EDUSUM

#1 Online Certification Guide

GIAC GWEB

GIAC Certified Web Application Defender Certification Questions & Answers

Exam Summary – Syllabus –Questions

GWEB

GIAC Web Application Defender

75 Questions Exam – 68% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your GWEB Certification Well:

The GWEB is best suitable for candidates who want to gain knowledge in the GIAC Cloud Security. Before you start your GWEB preparation you may struggle to get all the crucial GIAC Certified Web Application Defender materials like GWEB syllabus, sample questions, study guide.

But don't worry the GWEB PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the GWEB syllabus?
- How many questions are there in the GWEB exam?
- Which Practice test would help me to pass the GWEB exam at the first attempt?

Passing the GWEB exam makes you GIAC Web Application Defender. Having the GIAC Certified Web Application Defender certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GWEB GIAC Certified Web Application Defender Certification Details:

Exam Name	GIAC Web Application Defender (GWEB)
Exam Code	GWEB
Exam Price	$979 (USD)
Duration	180 mins
Number of Questions	75
Passing Score	68%
Books / Training	**SEC522: Application Security: Securing Web Applications, APIs, and Microservices**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GWEB Sample Questions**
Practice Exam	**GIAC GWEB Certification Practice Exam**

GWEB Syllabus:

Topic	Details
Access Control	- The candidate will demonstrate understanding of access control attacks and mitigation strategies, as well as applying the best practice in avoiding access control issues.
AJAX Technologies and Security Strategies	- The candidate will demonstrate an understanding of Asynchronous JavaScript and XML (AJAX) architecture, common attacks against AJAX technologies and best practices for securing applications using AJAX.
Authentication	- The candidate will demonstrate understanding of web authentication, single sign on methods, third party session sharing and common weaknesses, as well as how to develop test strategies, and apply best practices.
Cross Origin Policy Attacks and Mitigation	- The candidate will demonstrate an understanding of methods attackers use to circumvent single origin policy enforcement and best practices for preventing, detecting or mitigating these attacks in web applications.
CSRF	- The candidate will demonstrate understanding of the conditions that make a CSRF attack possible, the steps an attacker takes and how to mitigate CSRF attacks.
Encryption and Protecting Sensitive Data	- The candidate will demonstrate understanding of how cryptographic components work together to protect web application data in transit and in storage and also when and where to use encryption or tokenization to protect sensitive information.
File Upload, Response Readiness, Proactive Defense	- The candidate will demonstrate an understanding of incident response as well as file upload, logging, and anti automation issues
Input Related Flaws and Input Validation	- The candidate will demonstrate understanding of SQL injection, Cross site Scripting, HTTP Response splitting, and how to protect against them with proper input validation
Leading Edge Technologies and Web Security	- The candidate will demonstrate an understanding of leading edge web application security issues and technologies
Modern Application Framework Issues and Serialization	- The candidate will demonstrate understanding of miscellaneous security technolgies and techniques associated with web application security including REST, Java Frameworks, Serialization, and Browser Defense
Security Testing	- The candidate will demonstrate an understanding of

Topic	Details
	how to detect and respond to incidents and conduct security testing in the web application environment.
Session Security & Business Logic	- The candidate will demonstrate understanding of what sessions are, how to test and mitigate common weaknesses, and how to properly implement session tokens and cookies in a web application as well as security issues associated with business logic.
Web Application and HTTP Basics	- The candidate will demonstrate understanding of the building blocks of web applications and how components work together to provide HTTP content as well as high level attack trends.
Web Architecture and Configuration	- The candidate will demonstrate an understanding of web application architecture and controls needed to secure servers and services that host web applications.
Web Services Security	- The candidate will demonstrate an understanding of Service Oriented Architecture (SOA), common attacks against web services components (SOAP, XML, WSDL, etc) and best practices for securing web services.

GIAC GWEB Sample Questions:

Question: 1

AJAX calls can be vulnerable to interception and manipulation. Which of the following is an effective countermeasure to secure AJAX calls?

a) Using simple HTTP authentication for AJAX requests
b) Employing GET requests for transferring sensitive information
c) Allowing cross-origin requests without restrictions
d) Implementing strong session management with secure tokens

Answer: d

Question: 2

How does the use of third-party security services like Cloudflare or Akamai benefit web application security?

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

Question: 3

Which practice is essential for maintaining security in web applications that handle serialization and deserialization?

a) Using the most efficient serialization library
b) Restricting serialized data to authenticated users
c) Monitoring the size of serialized data
d) Logging all serialization and deserialization operations

Answer: b

Question: 4

What is the role of 'SameSite' cookie attribute in preventing CSRF attacks?

a) It prevents cookies from being sent in cross-site requests
b) It ensures cookies are only sent over HTTPS
c) It isolates cookies to specific domain paths to prevent unauthorized access
d) It encrypts cookies to prevent interception and tampering

Answer: a

Question: 5

Which technique is most effective in preventing SQL injection attacks?

a) Use of prepared statements and parameterized queries
b) Client-side input validation
c) Encryption of all data entered by the user
d) Limiting the length of input fields

Answer: a

Question: 6

What are effective proactive defense measures for a web application?
(Choose Two)

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

Question: 7

In a typical three-tier web application architecture, the _____ tier is responsible for processing business logic, performing computations, and making decisions.

a) Client
b) Presentation
c) Business Logic
d) Data

Answer: c

Question: 8

In the context of file uploads, what are two critical security checks to implement? (Choose Two)

a) Verifying the file extension only
b) Checking the file MIME type against a whitelist
c) Ensuring the uploaded file is not executable on the server
d) Allowing all file types but scanning for size

Answer: b, c

Question: 9

Which of the following is an essential security practice for protecting a web service using SOAP?

a) Utilizing SOAP attachments for all confidential data exchanges
b) Employing WS-Security standards for message integrity and confidentiality
c) Restricting SOAP messages to less than 2KB to prevent buffer overflow attacks
d) Using only HTTP GET requests to simplify SOAP message handling

Answer: b

Question: 10

When configuring CORS policies, what considerations should be made to ensure security? (Choose Two)

a) Always set the Access-Control-Allow-Origin header to "*"
b) Validate the origin before sending back any CORS headers
c) Use withCredentials for sensitive cross-origin requests
d) Restrict the HTTP methods that can be used cross-origin

Answer: b, d

Study Guide to Crack GIAC Certified Web Application Defender GWEB Exam:

- Getting details of the GWEB syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GWEB exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the GIAC provided training for GWEB exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GWEB sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GWEB practice tests is must. Continuous practice will make you an expert in all syllabus areas.