

Exam Code: 000-139

Exam Name: IBM Certified Specialist - IBM Rational
AppScan, Standard Ed

Vendor: IBM

Version: DEMO

Part: A

1: Which type of vulnerability can occur when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter?

- A. Cross-site Scripting
- B. Insecure Direct Object Reference
- C. Injection Flaw
- D. Cross Site Request Forgery

Correct Answers: B

2: Which lines in an HTTP response would trigger a positive result from an AppScan test for a vulnerability of type Possible Server Path Disclosure Pattern Found?

- A. `<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">`
- B. `<!--#include file="file.htm"-->`
- C. `d:\backup\website\oldfiles`
- D. `./images/header/ibm/logoBigBlue.jpg`

Correct Answers: C

3: In the AppScan Application Data view, what can help you determine if your application was fully explored? (Choose two.)

- A. Visited URLs
- B. JavaScripts
- C. Cookies
- D. Broken links

Correct Answers: A D

4: Which AppScan report type relates to Sarbanes-Oxley Act, HIPPA and FISMA?

- A. Compliance
- B. WASC Threat Classification
- C. OWASP Top 10
- D. Delta Analysis

Correct Answers: A

5: Which three actions should you take if your application requires form-based authentication? (Choose three.)

- A. record a login sequence
- B. configure platform authentication
- C. configure client-side certificates
- D. ensure that in-session detection is enabled and properly configured
- E. ensure that all session tokens are being tracked
- F. reduce the number of threads to one

Correct Answers: A D E

6: Which defense is most reliable in protecting a Web application from being hacked?

- A.set up an application firewall
- B.use SSL encryption
- C.set up an Intrusion Detection System
- D.write secure code

Correct Answers: D

7: You notice that when you run your scan, your login account gets locked out. How can you resolve the issue?

- A.disable tests on your login and logout pages
- B.disable JavaScript execute
- C.reduce the number of threads
- D.increase the timeout limit

Correct Answers: A

8: Directories containing sensitive files must be hidden from the user. What is the best way to hide the existence and content of such a directory?

- A.configure your Web server to issue a response: 403 ?Access forbidden
- B.configure your Web server to issue a response: 302 - Redirect to home
- C.list the directory contents
- D.configure your Web server to issue a response: 404 - Not Found

Correct Answers: D

9: Why is it important to encrypt the HTTP traffic for an authenticated connection between a client and Web server?

- A.to prevent SQL injection
- B.to prevent sensitive information from being stolen
- C.to prevent Cross-site Scripting
- D.to prevent Web site defacement

Correct Answers: B

10: After 30 minutes your scan stops with an out-of-session error. What is a possible cause of this error?

- A.Redundant path limit was too low.
- B.A parameter was not tracked.
- C.Flash parsing was turned off.
- D.Platform authentication was not configured.

Correct Answers: B

11: AppScan sent the following test HTTP request:

```
GET /web/content/index.php?file=../../../../../../../../etc/passwd%00 HTTP/1.0
```

Cookie:

```
JSESSIONID=dqt0LSnfhdVyTJkCwTwfLQQskTTGYX9D79tLLpT1yLQjVhSpZKP9!91437652  
3; customerLanguage=en
```

Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: www.ibm.com

Although, there is no indication in the response about the existence of a password file, AppScan reported a vulnerability with the following reasoning:

Global Validation found an embedded script in the response (<script>alert(25053)</script>), which was probably injected by a previous test.

The presence of this script in the site suggests that the application is vulnerable to which type of attack?

- A. Stored Cross-site Scripting
- B. Cross-site Scripting
- C. Namazu Path Traversal
- D. Directory Listing

Correct Answers: A

12: What information does difference displayed in the Request / Response tab provide?

- A. the difference between two tests
- B. how the vulnerability was resolved
- C. how AppScan constructed the test HTTP request
- D. how the Web application page has been modified from its previous version

Correct Answers: C

13: You are scanning a Web site in a pre-production environment. You notice that your scan is running very slowly and there are numerous communication errors. What would you do to resolve the problem?

- A. increase the number of threads and decrease the timeout limit
- B. decrease the number of threads and increase the timeout limit
- C. increase the number of threads and increase the timeout limit
- D. set the timeout to 0 for infinite timeout

Correct Answers: B

14: Which type of vulnerability allows an attacker to execute a malicious script in a user browser?

- A. Cross-site Scripting
- B. Injection Flaw
- C. Insecure Direct Object Reference
- D. Failure to restrict URL access

Correct Answers: A

15: Which statement is true about infrastructure vulnerabilities?

- A. They are caused by insecure coding and are fixed by modifying the application code.
- B. They are detected using application security scanners and exist in the Web application.
- C. They are known vulnerabilities and are fixed by modifying the application code.
- D. They exist in third-party components and are fixed by applying security patches.

Correct Answers: D

16: What does secure session management require?

- A.session tokens that are given long lifetimes
- B.session tokens that are invalidated when the user logs out
- C.session tokens that are persistent
- D.session tokens that are numeric

Correct Answers: B

17: Your site contains the following URL:

`http://www.mycompany.com/smb/default.jsp?page=wireless&productID=65343,`

In this URL, the page parameter defines a unique page and the productID parameter defines a different product page, based on a template.

How would you configure AppScan to thoroughly explore this site while avoiding redundant URLs? (Choose two.)

- A.ensure JavaScript Execute is turned on
- B.ignore the page parameter
- C.turn off Redundant Path limit
- D.track the page parameter
- E.Track the productID parameter
- F.Ignore the productID parameter

Correct Answers: C F

18: You are scanning a Web application in a pre-production environment. During your initial assessment, you notice that some of the links are specified by IP and some by host name. Your starting URL contains an IP address, `http://12.34.56.67/default.jsp`. When the scan completes, you discover that it has not covered a significant portion of your Web application. What could be the reason?

- A.The host name is not added to the list of additional domains and servers.
- B.The scan is configured to use only one connection.
- C.There is no route to IP 12.34.56.67.
- D.You are not licensed to scan IP 12.34.56.67.

Correct Answers: A

19: You expect your scan to cover around 500 pages, but instead it covers 55. What are three possible reasons for this? (Choose three.)

- A.You chose the wrong test policy.
- B.The login failed.
- C.You specified only one connection.
- D.JavaScript Execution was not enabled.
- E.The redundant path limit was set too low.

Correct Answers: B D E

20: Which Web application operation indicates that the application may be vulnerable to

Cross-site Request Forgery?

A.GET transferfunds.aspx?sacct=3434&dacct=56745&formtoken= YUR345

B.GET sendemail.aspx?address=jsmith@dfg.com&subject=hello&content=

C.GET search.aspx text=ersonal banking

D.GET login.aspx

Correct Answers: B