

BaroPAM 가이드 (Tomcat 콘솔)

목차

목차.....	0
1. BaroPAM 연동.....	1
1.1 개 요	1
1.2 BaroPAM 모듈 설치	3
1.3 BaroPAM 환경설정	5
1.4 BaroPAM 앱 설치 및 정보 설정.....	6
2. BaroPAM 적용.....	7
2.1 BaroPAM 적용 프로세스.....	7
2.2 BaroPAM 적용 화면	7
2.3 Tomcat 관리자 콘솔 로그인.....	8
3. About BaroPAM	10

1. BaroPAM 연동

1.1 개요

웹 애플리케이션 서버(WAS, Web Application Server)는 웹 애플리케이션과 서버 환경을 만들어 동작시키는 기능을 제공하는 소프트웨어 프레임워크이다. 인터넷 상에서 HTTP를 통해 사용자 컴퓨터나 장치에 애플리케이션을 수행해 주는 미들웨어(소프트웨어 엔진)로 볼 수 있다. 웹 애플리케이션 서버는 동적 서버 콘텐츠를 수행하는 것으로 일반적인 웹 서버와 구별이 되며, 주로 데이터베이스 서버와 같이 수행이 된다. 한국에서는 일반적으로 "WAS" 또는 "WAS S/W"로 통칭하고 있으며 공공기관에서는 "웹 애플리케이션 서버"로 사용되고, 영어권에서는 "Application Server" (약자 AS)로 불린다.

웹 애플리케이션 서버는 대부분이 자바 기반으로 주로 자바 EE 표준을 수용하고 있으나, 자바 기반이지만 자바 EE 표준을 따르지 않는 제품과 .NET이나 Citrix 기반인 비 자바 계열도 존재한다.

웹 애플리케이션 서버의 기본 기능은 3가지이다.

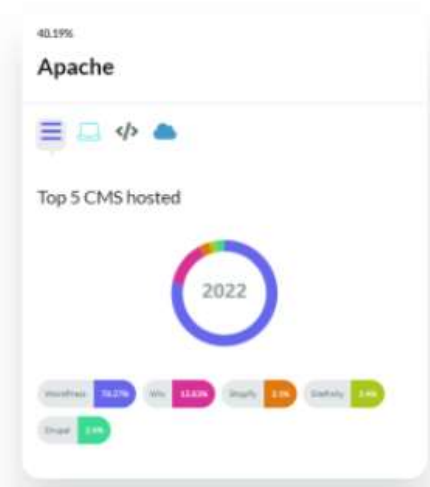
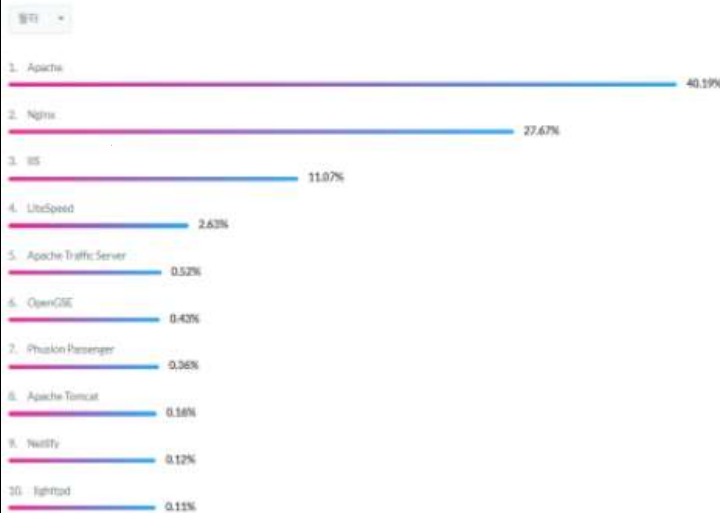
- 프로그램 실행 환경과 데이터베이스 접속 기능을 제공.
- 여러 개의 트랜잭션을 관리.
- 업무를 처리하는 비즈니스 로직을 수행.

다만, 웹 애플리케이션의 정확한 정의는 존재하지 않아서 일부 기능을 제공하지 않는 웹 애플리케이션 서버도 존재한다. 업체들은 이러한 3가지 기능 말고도 여러 기능을 추가하고 강화하고 있다.

