



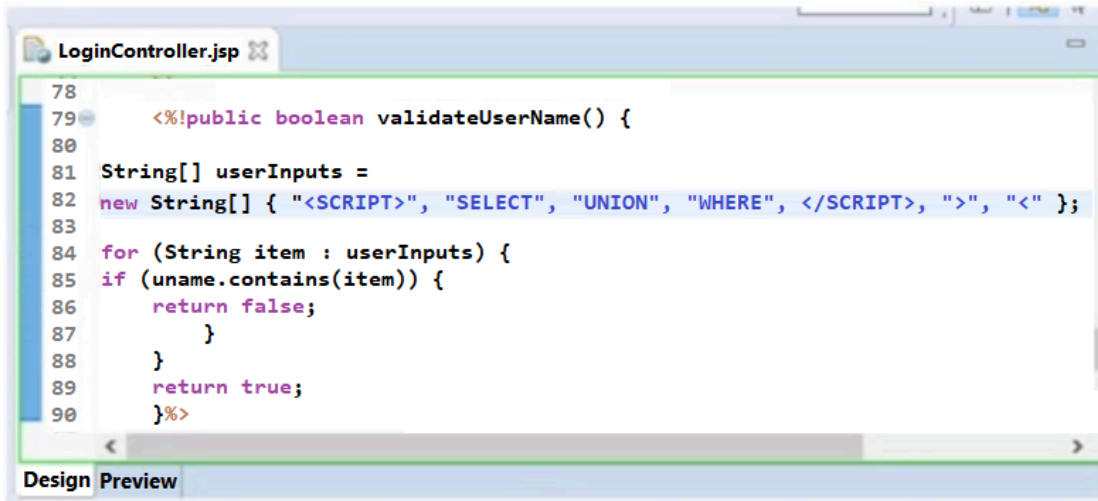
- Expert Verified, Online, **Free**.



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

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. Identify the security mistakes that the developer has coded?



```
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      }%>
```

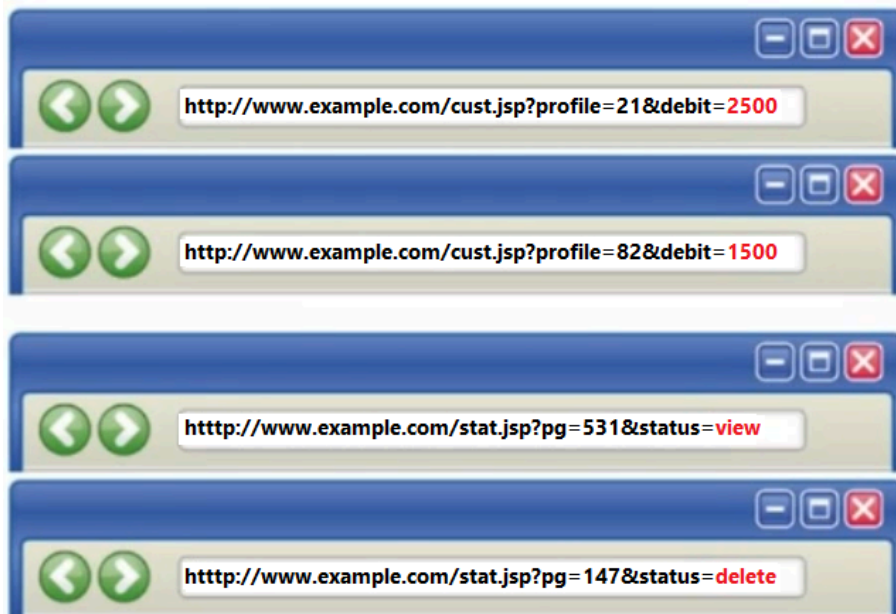
Design Preview

- 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

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

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

**Suggested Answer:** C

Currently there are no comments in this discussion, be the first to comment!

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

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

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

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

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

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

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

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" >

**Suggested Answer: C**

*Community vote distribution*

C (100%)

🗉 **victorfs** 1 year, 3 months ago

**Selected Answer: C**

The correct option IS C

upvoted 1 times

🗉 **DarrenSu** 1 year, 6 months ago

**Selected Answer: C**

C, module 10, "protect shutdown port"

upvoted 2 times

🗉 **Vaine** 1 year, 8 months ago

Is the answer not C??

upvoted 2 times

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

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

**Suggested Answer: A**

Currently there are no comments in this discussion, be the first to comment!

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

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

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

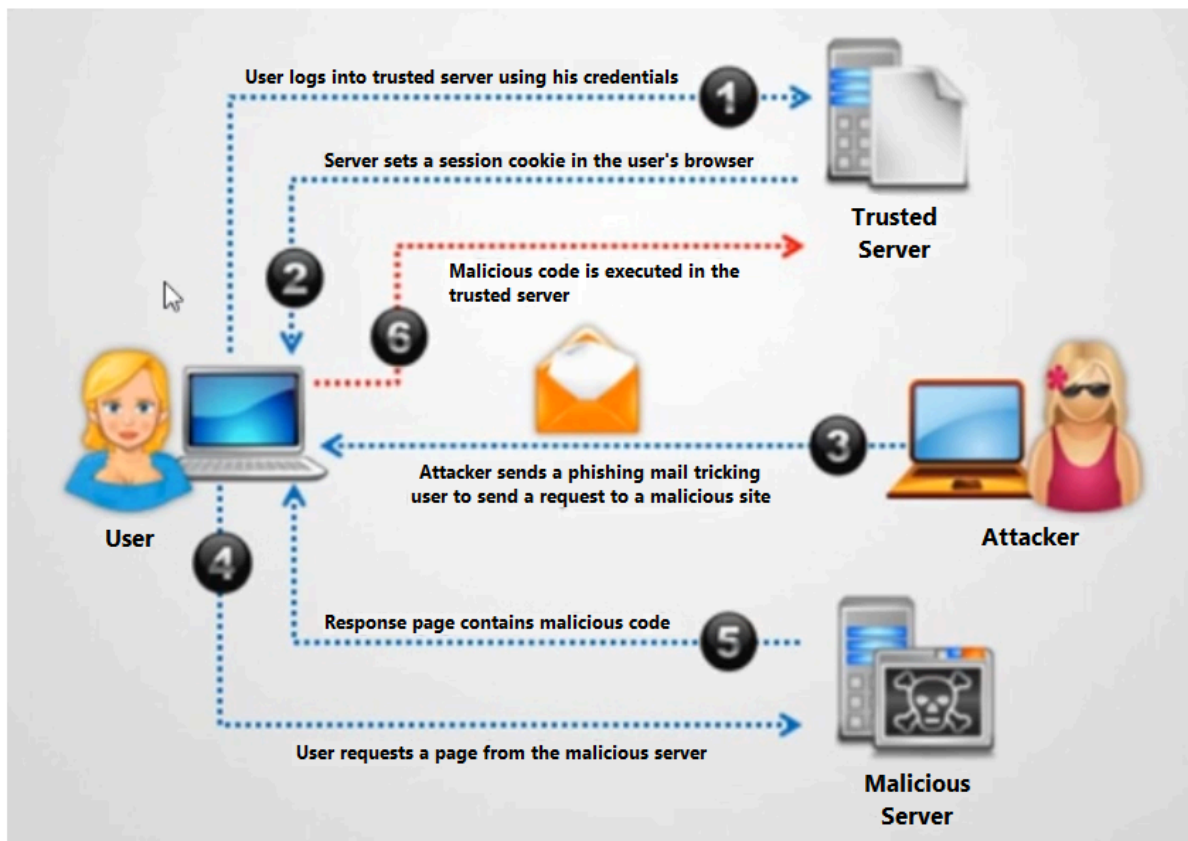
In which phase of secure development lifecycle the threat modeling is performed?

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

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

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

**Suggested Answer:** B

Currently there are no comments in this discussion, be the first to comment!

