



**000-139**

**AppScan Standard Edition**

**Exam number/code:** 000-139

**Exam name:** AppScan Standard Edition

**Questions & Answers:** 52 Q&A

**Related Certifications:** [Certified Specialist](#)



**Hundreds of people each day pass their IT certification exams with Testking guaranteed certification resources and training kits.**

Use the [IBM 000-139](#) questions and answers to practice for your next IBM certification exam. If you don't pass – you don't pay! Testking has the first and only 100% product satisfaction and exam passing guarantee. Advanced practice questions and answers help drive the information into your routine thinking and surpass 000-139 brain dumps in retention and skill building.

[IBM](#) 000-139 exam answers and practice questions can be used at home or office, installable on up to two PCs, or print the questions and answers to take with you and train on-the-go! IBM 000-139 preparation tools are the perfect fit for any IBM certification candidate with [000-139](#) training materials for every level of entry.

### **Exam Engine Features**

Control your IT training process by customizing your practice certification questions and answers. The fastest and best way to train.

- \* Truly interactive practice tests
- \* Create and take notes on any question
- \* Retake tests until you're satisfied
- \* YOU select the areas of the exam to cover
- \* Filter questions for a new practice test experience each time
- \* Re-visit difficult questions

**Exam: 000-139 Certification Questions & Answers**

**Question 1:**

Which type of vulnerability allows an attacker to browse files that shouldn't be accessible (e.g. \*.bak, "Copy of", \*.inc, etc.) or pages restricted for users with higher privileges?

- A. Failure to Restrict URL Access
- B. Injection Flaw
- C. Insecure Cryptographic Storage
- D. Insecure Communication

**Answer: A**

**Question 2:**

How does AppScan test a Web application?

- A. by sniffing network traffic
- B. by sending HTTP requests
- C. by scanning the Web server host machine
- D. by performing a port scan

**Answer: B**

**Question 3:**

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

**Answer: A**

**Question 4:**

Which HTTP response codes trigger Application Error vulnerabilities?

- A. 302
- B. 403
- C. 500
- D. 200

**Answer: C**

**Question 5:**

When would you set up a multi-step operation in AppScan?

- A. when your application requires specific user input
- B. when your application has two-factor authentication
- C. when your application requires JavaScript execution
- D. when your application requires a specific flow

**Answer: D**

**Question 6:**

What is indicative of Information Leakage vulnerability?

- A. The message script error: Please contact the Web site administrator! is displayed.
- B. The exception call stack is displayed.
- C. When the user logs in, hello, username! is displayed.
- D. The message incorrect username or password! is displayed.

**Answer: B**

**Question 7:**

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. d:\backup\website\oldfiles
- C. <!--#include file="file.htm"-->
- D. ./images/header/ibm/logoBigBlue.jpg

**Answer: B**

**Question 8:**

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

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

**Answer: A,B,E**

**Question 9:**

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

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

**Answer: D**

**Question 10:**

What information does reasoning displayed in the Request / Response tab provide?

- A. howAppScan constructed the test
- B. why this issue causes non-compliance
- C. whyAppScan concluded that there is an issue
- D. how to avoid this type of issue

**Answer: C**

**Question 11:**

Which three steps should you take before running a security scan with AppScan? (Choose three.)

- A. notify IT and Web Operations teams
- B. ensure only one thread is specified intheAppScan configuration
- C. notify application users
- D. back up your database
- E. ensure that you have specified which reports you want to create
- F. disable employed SMTP server

**Answer: A,D,F**

**Question 12:**

Your site contains the following URL:

<http://www.mycompany.com/smb/default.jsp?page=wireless>

In this URL, the Page parameter defines a unique page.

How would you configure AppScan to fully explore this site?

- A. track the Page parameter
- B. turn off Redundant Path limit
- C. ensure JavaScript Execute is turned on
- D. ignore the Page parameter

**Answer: B**

**Question 13:**

AppScan received the following test response:

An Error Has Occurred

Summary:

Syntax error in string in query expression 'userid = ". Error Message:

System.Data.OleDb.OleDbException: Syntax error in string in query expression 'userid = "  
at

System.Data.OleDb.OleDbCommand.ExecuteNonQueryForSingleResult(tagDBPARAM  
S dbParams, Object executeResult) at ?

Which type of vulnerability does this error message indicate?

- A. Possible Server Path Disclosure Found
- B. SQL Injection
- C. XSS
- D. Blind SQL Injection

**Answer: B**

**Question 14:**

Which statement is true about application-specific vulnerabilities?

