WEB GÜVENLİK TOPLULUĞU[4]

Apache Tomcat Güvenliği

Güvenlik Denetim Kılavuzu v1.1

Bedirhan Urgun

08/02/2009

Bu doküman, Linux sistemler üzerinde koşan Apache Tomcat kısmi J2EE container'ının güvenlik denetim adımlarını içerir. Dokümandaki bilgilerin bir bölümü OWASP[1], CIS[2], IASE[3] sitelerinde bulunan değerlendirme verilerinden oluşmaktadır. Daha detaylı bilgi için: ***www.webguvenligi.org***

GİRİŞ

Apache Tomcat[5], Apache Software Foundation[6]'ın Java Servlet[7] ve JavaServer Pages[8] teknolojilerinin gerçeklendiği açık kaynak kodlu temel bir J2EE container'ıdır. Yakın zamanda yapılmış araştırmalara göre geliştiricilerin %64'ü Tomcat sunucusunu seçmektedir[9]. Sonuçları çok kesin olmamakla beraber NetCraft raporları da Apache Tomcat'in üretim ortamlarında da kullanılan popüler temel bir uygulama sunucu olduğunu göstermektedir[10].

Bu doküman, kontroller diğer işletim sistemlerine de uygulanabilse de, Linux sistemler üzerinde koşan Apache Tomcat kısmi J2EE container'ının güvenlik denetim adımlarını tanımlamaya yönelik bir çalışmadır. Doküman adım adım kontrolleri detaylı anlatsa da, bu değerlendirme prosedürü açık kaynak kodlu otomatik bir araçla da desteklenecektir.

Doküman hakkında bütün görüşleriniz için; Bedirhan Urgun, urgunb@hotmail.com

1.1 FORMAT

Her kontrol adımı üç bölümden oluşmaktadır; testin amacı, teknik adımları ve beklenen sonucu. Dokümanda kullanılan formatlar aşağıda belirtilmiştir;

Kalın fontlar dikkat çekilmek istenen bilgileri belirtmektedir.

İtalik fontlar teknik terimleri ve kısa notları belirtmektedir.

`Komutlar ve çıktıları` çalıştırılması ve/veya aranması gereken yapıları belirtmektedir.

1.2 REFERANSLAR

[1] http://www.owasp.org/index.php/Securing_tomcat

[2] CIS_TomCat_Benchmark_v1.0 (tomcat-benchmark@lists.cisecurity.org e-posta listesi)

[3] http://iase.disa.mil/stigs/checklist/web_srr_checklist_tomcat_v6r1-3.zip

[4] http://www.webguvenligi.org

[5] http://tomcat.apache.org

[6] http://www.apache.org

[7] http://java.sun.com/products/servlets

[8] http://java.sun.com/products/jsp

[9] http://www.infoq.com/news/2007/12/tomcat-favorite-container

[10] http://survey.netcraft.com/Reports/200810/

1.3 TEŞEKKÜR

Dokümanın, alternatif adımlarla daha kullanışlı ve düzeltmelerle daha hatasız olmasında katkısı olan Gökhan Alkan'a (www.gokhanalkan.net) teşekkürler.

1.4 DEĞİŞİKLİLER

02.Aralık.2008: KOŞAN KULLANICI HAKLARI TESTİ adımının geliştirilmesi

08.Aralık.2008: 9. KAYIT İŞLEMİ VARLIĞI TESTİ adımının geliştirilmesi ($CATALINA_HOME/lib ve $CATALINA_HOME/common/classes)

09.Aralık.2008: VERSİYON BİLGİSİ TESTİ adımında ps komutu parametre değişiklikleri (ps -ef) ve CATALINA_HOME çevresel değişkenin alternatif bulunma yöntemlerinin (-Dcatalina.home=) eklenmesi

10.Aralık.2008: GEREKSİZ DOSYALAR/DİZİNLERİN VARLIĞI TESTİ adımında work dizini altındaki gereksiz olarak düşünülen dizinler de eklenmiştir.

11.Aralık.2008: VERSİYON BİLGİSİ SIZDIRMA TESTİ adımında unzip komut alternatifi getirilmiştir.

12.Aralık.2008: DOSYA HAKLARI TESTİ adımında standardlara daha uygun alternatif bir yol gösterilmiştir.

