



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



312-96 Dumps
312-96 Braindumps
312-96 Real Questions
312-96 Practice Test
312-96 Actual Questions



EC-COUNCIL

312-96

*Certified Application Security Engineer (C|ASE Java)
Certification*



Question: 56

Which of the following is a secure coding practice to prevent Remote Code Execution vulnerabilities?

- A. Allowing user-supplied input to be executed without proper validation
- B. Disabling input validation for code execution
- C. Implementing input validation and sanitization for code execution
- D. Using weak or common passwords

Answer: C

Explanation: Implementing input validation and sanitization for code execution is a secure coding practice to prevent Remote Code Execution vulnerabilities. By validating and sanitizing user-supplied input before executing it as code, the risk of malicious code execution can be mitigated. Allowing user-supplied input to be executed without proper validation, disabling input validation for code execution, and using weak or common passwords are insecure practices that can contribute to Remote Code Execution vulnerabilities.

Question: 57

Which of the following is a secure coding practice to prevent Security Vulnerabilities in third-party libraries?

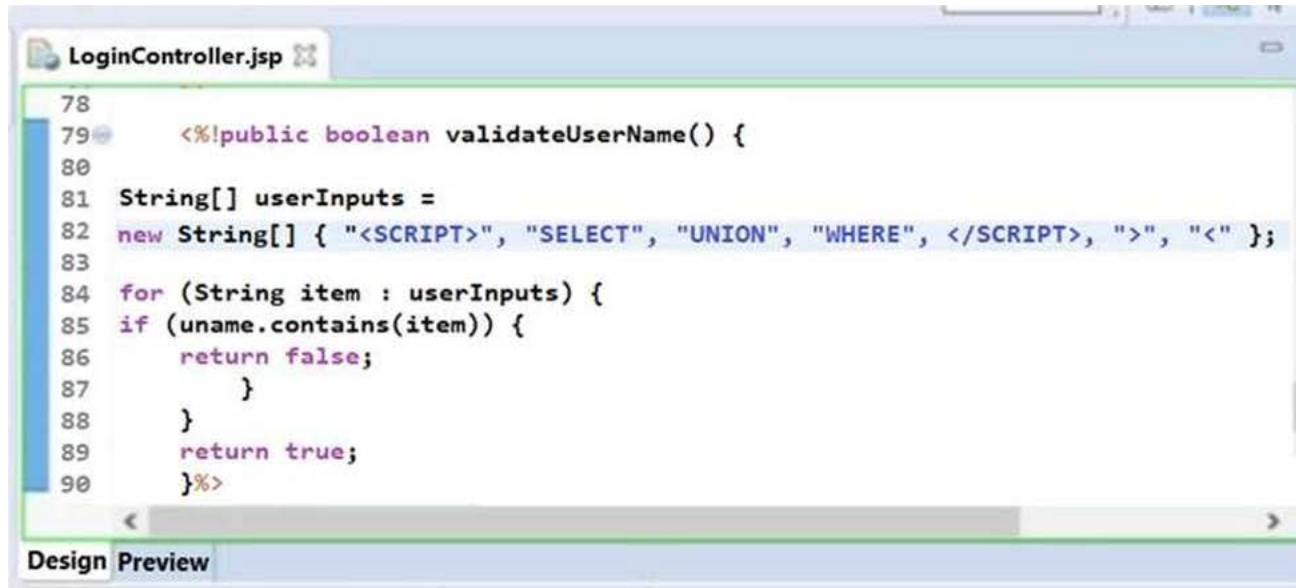
- A. Using outdated and unpatched libraries
- B. Disabling input validation for libraries
- C. Storing sensitive data in plain text in the libraries
- D. Implementing regular updates and patching for libraries

Answer: D

Explanation: Implementing regular updates and patching for libraries is a secure coding practice to prevent Security Vulnerabilities in third-party libraries. By keeping libraries up to date and applying patches promptly, the application can address known vulnerabilities and reduce the risk of exploitation. Using outdated and unpatched libraries, disabling input validation for libraries, and storing sensitive data in plain text in the libraries are insecure practices that can contribute to security vulnerabilities.

