HP

Exam HP0-M25

Assessing Web Application Security

Version: 5.0

[Total Questions: 120]

Topic 0, A

A

Question No : 1 - (Topic 0)

What are the Network Authentication techniques supported by WebInspect? (Select three.)

A. NTLM
B. Kerberos
C. htaccess
D. Cybersafe
E. HTTP Basic
F. Retinal Scan

Answer: A,B,E

Question No : 2 - (Topic 0)

Which state will be established once you have successfully authenticated to a Web site?

A. Normal state
B. Secure state
C. Session state
D. Balance state

Answer: C

Question No : 3 - (Topic 0)

Which correctly describes how the HTTP GET method is used?

A. by the client to initiate a secure connection
B. by the server to request data from the client
C. by the client to request data from the server
D. by the server to initiate a secure connection

Answer: C

Question No : 4 - (Topic 0)

How does HTTP differ from HTTPS?

A. HTTP is sent in plaintext TCP packets, where as HTTPS uses SSL on top of the TCP packets.
B. HTTPS was created to secure the web server from attackers because HTTP still allows attacks..
C. A HTTPS request is always from a validated source so it is more reliable than HTTP for secure traffic.
D. Because HTTP uses TCP it is unsecure. HTTPS does not use TCP packets so third parties cannot modify the traffic.

Answer: A

Question No : 5 - (Topic 0)

How are standard regular expressions used in WebInspect?

A. Regular Expressions are used for formatting reports.
B. Regular Expressions assign the location of string or value in an HTTP Response.
C. Regular Expressions are used to match the syntactical characteristics of a set of data.
D. Regular Expressions are used only when testing for SQL Injection in POST parameters.

Answer: C

Question No : 6 - (Topic 0)

What is the purpose of the setting "Enable Active Content in Browser Views"?

A. It permits the MSIE Helper object to load ActiveX during an assessment.
B. It permits the execution of Javascript and other dynamic content within the WebInspect GUI.
C. It permits WebInspect to make live requests against the target server during an assessment.
D. It permits the user to make live requests and view their responses within the Step-Mode pane.

Answer: B

Question No : 7 - (Topic 0)

What are Global Web Form Values?

A. Global Web Form Values are values applied to a parameter based only on its name and length.
B. Global Web Form Values are parameter values used to analyze the application server configuration.
C. Global Web Form Values are values that are susceptible to XSS attacks and require special handling.
D. Global Web Form Values are common values used in all applications and do not require any special attention.

Answer: A

Question No : 8 - (Topic 0)

In the Web Macro Recorder tool, what is the function of the Advanced button in the Toolbar area?

A. This button allows the user to view detailed information for each captured session.
B. This button activates Interactive Mode, so the user can step through the login process manually.
C. This button switches the Web Macro Recorder from recording a Start Macro to recording a Login Macro.
D. This button enables Interactive Scans, so WebInspect will be able to handle two-factor authentication and/or CAPTCHA.

Answer: A

Question No : 9 - (Topic 0)

How do you slow down a scan? Select two.

A. Turn off the submission of hidden forms.
B. Increase the Timeouts value and the Retries value.
C. Switch the Crawl and Audit method from Simultaneous to Sequential.
D. Drop the Requestor counts to 1 for Crawl threads and for Audit threads.
E. Change from the Standard scan policy to the Passive scan policy and run an Audit-Only Scan.

Answer: C,D

Question No : 10 - (Topic 0)

What is the difference between a Login Macro and a Start Macro? Select two.

A. The Start Macro will run any time state needs to be re-established.
B. The Start Macro is used to populate the assessment with known URLs.
C. The Login Macro runs any time a page response matches its logout signature.
D. The Login Macro only runs once to gain session state at the beginning of the assessment.
E. The Start Macro is the Login Macro being forced to run once at the beginning of the assessment.

Answer: B,C

Question No : 11 - (Topic 0)

Which regular expression best matches the string 345-12-9876?

A. \d
B. \d*.$
C. \d{3-2-4}
D. \d{3}-\d{2}-\d{4}

Answer: D

Question No : 12 - (Topic 0)

Which tool is used to record a Login Macro?

