیم گردد.

نحوه پیاده‌سازی:

Tomcat را با محدودیت پذیرش فعال کنید و موارد زیر را به اسکریپت راه‌انداز خود اضافه نمایید.

```
-Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true
```

SCWS-10-7: خاموش نمودن نشست façade recycling

شرح اجمالی:

در صورتی که façade جدید برای هر درخواست ایجاد شود، می‌توان RECYCLE_FACADES را مشخص کرد. ولی در صورتی که façade جدید ایجاد نشود، احتمال نشت اطلاعات از نشست‌های دیگر وجود خواهد داشت.

نحوه پیاده‌سازی:

Tomcat را با تنظیم RECYCLE_FACADES به true اجرا کرده و موارد زیر را به اسکریپت راه‌انداز خود اضافه نمایید.

```
-Dorg.apache.catalina.connector.RECYCLE_FACADES=true
```

SCWS-10-8: نپذیرفتن جداکننده‌های مسیر اضافی

شرح اجمالی:

فعال بودن قابلیت مجزاسازی مسیرهای مختلف در Tomcat این امکان را ایجاد می‌کند که یک مهاجم بتواند به برنامه‌هایی که قبلا توسط یک پروکسی مانند mod-proxy بلاک شده بودند، دسترسی یابد.

نحوه پیاده‌سازی:

Tomcat را با تنظیم ALLOW_BACKSLASH و ALLOW_ENCODED_SLASH به false اجرا کنید.

```
-Dorg.apache.catalina.connector.CoyoteAdapter.ALLOW_BACKSLASH=false
-Dorg.apache.Tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=false
```

SCWS-10-9: نپذیرفتن پیام‌های وضعیت هدر سفارشی

شرح اجمالی:

فعال بودن وضعیت هدر سفارشی موجب بروز حملات تزریق (injecte) می‌گردد. اگر پیام‌هایی با هدر سفارشی مورد نیاز باشند، مطمئن شوید که فقط US-ASCII هستند و شامل هیچ داده‌ی تامین شده توسط کاربر نمی‌شوند.

نحوه پیاده‌سازی:

Tomcat را با تنظیم USE_CUSTOM_STATUS_MSG_IN_HEADER به false اجرا کرده و موارد زیر را به اسکریپت راه‌انداز خود اضافه نمایید.

```
-Dorg.apache.coyote.USE_CUSTOM_STATUS_MSG_IN_HEADER=false
```

SCWS-10-10: پیکربندی connectionTimeout

شرح اجمالی:

تنظیم connectionTimeout، این امکان را برای Tomcat فراهم می‌کند که سوکت‌ها را پس از یک زمان معین ببندد تا منابع سیستم محفوظ بماند.

نحوه پیاده‌سازی:

اطمینان حاصل کنید که تنظیمات connectionTimeout در $CATALINA_HOME/conf/server.xml پیکربندی و براساس منابع سخت‌افزاری، بارگذاری و تعداد اتصالات همزمان بهینه شده است

```
connectionTimeout="60000"
```

SCWS-10-11: پیکربندی maxHttpHeaderSize

شرح اجمالی:

MaxHttpHeaderSize اندازه‌ی درخواست و پاسخ هدرهای تعریف شده را به‌صورت بایت محدود می‌کند. لذا درصورتی که تعیین نشده باشد، به‌صورت پیش‌فرض ۸۱۹۲ بایت است.

نحوه پیاده‌سازی:

از اینکه maxHttpHeaderSize در $CATALINA_HOME/conf/server.xml برای هر اتصال به‌طور مناسبی پیکربندی شده است، اطمینان حاصل نمایید.

```
maxHttpHeaderSize=”8192”
```

SCWS-10-12: ملزم نمودن استفاده از SSL برای همه‌ی برنامه‌ها

شرح اجمالی:

از ویژگی transport-guarantee به منظور اطمینان از مصون ماندن SSL هنگام دسترسی به همه برنامه‌ها استفاده نمایید. حتی در پیکربندی نرم‌افزار می‌توان آن را برای هر برنامه کاربردی غیر فعال کرد.