Question: 58

Sam, an application security engineer working in INFRA INC., was conducting a secure code review on an application developed in Java. He found that the developer has used a piece of code as shown in the following screenshot.



```
78
79 <%!public boolean validateUserName() {
80
81 String[] userInputs =
82 new String[] { "<SCRIPT>", "SELECT", "UNION", "WHERE", "</SCRIPT>", ">", "<" };
83
84 for (String item : userInputs) {
85 if (uname.contains(item)) {
86     return false;
87     }
88 }
89 return true;
90 }%>
```

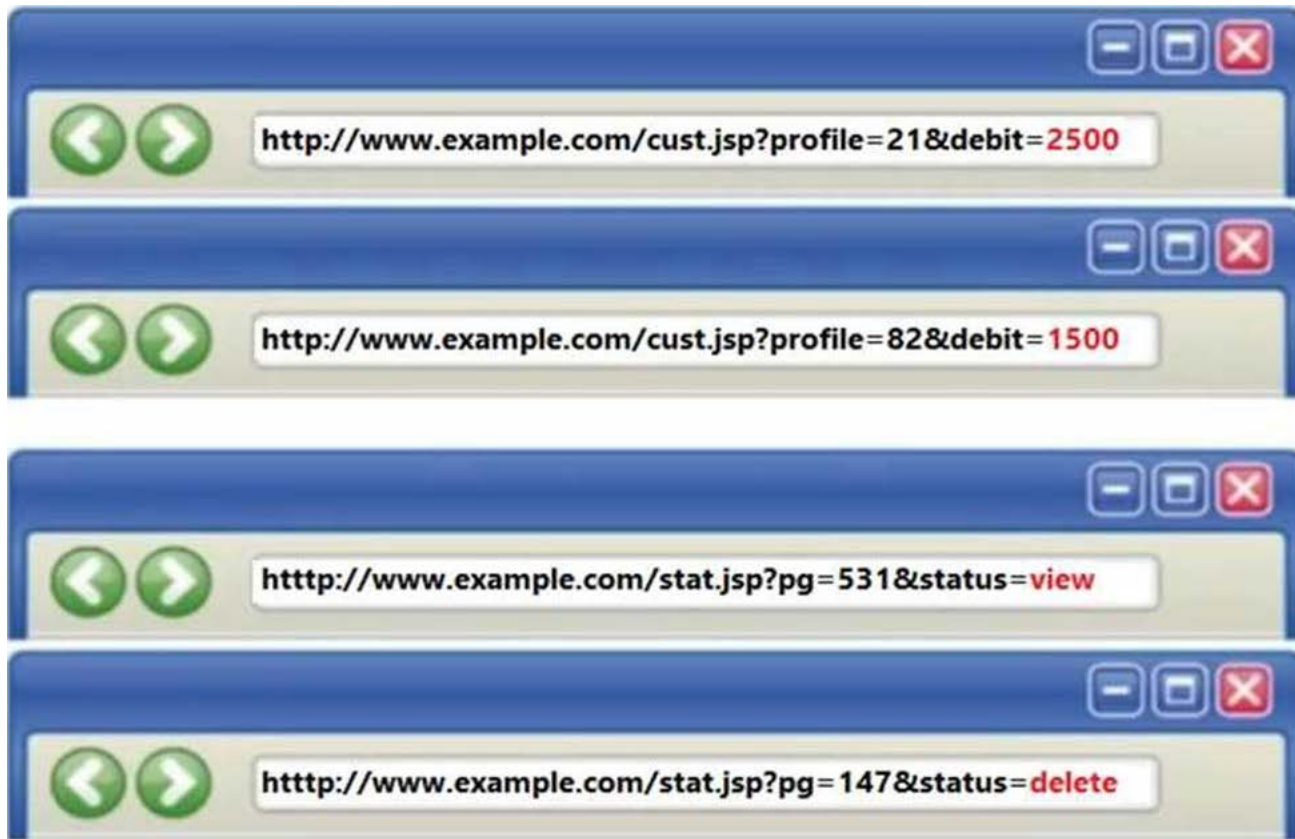
Identify the security mistakes that the developer has coded?

- A. He is attempting to use client-side validation
- B. He is attempting to use whitelist input validation approach
- C. He is attempting to use regular expression for validation
- D. He is attempting to use blacklist input validation approach

Answer: D

Question: 59

Identify the type of attack depicted in the following figure.



- A. SQL Injection Attacks
- B. Session Fixation Attack
- C. Parameter Tampering Attack
- D. Denial-of-Service Attack

Answer: C

Question: 60

According to secure logging practices, programmers should ensure that logging processes are not disrupted by:

- A. Catching incorrect exceptions
- B. Multiple catching of incorrect exceptions
- C. Re-throwing incorrect exceptions
- D. Throwing incorrect exceptions

Answer: D

Question: 61

Which of the threat classification model is used to classify threats during threat modeling process?