A. HTTP Editor
B. Macro Wizard
C. Server Analyzer
D. Web Macro Recorder

Answer: D

Question No : 13 - (Topic 0)

What is the difference in selecting a thread count of 1 vs. a thread count of 15? (Select

two.)

A. The 1 thread value will cause the scan to run faster.
B. The 1 thread value will cause the scan to run slower.
C. The 15 thread value will cause the scan to run faster.
D. The 15 thread value will cause the scan to run slower.

Answer: B,C

Question No : 14 - (Topic 0)

What is the difference between the proxy setting found under the Application Settings and the proxy setting found under the Scan Settings?

A. One controls the network path to access AMP and the other controls access to the Internet.
B. One controls the network path towards its scan targets and the other controls the network path to the scan data repository.
C. One controls the proxy port opened by WebInspect during Manual Step-Mode Crawl and the other controls the network path towards its scan
targets.
D. One controls the network path WebInspect uses to reach the Internet for updates and licensing, and the other controls the network path taken
towards its scan targets.

Answer: D

Question No : 15 - (Topic 0)

Which statement best describes Smart Credentials in the Web Form Editor?

A. Smart Credentials will apply Authentication values used during the scan.
B. The values entered into a parameter designated as a Smart Credential will be encrypted during the scan.
C. Designating a parameter as a Smart Credential causes a user to be prompted for an input during the execution of the scan.
D. The values entered into a parameter designated as a Smart Credential allow WebInspect to use digital certificates to authenticate to the
server.

Answer: A

Question No : 16 - (Topic 0)

What are the functions of the feature "Limit maximum single URL hits to (15)"? Select two.

A. visits the first 15 links on a page and stops
B. lighten the load on the target host by throttling the WebInspect scan
C. ensure that any single page will only be requested 15 times during the Crawl phase
D. save time by only visiting a limited number of page variations for any individual page
E. ensure that any single page will only be requested 15 times during the entire assessment

Answer: C,D

Question No : 17 - (Topic 0)

Which statement correctly describes how the Login Macro operates?

A. The Login Macro runs whenever its logout signature matches on an HTTP Request.
B. The Login Macro runs whenever its logout signature matches on an HTTP Response.
C. The Login Macro runs whenever a login form or pop-up appears asking for user credentials.
D. The Login Macro runs whenever an Interactive Form is encountered, provided the user previously marked that form in the Web Form Editor.

Answer: B

Question No : 18 - (Topic 0)

What is the function of the Smart Assessment feature?

A. It allows WebInspect to dictate which audit engines apply to the current assessment.
B. It allows the audit engines to omit security checks based on the target servers fingerprint.
C. It indicates to WebInspect that it is permitted to audit the off-site script includes, but not crawl those off-site hosts.
D. It allows the audit engines to re-order themselves for optimal performance based on the target servers file structure.

Answer: B

Question No : 19 - (Topic 0)

What purpose does adding a custom signature serve for a File Not Found (FNF) condition?

A. A custom signature correctly categorizes the Dashboard view.
B. A custom signature helps WebInspect identify when the StatusCode is 404.
C. A custom signature helps to correctly categorize the 404 pages in the Site Tree pane.
D. A custom signature instructs WebInspect that a response should be treated as a 404.

Answer: D

Question No : 20 - (Topic 0)

Which statement best describes the Web Form Values file?

A. The WebForm Values file is only necessary when not using a web macro during a scan.
B. The WebForm Values file contains only usernames and passwords to be used during the scan.
C. The WebForm Values file must always be redefined prior to executing a scan when using custom policies.
D. The WebForm Values file contains parameters and associated values that are applied to a matching parameter name on a page.

Answer: D

Question No : 21 - (Topic 0)

The default installation of Apache often includes a /Manuals/ directory full of copies of the manual in various languages, for example, English, Spanish, and French. How would you configure WebInspect to scan the whole site, to save on the scan duration time, and to omit those static folders?

A. Add a Session Exclusion for the URL = /Manuals/.
B. Enable the Smart Assessment feature so only Apache-centric checks will be sent.
C. Specify a deep-linked folder in the Starting URL field. Enable the Restrict to Folder setting for that directory and all subdirectories.
D. Create a customized policy with only the Apache web server branch enabled, omitting all those checks that pertain to non-Apache servers.

Answer: A