CLOUDFLARE



Exam Prep Guide

Cloudflare Application Security Associate Certification

Ready to prove your mastery of Cloudflare Application Security solutions?

This guide is a study guide to help you prepare for the Application Security Associate certification exam. The Associate level exam tests for foundational, entry-level understanding of the Cloudflare Application Security suite.

This exam prep guide includes information about logistics for taking the exam, along with resources to help you prepare for the exam.

- Exam format and schedule
- Exam categories with percentage weightings
- Detailed outline of topics covered per category
- Links to additional study resources
- Accommodation information

Passing the exam and earning a Cloudflare certification credential helps professional growth in many ways:

- Validates capabilities and grants formal recognition of Cloudflare Application Security knowledge
- Proves professional competence and expands opportunities for career advancement
- Sharpens skills, reduces risks of mistakes, and increases confidence of Cloudflare mastery

Questions?

Reach the Cloudflare certification and training team via certification@cloudflare.com.

Best of luck!

Exam details

Certification level

ASSOCIATE

Exam format

60 multiple choice and matching questions

90 min time limit

Proctored, live in classroom

Exam results

Exam results are provided immediately on screen upon completion of exam. Certification badges are emailed to those who passed within 5-7 business days

Certification is valid for 2 years.

© 2025 Cloudflare, Inc. All rights reserved.

Exam weighting & resources

The Application Security Associate certification exam assesses a candidate's foundational knowledge and capabilities related to the key areas outlined below. A detailed outline of topics covered within each domain is included in the following pages. Basic, hands-on experience with Cloudflare Application Security products is highly recommended prior to taking the Associate level exam.

Domains	Skills Validated	Exam Weighting
Threat recognition & impact analysis	Identify and analyze DDoS, bot activity, attack types, potential vulnerabilities, and data privacy risks	**30%**
Security monitoring & analysis	Recognize internet trends, utilize dashboard analytics, and integrate with security information systems	**35%**
Attack mitigation & traffic control	Implement mitigation strategies, prevent exploits, manage automation	**35%**

Target audience

Candidates for this exam are technology professionals or those who aspire to be technology professionals and want to demonstrate their fundamental knowledge of Cloudflare Application Services and Security products. This certification is ideal for individuals who either already work in cybersecurity or have a desire to embark on a career in cybersecurity and want to validate their foundational understanding of Cloudflare Application Security products. Candidates should possess a basic level of hands-on experience with Cloudflare's Application Security products and a general understanding of the OSI model.

Additional resources

Cloudflare Application Security Docs

Cloudflare Community

Cloudflare Glossary

Cloudflare Dashboard



© 2025 Cloudflare, Inc. All rights reserved. | 1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

Cloudflare Application Security Associate Exam Outline

Domain 1: Threat Recognition and Impact Analysis (30%)

1.1 Identify and analyze DDoS and DoS attack vectors

- 1.1.1 Identify application layer attack types and their characteristics
- 1.1.2 Differentiate between L-7 application layer and L-3 network layer attacks
- 1.1.3 Analyze protocol vulnerability denial of service attacks
- 1.1.4 Assess business impact of service disruption attacks

1.2 Identify and evaluate injection attacks and vulnerability exploits

- 1.2.1 Recognize reconnaissance and scanning activities including origin IP discovery, fuzzing, and WAF probing
- 1.2.2 Identify SQL injection and command injection attack patterns
- 1.2.3 Recognize exploitation techniques for known vulnerabilities (e.g., Log4Shell, SSRF, RCE)
- 1.2.4 Identify characteristics of zero-day vulnerability exploits with reference to historical cases (e.g Log4Shell, MOVEit)

1.3 Assess API security vulnerabilities and exploitation techniques

- 1.3.1 Identify authentication and authorization (session identifiers) flaws including BOLA and inconsistent authentication mechanisms
- 1.3.2 Identify API schema and its purpose
- 1.3.3 Differentiate between legitimate vs. malicious API traffic patterns

1.4 Identify bot activity and automation abuse

- 1.4.1 Detect malicious bot traffic targeting web and mobile applications
- 1.4.2 Recognize unauthorized automation including vulnerability scanners, competitor bots, AI bots, headless tools, and page/content scraping
- 1.4.3 Identify credential attacks(detection of brute force attempts and credential stuffing patterns), while evaluating the effectiveness of authentication controls.
- 1.4.4 Recognize business logic abuse by detecting signup manipulation, fake account creation, and inventory exploitation techniques, ensuring proper validation mechanisms are in place
- 1.4.5 Analyze payment fraud activities, including gift card and credit card abuse, through appropriate transaction monitoring and verification controls
- 1.4.6 Evaluate the business impact of automated attacks

1.5 Assess client-side and frontend security threats

- 1.5.1 Identify cross-site attacks including Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and clickjacking
- 1.5.2 Recognize modern client-side attack patterns (e.g Magecart, formjacking and JS injection

1.6 Analyze encryption, identity, and TLS vulnerabilities

- 1.6.1 Recognize broken SSL/TLS implementations and their security implications
- 1.6.2 Assess the business impact of encryption vulnerabilities on data privacy

1.7 Evaluate data protection and privacy risks

- 1.7.1 Identify sensitive data exposure vectors and leakage patterns
- 1.7.2 Recognize data exfiltration techniques and their indicators
- 1.7.3 Detect client-side data skimming via JavaScript injection
- 1.7.4 Assess the business and compliance impact of data privacy breaches