İÇİNDEKİLER

1. VERSİYON BİLGİSİ TESTİ

1.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat sunucusu ve bu sunucunun kullandığı Java platformunun en son kararlı sürümlerinin kullanıp kullanılmadığının anlaşılmasıdır.

1.2 TEST ADIMLARI

Sisteme root kullanıcısı olarak girilip, Tomcat servisinin sistem üzerinde hangi kullanıcı ile koşulduğu anlaşılmalıdır.

```
[root@sys ~]# ps -ef | grep "org.apache.catalina.startup.Bootstrap" | grep -v
grep

root        2774      1   0 Oct25 ?          00:02:46 /usr/java/jdk/bin/java -
Dcatalina.base=/opt/tomcat             -Dcatalina.home=/opt/tomcat             …
org.apache.catalina.startup.Bootstrap start
```

Kullanıcı ismi bulunduktan sonra, Tomcat servisinin home dizini bulunmalıdır.

```
[root@sys ~]# echo $CATALINA_HOME

/opt/tomcat
```

Yukarıdaki çevresel değişken boş değer dönerse ilk gösterilen ps komutu çıktısındaki –Dcatalina.home parametresinin değerinden de Tomcat servisinin ev dizini bulunabilir.

```
[root@sys ~]# ps -ef | grep "org.apache.catalina.startup.Bootstrap" | grep -v
grep

root        2774      1   0 Oct25 ?          00:02:46 /usr/java/jdk/bin/java -
Dcatalina.base=/opt/tomcat             -Dcatalina.home=/opt/tomcat             …
org.apache.catalina.startup.Bootstrap start
```

Dizin bulunduktan sonra, Apache Tomcat servisinin ve kullandığı Java platformu versiyonu bulunabilir.

```
[root@sys bin]# cd /opt/tomcat/bin

[root@sys bin]# /bin/bash ./version.sh

…

Server version: Apache Tomcat/5.5.25

…

JVM Version:    1.6.0_07-b06
```

```
JVM Vendor:     Sun Microsystems Inc.
```

1.3 TEST SONUCU

Hem Tomcat hem de Java ürün versiyonlarında son iki rakam bugfix açısından önemlidir (Tomcat/5.5.**25** ve 1.6.0_**07**). Bu rakamın yayınlanmış en son ürün ile aynı olması gerekmektedir.

2. KOŞAN KULLANICI HAKLARI TESTİ

2.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisini koşan kullanıcının haklarının, minimum hak prensibine uygun olup olmadığının anlaşılmasıdır.

2.2 TEST ADIMLARI

Sisteme root kullanıcısı olarak girilip, Tomcat servisinin sistem üzerinde hangi kullanıcı ile koşulduğu anlaşılmalıdır (Bknz. VERSİYON BİLGİSİ TESTİ). Koşan kullanıcı bulunduktan sonra bu kullanıcının sahip olduğu ID bulunmalıdır.

```
[root@sys bin]# cat /etc/passwd | grep tomcat

tomcat:x:200:201:tomcat:/home/tomcat:/bin/bash
```

2.3 TEST SONUCU

Tomcat servisini koşan kullanıcının ID'si 500 (/etc/login.defs) ve üzeri ise yüksek haklara sahip bir kullanıcı olmadığı anlaşılır.

3. DİZİN LİSTELEME ÖZELLİĞİ TESTİ

3.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin dizin içeriği listeleme özelliğinin kapalı olup olmadığını anlamaktır.

3.2 TEST ADIMLARI

Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ), conf/web.xml dosyası içerisinde bulunan, *listings* değerini içeren *param-name* elementinin eşlenik *param-value* element değeri kontrol edilmelidir.

```
…
   <init-param>
     <param-name>listings</param-name>
     <param-value>false</param-value>
   </init-param>
…
```

3.3 TEST SONUCU

Tomcat servisinin dizin içeriği listeleme özelliğinin (*listings* ⇔ *false*) kapalı olması gerekmektedir.

4. GEREKSİZ DOSYALAR/DİZİNLERİN VARLIĞI TESTİ

4.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinde güvenlik problemleri yaratabilecek gereksiz dizin ve/veya dosyalardan arındırılmış olup olmadığını kontrol etmektir.

