Call Us at +1-818-575-6625 | Sign Out | My Cart | Change Password

Welcome Tejesh !

Home » My Account » OCMJEA 5 Exam Simulator - Full Version » Objective - Security - Test » **Review of attempt 1**

Performance History

Objective - Security - Test

Review of attempt 1

Finish review

Started on	Monday, 18 November 2013, 04:40 AM
Completed on	Monday, 18 November 2013, 04:40 AM
Time taken	12 secs
Grade	**0** out of a maximum of 22 (**0**%)
Feedback	FAIL

Show **All** / Correct / In-correct

1. ScreamWorks, a cinema multiplex, has a website from which you may download signed applets with the latest movie trailers, show timings and so on. The applet works on Java 1.3 or higher. The applet needs to write user preferences to a temporary file in the host machine (where it is being executed).

Is this scheme possible? Note that the client has defined a usePolicy and the java.policy has granted no permissions for the applet.

○ a. No, applets,cannot be used here because even signed applets are untrusted if the necessary permissions are not granted. ✓

● b. Yes as the sandbox model does not apply to signed applets. ✗

Choice A is correct.

This question expects you to be familiar with the changes in the Java 2 Security model. In JDK1.2 and higher, all code local and remote can be subjected to a security policy.

By default, remote code will be constrained to the old Sandbox model. However, if a policy file is created with grant privileges, an applet will be restricted to the grants whether or not it is signed. Hence, choice A is correct.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

2. Consider the following scenario: An applet executing in a single thread (no new threads are created) attempts to use excessive amounts of memory by declaring huge arrays and populating them with random data.

Which of the following statement is correct?

○ a. The security manager only allocates a certain amount of memory so it is not possible for an applet to use excessive amounts of memory. ✗

● b. The security manager will effectively starve the applet when it starts to use excessive amounts of memory. ✗

○ c. The security manager will kill the applet when it starts to use excessive amounts of memory. ✗

○ d. The security manager only monitors CPU usage so it is possible for the applet to use an excessive amount of memory. ✗

○ e. The applet will execute without intervention from the security manager. ✓

Choice E is the correct answer.

The security manager does not monitor the memory, CPU or network bandwidth usage of an applet (It is assumed that the operating system will guard against an applet using an excessive amount of resources.). When an applet runs out of memory a java.lang.OutOfMemoryError will be thrown.

Choice A is inappropriate, if not completely incorrect. Generally, operating systems will allocate a certain amount of memory for processes to use but this is not fixed (an applet can ask for more and if available the O/S may assign it). The reason choice A is incorrect is that it is possible for applets to use excessive amounts of memory.

Choices B, C and D are incorrect because the security manager does not monitor an applet's CPU, memory or network bandwidth usage.

For more information please see: http://java.sun.com/sfaq/

Incorrect
Marks for this submission: 0/1.

Feedback to Author

3. Given the following architectural system specification, how would you secure it?

Company web server -5 Office machines -2 Development servers. The company web server needs to serve pages to remote users and office machines need access to the internet.

○ a. Place a firewall around all machines. ✗

○ b. Place the web server behind an outer firewall and all other office machines and development servers behind an inner firewall. ✓

○ c. Put the web server in front of an outer firewall, the office machines behind the outer firewall and the development servers behind an inner firewall. ✗

○ d. Put the web server and development servers behind an outer firewall and all other office machines behind an inner firewall. ✗

○ e. Put a firewall around the development servers. ✗

Choice B is the correct answer.

Given the above architectural system specification you should secure it by creating a DMZ that contains the company web server.

You should put machines that provide services to Internet clients in the DMZ and the office machines and development servers behind an inner firewall.

You would then configure a proxy server in the DMZ to forward the requests from the office machines to the Internet.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

4. The company you work for (Company A) needs to communicate with a new potential partner (Company B). They need to send you some more information regarding their North American sales figures but they do not have a key to encrypt the data. A competitor (Company X) desperately wants to see these figures and you are sure that they are sniffing all traffic between Company A and B.

Given this scenario, which of the following statements are true? Select two choices.

