ECCouncil.312-96.vAug-2023.by.Nuly,20q - DEMO

Number: 312-96
Passing Score: 800
Time Limit: 120 min
File Version: 5.0

Exam Code: 312-96

Exam Name: Certified Application Security Engineer (CASE) JAVA

Exam A

QUESTION 1

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?

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 >

Correct Answer: B
Section:
Explanation:

QUESTION 2

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

A. Threatens Relationship

B. Extend Relationship

C. Mitigates Relationship

D. Include Relationship

Correct Answer: B
Section:
Explanation:

QUESTION 3

Identify the formula for calculating the risk during threat modeling.

A. RISK = PROBABILITY 'Attack

B. RISK = PROBABILITY ' ASSETS

C. RISK = PROBABILITY * DAMAGE POTENTIAL

D. IRISK = PROBABILITY * VULNERABILITY

Correct Answer: C
Section:
Explanation:

QUESTION 4

The threat modeling phase where applications are decomposed and their entry points are reviewed from an attacker's perspective is known as ________

A. Attack Surface Evaluation

B. Threat Classification

C. Threat Identification

D. Impact Analysis

Correct Answer: A
Section:
Explanation:

QUESTION 5

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?

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

Correct Answer: A
Section:
Explanation:

QUESTION 6

A US-based ecommerce company has developed their website www.ec-sell.com to sell their products online. The website has a feature that allows their customer to search products based on the price. Recently, a bug bounty has discovered a security flaw in the Search page of the website, where he could see all products from the database table when he altered the website URL http://www.ec-sell.com/products.jsp?val=100 to http://www.ec-sell.com/products.jsp?val=200 OR '1'='1 -. The product.jsp page is vulnerable to

A. Session Hijacking attack

B. Cross Site Request Forgery attack

C. SQL Injection attack

D. Brute force attack

Correct Answer: C
Section:
Explanation:

QUESTION 7

A developer to handle global exception should use _________ annotation along with @ExceptionHandler method annotation for any class

A. @Advice

B. @ControllerAdvice

C. @globalControllerAdvice

D. @GlobalAdvice

Correct Answer: B
Section:
Explanation:

QUESTION 8

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

A. Include Relationship

B. Threatens Relationship

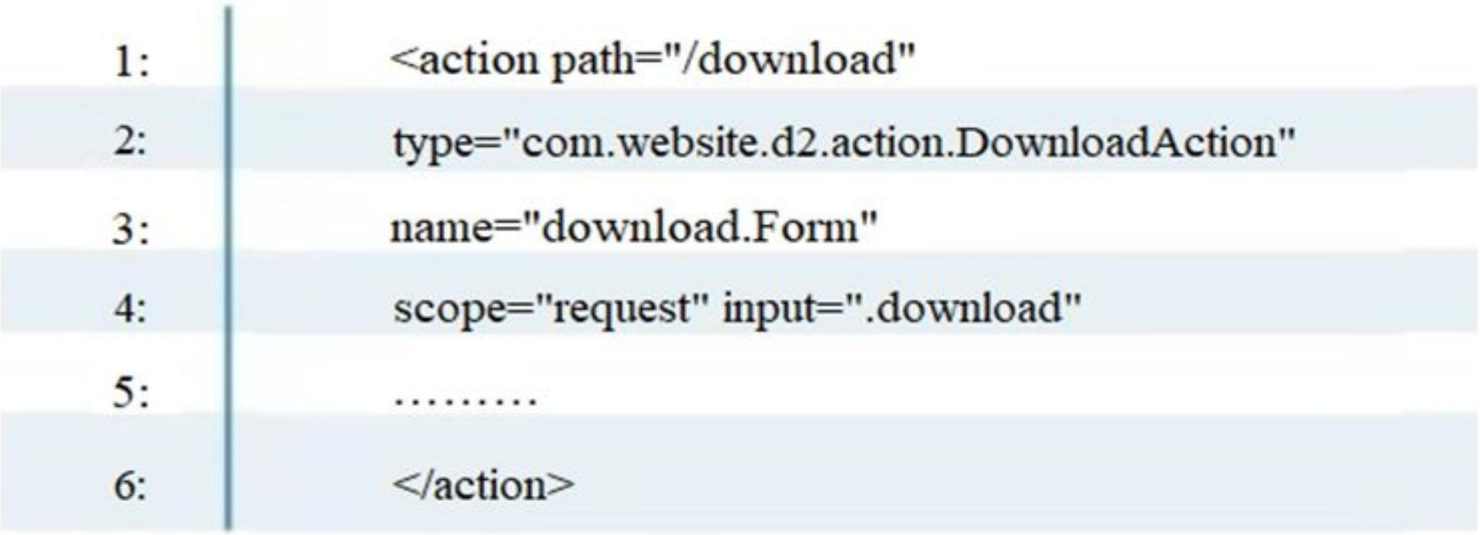
C. Extend Relationship

D. Mitigates Relationship

Correct Answer: B
Section:
Explanation:

