

F5 BIG-IP ASM: Application Security Manager

Learn to deploy and tune F5 BIG-IP ASM security policies to protect web applications from the OWASP Top 10 and other threats.

COURSE OVERVIEW

This course covers provisioning BIG-IP ASM and its resources, along with traffic processing through BIG-IP Local Traffic Manager and core web application security concepts. It addresses mitigating the OWASP Top 10 and other vulnerabilities through security policy deployment and tuning, attack signatures, threat campaigns, positive security building, and header and cookie protection. It then covers reporting and logging, advanced parameter handling, Automatic Policy Builder, integration with web vulnerability scanners, login enforcement, brute force and credential stuffing mitigation, session tracking, and parent and child policies. It concludes with Layer 7 DoS protection, Advanced Bot Defense configuration, and using DataSafe to secure the client side of the Document Object Model.

WHO THIS COURSE IS FOR

Security Engineers

Network Administrators

Application Security Analysts

Security Policy Administrators

Web Application Administrators

LEARNING OBJECTIVES

- Provision ASM and its associated resources
- Explain traffic processing with BIG-IP Local Traffic Manager
- Identify web application vulnerabilities such as the OWASP Top 10
- Deploy and tune security policies
- Apply attack signatures and threat campaigns
- Build positive security policies and secure cookies and headers
- Configure advanced bot defense and Layer 7 DoS protection
- Implement login enforcement, brute force and credential stuffing mitigation

23 Topics

TOPICS

- Provisioning ASM
- Resource provisioning for ASM
- Traffic processing with BIG-IP Local Traffic Manager (LTM)
- Web application concepts
- Mitigating the OWASP Top 10 and other vulnerabilities
- Security policy deployment
- Security policy tuning
- Deploying Attack Signatures and Threat Campaigns
- Positive security building
- Securing cookies and other headers
- Reporting and logging
- Advanced parameter handling
- Using Automatic Policy Builder
- Integrating with web vulnerability scanners
- Login enforcement for flow control
- Brute force and credential stuffing mitigation
- Session tracking for client reconnaissance
- Using Parent and Child policies

Layer 7 DoS Protection

TOPICS

Transaction Per Second-based DoS protection · Layer 7 Behavioral DoS Protection

Configuring Advanced Bot Defense

TOPICS

- Web Scraping and other Microservice Protection
- Working with Bot Signatures
- Using DataSafe to Secure the client side of the Document Object Model

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com