□ a. You should use asymmetric cryptography to send the message. ✓

□ b. You should use symmetric cryptography to send the message. ✗

□ c. It is not possible to securely send the message because you must first send the key to be used to sign the message with. ✗

□ d. The message must be sent over HTTPS. ✗

□ e. The message can be sent over HTTP. ✓

Choices A and E are the correct answers.

It is not possible to use symmetric cryptography to send this message because this would first require sending the key that is used to both encrypt and decrypt. Company X would see this and be able to read the message. With asymmetric cryptography there is a separate key for encrypting (public) and decrypting (private). This allows company A to send out its public key, company B can then encrypt the message with the public key (it doesn't matter that company X may have the public key because you cannot decrypt with this key).

Choice E is correct because the message that has already been encrypted can be sent over HTTP (no extra encryption is required).

For more information please see: http://java.sun.com/sfaq/

Incorrect
Marks for this submission: 0/1.

Feedback to Author

5. Which of the following attacks may be prevented using JSF Validation mechanism?

○ a. Denial of Service ✗

○ b. Man-in-the-Middle Attacks ✗

○ c. Cross-site scripting ✓

○ d. Phishing. ✗

Option C is correct.

Input parameters can be validated for expected input (String, integer, date etc.) through JSF validation thus filtering unwanted input inserted through cross-site scripting.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

6. A hacker is running a program to send a large number of HTTP requests to your website? Which of the following best describes the situation?

○ a. Denial of Service ✓

○ b. Man-in-the-Middle Attacks ✗

○ c. Cross-site scripting ✗

○ d. Phishing. ✗

Option A is correct.

This is an example of Denial of Service. A Denial-of-Service attack (also DoS attack) is an attack on a computer system or network that causes a loss of service to users. Usually it is realized through consuming all of the bandwidth available to the victim network or by overloading the computational resources of the victim system. It can be prevented by using Service Request Queue technique - limiting the number of concurrent requests one application can get while queuing all excess requests.

A Man-in-the-Middle (MitM) attack is a technique where an attack intercepts another user's session, inspects its contents and tries to modify its data or otherwise use it for malicious purposes. Measures to prevent these attacks are to use encryption of sensitive data and prevent the data being read. Some examples are using SSL, avoiding Frames/IFrames, avoid URL rewriting (SessionId is exposed).

Cross Site Scripting (XSS) is a type of computer security exploit where information from one context, where it is not trusted, can be inserted into another context, where it actually is trusted. From the trusted context, attacks can be launched. Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website.

Some of the measures to prevent it : encode the data on the generated pages, escape user input (special characters,tags), validate user input(maximum length) using Frameworks like Struts Validator, users disable javascript, avoid using Frames/IFrames.

Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a social engineering technique to fool users.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

7. Which of the following annotations can be used for securing web applications? Select two choices.

- □ a. @DeclareRoles ✓
- □ b. @RunAs ✓
- □ c. @PermitAll ✗
- □ d. @DenyAll ✗

Options A and B are correct.

Options C and D can be used for EJB.

@PermitAll - Indicates that the given method or all business methods of the given EJB are accessible by everyone.

@DenyAll - Indicates that the given method in the EJB cannot be accessed by anyone.

@RolesAllowed - Indicates that the given method or all business methods in the EJB can be accessed by users associated with the list of roles.

@DeclareRoles - Defines roles for security checking. To be used by EJBContext.isCallerInRole, HttpServletRequest.isUserInRole, and WebServiceContext.isUserInRole.

@RunAs - Specifies the run-as role for the given components.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

8. Which of the following can be configured in the EJB deployment descriptor? Select two choices.

- □ a. Configuration of the datasource accessed by code. ✗
- □ b. Security roles that are used by EJB ✓
- □ c. Security role references for programmatic security ✓
- □ d. EJB Authentication mechanism ✗

Options B and C are correct.

Options A and D are Java EE Server specific.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

9. A malicious hacker has created an applet to cause a denial-of-service style attack by sending packets from the client machine to a 'target' machine (different from the host machine).

Which of the following statements regarding this are true?

- ○ a. This will work as expected. ✗
- ○ b. This cannot be carried out by an applet. ✓
- ○ c. This will only work if the applet is signed. ✗
- ○ d. This may work, but it depends on the configuration of the users browser. ✗

Choice B is the correct answer.

Applets are permitted to make network connections back to the host that they were downloaded from. They aren't however allowed to connect to arbitrary hosts because this would provide a mechanism for denial of service attacks. Also if a firewall or server filters packets by IP address then it would be possible for a downloaded applet to be trusted automatically by the firewall/server (a downloaded applet sending requests from your machine would be sending them with your trusted IP address).

It is not possible to change the priority of the thread that was created by the browser for the applet to run in (to do this would require an O/S call). It is possible for an applet to create new threads and manipulate the threads in the thread group that the browser created for the applet.

The security manager does not monitor the memory, CPU or network bandwidth usage of an applet. (It is assumed that the operating system will guard against an applet using an excessive amount of resources). When an applet runs out of memory a java.lang.OutOfMemoryError will be thrown.Generally speaking, operating systems will allocate a certain amount of memory for processes to use but this not fixed (an applet can ask for more and if available the O/S may assign it).

For more information please see: http://java.sun.com/sfaq/

Incorrect
Marks for this submission: 0/1.

Feedback to Author

10. A disgruntled colleague has written an applet and uploaded on your company's website. The applet periodically spawns new threads to carry out time consuming tasks such as floating point arithmetic.

What effect will this applet have on your company's customers?

- ○ a. No effect, the security manager will not permit the applet to create new threads. ✗
- ○ b. If signed with the company's certificate the applet would execute as expected, using up resources on the customers machine. ✗
- ○ c. The applet would execute as expected, using up resources on the customers machine. ✓
- ○ d. The applet would execute as expected but when excessive amounts of resources were being used, the security manager would detect this and effectively starve the applet. ✗
- ○ e. The applet would execute as expected but when excessive amounts of resources were being used the security manager would detect this and kill the applet. ✗

Choice C is the correct answer.

It is possible for applets to spawn new threads and to manipulate threads within the thread group created by the browser. The security manager does not monitor the CPU, memory, or network bandwidth usage of an applet; instead it is assumed that the O/S will handle this.

Choice A is incorrect because applets can create new threads.

Choice B is incorrect because there is no need for the applet to be signed in order to create new threads.

Choices D and E are incorrect because the security manager does not monitor the resource usage of an applet.

For more information please see: http://java.sun.com/sfaq/

Incorrect
Marks for this submission: 0/1.

Feedback to Author

11. What is a Demilitarized Zone (DMZ)?

- ○ a. The logical separation of tiers in a J2EE application. Example: the separation between the Web Tier and the EJB Tier ✗
- ○ b. The logical separation of layers in a J2EE application. Example: The separation between the Operating System and the EJB Container. ✗
- ○ c. A type of protection offered by proxy firewalls, currently only available to the U.S armed forces under National Security laws. ✗
- ○ d. The region between two firewalls ✓

Choice D is correct.

Demilitarized Zone (DMZ) is an area between two firewalls. The outer firewall lets requests to publicly accessible services in. It will reject all other requests. The inner firewall will protect the company's internal network and prevent requests coming into the DMZ from passing through it.

Choice D is therefore correct.

Choices A, B and C are all incorrect.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

12.

You have a JAR file that has been signed by a third-party vendor. A Trusted Certificate Authority (CA) has signed the third-party vendor's certificate. Is it possible to add any more classes to this JAR file?

○ a. Yes ✓

○ b. No ✗

Choice A is correct, as it is possible to add more classes to the JAR file.

When you sign a JAR file, you are not signing the JAR file itself but individual files it contains. This means you can use a tool like WinZip to add new files (classes, images etc) to the existing JAR file without necessarily invalidating the signature.

Note: The files that are added later, will not be signed.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

13. You have received an email from your Bank about a new campaign where you could win 5000$ prize in case you immediately login into the internet banking site. Email also provides url to the internet banking site. On closer observation you see that it differs from the normal URL that you use. Which of the following best describes the situation?

○ a. Denial of Service ✗

○ b. Man-in-the-Middle Attacks ✗

○ c. Cross-site scripting ✗

○ d. Phishing. ✓

Option D is correct.This is an example of phishing.