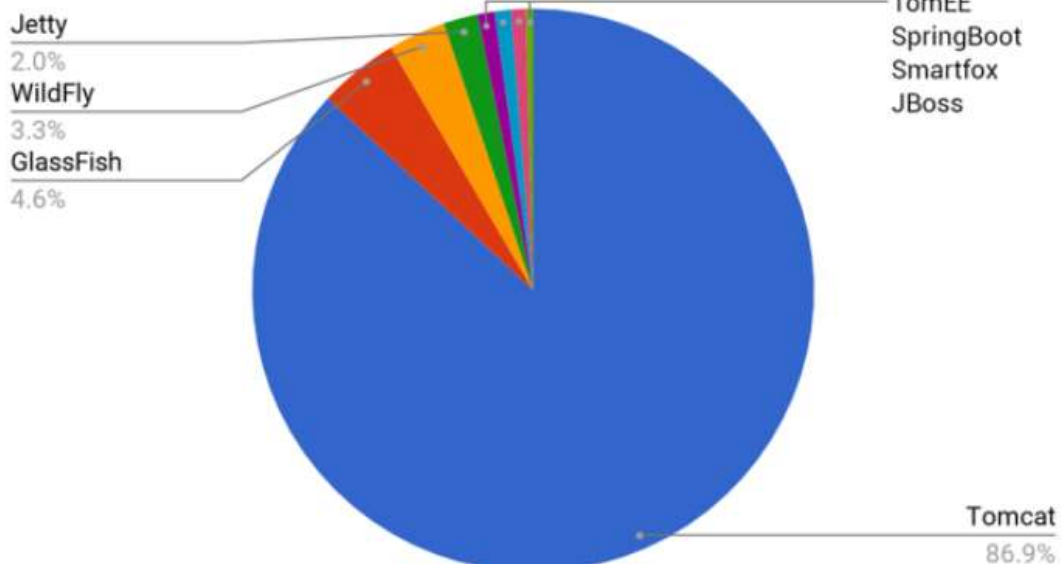
웹 애플리케이션 서버 중 적은 비용으로 고효율의 성능을 창출하기 위해 수많은 곳에서 오픈소스 소프트웨어인 Apache Tomcat으로 도입하는 곳이 늘어나고 있는 추세이다.

2022 글로벌 웹 서버 시장 점유율

다음은 세계적으로 사용자가 가장 많은 웹 서버입니다



Java Application Servers Usage



과거의 Apache Tomcat은 일부 제한된 소프트웨어 개발자들의 분야로 인식되어 왔지만 현재는 널리 사용될 정도로 안전성이 확보되었으며, 오픈소스 웹 애플리케이션 서버 중 선두주자로 높은 범용성과 뛰어난 성능을 보유하고 있다.

오픈소스 웹 애플리케이션 서버인 Apache Tomcat은 오픈 소스 재단 아파치 소프트웨어 재단의 오픈 소스 소프트웨어로 Apache와 연계하여 많이 사용하나, 간혹 독립적으로 Web 서비스를 사용하는 경우가 있다.

해커들은 피해자 PC에 초기 침투하기 위해 ▲어플리케이션 취약점 공격 ▲악성메일 ▲웹사이트에 특정 페이지에 악성코드를 심어두는 '위터링홀' 등 잘 알려진 공격기법을 주로 활용한다.

그 중 가장 많이 이용한 것은 '어플리케이션 취약점' 공격이다. MS익스체인지 · 오라클 웹로직 · 아파치 등 응용 소프트웨어의 보안 정책에서의 결함이나 시스템 개발에서의 눈에 띄지 않는 취약점을 공격하는 방법이다.

현재는 널리 사용하고 있어 그만큼 보안이 중요 하지만 Tomcat의 버그, 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 절차나 일련의 명령, 스크립트, 프로그램 또는 특정한 데이터 조각을 사용한 공격 행위를 이르기에도 한다.

이러한 취약점 공격(Exploit) 원인은 Tomcat의 디폴트 설정에 영향을 주며, 따라서 많은 서버들이 현재 취약점에 노출되어 있을 가능성이 높다. 사용자들이 디폴트 설정을 잘 바꾸지 않기 때문이다. 이 말은 많은 서버들이 현재 인터넷에 노출되어 있을 수 있다는 뜻이다.

최근에는 Tomcat의 취약점을 노린 공격이 증가하고 있다. 공격자가 취약점을 악용하여 취약한 서버에서 악성코드를 실행하고 제어권을 얻을 수 있다.