نحوه پیاده‌سازی:

در $CATALINA_HOME/conf/web.xml موارد زیر را تنظیم نمایید:

```
<user-data-constraint>
  <transport-guarantee>CONFIDENTIAL</transport-guarantee>
 <user-data-constraint>
```

SCWS-10-13: نپذیرفتن لینک‌گذاری نمادین

شرح اجمالی:

لینک‌های نمادین به یک برنامه اجازه می‌دهند که کتابخانه‌های برنامه دیگر را دربرگیرند. این کار امکان استفاده مجدد از کدها را فراهم می‌کند اما هنگامی که برنامه‌ها شامل کتابخانه‌ی برنامه دیگری باشد، مشکلات امنیتی بالقوه‌ای ایجاد می‌گردد. پس آن‌ها نباید به لینک نمادین دسترسی داشته باشند.

نحوه پیاده‌سازی:

در همه context.xml، ویژگی allowLinking را به false تنظیم نمایید.

```
<Context ... allowLinking=”false” />
```

SCWS-10-14: عدم اجرای برنامه‌ها به‌صورت privilege

شرح اجمالی:

تنظیمات مربوط به privilege یک برنامه بجای اشتراک گذاری class loader یک برنامه، آن را به class loader سرور تغییر می‌دهد.

نحوه پیاده‌سازی:

در همه context.xml، ویژگی privileged را به false تغییر دهید مگر برنامه‌هایی مانند برنامه مدیریت که به آن ویژگی نیاز دارد.

```
<Context ... privileged=”false” />
```

SCWS-10-15: نپذیرفتن درخواست‌های cross context

شرح اجمالی:

True بودن مقدار crossContext اجازه می‌دهد که یک نرم‌افزار، ServletConext.getContext را فراخوانی نموده تا بدین ترتیب امکان ارجاع و بازگشت برای نرم‌افزار دیگر مهیا گردد.

نحوه پیاده‌سازی:

در همه context.xml، ویژگی crossContext را به false تغییر دهید.

```
<Context ... crossContext=”false” />
```

SCWS-10-16: عدم لاگ‌گیری از درخواست ردگیری هاست‌ها

شرح اجمالی:

در صورتی که مقدار enableLookups در درخواست‌های DNS look-up قبل از لاگ‌گیری اطلاعات به True تنظیم شده باشد، باعث سربار می‌شود.

نحوه پیاده‌سازی:

در connector elements ویژگی enableLookups را به false تغییر دهید یا آن را حذف نمایید.

```
<Connector ... enableLookups="false" />
```

SCWS-10-17: فعال نمودن memory leak listener

شرح اجمالی:

قابلیت جلوگیری از نشت حافظه JRE در listener راه حلی برای محل‌های شناخته شده‌ای است که در JRE برای بارگذاری singleton در context class loader استفاده می‌شده و درصورتی که یک class loader در نرم‌افزار وب به عنوان یک context class loader به صورت همزمان استفاده گردد، منجر به نشت حافظه خواهد شد. راهکار این است که این singleton را زمانی مورد استفاده قرار دهیم که این listener به عنوان یک کلاس عمومی در Tomcat شروع بکار نماید و همزمان به صورت context class loader نیز عمل نماید.

این راهکار همچنین برای مشکلات شناخته شده که در اثر قفل شدن فایل‌های JAR وجود دارد استفاده می‌گردد.

نحوه پیاده‌سازی:

JRE Memory Leak Prevention Listener را در $CATALINA_HOME/conf/server.xml از حالت کامنت خارج نمایید.

```
<Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
```

SCWS-10-18: تنظیم چرخه حیات شنودگر امنیتی

شرح اجمالی:

زمانی که Tomcat اجرا می‌شود، امنیت چرخه‌حیات listener یک چک لیست امنیتی را انجام می‌دهد و در صورت رد این چک لیست، از اجرای Tomcat جلوگیری می‌گردد.

نحوه پیاده‌سازی:

برای فعال کردن آن می‌بایست قابلیت listener را در $CATALINA_BASE/conf/server.xml از حالت کامنت خارج نمود. اگر سیستم عامل از قابلیت umask پشتیبانی می‌کند، می‌بایست در $CATALINA_HOME/bin/catalina.sh قابلیت umask را نیز از حالت کامنت خارج کرد.

