Adv. Java means DURGA SIR..

ADV.JAVA

With

SCWCD / OCWCD

Question Bank

Chapter : 5. Web Application Security

DURGA M.Tech

(Sun certified & Realtime Expert)

Ex. IBM Employee

Trained Lakhs of Students
for last 14 years across INDIA

India's No.1 Software Training Institute

DURGASOFT

www.durgasoft.com Ph: 9246212143 ,8096969696

Unit-5 : Web Application Security

Objectives

1. Based on the servlet specification, compare and contrast the following security mechanisms: (a) authentication, (b) authorization, (c) data integrity, and (d) confidentiality.

2. In the deployment descriptor, declare a security constraint, a Web resource, the transport guarantee, the login configuration, and a security role.

3. Compare and contrast the authentication types (BASIC, DIGEST, FORM, and CLIENT-CERT); describe how the type works; and given a scenario, select an appropriate type.

Q1. Given:

```
3. class MyServlet extends HttpServlet {
4. public void doPut(HttpServletRequest req, HttpServletResponse resp) throws
ServletException,
IOException {
5. // servlet code here ...
26. }
27. }
```

If the DD contains a single security constraint associated with MyServlet and its only <http-method> tags
and <auth-constraint> tags are:

```
<http-method>GET</http-method>
<http-method>PUT</http-method>
<auth-constraint>Admin</auth-constraint>
```

Which four requests would be allowed by the container? (Choose four.)

A. A user whose role is Admin can perform a PUT.
B. A user whose role is Admin can perform a GET.
C. A user whose role is Admin can perform a POST.
D. A user whose role is Member can perform a PUT.
E. A user whose role is Member can perform a POST.
F. A user whose role is Member can perform a GET.

Answer: A, B, C, E

Q2. What is true about Java EE authentication mechanisms?

A. If your deployment descriptor correctly declares an authentication type of CLIENT_CERT, your users must have a certificate from an official source before they can use your application.

B. If your deployment descriptor correctly declares an authentication type of BASIC, the container automatically requests a user name and password whenever a user starts a new session.

C. If you want your web application to support the widest possible array of browsers, and you want to perform authentication, the best choice of Java EE authentication mechanisms is DIGEST.

D. To use Java EE FORM authentication, you must declare two HTML files in your deployment descriptor, and you must use a predefined action in the HTML file that handles your user's login.

Answer: D

Q3. If you want to use the Java EE platform's built-in type of authentication that uses a custom HTML page for authentication, which two statements are true? (Choose two.)

A. Your deployment descriptor will need to contain this tag:
<auth-method>CUSTOM</auth-method>.
B. The related custom HTML login page must be named loginPage.html.
C. When you use this type of authentication, SSL is turned on automatically.
D. You must have a tag in your deployment descriptor that allows you to point to both a login HTML page and an HTML page for handling any login errors.
E. In the HTML related to authentication for this application, you must use predefined variable names for the variables that store the user and password values.

Answer: D, E

Q4. Given this fragment in a servlet:
23. if(req.isUserInRole("Admin")) {
24. // do stuff
25. }
And the following fragment from the related Java EE deployment descriptor:
812. <security-role-ref>
813. <role-name>Admin</role-name>
814. <role-link>Administrator</role-link>
815. </security-role-ref>
900. <security-role>
901. <role-name>Admin</role-name>
902. <role-name>Administrator</role-name>
903. </security-role>
What is the result?

A. Line 24 can never be reached.
B. The deployment descriptor is NOT valid.
C. If line 24 executes, the user's role will be Admin.
D. If line 24 executes, the user's role will be Administrator.
E. If line 24 executes the user's role will NOT be predictable.
Answer: D

Q5. Given the security constraint in a DD:

101. <security-constraint>
102. <web-resource-collection>
103. <web-resource-name>Foo</web-resource-name>
104. <url-pattern>/Bar/Baz/*</url-pattern>
105. <http-method>POST</http-method>
106. </web-resource-collection>
107. <auth-constraint>

108. <role-name>DEVELOPER</role-name>
109. </auth-constraint>
110. </security-constraint>

And given that "MANAGER" is a valid role-name, which four are true for this security constraint?(Choose four.)

A. MANAGER can do a GET on resources in the /Bar/Baz directory.
B. MANAGER can do a POST on any resource in the /Bar/Baz directory.
C. MANAGER can do a TRACE on any resource in the /Bar/Baz directory.
D. DEVELOPER can do a GET on resources in the /Bar/Baz directory.
E. DEVELOPER can do only a POST on resources in the /Bar/Baz directory.
F. DEVELOPER can do a TRACE on any resource in the /Bar/Baz directory.

Answer: A, C, D, F

Q6. Given the security constraint in a DD:

101. <security-constraint>
102. <web-resource-collection>
103. <web-resource-name>Foo</web-resource-name>
104. <url-pattern>/Bar/Baz/*</url-pattern>
105. <http-method>POST</http-method>
106. </web-resource-collection>
107. <auth-constraint>
108. <role-name>DEVELOPER</role-name>
109. </auth-constraint>
110. </security-constraint>
And given that "MANAGER" is a valid role-name, which four are true for this security constraint?(Choose four.)

A. MANAGER can do a GET on resources in the /Bar/Baz directory.
B. MANAGER can do a POST on any resource in the /Bar/Baz directory.
C. MANAGER can do a TRACE on any resource in the /Bar/Baz directory.
D. DEVELOPER can do a GET on resources in the /Bar/Baz directory.
E. DEVELOPER can do only a POST on resources in the /Bar/Baz directory.
F. DEVELOPER can do a TRACE on any resource in the /Bar/Baz directory.

Answer: A, C, D, F

Q7. Which activity supports the data integrity requirements of an application?

A. using HTTPS as a protocol

B. using an LDAP security realm
C. using HTTP Basic authentication
D. using forms-based authentication

Answer: A

Q8. Which mechanism requires the client to provide its public key certificate?
A. HTTP Basic Authentication B. Form Based Authentication
C. HTTP Digest Authentication D. HTTPS Client Authentication
Answer: D

Q9. Given the two security constraints in a deployment descriptor:

101. <security-constraint>
102. <!--a correct url-pattern and http-method goes here-->
103. <auth-constraint><role-name>SALES</role-name></auth-
103. <auth-constraint>
104. <role-name>SALES</role-name>
105. </auth-constraint>
106. </security-constraint>
107. <security-constraint>
108. <!--a correct url-pattern and http-method goes here-->
109. <!-- Insert an auth-constraint here -->
110. </security-constraint>

If the two security constraints have the same url-pattern and http-method, which two, inserted independently at line 109, will allow users with role names of either SALES or MARKETING to access
this resource? (Choose two.)
A. <auth-constraint/>
B. <auth-constraint>
<role-name>*</role-name>
</auth-constraint>
C. <auth-constraint>
<role-name>ANY</role-name>
</auth-constraint>
D. <auth-constraint>
<role-name>MARKETING</role-name>
</auth-constraint>

Answer: B, D

Q10. Given this fragment in a servlet:

23. if(req.isUserInRole("Admin")) {
24. // do stuff
25. }
And the following fragment from the related Java EE deployment descriptor:

812. <security-role-ref>
813. <role-name>Admin</role-name>
814. <role-link>Administrator</role-link>
815. </security-role-ref>
900. <security-role>
901. <role-name>Admin</role-name>
902. <role-name>Administrator</role-name>
903. </security-role>
What is the result?
A. Line 24 can never be reached.
B. The deployment descriptor is NOT valid.
C. If line 24 executes, the user's role will be Admin.
D. If line 24 executes, the user's role will be Administrator.
E. If line 24 executes the user's role will NOT be predictable.

Answer: D

Q11.Which two are true about authentication? (Choose two.)
A. Form-based logins should NOT be used with HTTPS.
B. When using Basic Authentication the target server is NOT authenticated.
C. J2EE compliant web containers are NOT required to support the HTTPS protocol.
D. Web containers are required to support unauthenticated access to unprotected web resources.
E. Form-based logins should NOT be used when sessions are maintained by cookies or SSL session information.

Answer: B, D

Q12. If you want to use the Java EE platform's built-in type of authentication that uses a custom HTML page for authentication, which two statements are true? (Choose two.)

A. Your deployment descriptor will need to contain this tag: <auth-method>CUSTOM</auth-method>.
B. The related custom HTML login page must be named loginPage.html.
C. When you use this type of authentication, SSL is turned on automatically.
D. You must have a tag in your deployment descriptor that allows you to point to both a login HTML page and an HTML page for handling any login errors.
E. In the HTML related to authentication for this application, you must use predefined variable names for the variables that store the user and password values.

Answer: D, E

Q13. Given the two security constraints in a deployment descriptor:

101. <security-constraint>
102. <!--a correct url-pattern and http-method goes here-->
103. <auth-constraint><role-name>SALES</role-name></auth-
103. <auth-constraint>
104. <role-name>SALES</role-name>
105. </auth-constraint>
106. </security-constraint>
107. <security-constraint>
108. <!--a correct url-pattern and http-method goes here-->
109. <!-- Insert an auth-constraint here -->
110. </security-constraint>

If the two security constraints have the same url-pattern and http-method, which two, inserted independently at line 109, will allow users with role names of either SALES or MARKETING to access this resource? (Choose two.)

A. <auth-constraint/>
B. <auth-constraint>
<role-name>*</role-name>
</auth-constraint>
C. <auth-constraint>
<role-name>ANY</role-name>
</auth-constraint>
D. <auth-constraint>
<role-name>MARKETING</role-name>

</auth-constraint>

Answer: B, D

Q14. Which two are valid values for the <transport-guarantee> element inside a <security-constraint> element of a web application deployment descriptor? (Choose two.)

A. NULL
B. SECURE
C. INTEGRAL
D. ENCRYPTED
E. CONFIDENTIAL

Answer: C, E

Q15. Which basic authentication type is optional for a J2EE 1.4 compliant web container?

A. HTTP Basic Authentication
B. Form Based Authentication
C. HTTP Digest Authentication
D. HTTPS Client Authentication

Answer: C

Q16. Which security mechanism uses the concept of a realm?

A. authorization
B. data integrity
C. confidentiality
D. authentication

Answer: D

Q17. Which two security mechanisms can be directed through a sub-element of the <user-data-constraint> element in a web application deployment descriptor? (Choose two.)

A. authorization
B. data integrity

C. confidentiality D. authentication

Answer: B, C

Q18. Which two statements are true about the security-related tags in a valid Java EE deployment descriptor? (Choose two.)

A. Every <security-constraint> tag must have at least one <http-method> tag.
B. A <security-constraint> tag can have many <web-resource-collection> tags.
C. A given <auth-constraint> tag can apply to only one <web-resource-collection> tag.
D. A given <web-resource-collection> tag can contain from zero to many <url-pattern> tags.
E. It is possible to construct a valid <security-constraint> tag such that, for a given resource, no user roles can access that resource.

Answer: B, E

Q19. Which element of a web application deployment descriptor <security-constraint> element is required?

A. <realm-name> B. <auth-method>
C. <security-role> D. <transport-guarantee>
E. <web-resource-collection>

Answer: E

Q 20 Which two are required elements for the <web-resource-collection> element of a web application deployment descriptor? (Choose two.)
A. <realm-name> B. <url-pattern>
C. <description> D. <web-resource-name>
E. <transport-guarantee>
Answer: B, D

Q21. Given:

3. class MyServlet extends HttpServlet {
4. public void doPut(HttpServletRequest req,
HttpServletResponse resp)

throws ServletException, IOException {
5. // servlet code here
...
26. }
27. }

If the DD contains a single security constraint associated with MyServlet and its only <http-method> tags and <auth-constraint> tags are:
<http-method>GET</http-method>
<http-method>PUT</http-method>
<auth-constraint>Admin</auth-constraint>

Which four requests would be allowed by the container? (Choose four.)

A. A user whose role is Admin can perform a PUT.
B. A user whose role is Admin can perform a GET.
C. A user whose role is Admin can perform a POST.
D. A user whose role is Member can perform a PUT.
E. A user whose role is Member can perform a POST.
F. A user whose role is Member can perform a GET.

Answer: A, B, C, E

aQ22. What is true about Java EE authentication mechanisms?

A. If your deployment descriptor correctly declares an authentication type of CLIENT_CERT, your users must have a certificate from an official source before they can use your application.
B. If your deployment descriptor correctly declares an authentication type of BASIC, the container automatically requests a user name and password whenever a user starts a new session.
C. If you want your web application to support the widest possible array of browsers, and you want to perform authentication, the best choice of Java EE authentication mechanisms is DIGEST.
D. To use Java EE FORM authentication, you must declare two HTML files in your deployment descriptor, and you must use a predefined action in the HTML file that handles your user's login.

Answer: D

Q23. Which two statements are true about using the isUserInRole method to implement security in a Java EE application? (Choose two.)

A. It can be invoked only from the doGet or doPost methods.
B. It can be used independently of the getRemoteUser method.

C. Can return "true" even when its argument is NOT defined as a valid role name in the deployment descriptor.
D. Using the isUserInRole method overrides any declarative authentication related to the method in which it is invoked.
E. Using the isUserInRole method overrides any declarative authorization related to the method in which it is invoked.

Answer: B, C

Q24.developer has used this code within a servlet:
62. if(request.isUserInRole("vip")) {
63. // VIP-related logic here
64. }
What else must the developer do to ensure that the intended security goal is achieved?

A. create a user called vip in the security realm
B. define a group within the security realm and call it vip
C. define a security-role named vip in the deployment descriptor
D. declare a security-role-ref for vip in the deployment descriptor

Answer: D


LEARN FROM EXPERTS ...
COMPLETE JAVA
CORE JAVA, ADV. JAVA, ORACLE, STRUTS, HIBERNATE, SPRING, WEB SERVICES,...
COMPLETE .NET
C#.NET, ASP.NET, SQL SERVER, MVC 5 & WCF
TESTING TOOLS
MANUAL + SELENIUM
ORACLE
D2K
MSBI
SHARE POINT
HADOOP
ANDROID
C, C++, DS, UNIX
CRT & APTITUDE TRAINING
AN ISO 9001:2008 CERTIFIED
DURGA
Software Solutions
202, 2nd Floor, HUDA Maitrivanam,
Ameerpet, Hyd. Ph: 040-64512786,
9246212143, 8096969696
www.durgasoft.com