4.2 TEST ADIMLARI

Sistem üzerinde Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ), aşağıdaki dosya ve dizinlerin varlığı kontrol edilmelidir.

```
$CATALINA_HOME/webapps/ROOT

$CATALINA_HOME/webapps/balancer

$CATALINA_HOME/webapps/jsp-examples

$CATALINA_HOME/webapps/servlet-examples

$CATALINA_HOME/webapps/tomcat-docs

$CATALINA_HOME/webapps/webdav

$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

$CATALINA_HOME/work/Catalina/localhost/docs

$CATALINA_HOME/work/Catalina/localhost/examples

$CATALINA_HOME/work/Catalina/localhost/host-manager

$CATALINA_HOME/work/Catalina/localhost/manager
```

Not: Bu dizinlerin ve dosyaları silmeden önce yedeğini almalısınız.

Bu dizinler ve dosyalar sistemden silindikten sonra tomcat yeniden çalıştırılmalıdır.

4.3 TEST SONUCU

Tomcat kurulumu ile gelen örnek ve kullanılmayan uygulamalar saldırı yüzeyini küçültmek için sistem üzerinde bulunmamalıdırlar.

5. VERSİYON BİLGİSİ SIZDIRMA TESTİ

5.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin HTTP/S cevaplarında HTTP başlıklarında veya hata sayfalarında detaylı versiyon bilgisi sızdırıp sızdırmadığını kontrol etmektir.

5.2 TEST ADIMLARI

Sistem üzerinde Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ), üretilen HTTP hata sayfalarında gösterilen versiyon bilgisini görebilmek için aşağıdaki adımlar $CATALINA_HOME/server/lib/catalina.jar dosyası üzerinde uygulanır.

```
[root@sys tomcat]# cd $CATALINA_HOME/server/lib/

[root@sys lib]# jar xf catalina.jar org/apache/catalina/util/ServerInfo.properties

[root@sys lib]# cat org/apache/catalina/util/ServerInfo.properties

server.info=Apache Tomcat/5.5.25

server.number=5.5.25.0

server.built=Aug 24 2007 05:33:50
```

Eğer sistemde jar komutu yoksa unzip komutunu da kullanılabilir.

```
[root@sys tomcat]# cd $CATALINA_HOME/server/lib/

[root@sys lib]# unzip -q catalina.jar –d /tmp

[root@sys lib]# cat /tmp/org/apache/catalina/util/ServerInfo.properties

server.info=Apache Tomcat/5.5.25

server.number=5.5.25.0

server.built=Aug 24 2007 05:33:50
```

Sunucuya yapılan HTTP isteklerine dönen cevaplarda bulunan HTTP başlıklarındaki detaylı versiyon bilgisinin başka bir bilgi ile değiştirilip değiştirilmediğini görmek için *server* attribute'u $CATALINA_HOME/conf/server.xml dosyası içinde *Connector* elementi içinde aranır.

```
<Connector port="8080" … redirectPort="8443"

server="Apoche"/>

…

<Connector port="8443" … clientAuth="false" sslProtocol="TLS" server="Apoche" />
```

…

5.3 TEST SONUCU

HTTP hata sayfalarında detaylı sunucu versiyonunun gözükmemesi için *ServerInfo.properties* dosyasındaki *server.info* parametresinin değeri, detaylı sunucu versiyon bilgisinden farklı olmalıdır.

HTTP başlıklarındaki detaylı versiyon bilgisinin gözükmemesi için *Connector* elementinin *server* attribute'u etkin olmalıdır.

6. VARSAYILI HATA SAYFASI TESTİ

6.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin detaylı uygulama çatısı hata mesajlarının (stacktrace) bilmesi gereken prensibine göre sistem genelinde varsayılı özel bir hata sayfası ile değiştirilip değiştirilmediğini anlamaktır.

6.2 TEST ADIMLARI

Sistem üzerinde Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ), sunucu genelinde kullanıcılara detaylı hata mesajları gönderilmesini engelleyici yapıların olup olmadığı $CATALINA_HOME/conf/web.xml dosyasında aşağıdaki gibi element yapısı aranarak anlaşılır.

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

6.3 TEST SONUCU

Son kullanıcılara detaylı hata mesajları (stacktrace) gönderilmesini engellemek amacı $CATALINA_HOME/conf/web.xml dosyasında *error-page* direktiflerinin kullanılması gerekmektedir.

7. VARSAYILI SİSTEM DURDURMA PORTU VE ŞİFRESİ TESTİ

7.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin yerel adresten dinlediği durdurma portunun ve şifresinin herkes tarafından bilinen varsayılı değerler (8005 ve SHUTDOWN) olup olmadığını anlamaktır.