1.8 Identify infrastructure and delivery chain vulnerabilities

- 1.8.1 Identify CDN abuse patterns (cache busting, origin IP exposure, and hotlinking)
- 1.8.2 Identify risk of TLS downgrade attacks and misconfigurations
- 1.8.3 Detect DNS exploitation techniques including poisoning, hijacking, and domain shadowing
- 1.8.4 Evaluate the business impact of infrastructure attacks on application availability and integrity

Domain 2: Security Monitoring and Analysis (35%)

2.1 Recognize and analyze internet trends

- 2.1.1 Monitor and analyze global security patterns using Cloudflare Radar to identify emerging threats and anticipate potential attack vectors.
- 2.1.2 Review industry attack trend reports and security blogs to maintain awareness of evolving threat landscapes.
- 2.1.3 Interpret attack trends using application security telemetry (e.g., WAF logs, rate limiting events)

2.2 Utilize Cloudflare dashboard analytics for security investigation

- 2.2.1 Establish baseline metrics for legitimate traffic patterns to effectively identify anomalous activity
- 2.2.2 Apply appropriate filters and time duration settings to isolate and investigate security events
- 2.2.3 Interpret security events and accurately identify their sources through dashboard data analysis
- 2.2.4 Navigate and analyze account-level security analytics to identify organization-wide threats.
- 2.2.5 Utilize zone-level analytics to detect and investigate zone-specific security incidents.
- 2.2.6 Leverage Security Center dashboards and intelligence to prioritize and respond to threats.
- 2.2.7 Analyze Cloudflare's scoring mechanisms for attack detection and bot traffic identification

2.3 Utilize logs and notifications across security infrastructure

- 2.3.1 Differentiate between dashboard sampling logs and comprehensive logpush data to select appropriate analysis methods.
- 2.3.2 Extract and interpret relevant security data from Cloudflare logs and notifications.
- 2.3.3 Analyze logs and notifications to identify attack indicators and correlate with Cloudflare security events.
- 2.3.4 Configure WAF rules in log-only mode to monitor rule effectiveness and potential impacts

2.4 Integrate with security information management systems

- 2.4.1 Integrate Cloudflare security data with SIEM (Security Information and Event Management) solutions for comprehensive security monitoring

Domain 3: Attack Mitigation and Traffic Control (35%)

3.1 Implement DDoS attack mitigation strategies

- 3.1.1 Implement comprehensive protection strategies for DDoS and DoS attacks across application and network layers
- 3.1.2 Deploy rate limiting strategies to control and reduce potential attack traffic
- 3.1.3 Utilize global Cloudflare solutions (ie. rapid reset techniques to respond to emerging threats)
- 3.1.4 Protect origin(s) from direct attacks

3.2 Prevent injection and exploits

- 3.2.1 Apply OWASP core managed rules to protect against common injection vulnerabilities
- 3.2.2 Design custom WAF rules using score-based methodologies for layered threat detection
- 3.2.3 Configure rate limiting to prevent exploitation attempts
- 3.2.4 Develop strategies to minimize false positive triggers while maintaining robust security

3.3 Prevent API Abuse and Unauthorized Access

- 3.3.1 Implement API Protection based on endpoints and request
- 3.3.2 Deploy mutual TLS (mTLS) for enhanced authentication and encryption

3.4 Manage Bots and Automation

- 3.4.1 Configure Cloudflare Bot solutions to identify and block malicious attacks
- 3.4.2 Usage of Bot Management variables in custom rules
- 3.4.3 Implement strategies to reduce false positives in bot detection mechanisms
- 3.4.4 Control AI traffic going to an application

3.5 Implement Rate Limiting to Mitigate Abuse and Scraping

- 3.5.1 Establish appropriate rate limiting thresholds for different endpoints
- 3.5.2 Implement rate limiting rules based on traffic patterns
- 3.5.3 Configure rate limiting response actions for different scenarios
- 3.5.4 Monitor rate limiting effectiveness through logs and analytics
- 3.5.5 Optimize rate limiting settings to balance security and user experience

3.6 Implement Encryption, Identity, and TLS Security

- 3.6.1 Implement edge SSL certificates to secure communications
- 3.6.2 Configure HTTP Strict Transport Security (HSTS) to enforce secure connections
- 3.6.3 Enforce secure origin connections using mTLS and authenticated origin pull

Cloudflare Certifications: Reasonable Accommodations Policy

At Cloudflare, we're dedicated to making sure everyone has a fair and equal opportunity to demonstrate their knowledge and skills. We understand that some individuals with qualified disabilities may need reasonable accommodations to take our exams.

How to Request an Accommodation

If you need an accommodation, please email certification@cloudflare.com at least 7 days before your scheduled exam. This will give us enough time to review your request and make the necessary arrangements. Please note that all accommodations must be arranged in advance.

Types of Accommodations

Accommodation needs are considered on a case-by-case basis. While there is no one-size-fits-all solution, we are open to approving accommodations such as:

- Extended time for learning disabilities
- Use of an assisted device, such as a screen reader or magnifier, for visual disabilities
- Other accommodations as needed

As part of our accommodation review process, Cloudflare reserves the right to request documentation substantiating your accommodation needs.

If you are in need of a special accommodation, please email certification@cloudflare.com.