이런 취약점을 방치해둔 상태로 운영하게 된다면 취약점을 공격해 악성코드를 실행하여 악성코드 유포 및 운영 서버에 손상이 가해지거나 데이터가 약탈되는 등 다양한 취약점을 악용하는 사례가 늘어나고 있다.

예) 관리자 콘솔 취약점

- Tomcat은 Web 환경의 관리자 콘솔을 제공함.
- 관리자 콘솔이 외부로부터 침해되는 경우 Web에 관련된 모든 권한을 누출할 수 있으므로 관리에 주의해야 함.
- 관리자 인증을 위한 페이지가 쉽게 인지 가능하거나 유추로 인해 접근 되어지는 경우에는 취약함.
- 관리자 인증 시 사용하는 Username/Password가 암호화 되지 않은 원문(평문)으로 저장 (tomcat-users.xml) 되어 있어서 보안에 취약함.

예) tomcat-users.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<tomcat-users xmlns="http://tomcat.apache.org/xml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
  version="1.0">
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <role rolename="manager-gui"/>
  <user username="tomcat" password="tomcat" roles="tomcat,manager-gui"/>
</tomcat-users>
```

Tomcat 관리자 콘솔의 로그인 시 사용하는 Username/Password는 "tomcat-users.xml" 파일에 암호화되지 않은 원문인 평문으로 저장되어 있어서 보안에 그만큼 취약하다.

1.2 BaroPAM 모듈 설치

BaroPAM에서 사용하는 인증 코드인 **일회용 인증키**는 Java를 기반으로 작성되었기 때문에 반드시 최신 **JDK 6.x 이상**에서 적용 가능하다.

1) 일회용 인증키 검증 모듈(barokey.jar)

Tomcat 관리자 콘솔에 로그인 시 비밀번호란에 입력한 **일회용 인증키**를 검증하는 API는 "barokey.jar"로

제공되며, WAS(Web application Server)의 lib 디렉토리에 "barokey.jar"를 위치시키거나 classpath에 "barokey.jar"가 존재하는 디렉토리를 포함해서 설정해 주면 된다.

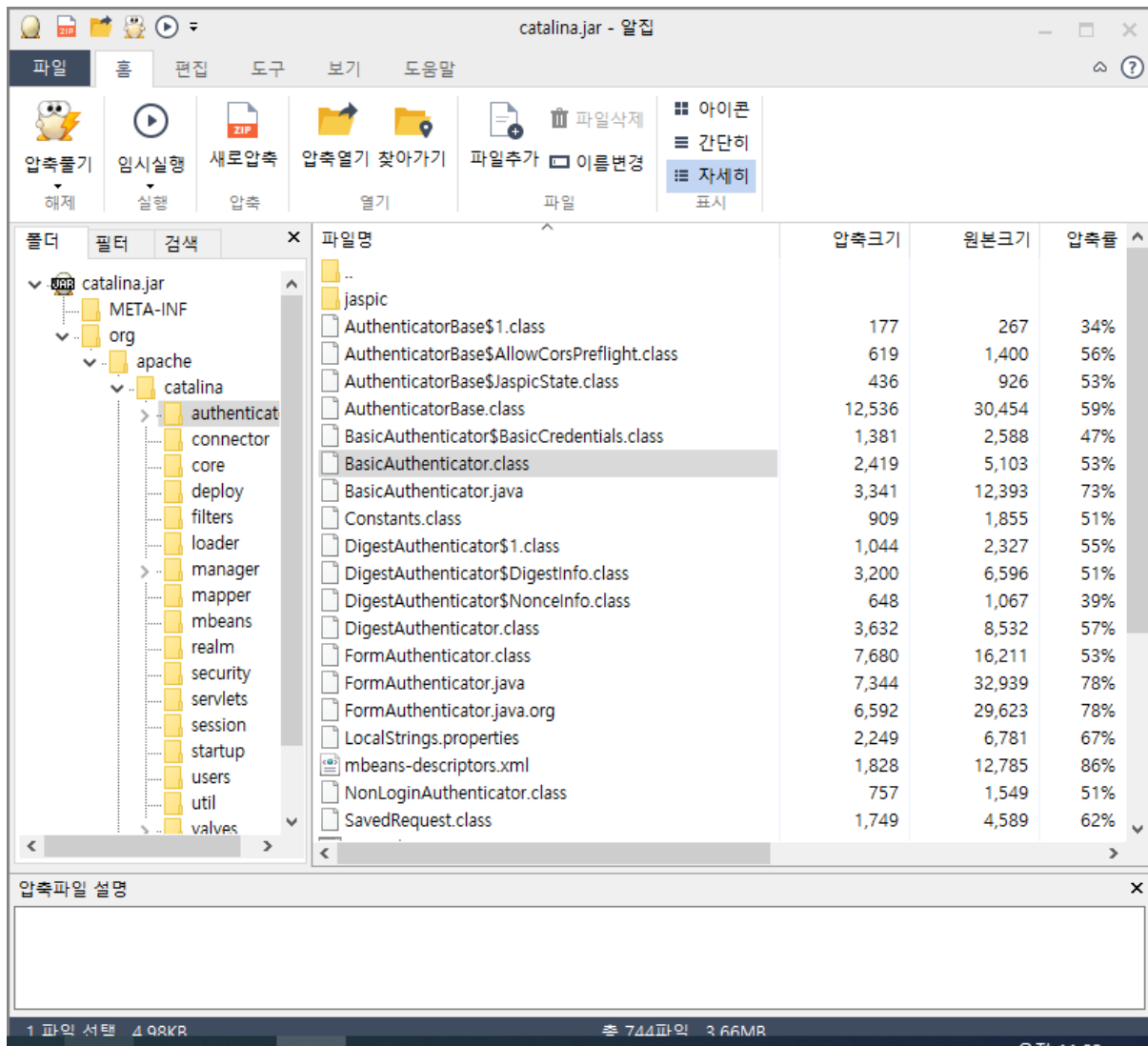
```
[root] /home/tomcat/lib > ls -al
total 23100
drwxrwxrwx 2 root root 4096 May 22 13:29 .
drwxr-xr-x 13 root root 4096 Aug 14 2017 ..
-rw-r--r-- 1 root root 2550 Apr 23 2022 .bash_history
-rwxrwxrwx 1 root root 15240 Sep 18 2014 annotations-api.jar
-rw-r--r-- 1 root root 16864 May 22 15:10 barokey.jar
-rw-r--r-- 1 root root 16730 Mar 14 14:08 barokey.jar.old
-rwxrwxrwx 1 root root 54565 Sep 18 2014 catalina-ant.jar
-rwxrwxrwx 1 root root 132132 Sep 18 2014 catalina-ha.jar
-rwxrwxrwx 1 root root 237521 Sep 18 2014 catalina-tribes.jar
-rwxrwxrwx 1 root root 1243752 Sep 18 2014 catalina.jar
.....
```

2) Tomcat 관리자 콘솔 로그인 모듈(BasicAuthenticator.class)

Tomcat 관리자 콘솔에 로그인과 관련된 "BasicAuthenticator.class" 파일 존재하는 jar 파일은 "catalina.jar"이다.

```
[root] /home/tomcat/lib > ls -al
total 23100
drwxrwxrwx 2 root root 4096 May 22 13:29 .
drwxr-xr-x 13 root root 4096 Aug 14 2017 ..
-rw-r--r-- 1 root root 2550 Apr 23 2022 .bash_history
-rwxrwxrwx 1 root root 15240 Sep 18 2014 annotations-api.jar
-rw-r--r-- 1 root root 16864 May 22 15:10 barokey.jar
-rw-r--r-- 1 root root 16730 Mar 14 14:08 barokey.jar.old
-rwxrwxrwx 1 root root 54565 Sep 18 2014 catalina-ant.jar
-rwxrwxrwx 1 root root 132132 Sep 18 2014 catalina-ha.jar
-rwxrwxrwx 1 root root 237521 Sep 18 2014 catalina-tribes.jar
-rwxrwxrwx 1 root root 1243752 Sep 18 2014 catalina.jar
.....
```

Tomcat 관리자 콘솔에 로그인과 관련된 jar 파일인 "catalina.jar" 파일에서 "org.apache.catalina.authenticator" 디렉토리 내의 "BasicAuthenticator.class" 파일을 Tomcat 버전에 맞는 파일로 교체한다.



1.3 BaroPAM 환경설정

반드시 연동 API인 "barokey.jar"에서 사용하는 "BAROPAM"과 "BAROCONF" 환경변수를 설정해야 한다.