A Denial-of-Service attack (also DoS attack) is an attack on a computer system or network that causes a loss of service to users. Usually it is realized through consuming all of the bandwidth available to the victim network or by overloading the computational resources of the victim system. It can be prevented by using Service Request Queue technique - limiting the number of concurrent requests one application can get while queuing all excess requests.

A Man-in-the-Middle (MitM) attack is a technique where an attack intercepts another user's session, inspects its contents and tries to modify its data or otherwise use it for malicious purposes. Measures to prevent these attachs are to use encryption of sensitive data and prevent the data being read. Some examples are using SSL, avoiding Frames/IFrames, avoid URL rewriting (SessionId is exposed).

Cross Site Scripting (XSS) is a type of computer security exploit where information from one context, where it is not trusted, can be inserted into another context, where it actually is trusted. From the trusted context, attacks can be launched.

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message.

Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website.

Some of the measures to prevent it : encode the data on the generated pages, escape user input (special characters,tags), validate user input(maximum length) using Frameworks like Struts Validator, users disable javascript, avoid using Frames/IFrames.

Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a social engineering technique to fool users.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

14. You as a J2EE Architect of a Healthcare company are designing a website where user login and add their dependent details online. It involved basic database updates and retrieval of data. Your senior has suggested to filter special characters such as "; ? -- | " from text boxes.

What could be the reason for his suggestion?

- ○ a. To prevent buffer overflow ✗
- ○ b. To prevent SQL Injection ✓
- ○ c. To prevent weird output errors ✗
- ○ d. It is better to stop the invalid input in the web layer itself, as names seldom have these special characters. ✗

Option B is correct.

Hackers can input these characters and force some unnecessary SQL queries by sending them in input fields. Filtering such special characters can prevent SQL Injection. In similar way, hackers can also send standard HTML tags, which may spoil the display on subsequent pages. Since question does not mention filtering for HTML-related strings, option C is incorrect.

Java language is type-safe, and the runtime provides automatic memory management and range-checking on arrays. These features also make Java programs immune to the buffer overflow attacks possible in the C and C++ programming languages.So, option A is incorrect.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

15. Which of the following is true about annotations for security roles in EJB?

- ○ a. Security roles must be defined either through annotations or ejb-jar.xml but not in both ✗
- ○ b. Security roles can be defined by both mechanisms (annotations & deployment descriptor) but annotations override settings in Deployment Descriptor ✗
- ○ c. Security roles can be defined by both mechanisms (annotations & deployment descriptor) but settings in deployment descriptor override annotations ✓
- ○ d. Both annotations & deployment descriptoy can be used and one of them can be chosen at deploy time. ✗

Option C is a correct statement.

Security roles can be defined by both mechanisms (annotations & Deployment descriptor) but settings in deployment descriptor override annotations.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

16. Which of the following could be used for programmatic security in EJB applications? Select two choices.

- □ a. EJBContext.getUserTransaction().isSecureTransaction ✗
- □ b. UserTransaction.isUserInRole ✗
- □ c. EJBContext.isCallerInRole ✓

Options C and D are correct.

Options A and B are incorrect as there are no such methods.

The javax.ejb.EJBContext application programming interface (API) provides two methods whereby the bean provider can access security information about the enterprise bean caller: isCallerInRole(String rolename) determines if a user is in a specific security role, getCallerPrincipal returning the java.security.Principal object.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

17. You are developing a paint application for use on the web. The application is an applet. As part of the application you need to read a system property that contains information about the user's graphics card. Depending upon the graphics memory, the paint auto-selects a resolution mode to execute in.

Which of the following statements regarding this scenario is true?

- ○ a. This will work as expected. ✗
- ○ b. This cannot be carried out by an applet. ✗
- ○ c. This will only work if the applet is signed. ✗
- ○ d. This may work, but it depends on the configuration of the user's browser. ✓

Choice D is the correct answer.

An applet may or may not be able to read system properties. Some system properties will require an applet to be signed but others can be read without this requirement. System properties can never be modified. Applets are permitted to make network connections back to the host that they were downloaded from.