- A. RED
- B. STRIDE
- C. DREAD
- D. SMART

Answer: B

Question: 62

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:  }
```

- A. Line No. 1
- B. Line No. 3
- C. Line No. 4
- D. Line No. 5

Answer: B

Question: 63

Alice, a Server Administrator (Tomcat), wants to ensure that Tomcat can be shut down only by the user who owns the Tomcat process. Select the appropriate setting of the CATALINA_HOME/conf in server.xml that will enable him to do so.

- A. < server port="" shutdown="" >
- B. < server port="-1" shutdown="*" >
- C. < server port="-1" shutdown="SHUTDOWN" >
- D. < server port="8080" shutdown="SHUTDOWN" >

Answer: B

Question: 64

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

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

Answer: A

Question: 65

Which of the following elements in web.xml file ensures that cookies will be transmitted over an encrypted channel?

- A. < connector IsSSEnabled="Yes" / >
- B. < connector EnableSSL="true" / >
- C. < connector SSLEnabled="false" / >
- D. < connector SSLEnabled="true" / >

Answer: D

Question: 66

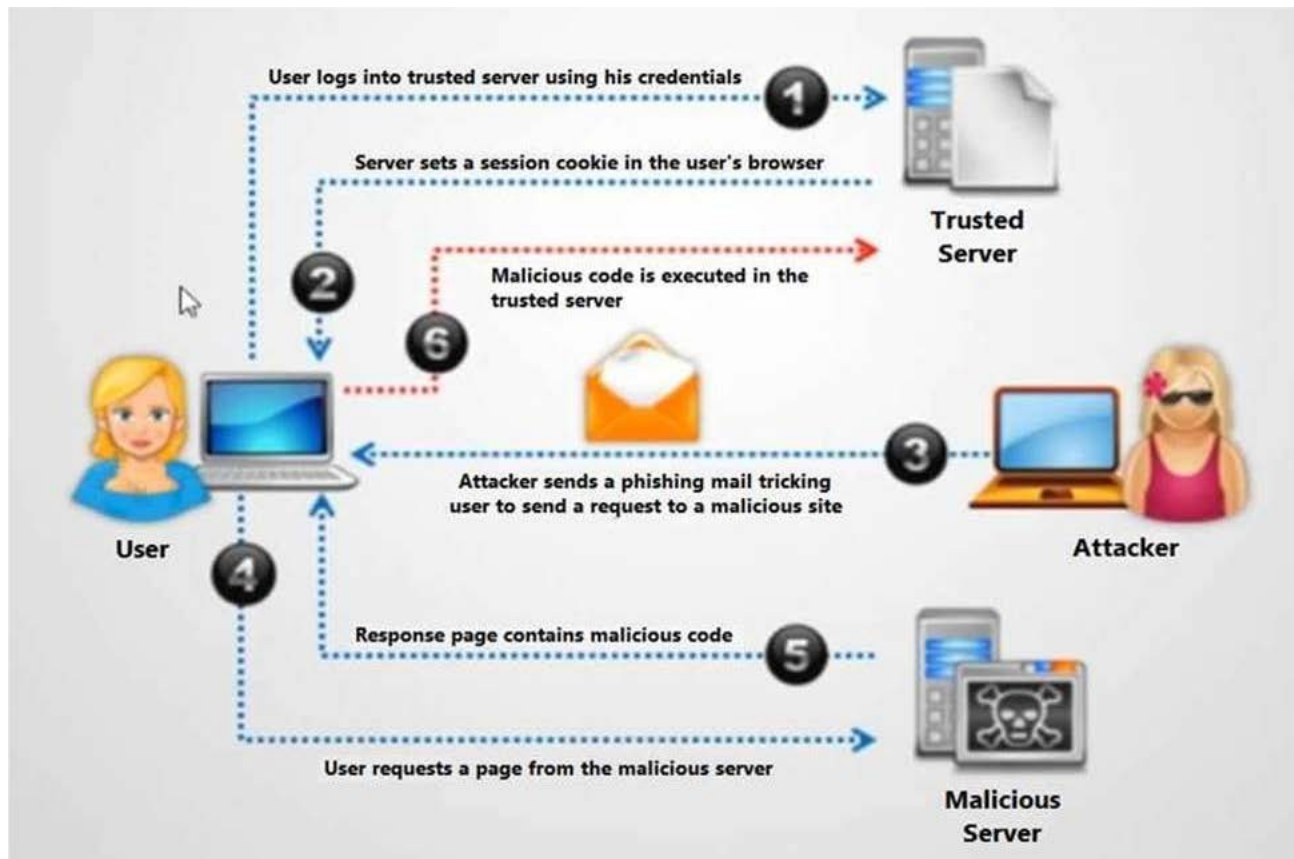
In which phase of secure development lifecycle the threat modeling is performed?

- A. Coding phase
- B. Testing phase
- C. Deployment phase
- D. Design phase

Answer: D

Question: 67

Identify the type of attack depicted in the figure below:



- A. XSS
- B. Cross-Site Request Forgery (CSRF) attack

- C. SQL injection attack
- D. Denial-of-Service attack

Answer: B



SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps: *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests: *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success: *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support: *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>
Kill your exam at First Attempt....Guaranteed!