QUESTION 9

To enable the struts validator on an application, which configuration setting should be applied in the struts validator configuration file?



```
<action path="/download"
type="com.website.d2.action.DownloadAction"
name="download.Form"
scope="request" input=".download"
.........
</action>
```

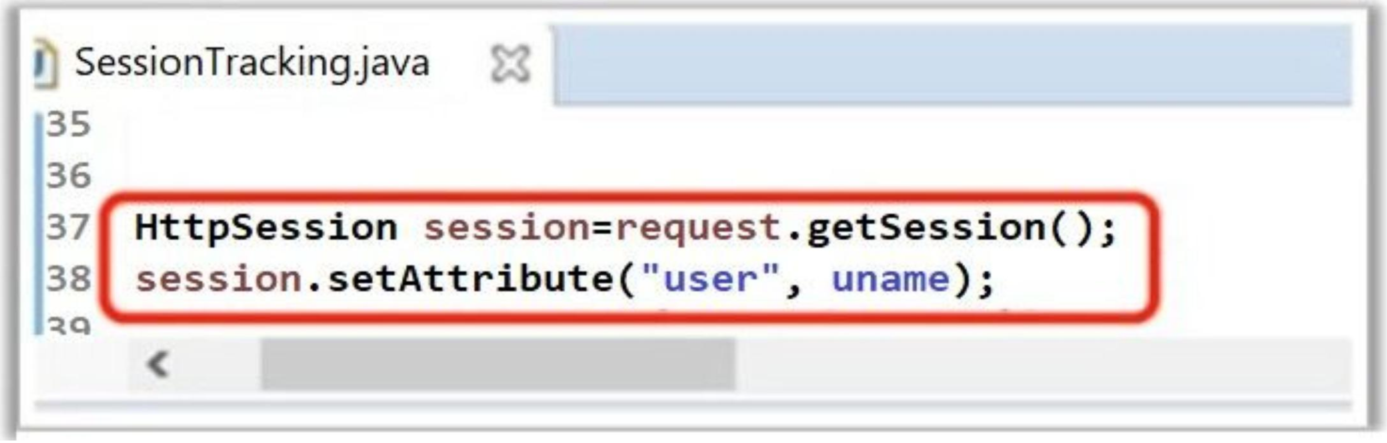
A. valid ate-'true'
B. IsNotvalidate='disabled'
C. IsNotvalidate='false'
D. validate='enabled'

Correct Answer: A
Section:
Explanation:

QUESTION 10
Suppose there is a productList.jsp page, which displays the list of products from the database for the requested product category. The product category comes as a request parameter value. Which of the following line of code will you use to strictly validate request parameter value before processing it for execution?
A. public boolean validateUserName() {String CategoryId= request.getParameter('CatId');}
B. public boolean validateUserName() { Pattern p = Pattern.compile('[a-zA-Z0-9]*$'); Matcher m = p.matcher(request.getParameter(CatId')); boolean result = m.matches(); return result;}
C. public boolean validateUserName() { if(request.getParameter('CatId')!=null) String CategoryId=request.getParameter('CatId');}
D. public.boolean validateUserName() { if(!request.getParamcter('CatId').equals('null'))}
Answer: B

Correct Answer: B
Section:
Explanation:

QUESTION 11
A developer has written the following line of code to handle and maintain session in the application. What did he do in the below scenario?



```
HttpSession session=request.getSession();
session.setAttribute("user", uname);
```

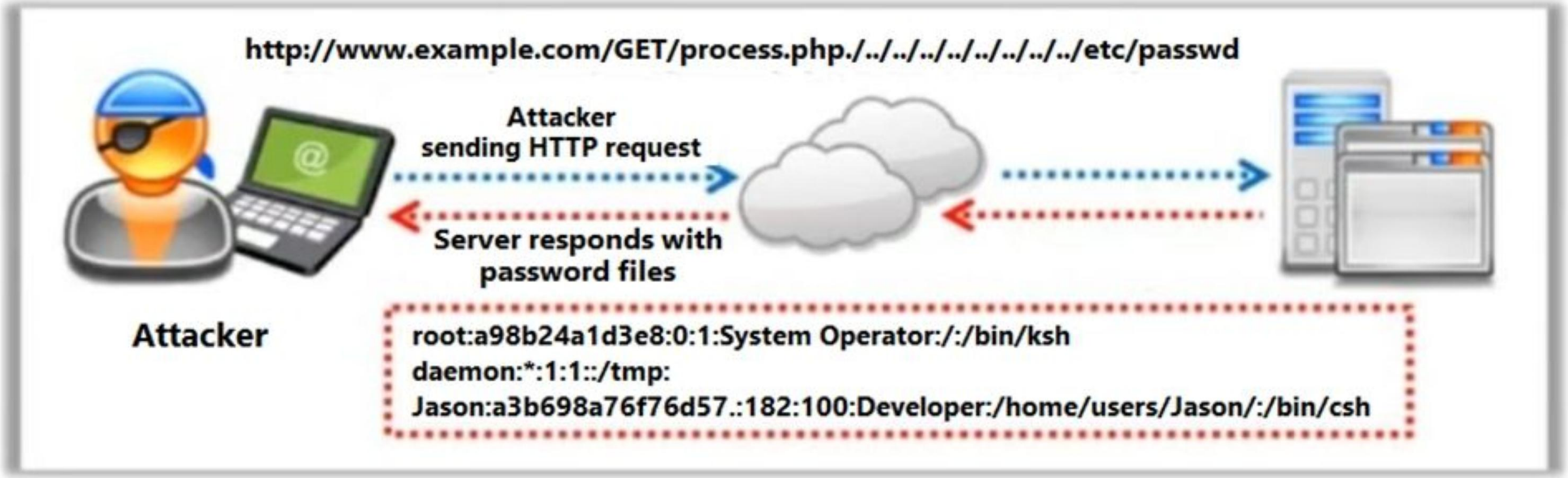
A. Maintained session by creating a Session variable user with value stored in uname variable.
B. Maintained session by creating a HTTP variable user with value stored in uname variable.
C. Maintained session by creating a Cookie user with value stored in uname variable.
D. Maintained session by creating a hidden variable user with value stored in uname variable.

