



Free Questions for 312-96 by [braindumpscollection](#)

Shared by [Hartman](#) on 24-05-2024

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

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 2

Question Type: MultipleChoice

Which of the following Spring Security Framework configuration setting will ensure the protection from session fixation attacks by not allowing authenticated user to login again?

Options:

- A- session-fixation-protection ='newSessionID'
- B- session-fixation-protection ='.'
- C- session-fixation-protection ='enabled'
- D- session-fixation-protection ='.'

Answer:

B

Question 3

Question Type: MultipleChoice

Which of the risk assessment model is used to rate the threats-based risk to the application during threat modeling process?

Options:

A- DREAD

B- SMART

C- STRIDE

D- RED

Answer:

C

Question 4

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 5

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

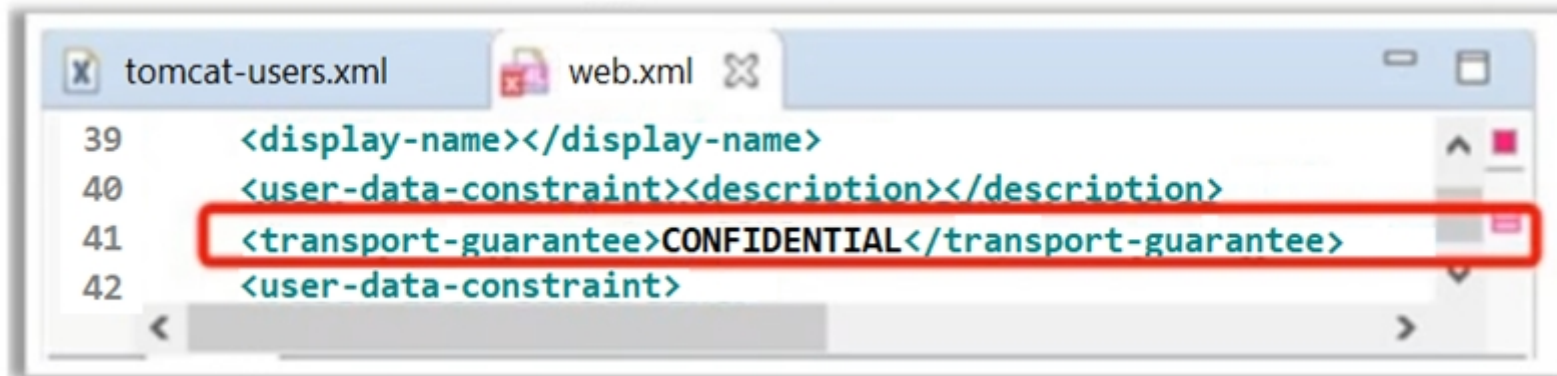
Answer:

D

Question 6

Question Type: MultipleChoice

Oliver, a Server Administrator (Tomcat), has set configuration in web.xml file as shown in the following screenshot. What is he trying to achieve?



The screenshot shows a code editor with two tabs: 'tomcat-users.xml' and 'web.xml'. The 'web.xml' tab is active and shows the following XML code:

```
39 <display-name></display-name>
40 <user-data-constraint><description></description>
41 <transport-guarantee>CONFIDENTIAL</transport-guarantee>
42 <user-data-constraint>
```

The line containing the configuration `<transport-guarantee>CONFIDENTIAL</transport-guarantee>` is highlighted with a red rectangle.

Options:

- A- He wants to transfer the entire data over encrypted channel
- B- He wants to transfer only response parameter data over encrypted channel
- C- He wants to transfer only request parameter data over encrypted channel
- D- He wants to transfer only Session cookies over encrypted channel

Answer:

A

To Get Premium Files for 312-96 Visit

<https://www.p2pexams.com/products/312-96>

For More Free Questions Visit

<https://www.p2pexams.com/eccouncil/pdf/312-96>

