

Configuring F5 Advanced WAF

Course code: F5_AWF

In this 4 day course, students are provided with a functional understanding of how to deploy, tune, and operate F5 Advanced Web Application Firewall to protect their web applications from HTTP-based attacks. The course includes lecture, hands-on labs, and discussion about different F5 Advanced Web Application Firewall tools for detecting and mitigating threats from multiple attack vectors such web scraping, Layer 7 Denial of Service, brute force, bots, code injection, and zero day exploits. This course is on the list of approved study resources for the F5 ASM 303 certification exam

| Affiliate | Duration | Course price | ITB |
|------------|----------|--------------|-----|
| Praha | 4 | 75 300 Kč | 0 |
| Bratislava | 4 | 2 990 € | 0 |

The prices are without VAT.

Course terms

| Date | Duration | Course price | Type | Course language | Location |
|------------|----------|--------------|----------|-----------------|-------------------|
| 04.02.2025 | 4 | 75 300 Kč | Presence | CZ/SK | Praha - ALEF NULA |

The prices are without VAT.

What we teach you

- Describe the role of the Advanced Web Application Firewall
- Describe how F5 Advanced Web Application Firewall protects a web application by securing file types, URLs, and parameters
- Deploy F5 Advanced Web Application Firewall policies
- Define learn, alarm, and block settings as they pertain to configuring F5 Advanced Web Application Firewall
- Define attack signatures and explain why attack signature staging is important
- Deploy Threat Campaigns to secure against CVE threats
- Deploy policie using manual or automated approach
- Deploy Advanced Bot Defense against web scrapers, all known bots, and other automated agents
- Deploy DataSafe to secure client-side data

Required skills

- Basic HTTP and HTML concepts
- Basic security concepts
- Common network terminology
- Web application terminology

Course outline

- Resource provisioning for F5 Advanced Web Application Firewall
- 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

GOPAS Praha

Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno

Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava

Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk



Copyright © 2020 GOPAS, a.s.,
All rights reserved

Configuring F5 Advanced WAF

- 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 Transaction Per Second-based DoS protection Layer 7 Behavioral DoS Protection
- Configuring Advanced Bot Defense Web Scraping and other Microservice Protection Working with Bot Signatures
- Using DataSafe to Secure the client side of the Document Object Model

GOPAS Praha

Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno

Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava

Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk



Copyright © 2020 GOPAS, a.s.,
All rights reserved