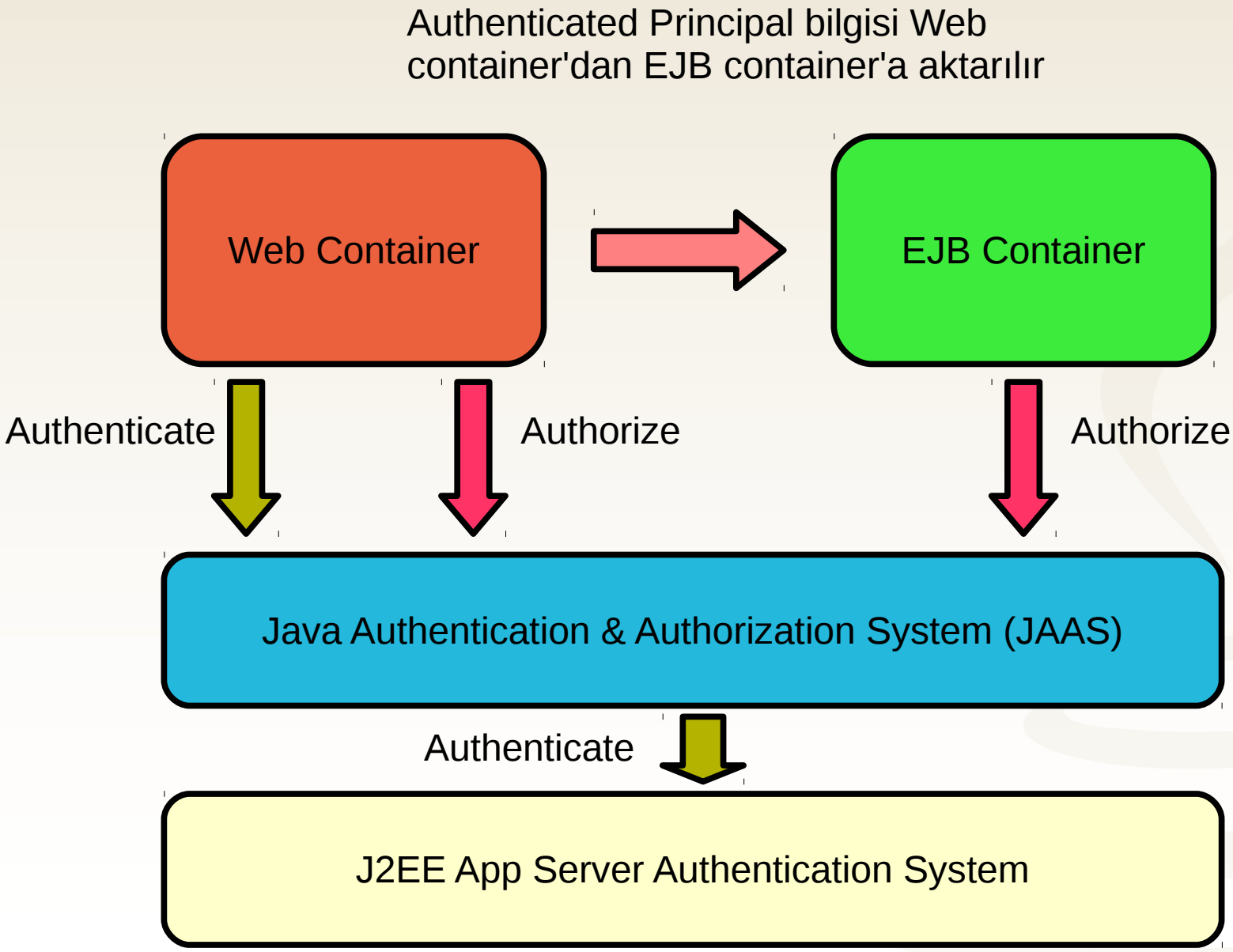
Java EE ve Güvenlik

harezmi bilişim çözümleri

JavaEE Güvenlik Mimarisi



Web Uygulamalarında Güvenlik

JAVA Eğitimleri

- **Web.xml Security** olarak da bilinir
- **Authentication** ve **authorization** kabiliyetleri sunar
- Basic, digest, form veya sertifika tabanlı **authentication yöntemleri** kullanılabilir
- Sadece **web kaynaklarına erişim** düzeyinde yetkilendirme yapılabilir
- Web.xml ve web container'a özel **konfigürasyon dosyalarında tanımlar** yapmak gerekir

