Forti-Web Administrator 6.4 Course

Course Duration: 24 Hrs. **Course Code: FWB-ADM-6.4**

Course Overview

The **FortiWeb Administrator 6.4 Course** is designed to equip security professionals with the skills required to deploy, configure, and manage FortiWeb Web Application Firewall (WAF) solutions. This course focuses on protecting web applications from common and advanced threats such as OWASP Top 10 attacks, bot abuse, and API vulnerabilities. Participants will gain hands-on experience in configuring security policies, monitoring traffic, and ensuring compliance using FortiWeb 6.4 in enterprise environments.

What You'll Learn?

By the end of this course, you will be able to:

- Understand FortiWeb architecture and deployment modes
- Deploy FortiWeb 6.4 in inline, transparent, and reverse proxy modes
- Configure web application security policies
- Protect applications against OWASP Top 10 vulnerabilities
- Implement bot mitigation and API security
- Configure SSL inspection and certificate management
- Monitor logs, reports, and alerts
- Troubleshoot common FortiWeb issues

Target Audience

This course is ideal for:

- Web Application Security Administrators

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- Network and Security Engineers
- SOC Analysts and Security Operations Teams
- IT Infrastructure Professionals
- Professionals responsible for web and API security

Pre-Requisites

Participants should have:

- Basic understanding of networking concepts
- Knowledge of web applications and HTTP/HTTPS
- Familiarity with security fundamentals
- Prior experience with Fortinet products is recommended

Course Content

Module 1: Introduction to FortiWeb and Web Application Security

- Web application security fundamentals
- FortiWeb features and architecture
- Deployment scenarios and use cases

Module 2: FortiWeb Deployment and Initial Configuration

- FortiWeb 6.4 installation and setup
- Inline, reverse proxy, and transparent modes
- Network and interface configuration

Module 3: Web Protection Profiles and Policies

- Creating and managing server objects
- Configuring web protection profiles

- Applying security policies

Module 4: Protection Against Web Attacks

- OWASP Top 10 threat protection
- SQL injection and XSS prevention
- Advanced threat detection techniques

Module 5: Bot Mitigation and API Security

- Bot detection and mitigation strategies
- API protection concepts
- Rate limiting and anomaly detection

Module 6: SSL, Authentication, and Compliance

- SSL inspection and certificate handling
- User authentication and access control
- Compliance and security best practices

Module 7: Monitoring, Logging, and Troubleshooting

- Logs, dashboards, and reports
- Alerting and event management
- Troubleshooting performance and security issues