Stephen is a web developer in the InterCall Systems. He was working on a Real Estate website for one of his clients. He was given a task to design a web page with properties search feature. He designed the following searchpage.jsp

```
< form Id="form1" method="post" action="SearchProperty.jsp" >  
< input type="text" id="txt_Search" name="txt_Search" placeholder="Search Property..." / >  
< input type="Submit" Id="Btn_Search" value="Search" / >  
< /form >
```

However, when the application went to security testing phase, the security tester found an XSS vulnerability on this page. How can he mitigate the XSS vulnerability on this page?

- A. He should write code like out.Write ("You Searched for: " +ESAPI.encoder().encodeForHTML(search));
- B. He should write code like out.write ("You Searched for: " + request.getParameter("search").toString());
- C. He should write code like out.write ("You Searched for: " + request.getParameter("txt\_Search"));
- D. He should write code like out.write (("You Searched for: " +(search));

**Suggested Answer: A**

Currently there are no comments in this discussion, be the first to comment!

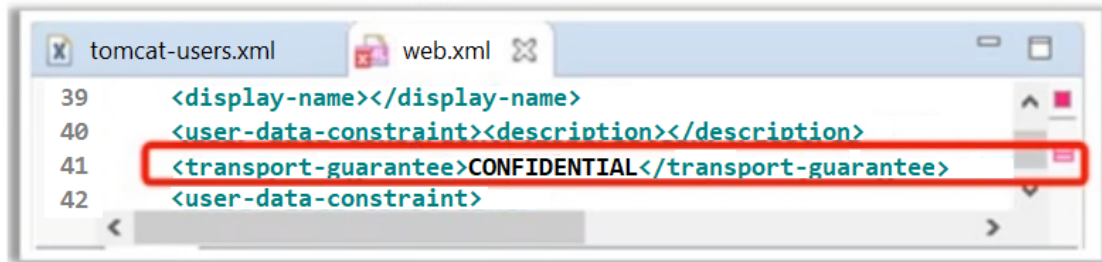
Jacob, a Security Engineer of the testing team, was inspecting the source code to find security vulnerabilities.  
Which type of security assessment activity Jacob is currently performing?

- A. SCST
- B. DAST
- C. CAST
- D. SAST

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

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



- 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

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

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?

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

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

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.

- A. Failure to Restrict URL
- B. Broken Authentication
- C. Unvalidated Redirects and Forwards
- D. Denial-of-Service (DoS)

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

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

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

**Suggested Answer: A**

Community vote distribution

A (100%)

 **TheRodGpe** Highly Voted 1 year, 10 months ago

**Selected Answer: A**

"DREAD model is used to rate the various security threats on the application by calculating risks of each threats" From the page 97 of CASE .NET Courseware  
upvoted 6 times

 **yawmumma** Highly Voted 1 year, 10 months ago

The DREAD model is commonly used to rate the threats-based risk to an application during the threat modeling process. DREAD stands for:

Damage: How bad would an attack be?

Reproducibility: How easy is it to reproduce the attack?

Exploitability: How much work is it to launch the attack?

Affected Users: How many people will be impacted?

Discoverability: How easy is it to discover the threat?

Each category is usually given a score, and the scores are then used to prioritize threats.

So the correct answer is:

A. DREAD

The other options are not standard risk assessment models used for rating threats in threat modeling:

SMART is often used for goal-setting (Specific, Measurable, Achievable, Relevant, Time-bound).

STRIDE is another threat modeling methodology that identifies threats but doesn't rate them (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges).

RED is not a standard risk assessment model in this context.

Therefore, DREAD is the model used for rating threats during the threat modeling process.

upvoted 5 times

 **victorfs** Most Recent 1 year, 3 months ago

**Selected Answer: A**

The correcto is DREAD!

upvoted 2 times

 **Aalkinani** 1 year, 8 months ago

A. DREAD

DREAD is an acronym that stands for:

Damage Potential: How bad would an attack be?

Reproducibility: How easy is it to reproduce the attack?

Exploitability: How easy is it to launch the attack?

Affected Users: How many users would be impacted?

Discoverability: How easy is it to discover the threat?

While STRIDE is used to identify threats (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege), DREAD is used to rate and prioritize those threats.

upvoted 3 times

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?