7.2 TEST ADIMLARI

Sistem üzerinde Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ), sunucu durdurma işlemi için kullanılan varsayılı port ve şifrenin değiştirilip değiştirilmediğini görmek için $CATALINA_HOME/conf/server.xml dosyası içinde port attribute'unun 8080 ve shutdown attribute'unun "SHUTDOWN" olup olmadığı kontrol edilir.

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

7.3 TEST SONUCU

Lokal adresten dinleyen durdurma servisinin daha da güvenli hale getirilmesi için, port attribute'unun 8080'den farklı (veya bu portu kapatmak için -1) ve shutdown attribute'unun "SHUTDOWN"'dan farklı olması gerekmektedir.

8. ADMIN VE MANAGER UYGULAMALARI IP KISITLAMA TESTİ

8.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin bilinen sunucu yapılandırma dosyaları kullanılarak kullanılıyorsa admin ve manager uygulamalarına IP kısıtlama yöntemi kimlik doğrulama/yetkilendirme işlemleri uygulanıp, uygulanmadığının anlaşılmasıdır.

8.2 TEST ADIMLARI

Sistem üzerinde Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ);

admin uygulaması için $CATALINA_HOME/conf/Catalina/localhost/admin.xml veya $CATALINA_HOME/webapps/host-manager/admin.xml dosyasında aşağıdaki xml elementinin yorum halinde bulunmadığı (yani <!-- --> karakter dizgileri içinde olmadıkları) kontrol edilmelidir.

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

manager uygulaması için $CATALINA_HOME/conf/Catalina/localhost/manager.xml veya $CATALINA_HOME/webapps/host-manager/manager.xml dosyasında aşağıdaki xml elementinin yorum halinde bulunmadığı kontrol edilmelidir.

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

Not: Allow parametresi içindeki IP farklı olabilir.

8.3 TEST SONUCU

Sistem üzerinde admin ve/veya manager uygulamaları kullanılmakta ise bu IP kısıtlamalarının ilgili yapılandırma dosyaları kullanılarak yapılması gerekmektedir. (Güvenlik sıkılaştırması adına yapılabilecek bir adım olarak) uygulama isimleri değiştirilmiş ise aynı isimde xml dosyaları kontrol edilmelidir.

9. KAYIT İŞLEMİ VARLIĞI TESTİ

9.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin ve yüklenmiş web uygulamalarının kayıt tutma politikalarının varlığını ve işlerliğini anlamaktır.

9.2 TEST ADIMLARI

Sistem üzerinde Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ) $CATALINA_HOME/logs dizini içinde;

```
catalina.YYYY-MM-DD.log

catalina.out
```

dosyalarının var olup olmadığı araştırılır. Ayrıca sistemdeki uygulamaların kayıt tutma özelliklerinin var olup olmadığını araştırmak için, genellikle uygulamaların yer aldığı

```
$CATALINA_HOME/webapps/[APP_NAME]/WEB-INF/classes
```

veya (tomcat 5.5)

```
$CATALINA_HOME/common/classes
```

veya (tomcat 6.x)

```
$CATALINA_HOME/lib
```

dizinleri içerisindeki *logging.properties* veya *log4j.properties* dosyalarının varlığı araştırılır.

Not: [APP_NAME], uygulamanın context ismi olup farklılık gösterebilir.

9.3 TEST SONUCU

$CATALINA_HOME/logs dizini içinde yer alana varsayılı Tomcat kayıt dosyalarının yanında uygulamaların da kayıtlarını almış olmaları önerilmektedir.

10. SSL KULLANIMI TESTİ

10.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin web uygulamaları için SSL desteği ile yapılandırılıp, yapılandırılmadığını anlamaktır.

