Advanced Web App Firewalls (WAF)Configuration Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today?ÇÖs hyper-connected, cloud-native digital landscape, securing web applications requires moving far beyond basic signature-based Web Application Firewalls (WAFs). The industry has rapidly shifted to Web Application and API Protection (WAAP) platforms to counter polymorphic and sophisticated Layer 7 attacks, including advanced botnets and zero-day exploits Advanced Web App Firewalls (WAF)Configuration Training Course provides hands-on, deep-dive training into the advanced WAF configuration, tuning, and operationalization techniques necessary to establish a robust security posture. We will focus on implementing cutting-edge technologies like Machine Learning (ML)-driven anomaly detection, establishing precise positive security models, and integrating WAF governance directly into DevSecOps pipelines for true Shift-Left security.

This intensive program moves participants from foundational WAF management to expert-level threat mitigation and operational efficiency. You will master critical skills such as deploying advanced API security measures, configuring behavioral analysis for DDoS mitigation, and orchestrating complex credential stuffing defenses. By mastering these advanced concepts, you will be equipped to defend modern, high-value applications across multi-cloud environments, ensuring PCI DSS and GDPR compliance while minimizing costly false positives and maintaining optimal application performance and availability.

Programme Curriculum

Advanced Web App Firewalls (WAF)Configuration Training Course

Introduction

In today?ÇÖs hyper-connected, cloud-native digital landscape, securing web applications requires moving far beyond basic signature-based Web Application Firewalls (WAFs). The industry has rapidly shifted to Web Application and API Protection (WAAP) platforms to counter polymorphic and sophisticated Layer 7 attacks,

including advanced botnets and zero-day exploits Advanced Web App Firewalls (WAF)Configuration Training Course provides hands-on, deep-dive training into the advanced WAF configuration, tuning, and operationalization techniques necessary to establish a robust security posture. We will focus on implementing cutting-edge technologies like Machine Learning (ML)-driven anomaly detection, establishing precise positive security models, and integrating WAF governance directly into DevSecOps pipelines for true Shift-Left security.

This intensive program moves participants from foundational WAF management to expert-level threat mitigation and operational efficiency. You will master critical skills such as deploying advanced API security measures, configuring behavioral analysis for DDoS mitigation, and orchestrating complex credential stuffing defenses. By mastering these advanced concepts, you will be equipped to defend modern, high-value applications across multi-cloud environments, ensuring PCI DSS and GDPR compliance while minimizing costly false positives and maintaining optimal application performance and availability.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Transition from traditional WAF concepts to modern Web Application and API Protection (WAAP) strategies.
2. Develop and enforce granular, low-false-positive Positive Security Profiles for critical application flows.
3. Embed WAF configuration as code using Infrastructure as Code (IaC) tools into CI/CD pipelines
4. Utilize API Discovery tools to secure all exposed endpoints, including GraphQL and gRPC, against BOLA and Injection attacks.
5. Implement and fine-tune Machine Learning models for adaptive, real-time anomaly detection and zero-day protection.
6. Configure multi-layered Advanced Bot Defense profiles to defeat web scraping, ad fraud, and advanced persistent bots.
7. Implement Behavioral DoS Mitigation techniques, including TPS-based and stress-based detection, to maintain service availability.
8. Integrate external Vulnerability Scanners to rapidly generate and deploy virtual patches.
9. Configure Credential Stuffing and Brute Force defenses, including session tracking and multi-factor enforcement.
10. Utilize advanced features like DataSafe to secure sensitive data entry fields and protect against Supply Chain Attacks
11. Expertly manage Staging and Enforcement periods to reduce operational risk and optimize policy readiness.
12. Integrate and leverage external Threat Intelligence Feeds for dynamic IP reputation and threat campaign protection.
13. Audit and configure WAF policies to meet regulatory mandates, specifically PCI DSS and applicable data privacy laws

Target Audience

1. SecOps Engineers.
2. DevSecOps Specialists.
3. Cloud Security Architects
4. Network Security Engineers.

5. Application Developers.
6. Vulnerability Management Specialists.
7. Cybersecurity Consultants.
8. IT Compliance and Audit Personnel

Course Modules

Module 1: WAF to WAAP Evolution and Advanced Concepts

- Understanding the shift from traditional WAF to WAAP
- Deep-dive into the OWASP Top 10 2021 and OWASP API Security Top 10 vulnerabilities.
- Differentiating between network-based, host-based, and cloud-native WAF deployment models.
- Analyzing the full HTTP request flow and WAF inspection points in a modern microservices architecture.
- Defining Security Policy components
- Case Study: Analyzing a large e-commerce platform's shift from an appliance-based WAF to a Multi-Cloud WAAP solution to handle seasonal traffic spikes and microservices complexity.

Module 2: Positive vs. Negative Security Model Mastery

- Detailed configuration of Negative Security Policies using advanced attack signatures and threat campaigns.
- Implementing and maintaining the Positive Security Model for high-value applications.
- Techniques for minimizing false positives and false negatives through signature customization.
- Configuring custom signature sets and integrating third-party feeds into the WAF policy.
- Using violation staging and severity ratings to prioritize security events.
- Case Study: Building a tight positive security profile for a banking API endpoint, ensuring only defined JSON payloads and HTTP methods are permitted.

Module 3: Policy Learning, Staging, and Automatic Building

- Understanding the Learning Process and defining learning speed parameters.
- Managing the Enforcement Readiness Period and transitioning policies from transparent to blocking mode.
- Utilizing Automatic Policy Building templates and fine-tuning auto-generated policies.
- Defining Trusted/Untrusted IP addresses and managing IP reputation features.
- Using Learning Suggestions to iteratively tighten security policies without breaking application functionality.
- Case Study: Implementing a policy upgrade for a legacy application: utilizing a 48-hour ERP with traffic sampling to move from an alarm-only to a blocking policy with zero production impact.

Module 4: DevSecOps and WAF-as-Code Integration

- Integrating WAF policy configuration into CI/CD pipelines using Infrastructure as Code tools
- Implementing WAF Configuration Version Control and managing policy rollbacks.
- Automated testing of WAF rules against simulated attacks before production deployment.
- Using APIs to deploy and manage policy changes programmatically
- Principles of Shift-Left Security allowing developers to see WAF violations early in testing.
- Case Study: Designing a DevSecOps pipeline where WAF rules for new microservices are automatically generated and deployed alongside the application code via a single Jenkins/GitLab pipeline trigger.

Module 5: Comprehensive API Security and Endpoint Protection

- API Discovery and Posture Management to identify all public and shadow APIs.
- Protecting REST, SOAP, and modern protocols like GraphQL and gRPC via custom profiles.
- Mitigating the OWASP API Security Top 10, with a focus on Broken Object Level Authorization and Excessive Data Exposure.
- Validating JSON/XML schema and payload structures against predefined contracts.
- Implementing per-API rate limiting and advanced authentication enforcement.
- Case Study: Securing a high-volume public-facing payment API by enforcing strict JSON validation schema and blocking unauthorized PUT/DELETE methods on specific endpoints.

Module 6: AI/ML-Powered Adaptive Threat Detection

- Deep dive into how Machine Learning is used to establish behavioral baselines of 'normal' traffic.
- Configuring WAFs for Adaptive Security to automatically detect and block anomalies without relying on explicit signatures.
- Techniques for reducing the training data bias and managing ML models to minimize false positives.
- Using Behavioral Analysis to track user sessions and identify deviations indicating account compromise.
- Understanding and configuring the Threat Campaign feature for zero-day and CVE protection.
- Case Study: Investigating an attempted zero-day attack where the ML model successfully identified a novel encoding technique used in a SQLi payload, blocking the request before a signature was available.

Module 7: Advanced Bot Defense and Mitigation

- Classification of malicious bots
- Implementing Proactive Bot Defense
- Configuring dedicated profiles for Web Scraping Mitigation and protecting business logic from automated abuse.
- Integrating CAPTCHA and reCAPTCHA challenges dynamically based on bot score.
- Analyzing bot defense reports to measure ROI and impact on overall traffic composition.
- Case Study: Deployment of Advanced Bot Defense for an online ticketing service, reducing competitor scraping traffic by 95% and mitigating a simultaneous inventory denial attack.

Module 8: Layer 7 DDoS Mitigation and Protection Profiles

- Defining Layer 7 Denial of Service attacks
- Configuring DoS Protection Profiles using transaction per second limits and request length controls.
- Implementing Behavioral DoS Detection automatically adjusting thresholds based on application load and traffic history.
- Utilizing Stress-Based Detection to identify and mitigate attacks targeting specific high-cost URLs or application resources.
- Advanced techniques for traffic shaping and applying mitigation to suspected malicious sources only.
- Case Study: Responding to a Layer 7 DDoS event targeting the search function of a media site, using behavioral throttling to maintain service for legitimate users while blocking the automated flood.

Module 9: Brute Force and Credential Stuffing Mitigation

- Defining login pages for flow control and configuring automatic login page detection.
- Configuring Brute Force Protection using IP-based, session-based, and source-based tracking mechanisms.
- Implementing and configuring Credential Stuffing mitigation via blacklisting known compromised credential pairs.
- Enforcing dynamic challenges or account lockouts upon credential theft violation detection.

- Using session tracking to enforce a logical workflow and prevent out-of-sequence access.
- Case Study: Setting up protection for a banking portal's login page, integrating the WAF with an external threat intelligence list to automatically block logins attempted with leaked credentials.

Module 10: Client-Side Protection and Supply Chain Security

- Understanding the risk of client-side vulnerabilities, including Magecart and skimming attacks.
- Implementing Content Security Policy using the WAF to control external script execution.
- Utilizing DataSafe or equivalent features to encrypt/obfuscate sensitive data fields in the browser before transmission.
- Protecting against DOM-based XSS attacks and unauthorized client-side script modifications.
- Configuring WAF rules to audit and alert on unusual script loading or third-party inclusion.
- Case Study: Applying DataSafe to the checkout process of a retail site, ensuring payment card details are encrypted at the point of entry to defeat client-side data exfiltration attempts.

Module 11: Vulnerability Scanner Integration and Virtual Patching

- Integrating output from leading vulnerability scanners into the WAF platform.
- Automatically or manually generating WAF rules based on scanner findings.
- Managing the lifecycle of a virtual patch until the underlying application code is remediated.
- Configuring WAF policies to enforce secure cookie attributes
- Using WAF features to block specific, targeted exploits associated with recently announced CVEs.
- Case Study: Receiving a critical vulnerability finding from a scanner, and immediately deploying a temporary WAF rule as a virtual patch within 30 minutes to shield the application.

Module 12: Reporting, Logging, and Threat Intelligence

- Configuring advanced logging profiles to capture necessary security event data.
- Integrating WAF logs with SIEM/SOAR platforms for centralized analysis and automated response.
- Creating custom security reports and dashboards to visualize top attacks, policy effectiveness, and compliance status.
- Utilizing Geolocation Enforcement and IP Reputation services to filter suspicious traffic sources.
- Analyzing violation ratings and enforcement readiness summaries to assess organizational risk.
- Case Study: Setting up an automated response playbook: WAF violation logs are forwarded to a SOAR platform which, upon high-severity detection, automatically adds the source IP to a custom blocklist.

Module 13: Cloud-Native and Multi-Cloud WAF Architectures

- Reviewing native WAF solutions and their integration with cloud services
- Designing WAF architectures for Microservices and Kubernetes environments
- Implementing policy consistency across hybrid and multi-cloud deployments.
- Using WAF features for traffic manipulation, header rewriting, and content transformation.
- Optimizing WAF performance and scaling based on traffic load and cloud-specific configurations.
- Case Study: Designing a hybrid WAF deployment where an on-premises WAF uses Parent/Child policies to ensure policy consistency across its edge deployment and a new Azure-hosted application gateway.

Module 14: Custom Policy Language and Advanced Profiling

- Introduction to custom policy languages for advanced WAF logic.
- Creating custom security policies to address unique business logic vulnerabilities

- Deep diving into Advanced Parameter Handling
- Configuring cryptographic protection for application cookies and hidden fields.
- Advanced tuning for file upload protection and blocking malicious file types/extensions.
- Case Study: Writing a custom WAF rule to detect and block automated attempts to exploit a known business logic flaw that is not covered by standard signatures.

Module 15: Governance, Compliance, and Audit Readiness

- Mapping WAF controls to PCI DSS Requirement 6.6 and other mandatory compliance frameworks.
- Conducting WAF policy audits and using built-in compliance reporting features.
- Establishing a formal WAF change management and review process.
- Best practices for WAF policy documentation and knowledge transfer.
- Designing and performing WAF effectiveness testing
- Case Study: Conducting a pre-audit review for a PCI DSS assessment, proving the WAF's effectiveness in protecting cardholder data by presenting customized compliance reports and policy enforcement summaries.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com