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

**Answer: B**

**Question 15:**

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

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

**Answer: B**

**Related 000-139 Exams:**

<a href="#">000-132</a>	<a href="#">000-130</a>	<a href="#">000-190</a>	<a href="#">000-428</a>	<a href="#">000-427</a>
<a href="#">000-917</a>	<a href="#">000-425</a>	<a href="#">000-424</a>	<a href="#">000-816</a>	<a href="#">000-389</a>
<a href="#">000-974</a>	<a href="#">000-229</a>	<a href="#">000-388</a>	<a href="#">000-973</a>	<a href="#">000-228</a>
<a href="#">000-387</a>	<a href="#">000-386</a>	<a href="#">000-385</a>	<a href="#">000-223</a>	<a href="#">000-382</a>
<a href="#">000-222</a>	<a href="#">000-512</a>	<a href="#">000-671</a>	<a href="#">000-085</a>	<a href="#">000-906</a>
<a href="#">000-081</a>	<a href="#">000-969</a>	<a href="#">000-968</a>	<a href="#">000-966</a>	<a href="#">000-965</a>
<a href="#">000-961</a>	<a href="#">000-866</a>	<a href="#">000-960</a>	<a href="#">000-864</a>	<a href="#">000-119</a>
<a href="#">000-863</a>	<a href="#">000-118</a>	<a href="#">000-370</a>	<a href="#">000-210</a>	<a href="#">000-115</a>
<a href="#">000-114</a>	<a href="#">000-113</a>	<a href="#">000-111</a>	<a href="#">000-601</a>	<a href="#">000-600</a>
<a href="#">000-665</a>	<a href="#">000-014</a>	<a href="#">000-079</a>	<a href="#">000-076</a>	<a href="#">000-074</a>
<a href="#">000-071</a>	<a href="#">000-070</a>	<a href="#">000-858</a>	<a href="#">000-208</a>	<a href="#">000-857</a>
<a href="#">000-207</a>	<a href="#">000-856</a>	<a href="#">000-206</a>	<a href="#">000-855</a>	<a href="#">000-205</a>
<a href="#">000-204</a>	<a href="#">000-203</a>	<a href="#">000-268</a>	<a href="#">000-202</a>	<a href="#">000-201</a>
<a href="#">000-266</a>	<a href="#">000-200</a>	<a href="#">000-754</a>	<a href="#">000-753</a>	<a href="#">000-752</a>
<a href="#">000-751</a>	<a href="#">000-750</a>	<a href="#">000-551</a>	<a href="#">000-550</a>	<a href="#">000-357</a>
<a href="#">000-749</a>	<a href="#">000-351</a>	<a href="#">000-748</a>	<a href="#">SPS-100</a>	<a href="#">000-747</a>
<a href="#">000-M64</a>	<a href="#">000-746</a>	<a href="#">000-745</a>	<a href="#">000-253</a>	<a href="#">000-252</a>
<a href="#">000-743</a>	<a href="#">000-742</a>	<a href="#">000-741</a>	<a href="#">000-740</a>	<a href="#">000-645</a>
<a href="#">000-153</a>	<a href="#">000-152</a>	<a href="#">000-642</a>	<a href="#">000-641</a>	<a href="#">000-050</a>

## TestKing [IBM 000-139](#) Exam Questions & Answers

<a href="#">000-839</a>	<a href="#">000-639</a>	<a href="#">000-798</a>	<a href="#">000-638</a>	<a href="#">000-637</a>
<a href="#">000-636</a>	<a href="#">000-635</a>	<a href="#">000-634</a>	<a href="#">000-633</a>	<a href="#">000-535</a>
<a href="#">000-923</a>	<a href="#">000-239</a>	<a href="#">000-331</a>	<a href="#">000-330</a>	<a href="#">000-884</a>

### Popular Certification Exams:

<a href="#">HP0-M39</a>	<a href="#">E20-097</a>	<a href="#">HP0-S18</a>	<a href="#">000-719</a>	<a href="#">000-775</a>
<a href="#">HP0-Y19</a>	<a href="#">090-600</a>	<a href="#">E20-532</a>	<a href="#">510-308</a>	<a href="#">70-232</a>
<a href="#">000-733</a>	<a href="#">HP0-J27</a>	<a href="#">220-221</a>	<a href="#">HP2-E19</a>	<a href="#">642-241</a>

### Hot Certifications:

<a href="#">Ericsson Certification</a>	<a href="#">ENS</a>	<a href="#">MCITP: Enterprise Messaging Administrator 2010</a>	<a href="#">Oracle EBS</a>	<a href="#">Associate BPM Program Manager</a>
--	---------------------	--	----------------------------	---

### Popular Certification Providers:

<a href="#">Isaca</a>	<a href="#">SPSS</a>	<a href="#">TIA</a>	<a href="#">APC</a>	<a href="#">Ruby</a>
-----------------------	----------------------	---------------------	---------------------	----------------------