10.2 TEST ADIMLARI

Sistem üzerinde Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ) $CATALINA_HOME/conf/server.xml dosyası içerisinde

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
     port="8443" keypass="xyz" scheme="https" …
     secure="true" clientAuth="false" sslProtocol="TLS"
/>
```

elementine benzer yapılandırma bölümlerinin varlığı (<!-- --> yorum elementleri dışında) araştırılmalıdır.

10.3 TEST SONUCU

Apache Tomcat servisinin veri gizliliğini koruması için gerçekleştirmesi gereken adımlardan biri olan SSL desteğinin $CATALINA_HOME/conf/server.xml dosyası içerisinde açık olması gerekmektedir.

11. JAVA SECURITY MANAGER TESTİ

11.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin üzerinde koşan uygulamalara Java güvenlik politikası yapılandırması ile kısıtlamalar getirip, getirmediğini anlamaktır.

11.2 TEST ADIMLARI

Sisteme root kullanıcısı olarak girilip, Tomcat servisinin java security manager ile çalıştırılıp çalıştırılmadığı anlamak için

```
[root@sys ~]# ps -ef | grep "org.apache.catalina.startup.Bootstrap" | grep -v grep

root        2774       1   0 Oct25 ?           00:02:46 /usr/java/jdk/bin/java -Dcatalina.base=/opt/tomcat      -Dcatalina.home=/opt/tomcat      -security      … org.apache.catalina.startup.Bootstrap start
```

komutunun sonucunda *-security* opsiyonunun kullanılıp kullanılmadığı anlaşılmalıdır. Bazı sistemlerde aynı komutun çalıştırılması sonucu aşağıdaki gibi bir çıktı da alınabilir.

```
[root@sys ~]# ps -ef | grep "org.apache.catalina.startup.Bootstrap" | grep -v grep

tomcat    19630      1   7 15:13 pts/2    00:00:01 /usr/java/jre1.6.0_10/bin/java … -Djava.security.manager -Djava.security.policy==/opt/apache-tomcat-6.0.18-secure/conf/catalina.policy -Dcatalina.base=/opt/apache-tomcat-6.0.18-secure -Dcatalina.home=/opt/apache-tomcat-6.0.18-secure … org.apache.catalina.startup.Bootstrap start
```

Bu çıktı da *-Djava.security.manager* olması sunucunun java security manager ile çalıştırıldığını göstermektedir.

11.3 TEST SONUCU

Java Security manager koşan web uygulamalarının sistem üzerinde elde ettikleri hakları kısıtlamaya yardımcı olan bir Java teknolojisidir. Java Security manager kurulu bir tomcat servisi *-security* sekmesi ile başlatılmış olmalıdır.

12. DOSYA HAKLARI TESTİ

12.1 TEST AMACI

Bu test adımında amaç, sistemde kurulu Apache Tomcat servisinin dosya haklarının bilmesi gereken prensibine göre ayarlanıp ayarlanmadığını anlaşılmasıdır.

12.2 TEST ADIMLARI

Tomcat servisinin home dizini bulunduktan sonra (Bknz. VERSİYON BİLGİSİ TESTİ), $CATALINA_HOME dizini altındaki bütün dosya ve dizin sahipliğinin düşük haklara sahip kullanıcı ve gruba ait olduğu görülmelidir (bu kullanıcı ve gruba *tomcat* diyelim).

Ayrıca,

- $CATALINA_HOME/conf dizinine *sadece okuma* ve çalıştırma *(500)*, bu dizinin içindekilere ise sadece okuma *(400)*
- $CATALINA_HOME/logs ve içindekilere dizinine sadece okuma/*yazma ve çalıştırma (700)* haklarının *(eğer log dosyaları okunmayacaksa, 300)*
- Son olarak *tomcat* kullanıcısına /tmp (veya $CATALINA_HOME/temp) dizinine ve içindekilere sadece *okuma ve yazma (600)* hakkı verilmelidir.

Alternatif olarak yukarıdaki izinleri standartlara biraz daha yaklaştırmak gerekirse,

- $CATALINA_HOME/ dizini altında her maddenin (dosya/dizin) sahipleri root:tomcat
- $CATALINA_HOME/ dizini altındaki bütün dizinlere, sahibi ve grubu için *okuma ve çalıştırma* (550)
- $CATALINA_HOME/ dizini altındaki bütün dosyalara, sahibi ve grubu için *okuma* (440)
- $CATALINA_HOME/bin dizini altındaki sh uzantılı dosyalara, sahibi ve grubu için *okuma ve çalıştırma* (550)
- $CATALINA_HOME/logs dizini (veya log dosyaları başka bir dizin altında tutuluyorsa) altındaki sadece log dosyalarına, sahibi için okuma ve grubu için *okuma ve yazma* (460) verilmelidir.

12.3 TEST SONUCU

Apache Tomcat servisinin dosya haklarının bilmesi gereken prensibine göre dosya haklarının sıkılaştırılmış olması gerekmektedir.