- A. session-fixation-protection ="newSessionID"
- B. session-fixation-protection ="migrateSession"
- C. session-fixation-protection ="enabled"
- D. session-fixation-protection ="protectSession"

**Suggested Answer: B**

  **yawmumma** 1 year, 3 months ago

In Spring Security, the configuration setting that helps protect against session fixation attacks by migrating the session after the user is authenticated is migrateSession. When this setting is used, Spring Security will ensure that a new session is created upon authentication, thereby invalidating the old session and mitigating the risk of session fixation attacks.

So the correct answer is:

B. session-fixation-protection ="migrateSession"

Here's how you might use it in XML-based Spring Security configuration:

```
<session-management session-fixation-protection="migrateSession" />
```

The other options are not standard settings for session fixation protection in Spring Security:

newSessionID: This is not a standard Spring Security setting for session fixation protection.

enabled: While enabling session management is important, this specific value is not used for session fixation protection in Spring Security.

protectSession: This is not a standard Spring Security setting for session fixation protection.

Therefore, migrateSession is the correct choice for protecting against session fixation attacks by ensuring that authenticated users get a new session.

upvoted 2 times

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-listings < param-value>true < /init-param >`
- B. `< int param > < param-name>directory-listings < param-value>false < /init-param >`
- C. `< int-param > < param-name>listings < param-value>true < /init-param >`
- D. `< int-param > < param-name>listings < param-value>false < /init-param >`

**Suggested Answer: B**

Community vote distribution

D (100%)

🗳️ 👤 **DarrenSu** 1 year, 2 months ago

**Selected Answer: D**

just goolged

upvoted 2 times

🗳️ 👤 **yawmumma** 1 year, 3 months ago

The security risk described is that users can view the website structure and file names, which is commonly known as "Directory Listing." To mitigate this risk, directory listings should be disabled.

The correct option to disable directory listings would be:

D. `<init-param> <param-name>listings</param-name> <param-value>false</param-value> </init-param>`

This setting will ensure that the server does not display a list of files in a directory when there is no default index file (like index.html or index.jsp).

Note: The XML tags in the options provided seem to have typos like int-param and int param, which should ideally be init-param.

So, Alice should use option D to mitigate the security risk of exposing directory listings to users.

upvoted 2 times

🗳️ 👤 **great\_chainick** 1 year, 4 months ago

I think the correct answer is D, because <https://tomcat.apache.org/tomcat-9.0-doc/default-servlet.html>

upvoted 2 times

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

**Suggested Answer: B**

*Community vote distribution*

C (100%)

🗉 👤 **victorfs** 1 year, 4 months ago

**Selected Answer: C**

The correct is C. Mitigates  
upvoted 1 times

🗉 👤 **Seisosakura** 1 year, 10 months ago

C - Mitigates Relationship is the right option  
upvoted 2 times

🗉 👤 **great\_chainick** 1 year, 11 months ago

C. Mitigates Relationship

The "Mitigates Relationship" is used to describe a security use case scenario where a particular security control or countermeasure is employed to reduce or mitigate a specific threat or risk. It shows how a security measure is implemented to address potential security issues identified in the system.

upvoted 2 times

Identify the formula for calculating the risk during threat modeling.

- A.  $\text{RISK} = \text{PROBABILITY} * \text{Attack}$
- B.  $\text{RISK} = \text{PROBABILITY} * \text{ASSETS}$
- C.  $\text{RISK} = \text{PROBABILITY} * \text{DAMAGE POTENTIAL}$
- D.  $\text{RISK} = \text{PROBABILITY} * \text{VULNERABILITY}$

**Suggested Answer:** C

Currently there are no comments in this discussion, be the first to comment!

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

**Suggested Answer: A**

Currently there are no comments in this discussion, be the first to comment!

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

**Suggested Answer:** A

Currently there are no comments in this discussion, be the first to comment!

A US-based ecommerce company has developed their website [www.ec-sell.com](http://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

**Suggested Answer:** C

Currently there are no comments in this discussion, be the first to comment!

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`

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!