Tomcat 서버 버전정보 숨기기

- description : Tomcat 서버의 버전정보를 숨기는 방법
- author : 김토피아, 밤즌
- email : kimmk@repia.com
- lastupdate : 2020-04-06 → 2022-07-21

Intro

Tomcat은 Apache와 연계하여 많이 사용하나, 독립적으로 Web 서비스를 사용하는 경우가 있다.
이때 기본 설정으로만 서비스 구동 시에 Response Header나 Default Error Page 등에서 톰캣 버전이 노출된다.
이렇게 버전이 노출이 된 경우 현재 사용하고 있는 해당 톰캣 버전에 알려진 취약점을 이용하여 좀 더 쉽게 공격이 가능하다.

취약점 정리

1-1. 기본 에러 페이지 정보 제거

1) CATALINA_HOME/server/lib 으로 이동

```
cd {$CATALINA_HOME}/lib
```

2) catalina.jar 에서 ServerInfo.properties 파일만 압축 해제

```
jar xvf catalina.jar org/apache/catalina/util/ServerInfo.properties
```

3) ServerInfo.properties 수정

```
server.info=Apache Tomcat
server.number=
server.built=
```

4) catalina.jar ServerInfo.properties파일 repackage

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

1-2. Header(헤더) 버전 정보 제거
server.xml 파일 수정
Connector 태그에 server 속성을 추가.

```
vi {$CATALINA_HOME}/conf/server.xml
<Connector port="8080"  ...  server="apache tomcat" />
```

> 결과

```
curl -i 192.168.10.86:8080/search/front/Search.jsp

HTTP/1.1 200 OK
Server: apache tomcat
Content-Type: text/html;charset=UTF-8
Content-Language: koTransfer-Encoding: chunked
Date: Tue , 02 Jan 2018 04:33:57 GMT
```

1-3. ErrorReportValve 설정을 통한 정보 제거
- server.xml 파일 수정 <Host> </Host> 사이에 <Valve> 추가
<Valve> 태그를 통해 Tomcat에 들어오는 각 요청에 대한 전처리를 수행할 수 있다.

> 아래 내용 추가

```
<Valve className="org.apache.catalina.valves.ErrorReportValve"
showReport="false" showServerInfo="false"/>
```

2. 불필요한 examples 디렉토리(/examples) 제거

```
서버에 대한 상세 정보를 제공하고 있고, 예제 프로그램 취약점 공격 예방을 위해서 삭제.
 {$CATALINA_HOME}/webapps/examples 폴더 삭제
```

3. 공격자가 대상 시스템의 정보를 획득하기 위해 고의적으로 다양한 에러를 유발하여 돌아오는 에러 메시지를 통해 웹 프로그램의 구조 및 환경 설정을 추정할 수 있음.
{$CATALINA_HOME}/conf web.xml에 에러 페이지 설정

web.xml 제일 하단 </web-app> 안쪽에 넣는다.

```
<error-page>
<error-code>401</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>402</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>403</error-code>
```

```
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>404</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>405</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>406</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>407</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>408</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>409</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>410</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>411</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>412</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>413</error-code>
<location>/error.jsp</location>
```

```
</error-page>

<error-page>
<error-code>414</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>415</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>500</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>501</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>502</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>503</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>504</error-code>
<location>/error.jsp</location>
</error-page>

<error-page>
<error-code>505</error-code>
<location>/error.jsp</location>
</error-page>
```

From:
http://125.132.25.164/dokuwiki/ - **문제를 잘 정의하는 것은 문제를 절반 해결한 것이다. - 2023.12**

Permanent link:
http://125.132.25.164/dokuwiki/doku.php?id=wiki:was:tomcat:tip:tomcat_%EB%B2%84%EC%A0%84_%EC%A0%95%EB%B3%B4_%EC%88%A8%EA%B8%B0%EA%B8%B0&rev=1658464386

Last update: **2022/07/22 13:33**