```
[root] /home/tomcat/conf > ls -al
total 372
drwxrwxrwx 3 root root 4096 May 23 10:44 .
drwxr-xr-x 13 root root 4096 Aug 14 2017 ..
-r--r--r-- 1 root root 89 May 8 2019 .baro_nurit
-rw-r--r-- 1 root root 5133 Apr 23 2022 .bash_history
drwxr-xr-x 5 root root 4096 Sep 18 2014 Catalina
-rw-r--r-- 1 root root 23 Apr 20 11:14 .baropam.conf
-rwxrwxrwx 1 root root 10858 Sep 18 2014 catalina.policy
-rwxrwxrwx 1 root root 3794 Sep 18 2014 catalina.properties
-rwxrwxrwx 1 root root 2998 Jul 29 2022 context.xml
```

설정 예)

```
export BAROPAM=/home/tomcat/conf/.baro_nurit
export BAROCONF=/home/tomcat/conf/baropam.conf
```

참고) ".baro_nurit" 파일의 내용 변경 시 일회용 인증키 검증 오류가 발생한다. 또한 ".baropam.conf"은 "Secure key, 생성주기, 최종로그인시간, 로깅여부(Y/N)" 구조로 되어 있다.

1.4 BaroPAM 앱 설치 및 정보 설정

BaroPAM 앱 다운로드

BaroPAM 환경 설정 파일 (.baropam.conf)