Web Uygulamalarında Güvenlik

- Servlet Container ile kullanıcı bilgilerinin tutulduğu yer arasındaki entegrasyon **standart değil**dir
- Bu nedenle her Web container kendine özgü bir **user realm erişim mekanizması** sunar
- Tomcat için bu default **conf/tomcat-users.xml** dosyası ile in-memory user realm oluşturmak şeklindedir

Web.xml Güvenlik Konfigürasyonu

```
<web-app>
  <security-constraint>
    <web-resource-collection>
        <web-resource-name>SecureResources</web-resource-name>
        <url-pattern>/secured/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
        <role-name>user</role-name>
        <role-name>admin</role-name>
    </auth-constraint>
  </security-constraint>

  <login-config>
    <auth-method>FORM</auth-method>
    <form-login-config>
        <form-login-page>/login.jsp</form-login-page>
        <form-error-page>/loginError.jsp</form-error-page>
    </form-login-config>
  </login-config>

  <security-role>
    <role-name>user</role-name>
  </security-role>
  <security-role>
    <role-name>admin</role-name>
  </security-role>
</web-app>
```

Hangi web kaynağına
Hangi rollerin
Erişebileceği
tanımlanır

Authentication
Yöntemi belirtilir
FORM, BASIC, DIGEST
veya CLIENT-CERT
olabilir

Uygulama için geçerli roller tanımlanır

Form Login Sayfası

```
<html>
    <body>
        <form method="POST" action="j_security_check">
        <table border="0">
            <tr>
                <td>Login</td>
                <td><input type="text" name="j_username"></td>
            </tr>
            <tr>
                <td>Password</td>
                <td><input type="password"
name="j_password"></td>
            </tr>
        </table>
        <input type="submit" value="Login!">
        </form>
    </body>
</html>
```

HttpServletRequest'deki Güvenlikle İlgili Metotlar

```
<html>
    <body>
        Current user :${pageContext.request.userPrincipal.name}<br/>
        Current user :${pageContext.request.remoteUser}<br/>
        <%
            if(request.isUserInRole("admin"))
                out.println("Admin user");
            else
                out.println("Normal user");
        %>
    </body>
</html>
```

HttpServletRequest.isUserInRole() metodu ile Mevcut kullanıcının belirtilen role sahip olup Olmadığı sorgulanabilir

HttpServletRequest.getUserPrincipal() Ve getRemoteUser() metotları sisteme Login olmuş olan kullanıcı hakkında bilgi Dönen metotlardır

HttpServletRequest'de güvenlikle ilgili diğer metotlar: getAuthType(), getProtocol(), isSecure()

EJB 3.x ve Güvenlik

- **@DeclareRoles**
  - EJB sınıfı veya metotları düzeyinde kullanılır
  - EJB sınıfının metotlarında kullanılan rolleri tanımlar
  - Opsiyoneldir, kullanılmaz ise @RolesAllowed ile belirtilen roller tanım olarak kullanılır
- **@RolesAllowed**
  - EJB sınıfı veya metotları düzeyinde kullanılır
  - İlgili metotlara hangi rollerin erişebileceğini tanımlar

EJB 3.x ve Güvenlik

- **@PermitAll**
  - EJB sınıfı veya metotları düzeyinde kullanılır
  - İlgili metotlara herkesin erişebileceğini belirtir
- **@DenyAll**
  - EJB sınıfı veya metotları düzeyinde kullanılır
  - İlgili metotlara erişimi tamamen engeller
- **@RunAs**
  - EJB sınıfı veya metotları düzeyinde kullanılır
  - İlgili metot çağrısı boyunca kullanıcının belirtilen rollere'de ilaveten sahip olmasını sağlar

EJBContext'deki Güvenlik Metotları

JAVA Eğitimleri

```
public class PetClinicServiceEJB {

    @Resource
    private SessionContext context;


    public void createVet(Vet vet) {

        if(context.getCallerPrincipal()
                .getName().equals("ksevindik")) {
            //...
        }


        if(!context.isCallerInRole("ADMIN")) {
            //...
        }
    }
}
```

İletişim

www.harezmi.com.tr

www.java-egitimleri.com

info@harezmi.com.tr

info@java-egitimleri.com

@HarezmiBilisim

@JavaEgitimleri