

IBM 000-139

000-139 AppScan Standard Edition

Practice Test

Version 1.1

QUESTION NO: 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

Answer: B

QUESTION NO: 2

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.

Answer: B

QUESTION NO: 3

AppScan sent the following test HTTP request:

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

Cookie:

```
JSESSIONID=dqt0LSnfhdVyTJkCwTwfLQQSkTTGYX9D79tLLpT1yLQjVhSpZKP9!914376523;  
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 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

Answer: A

QUESTION NO: 4

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

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

Answer: C

QUESTION NO: 5

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

Answer: B

QUESTION NO: 6

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