```
JlqlcHbVqdel7b4PzBpM2DileBvmHFV/3055915874,Y
JlqlcHbVqdel7b4PzBpM2DileBvmHFV/3055915874,Y
```

Secure key 생성주기 최종로그인시간 로깅여부(Y/N)

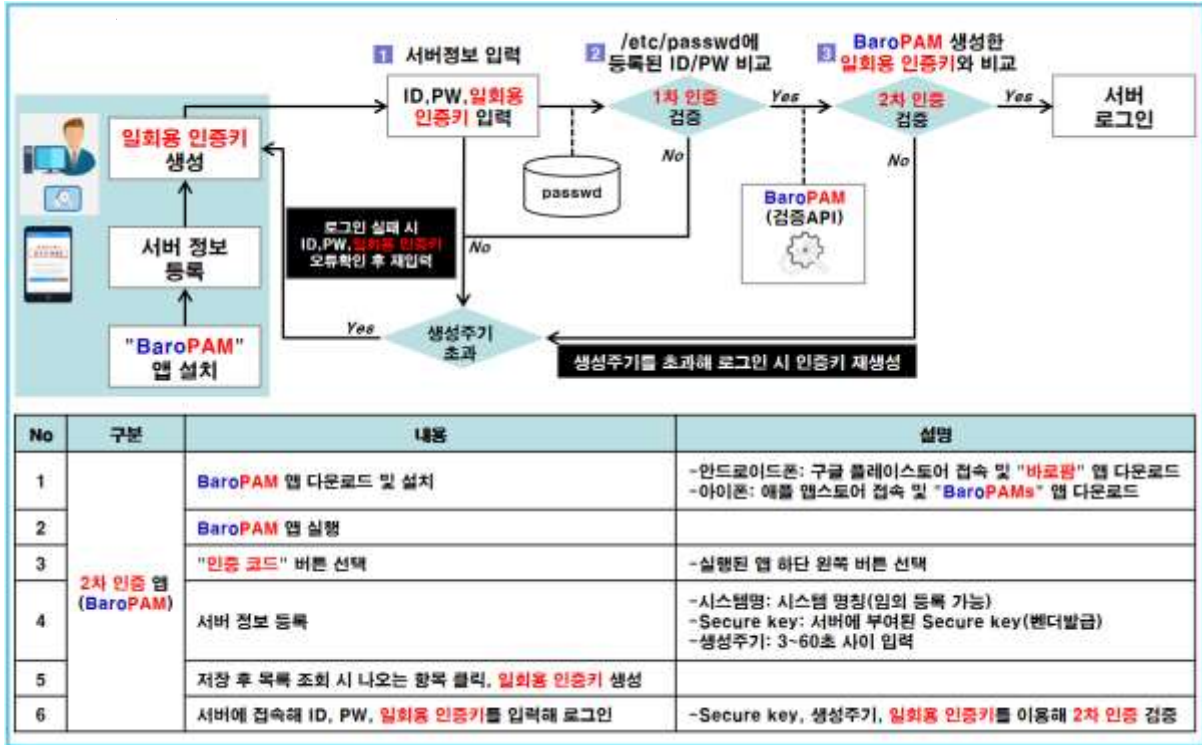
BaroPAM 앱은 Android 6.0 (Marshmallow) API 23, iOS 13.0 이상에서 사용 가능하며, 가로보기 모드를 지원하지 않는다.

BaroPAM 앱을 설치한 후 BaroPAM 앱을 실행하여 메뉴 선택화면에서 "인증 코드" 버튼을 클릭하여 BaroPAM의 환경설정 파일인 ".baropam.conf"에 설정한 "Secure key, 생성주기"를 BaroPAM 앱의 "서버 정보 등록" 화면에서 동일하게 입력해야 한다.

현상: 안드로이드폰 또는 아이폰의 날짜와 시간이 현재 시간과 차이가 발생하여 "일회용 인증키"가 맞지 않은 경우
원인: 안드로이드폰 또는 아이폰의 날짜와 시간이 네트워크에서 제공하는 시간을 사용하지 않아서 발생.
조치: 안드로이드폰인 경우는 폰의 "설정" -> "일반" -> "날짜 및 시간" -> "날짜 및 자동 설정" 과 "시간대 자동 설정" -> "허용"
 아이폰인 경우는 폰의 "설정" -> "날짜 및 시간" -> "자동으로 설정" -> "허용"

2. BaroPAM 적용

2.1 BaroPAM 적용 프로세스



2.2 BaroPAM 적용 화면



2.3 Tomcat 관리자 콘솔 로그인

인터넷 공유기, 무선 AP, IoT, 라우터, 스위치 장비 등 모든 네트워크 장비의 비밀번호를 입력할 경우, 비밀번호를 먼저 입력하고 공백 없이 이어서 **일회용 인증키**를 입력하는 방식을 적용하면 된다.

예를 들어, 비밀번호가 "baropam" 이고, **일회용 인증키**가 "123456" 이라면 비밀번호 입력란에 "baropam123456"으로 입력하면 된다.

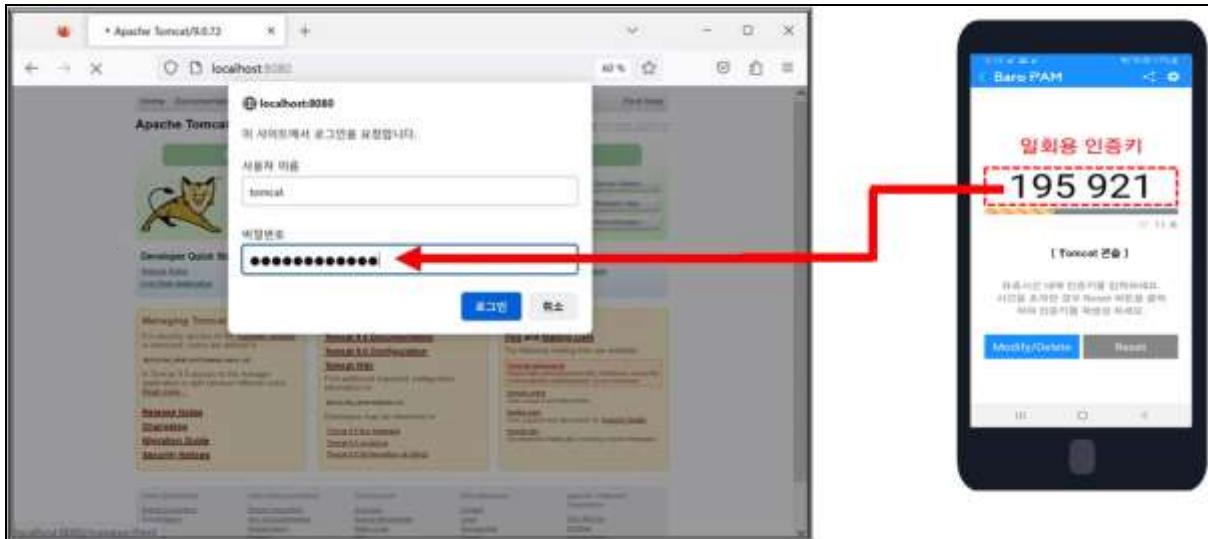
