Eccouncil 312-96 Practice Questions

Shared by Bean on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The developer wants to remove the HttpSessionobject and its values from the client' system.

Which of the following method should he use for the above purpose?

Options:

A- sessionlnvalidateil
B- Invalidate(session JSESSIONID)
C- isValidateQ
D- invalidateQ

Answer:

D

Question 2

Question Type: MultipleChoice

Which line of the following example of Java Code can make application vulnerable to a session attack?

```
1:  Public class storecookie extends HttpServlet {
2:  Public void doGet () {
3:  Cookie ssnCookie = new Cookie ("Session Cookie"+ value);
4:  ssnCookie.setMaxAge (3600);
5:  response.addCookie (ssnCookie);
6:  }
```

Options:

A- Line No. 1
B- Line No. 3
C- Line No. 4

D- Line No. 5

Answer:

B

Question 3

Question Type: MultipleChoice

Which of the following authentication mechanism does J2EE support?

Options:

A- Windows, Form based. Role Based, Client/Server Mutual Authentication
B- Role Based, Http Basic, Windows, Http Digest Authentication
C- Http Basic, Form Based, Client/Server Mutual, Role Based Authentication
D- Http Basic, Form Based, Client/Server Mutual, HTTP Digest Authentication

Answer:

D

Question 4

Question Type: MultipleChoice

Which of the following method will help you check if DEBUG level is enabled?

Options:

A- isDebugEnabled()
B- EnableDebug ()
C- IsEnableDebug ()
D- DebugEnabled()

Answer:

A

Question 5

Question Type: MultipleChoice

Which of the following relationship is used to describe abuse case scenarios?

Options:

A- Include Relationship
B- Threatens Relationship
C- Extend Relationship
D- Mitigates Relationship

Answer:

B

Question 6

Question Type: MultipleChoice

Alice, a security engineer, was performing security testing on the application. He found that users can view the website structure and file names. As per the standard security practices, this can pose a serious security risk as attackers can access hidden script files in your directory. Which of the following will mitigate the above security risk?

Options:

A- < int-param > < param-name>directory-listinqs < param-value>true < /init-param >
B- < int param > < param-name>directorv-listinqs < param-value>false < /init-param >
C- < int-param > < param-name>listinqs < param-value>true < /init-param
D- < int-param > < param-name>listinqs < param-value>false < /init-param >

Answer:

B

Question 7

Question Type: MultipleChoice

Oliver is a web server admin and wants to configure the Tomcat server in such a way that it should not serve index pages in the absence of welcome files. Which option best settings in CATALINA_HOME/conf/ in web.xml will solve his problem?

Options:

A- < servlet > < servlet-name > default < /servlet-name > < servlet-class > org.apache.catalina.servlets.DefaultServlet < /servlet-class > < init-param > < param-name > debug < /param-name > < param-value > 0 < /param-value > < /init-param > < init-param > < param-name > listings < /param-name > < param-value > false < /param-value > < /init-param > < load-on-startup > 1 < /load-on-startup > < servlet >
B- < servlet > < servlet-name > default < /servlet-name > < servlet-class > org.apache.catalina.servlets.DefaultServlet < /servlet-class > < init-param > < param-name > debug < /param-name > < param-value > 0 < /param-value > < /init-param > < init-param > < param-name > listings < /param-name > < param-value > disable < /param-value> < /init-param > < load-on-startup > 1 < /load-on-startup> < /servlet >
C- < servlet > < servlet-name > default < /servlet-name > < servlet-class > org.apache.catalina.servlets.DefaultServlet < /servlet-class > < init-param > < param-name > debug < /param-name>< param-value> 0 < /param value>< /init-param > < init-param > < param-name> listings < /param-name > < param-value > enable < /param-value > < /init-param > < load-on-startup> 1 < /load-on-startup > < /servlet >
D- < servlet > < servlet-name > default < servlet-name > < servlet-class > org.apache.catalina.servlets.DefaultServlet < /servlet-class > < init-param > < param-name > debug < /param-name> < param-value > 0 < /param-value > < /init-param > < init-param > < param-name > listings < /param-name > < param-value > true < /param-value > < /init-param > < load-on-startup > l < /load-on-startup > < /servlet >

Answer:

B

Question 8

Question Type: MultipleChoice

Alice works as a Java developer in Fygo software Services Ltd. He is given the responsibility to design a bookstore website for one of their clients. This website is supposed to store articles in .pdf format. Alice is advised by his superior to design ArticlesList.jsp page in such a way that it should display a list of all the articles in one page and should send a selected filename as a query string to redirect users to articledetails.jsp page.

Alice wrote the following code on page load to read the file name.

String myfilename = request.getParameter("filename");

String txtFileNameVariable = myfilename;

String locationVariable = request.getServletContext().getRealPath("/");

String PathVariable = "";

PathVariable = locationVariable + txtFileNameVariable;

BufferedInputStream bufferedInputStream = null;

Path filepath = Paths.get(PathVariable);

After reviewing this code, his superior pointed out the security mistake in the code and instructed him not repeat the same in future. Can you point the type of vulnerability that may exist in the above code?

Options:

A- URL Tampering vulnerability
B- Form Tampering vulnerability
C- XSS vulnerability
D- Directory Traversal vulnerability

Answer:

D

Question 9

Question Type: MultipleChoice

Thomas is not skilled in secure coding. He neither underwent secure coding training nor is aware of the consequences of insecure coding. One day, he wrote code as shown in the following screenshot. He passed 'false' parameter to setHttpOnly() method that may result in the existence of a certain type of vulnerability. Identify the attack that could exploit the vulnerability in the above case.

Options:

A- Denial-of-Service attack
B- Client-Side Scripts Attack
C- SQL Injection Attack
D- Directory Traversal Attack

Answer:

B

Question 10

Question Type: MultipleChoice

In a certain website, a secure login feature is designed to prevent brute-force attack by implementing account lockout mechanism. The account will automatically be locked after five failed attempts. This feature will not allow the users to login to the website until their account is unlocked. However, there is a possibility that this security feature can be abused to perform _____ attack.

Options:

A- Failure to Restrict URL
B- Broken Authentication
C- Unvalidated Redirects and Forwards
D- Denial-of-Service [Do

Answer:

D

Question 11

Question Type: MultipleChoice

Ted is an application security engineer who ensures application security activities are being followed during the entire lifecycle of the project. One day, he was analyzing various interactions of users depicted in the use cases of the project under inception. Based on the use case in hand, he started depicting the scenarios where attacker could misuse the application. Can you identify the activity on which Ted is working?

Options:

A- Ted was depicting abuse cases
B- Ted was depicting abstract use cases
C- Ted was depicting lower-level use cases
D- Ted was depicting security use cases

Answer:

A

Question 12

Question Type: MultipleChoice

Which of the following relationship is used to describe security use case scenario?

Options:

A- Threatens Relationship
B- Extend Relationship
C- Mitigates Relationship
D- Include Relationship

Answer:

B