They aren't however allowed to connect to arbitrary hosts because this would provide a mechanism for denial of service attacks. Also if a firewall or server filters packets by IP address, then it would be possible for a downloaded applet to be trusted automatically by the firewall/server (a downloaded applet sending requests from your machine would be sending them with your trusted IP address). It is not possible to change the priority of the thread that was created by the browser for the applet to run in (to do this would require an O/S call).

It is possible for an applet to create new threads and manipulate the threads in the thread group that the browser created for the applet. The security manager does not monitor the memory, CPU or network bandwidth usage of an applet. (It is assumed that the operating system will guard against an applet using an excessive amount of resources). When an applet runs out of memory, a java.lang.OutOfMemoryError will be thrown. Generally, operating systems will allocate a certain amount of memory for processes to use but this not fixed (an applet can ask for more and if available the O/S may assign it).

For more information please see: http://java.sun.com/sfaq/

Incorrect
Marks for this submission: 0/1.

Feedback to Author

18. Which of the following are NOT permitted by applets?

- ○ a. Creating new threads ✗
- ○ b. Changing the priority of O/S threads ✓
- ○ c. Using excessive amounts of memory ✗
- ○ d. Using excessive amounts of CPU time ✗
- ○ e. Using excessive amounts of network bandwidth ✗

Choice B is the correct answer.

It is not possible to change the priority of the thread that was created by the browser for the applet to run in (to do this would require an O/S call). Choices A, C, D and E are incorrect. It is possible for an applet to create new threads and manipulate the threads in the thread group that the browser created for the applet.

The security manager does not monitor the memory, CPU, or network bandwidth usage of an applet. (It is assumed that the operating system will guard against an applet using an excessive amount of resources). When an applet runs out of memory a java.lang.OutOfMemoryError will be thrown. Generally, operating systems will allocate a certain amount of memory for processes to use but this not fixed (an applet can ask for more and if available, the O/S may assign it).

For more information please see: http://java.sun.com/sfaq/

Incorrect
Marks for this submission: 0/1.

Feedback to Author

19. Which of the following measures can be used in applications for mitigating phishing?

○ a. Use SSL ✗

○ b. Do not use Frames/IFrames. Disable JavaScript ✗

○ c. Add an Intercepting Validation filter to your system to filter our special characters ✗

○ d. None of the above ✓

Since phishing is a social engineering threat, option D is correct.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

20. You have a requirement that the PIN of the customer used for ATM transactions must be encrypted using a one-way encryption algorithm to prevent data theft. Which of the following would you choose?

○ a. 3DES. ✗

○ b. SHA. ✓

○ c. Blowfish. ✗

○ d. RSA ✗

Explanation :
Option B is correct.

This Standard one way encryption using Secure Hash Algorithm, SHA, for computing a condensed representation of a message or a data file. When a message of any length < 264 bits is input, the SHA produces a 160-bit output called a message digest. Hence, ATM PIN will be encrypted using SHA is the best choice.

Option A is incorrect because it is a symmetrical encryption algorithm.

Option C is incorrect because it is a symmetrical encryption algorithm.

Option D is incorrect because it is a asymmetrical encryption algorithm.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

21. Which security constraints can be specified in the web.xml deployment descriptor?

○ a. Restrictions based on user login. ✗

○ b. Restriction on Struts actions. ✗

○ c. Restrictions on encryption methods ✗

○ d. Restriction based on role name. ✓

Option A is incorrect because this is vendor specific.

Option B is incorrect because this is handled in different .xml files.

Option C is incorrect because you can only specify a transport guarantee. The browser and SSL server determine the protocol.

Option D is correct.

Incorrect

Marks for this submission: 0/1.

Feedback to Author

22. Which of the following can be configured through Java EE deployment descriptors?

- ○ a. Ports such as HTTP, HTTPS ✗
- ○ b. Connection pool configuration ✗
- ○ c. Fine-tuned Security constraints in the application code ✓
- ○ d. JTA Transaction timeout ✗

Option C is correct.

Options A, B and D are Java EE Server specific. You can mention roles and role references in web.xml.

Incorrect
Marks for this submission: 0/1.

Feedback to Author

Finish review