일회용 인증키 생성 주기가 30초면 30초 마다 **일회용 인증키**가 바뀌기 때문에 고정된 비밀번호와 결합하면 **일회용 인증키** 생성 주기 마다 새로운 비밀번호가 생성되기 때문에 고전적 방법인 주기적으로 Tomcat 관리자 콘솔의 비밀번호를 바꿀 필요가 없게 된다.

만약, **2-factor 인증** 솔루션이 적용되어 있다면 비밀번호 입력란에 고정된 비밀번호만 입력하는 경우 Tomcat 관리자 콘솔에 로그인을 할 수 없게 된다.

그러므로, 정보자산 로그인 시 비밀번호 만으로는 결코 안전하지 않으며 매번 사용할 때마다 비밀번호를 대체할 수 있는 **새로운 적용 방안(추가 인증, 비밀번호 대체, 새로운 비밀번호)**이 필요하다.

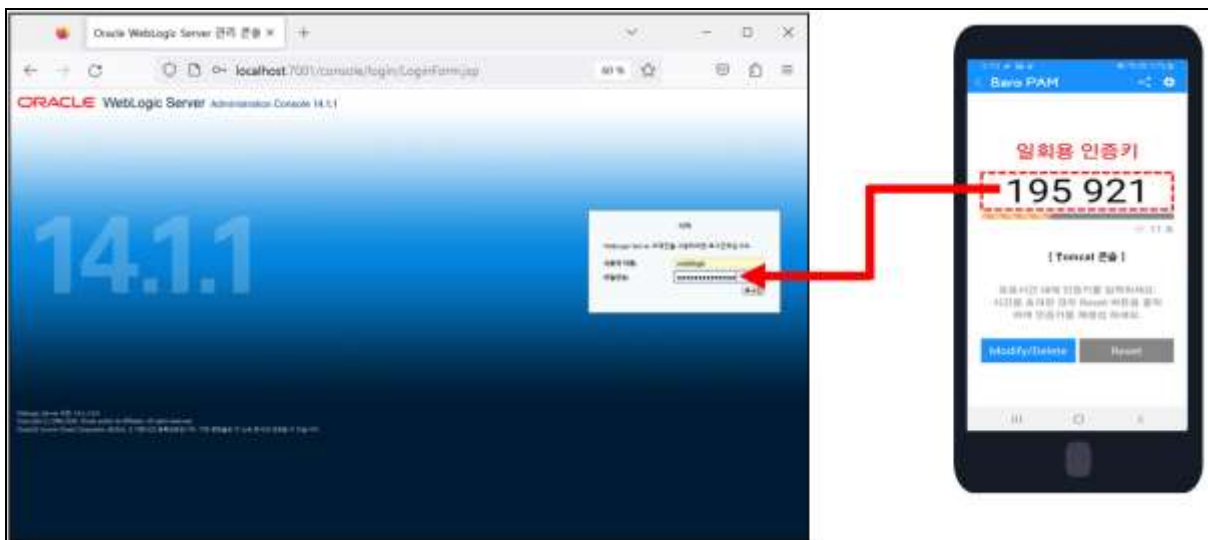
지금까지 보안상 분기마다 한번씩 주기적으로 비밀번호 변경 규정에 따른 복잡한 비밀번호를 변경(비밀번호 증후군/리셋 증후군 호소)하는 것 보다 생각의 전환이 필요한 것 같다.

예) Tomcat 관리자 콘솔



Tomcat 콘솔 로그인 화면에서 비밀번호를 먼저 입력하고 공백 없이 이어서 **일회용 인증키**를 입력해야 한다. 예를 들어, 비밀번호가 "tomcat" 이고, **일회용 인증키**가 "195921" 이라면 "tomcat195921"으로 입력한다

예) Oracle Weblogic Server 관리자 콘솔



설명, Tomcat 콘솔 로그인 정보인 User name/Password가 유출되어도 비밀번호 뒤에 덧붙인 **일회용 인증키**를 유추할 수 없어서 강력한 보안을 적용할 수 있다.

3. About BaroPAM



Version 1.0 – Official Release – 2016.12.1
Copyright © Nurit corp. All rights reserved.
<http://www.nurit.co.kr>

제 조 사 : 주식회사 누리아이티
등록번호 : 258-87-00901
대표이사 : 이종일
대표전화 : 02-2665-0119(영업문의/기술지원)
이 메 일 : mc529@nurit.co.kr
주 소 : 서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)