در داخل سرور عناصر ذیل اضافه گردد:

CheckedOsUsers: کاربران سیستم عامل توسط یک کاما از هم جدا شوند تا در اجرای Tomcat استفاده نگردد. اگر این چنین نیست، به‌طور پیش‌فرض از root استفاده می‌شود.

MinimumUmask: باید قبل از اجرای Tomcat محدودیت umask پیکربندی گردد. در غیر این صورت به‌طور پیش‌فرض 0007 استفاده می‌گردد.

```
<Listener className="org.apache.catalina.security.SecurityListener"
checkedOsUsers="alex,bob" minimumUmask="0007" />
```

SCWS-10-19: استفاده از logEffectiveWebXml و metadata-complete برای استقرار نرم‌افراز در محصول

شرح اجمالی:

هر دو مورد قطعه بندی (Fragment) و حاشیه نویسی (Annotation) منجر به افزایش نگرانی‌های امنیتی می‌شود. Web.xml حاوی یک المان به نام web-app است که خود دارای یک صفت (Attribute) به نام Metadata-Complete می‌باشد. المان نام برده دارای مقادیر داده‌ای باینری است که بیانگر متا دیتای سایر منابع نیز می‌شود و می‌بایست در زمان deploy نمودن برنامه کاربردی تحت وب، مورد توجه قرار گیرند. این منابع شامل حاشیه نویسی و یادداشت بر روی فایل‌های کلاس (@WebServlet، همچنین @WebListener، @WebFilter و ...) و web-fragment.xml همانند کلاس‌های موجود در WEB-INF/classes می‌باشد. همچنین با لاگ‌گیری، شما قادر خواهید بود آن را بررسی کنید و متوجه شوید واقعا چه می‌خواهید.

نحوه پیاده‌سازی:

- برای همه برنامه‌ها مقدار metadata-complete در web.xml را true کنید. زمانی که نرم‌افراز وب مستقر می‌شود، web.xml شامل یک metadata-complete در نرم‌افراز وب است که مقداری باینری دارد تا دیگر منابع متادیتا در نظر گرفته شود و شامل حاشیه نویسی و یادداشت بروی فایل‌های کلاس (@WebServlet, but also @WebListener, @WebFilter, ...) و web-fragment.xml مانند کلاس‌های واقع در WEB-INF/classes، می‌باشد. اگر مقدار true باشد، همه این‌ها نادیده گرفته می‌شود و web.xml فقط متادیتا را در نظر می‌گیرد.

توجه: گزینه metadata-complete برای غیرفعال کردن اسکن همه حاشیه نویسی‌ها و یادداشت‌ها کافی نیست. اگر ServletContainerInitializer با حاشیه نویسی @HandlesTypes وجود داشته باشد، Tomcat برنامه شما را برای کلاس‌هایی که از حاشیه نویسی و یا رابط‌های مشخص شده در حاشیه نویسی استفاده می‌کند، اسکن می‌نماید.

- برای همه برنامه‌ها مقدار logEffectiveWebXml را در context.xml به true تنظیم کنید.

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 پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCWS-1		حذف منابع غیراصلی			
SCWS-1-1		حذف فایل‌ها و دایرکتوری‌ها غیراصلی		بسته به روش نصب، منابع غیراصلی پیش‌فرض متفاوت خواهد بود.	حذف فایل‌ها و دایرکتوری‌های غیراصلی
SCWS-1-2		غیر فعال نمودن اتصالات استفاده نشده		A non-SSL Connector bound to port 8080 An AJP 1.3 Connector bound to port 8009	غیر فعال نمودن اتصالات استفاده نشده
SCWS-2		محدود کردن نشت اطلاعات مربوط به پلتفرم سرور			
SCWS-2-1		تغییر محتویات فایل server.info		Apache Tomcat/.. به عنوان مثال: Apache Tomcat/7.0	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-2-2		تغییر بنر فایل server.number		دارای ۴ بخش شماره نسخه همانند 5.5.20.0	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-2-3		تغییر بنر server.built Data		همانند Jul 8 2008 11:40:35	مطابق نحوه پیاده‌سازی اجرا گردد.