Correct Answer: A
Section:
Explanation:

QUESTION 12
Which of the following configuration settings in server.xml will allow Tomcat server administrator to impose limit on uploading file based on their size?
A. < connector... maxFileLimit='file size' / >
B. < connector... maxPostSize='0'/>
C. < connector... maxFileSize='file size' / >
D. < connector... maxPostSize='file size' / >

Correct Answer: D
Section:
Explanation:

QUESTION 13
Identify the type of attack depicted in the following figure.



```
http://www.example.com/GET/process.php./../../../../../../../../etc/passwd
```

```
root:a98b24a1d3e8:0:1:System Operator:/:/bin/ksh
daemon:*:1:1::/tmp:
Jason:a3b698a76f76d57.:182:100:Developer:/home/users/Jason/:/bin/csh
```

A. Denial-of-service attack
B. SQL Injection attack
C. Directory Traversal Attack
D. Form Tampering Attack

Correct Answer: C
Section:
Explanation:

QUESTION 14
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 of the following settings in CATALINA_HOME/conf/ in web.xml will solve his problem?
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 >

Correct Answer: B
Section:
Explanation:

QUESTION 15
The software developer has implemented encryption in the code as shown in the following screenshot.
However, using the DES algorithm for encryption is considered to be an insecure coding practice as DES is a weak encryption algorithm. Which of the following symmetric encryption algorithms will you suggest for strong encryption?
A. MD5
B. SHA-1
C. Triple DES
D. AES

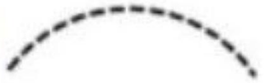
Correct Answer: D
Section:
Explanation:

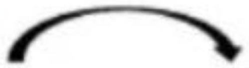
QUESTION 16
James is a Java developer working INFR INC. He has written Java code to open a file, read it line by line and display its content in the text editor. He wants to ensure that any unhandled exception raised by the code should automatically close the opened file stream. Which of the following exception handling block should he use for the above purpose?
A. Try-Catch-Finally block
B. Try-Catch block
C. Try-With-Resources block
D. Try-Catch-Resources block

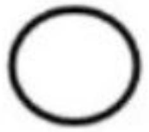
Correct Answer: C
Section:
Explanation:

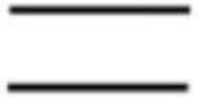
QUESTION 17

Which of the following DFD component is used to represent the change in privilege levels?

1) 

2) 

3) 

4) 

A. 3
B. 4
C. 1
D. 2

Correct Answer: D
Section:
Explanation:

QUESTION 18
Which of the following configurations can help you avoid displaying server names in server response header?
A. < Connector port='8080' protocol='HTTP/1.1' connectionTimeout='20000' redirectPort= '8443' / >
B. < Connector port='8080' protocol='HTTP/1.1' connectionTimeout='20000' ServerName=' disable' redirectPort='8443' / >
C. < Connector port='8080' protocol='HTTP/1.1' connectionTimeout='20000' Server = ' ' redirectPort='8443' / >
D. < Connector port='8080' protocol='HTTP/1.1' connectionTimeout='20000' ServerName ='null ' redirectPort='8443'' / >

Correct Answer: B
Section:
Explanation:

QUESTION 19
Which of the following can be derived from abuse cases to elicit security requirements for software system?
A. Misuse cases
B. Data flow diagram
C. Use cases
D. Security use cases

Correct Answer: D
Section:
Explanation:

QUESTION 20

Which of the following state management method works only for a sequence of dynamically generated forms?

A. Cookies
B. Sessions
C. Hidden Field
D. URL-rewriting

Correct Answer: C
Section:
Explanation: