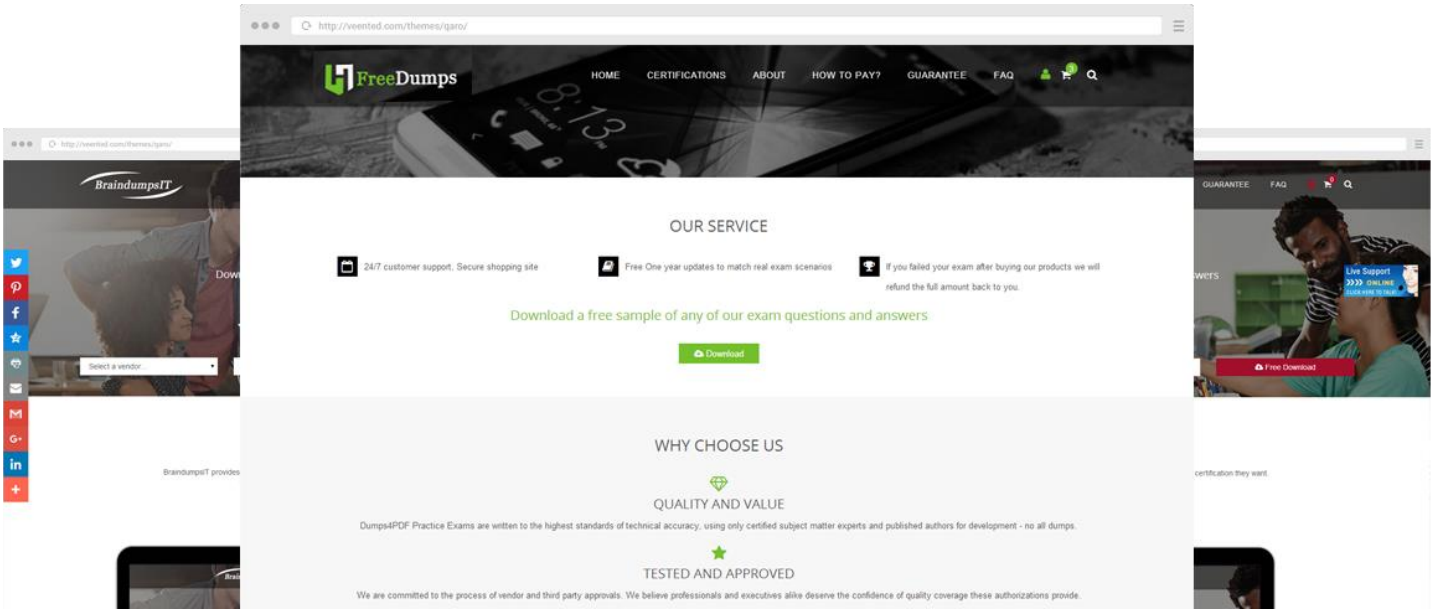
FreeDumps



WHAT PEOPLE SAY

Disclaimer Policy: The site does not guarantee the content of the comments. Because of the different time and the changes in the scope of the exam, it can produce different effect. Before you purchase the dump, please carefully read the product introduction from the page. In addition, please be advised the site will not be responsible for the content of the comments and contradictions between users.

> *Can not believe C2040-440! it is really same with the exam*

ATWOOD

> *If you want to pass exam casually I advise you to purchase study guide. A2010-578 study guide have a part of questions with real test.*

MILES

http://www.freedumps.top

Latest valid dumps torrent and free demo for certification exam prep

Exam : **GWEB**

Title : GIAC Certified Web Application Defender

Vendor : GIAC

Version : DEMO

NO.1 What is the primary function of two-factor authentication (2FA)?
Response:
A. To limit the number of login attempts
B. To provide an additional layer of security by requiring two forms of identity verification
C. To block all failed login attempts
D. To improve application speed
Answer: B

NO.2 How does the use of third-party security services like Cloudflare or Akamai benefit web application security?
Response:
A. They provide outsourced content management systems
B. They offer distributed denial of service (DDoS) protection
C. They replace the need for web application firewalls
D. They offer free hosting services
Answer: B

NO.3 What are effective proactive defense measures for a web application?
(Choose Two)
Response:
A. Deploying a web application firewall (WAF)
B. Implementing network-level DDoS protection
C. Conducting regular security awareness training
D. Using intrusion detection systems at the application layer
Answer: A,D

NO.4 What role does a Web Application Firewall (WAF) play in modern web application security?
Response:
A. Acts as a reverse proxy to intercept and analyze HTTP/S traffic
B. Provides a physical barrier between the web server and the internet
C. Encrypts data transmitted between the client and the server
D. Serves as the primary authentication mechanism
Answer: A

NO.5 In the context of single sign-on (SSO), which of the following statements accurately describe its benefits?
(Choose Two)
Response:
A. SSO reduces the number of passwords users need to remember.
B. SSO increases the complexity of password management.
C. SSO can reduce help desk costs related to password resets.
D. SSO requires additional authentication steps for each application, enhancing security.
Answer: A,C

NO.6 What is the purpose of HTTP status code 404?
Response:
A. Server error
B. Not found
C. Unauthorized
D. Forbidden
Answer: B

NO.7 What is the primary benefit of using asymmetric encryption over symmetric encryption for data in transit?
Response:
A. Higher encryption speed
B. No need for key exchange
C. Better compatibility with older systems
D. More options for key lengths
Answer: B

NO.8 Which encryption algorithm is recommended for securing sensitive data at rest?
Response:
A. AES
B. DES
C. SHA-1
D. RC4
Answer: A

NO.9 Which type of security testing focuses on identifying security vulnerabilities in the application's source code?
Response:
A. Dynamic Application Security Testing (DAST)
B. Static Application Security Testing (SAST)
C. Functional testing
D. Load testing
Answer: B

NO.10 What is a common vulnerability associated with the improper handling of session tokens?
Response:
A. The website becomes more susceptible to SQL injection attacks.
B. Session tokens may be leaked through Referrer headers.
C. Increased vulnerability to cross-site scripting (XSS) attacks.
D. Allowing unlimited file size uploads.
Answer: B

NO.11 What is the primary role of a reverse proxy in a web application architecture?

Response:
A. To distribute load among several servers.
B. To encrypt outgoing server responses.
C. To act as an intermediary for requests from clients seeking resources from servers.
D. To provide additional compute resources to a server.
Answer: C

NO.12 Which of the following cryptographic techniques is commonly used to secure data in transit for web applications?
Response:
A. AES encryption
B. RSA encryption
C. TLS/SSL
D. MD5 hashing
Answer: C

NO.13 When is it appropriate to use encryption over tokenization for protecting sensitive data?
Response:
A. When the data needs to be processed or analyzed
B. When there is no requirement for direct data retrieval
C. When replacing data with a token suffices for processing
D. When minimal changes to the existing system are preferred
Answer: A

NO.14 Which of the following would be an effective method for detecting vulnerabilities in a web application?
Response:
A. Performing regular backups of website data.
B. Conducting penetration testing using both automated tools and manual techniques.
C. Analyzing the website's traffic statistics for marketing purposes.
D. Reviewing the website's source code for compliance with coding standards.
Answer: B

NO.15 How can token-based authentication be compromised in a web application?
Response:
A. Through physical theft of the server.
B. By intercepting unencrypted tokens transmitted over an insecure channel.
C. By obtaining a user's password through social engineering.
D. By executing a DDoS attack on the web server.
Answer: B

NO.16 What is a key risk of not implementing access control validation in a web application?
Response:

A. Increased load time for web pages
B. Unrestricted access to sensitive data by unauthorized users
C. Improved performance of the application
D. Better collaboration between departments
Answer: B

NO.17 When securing a web service, why is it important to have a robust XML parsing mechanism?
Response:
A. To improve the parsing speed and efficiency of XML documents
B. To prevent XML External Entity (XXE) attacks
C. To ensure that XML documents are compliant with W3C standards
D. To facilitate seamless integration with AJAX-based clients
Answer: B

NO.18 Which of the following practices are effective in preventing unauthorized access? (Choose two)
Response:
A. Enforcing multi-factor authentication (MFA)
B. Allowing unlimited login attempts
C. Implementing least privilege principles
D. Using single sign-on (SSO) without encryption
Answer: A,C

NO.19 What are common techniques to prevent input-related vulnerabilities in web applications? (Choose two)
Response:
A. Disabling input validation for specific users
B. Implementing output encoding for all user input
C. Validating input length, type, and format
D. Allowing arbitrary input into SQL queries
Answer: B,C