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCWS-2-4		غیر فعال نمودن X-Powered-By از هدر HTTP و تغییر نام سرور برای تمام اتصالات		false	false
SCWS-2-5		غیر فعال نمودن Stack Traces کاربر		ارائه اطلاعات debug به صورت پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-2-6		خاموش کردن TRACE		false	false
SCWS-3		**محافظت از پورت Shutdown**			
SCWS-3-1		نامعین کردن مقدار Shutdown		SHUTDOWN	مقدار NONDETERMINISTICVALUE به SHUTDOWN
SCWS-3-2		غیرفعال نمودن پورت Shutdown		پورت Shutdown بر روی TCP پورت 8005 فعال می‌باشد.	۱-
SCWS-4		**محافظت از تنظیمات Tomcat**			
SCWS-4-1		محدود نمودن دسترسی به CATALINA_HOME$		ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-4-2		محدود نمودن دسترسی CATALINA_BASE$		ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-4-3		محدود نمودن دسترسی به دایرکتوری پیکربندی Tomcat		مجوز پیش‌فرض ۷۷۰	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-4-4		محدودیت در دسترسی به دایرکتوری لاگ‌ها در Tomcat		مجوز پیش‌فرض ۷۷۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه
SCWS-4-5		محدودیت در دسترسی به پوشه‌های موقت Tomcat		مجوز پیش‌فرض ۷۷۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه
SCWS-4-6		محدود نمودن دسترسی به دایرکتوری باینری Tomcat		مجوز پیش‌فرض ۷۷۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه
SCWS-4-7		محدودیت در دسترسی به دایرکتوری اپلیکیشن وب Tomcat		مجوز پیش‌فرض ۷۷۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCWS-4-8		محدود نمودن دسترسی به catalina.policy در Tomcat		مجوز پیش‌فرض ۶۰۰	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-4-9		محدود نمودن دسترسی به catalina.properties در Tomcat		مجوز پیش‌فرض ۶۰۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه حذف مجوز نوشتن برای گروه
SCWS-4-10		محدود نمودن دسترسی به context.xml در Tomcat		مجوز پیش‌فرض ۶۰۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه حذف مجوز نوشتن برای گروه
SCWS-4-11		محدود نمودن دسترسی به logging.properties در Tomcat		مجوز پیش‌فرض ۶۰۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه حذف مجوز نوشتن برای گروه
SCWS-4-12		محدود نمودن دسترسی به server.xml در Tomcat		مجوز پیش‌فرض ۶۰۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه حذف مجوز نوشتن برای گروه
SCWS-4-13		محدود نمودن دسترسی به Tomcat-users.xml در Tomcat		مجوز پیش‌فرض ۶۰۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه حذف مجوز نوشتن برای گروه
SCWS-4-14		محدود نمودن دسترسی به web.xml در Tomcat		مجوز پیش‌فرض ۴۰۰	حذف مجوزهای خواندن، نوشتن و اجرا برای همه حذف مجوز نوشتن برای گروه
SCWS-5		**پیکربندی حوزه‌ها**			
SCWS-5-1		استفاده از حوزه‌های امن		ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-5-2		استفاده از Realms lockout		ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCWS-6		امنیت اتصال (Connector Security)			
SCWS-6-1		تنظیم احراز هویت Client-cert		پیکربندی نشده است.	true
SCWS-6-2		اطمینان از True بودن مقدار SSLEnable برای اتصالات حساس		false	true
SCWS-6-3		اطمینان از تنظیم دقیق طرح (scheme)		http	http برای اتصالات http https برای اتصلات https
SCWS-6-4		اطمینان از اینکه secure بر روی مقدار True و فقط برای اتصالات SSL-Enabled تنظیم شده است.		false	true
SCWS-6-5		اطمینان از تنظیم TLS در پروتکل SSL برای اتصالات ایمن		TLS	TLS
SCWS-7		ایجاد و حفاظت از لاگ‌ها			
SCWS-7-1		نرم‌افزار مخصوص لاگ‌گیری		پیکربندی نشده است.	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-7-2		تعیین فایل مدیریت کننده در logging.properties		عدم وجود مقدار پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-7-3		اطمینان از تنظیم صحیح className در context.xml		عدم ایجاد به‌صورت پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-7-4		اطمینان از امن بودن آدرس در context.xml		عدم ایجاد به‌صورت پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-7-5		اطمینان از تنظیم درستی الگو در context.xml		عدم ایجاد به‌صورت پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-7-6		اطمینان امن بودن دایرکتوری logging.properties		دایرکتوری $CATALINA_BASE/logs	مطابق نحوه پیاده‌سازی اجرا گردد.

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCWS-7-7		تنظیم اندازه فایل لاگ		عدم وجود محدودیت	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-8		پیکربندی سیاست Catalina			
SCWS-8-1		محدودیت دسترسی زمان اجرا برای پکیج‌های حساس		مطابق بند ۱ از توضیحات پیش‌فرض جدول	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-9		استقرار برنامه			
SCWS-9-1		شروع Tomcat با مدیریت امنیتی		عدم بکارگیری - security	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-9-2		غیر فعال کردن خود استقراری برنامه‌ها		true	false
SCWS-9-3		غیرفعال کردن استقرار در شروع برنامه‌ها		true	false
SCWS-10		دیگر تنظیمات پیکربندی			
SCWS-10-1		اطمینان از قرارگیری دایرکتوری محتوای وب در بخش جداگانه‌ای از فایل‌های سیستمی Tomcat		عدم قابلیت اجرا	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-10-2		محدود نمودن دسترسی به دایرکتوری مدیریت وب		عدم وجود پیکربندی پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-10-3		محدودسازی برنامه‌های مدیریتی		عدم وجود تنظیمات نحوه پیاده‌سازی	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-10-4		هنگام دسترسی به برنامه‌ی مدیریتی، SSL را اجباری کنید.		عدم وجود پیکربندی پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-10-5		تغییر نام برنامه مدیریت		manager	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-10-6		فعال نمودن محدودیت پذیرش servlet		عدم وجود پیکربندی پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی	مقدار پیش‌فرض	مقدار مطلوب
SCWS-10-7		خاموش نمودن نشست façade recycling		false	true
SCWS-10-8		نپذیرفتن جداکننده‌های مسیر اضافی		false	false
SCWS-10-9		نپذیرفتن پیام‌های وضعیت هدر سفارشی		false	false
SCWS-10-10		پیکربندی connectionTimeout		۶۰۰۰۰	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-10-11		پیکربندی maxHttpHeaderSize		۸۱۹۲	۸۱۹۲
SCWS-10-12		ملزم نمودن استفاده از SSL برای همه‌ی برنامه‌ها		عدم وجود پیکربندی پیش‌فرض	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-10-13		نپذیرفتن لینک‌گذاری نمادین		false	false
SCWS-10-14		عدم اجرای برنامه‌ها به‌صورت privilege		false	false
SCWS-10-15		نپذیرفتن درخواست‌های cross context		false	false
SCWS-10-16		عدم لاگ‌گیری از درخواست ردگیری هاست‌ها		DNS lookups غیرفعال می‌باشد.	false
SCWS-10-17		فعال نمودن memory leak listener		ندارد	خارج کردن JRE Memory Leak Prevention Listener از حالت کامنت
SCWS-10-18		تنظیم امنیت چرخه شنود		۰۰۰۷	مطابق نحوه پیاده‌سازی اجرا گردد.
SCWS-10-19		استفاده از logEffectiveWebXml و metadata-complete برای استقرار نرم‌افزار در محصول		false	مطابق نحوه پیاده‌سازی اجرا گردد.

توضیحات مقادیر پیش‌فرض جدول:

۱. SCWS-8-1: بطور پیش‌فرض مقدار package.access در $CATALINA_BASE/conf/catalina.properties به صورت زیر می‌باشد.

```
package.access = sun., org.apache.catalina., org.apache.coyote.,org.apache.Tomcat., org.apache.jasper
```