F5 AWAF Modern Application (formerly Configuring F5 Advanced WAF)

Learn to deploy and operate F5 Advanced WAF to protect web applications from the most critical security risks as described in the OWASP Top 10 list, from bots and other automated agents, and from Denial of Service (DoS) attacks operating at the HTTP layer of the web application delivery ecosystem. Through a combination of lecture, hands-on labs, and discussion, secure applications from the majority of common attacks by the end of the first day. Take technical deep dives into mitigating web scraping, account aggregation, account creation, ad fraud, CAPTCHA defeat, card cracking, carding, cashing out, credential stuffing, and other unwanted automated application abuse as described in the OWASP automated threats list.

Observe various vulnerability mitigations in real time by playing the role of an attacker in lab exercises. Gain context for securing applications, including analysis of HTTP and the elements of both modern and traditional web applications such as file types, parameters, URLs, and login pages. Learn to recognize client and server-side technologies such as JSON and AJAX, and learn to address vulnerabilities that might be present in common application development tools such as PHP, AngularJS, and others.

Review recommended practices for reporting, security event logging, and integration with third-party web application vulnerability scanners in detail. Follow prescribed step-by-step directions for activities initially, and gradually gain proficiency so that, by the end of class, little or no instruction is needed to complete simple to more complex configurations.

Course Contents
- Introducing the BIG-IP System
- Traffic Processing with BIG-IP
- Overview of Web Application Processing
- Overview of Web Application Vulnerabilities
- Security Policy Deployments: Concepts and Terminology
- Policy Tuning and Violations
- Using Attack Signatures and Threat Campaigns
- Positive Security Policy Building
- Securing Cookies and other Header Topics
- Visual Reporting and Logging
- Lab Project 1
- Advanced Parameter Handling
- Automatic Policy Building
- Integrating with Web Application Vulnerability Scanners
- Deploying Layered Policies
- Login Enforcement and Brute Force Mitigation
- Reconnaissance with Session Tracking
- Layer 7 Denial of Service Mitigation
- Advanced Bot Defense
- Final Projects

Target Group
This course is intended for SecOps personnel responsible for the deployment, tuning, and day-to-day maintenance of F5 Adv. WAF. Participants will obtain a functional level of expertise with F5 Advanced WAF, including comprehensive security policy and profile configuration, client assessment, and appropriate mitigation types.

Experience with LTM and prior WAF knowledge are not required.

Prerequisites
The following free Self-Directed Training (SDT) courses, although optional, are helpful for any student with limited BIG-IP administration and configuration experience:
- Getting Started with BIG-IP
- Getting Started with Local Traffic Manager (LTM)
- Getting Started with F5 Advanced WAF

These courses are available at F5 University

General network technology knowledge and experience are recommended before attending any F5 Global Training Services instructor-led course, including OSI model encapsulation, routing and switching, Ethernet and ARP, TCP/IP concepts, IP addressing and subnetting, NAT and private IP addressing, NAT and private IP addressing, default gateway, network firewalls, and LAN vs. WAN.

Course Target
Exam 303 - BIG-IP ASM Specialist

Prerequisites: Valid F5-CA, BIG-IP Certification

Upon passing Exam 303, candidates receive their F5 Certified Technology Specialist, BIG-IP ASM certification.

This certification verifies that a candidate is fully qualified to design, implement, and maintain BIG-IP ASM, integrating BIG-IP ASM with other platforms and products in a manner that is application-specific and appropriate to organizational policies, needs, and requirements.

Receiving the F5-CTS, BIG-IP ASM certification is a prerequisite for the Security Solutions Expert certification track.

Status 05/25/2025

This Course in the Web

You can find the up-to-date information and options for ordering under the following link:
www.experteach-training.com/go/**FWAF**

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
Classes in Germany	**4 Days**	**€ 4,400**
Online Training	**4 Days**	**€ 4,400**
Date/course venue	Course language English	
15/09-18/09/25 ONOnline	17/11-20/11/25 ONOnline	

Table of Contents

F5 AWAF Modern Application (formerly Configuring F5 Advanced WAF)

ExperTeach Benelux B.V.
Ceresstraat 1· 4811 CA Breda· Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach-training.com