Alonso Eduardo
Caballero Quezada
(ReYDeS)

Curso WAF con ModSecurity y OWASP CRS 2026

2	6	En vivo, Virtual, o Personalizado
Sesiones	Horas	



Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Redes Sociales

LinkedIn

X (Twitter)

YouTube

Facebook

Sitio Web

e-mail

WhatsApp

Presentación

En todos los ámbitos digitales actuales, las aplicaciones web se han convertido en la superficie de ataque más expuesta de cualquier organización. Con una gran parte de las intrusiones orientadas específicamente contra la capa de aplicación, depender exclusivamente de firewalls de red tradicionales deja a los servidores web desprotegidos ante una diversidad de ataques críticos como inyecciones SQL, Cross-Site Scripting (XSS), Inclusión Remota y Local de Archivos (RFI/LFI), o la explotación de vulnerabilidades en producción.

Este curso expone como realizar la protección de Aplicaciones Web utilizando un Firewall de Aplicación Web (WAF), combinando ModSecurity y OWASP CRS (Core Rule Set). Siendo diseñado y dirigido a administradores de sistemas, ingenieros DevOps, y profesionales en ciberseguridad, quienes buscan implementar una defensa perimetral avanzada utilizando sólidas y excelentes tecnologías Open Source.

A lo largo de este curso se aprenderá a desplegar y configurar ModSecurity acoplado con Apache HTTP Server, integrando de manera óptima el estándar mundial OWASP Core Rule Set (CRS). Se comprenderá la lógica detrás de las fases de inspección de peticiones HTTP, la utilización de umbrales para puntuación de anomalías, y la transición vital entre el modo para detección pasiva y el bloqueo activo en tiempo real.

Este curso profundiza en las habilidades operativas indispensables, tales como la lectura de registros detallados de auditoría, el análisis de falsos positivos en entornos corporativos, y la creación de reglas específicas de exclusión por ruta URI. Asimismo se dominará la redacción de reglas personalizadas para ejecutar técnicas efectivas de parcheo virtual ante amenazas imprevistas.

Al finalizar se está en la capacidad de blindar cualquier infraestructura web, garantizando la continuidad de la empresa, y elevando significativamente el nivel de protección de todos los servicios expuestos hacia Internet, sin depender de licencias costosas o soluciones comerciales.

Alonso Eduardo
Caballero Quezada
(ReYDeS)

Curso WAF con ModSecurity y OWASP CRS 2026

Temario

- ¿Porqué la Seguridad Perimetral Tradicional no Basta?
- Concepto y Rol del Web Application Firewall (WAF)
- Arquitectura de ModSecurity en Apache HTTP Server
- Las 5 Fases de Procesamiento de ModSecurity
- Modos de Operación del Motor de Reglas
- Requisitos del Entorno de Laboratorio
- Instalación de Apache2 y ModSecurity
- Configuración Inicial de modsecurity.conf
- ¿Qué es OWASP Core Rule Set (CRS)?
- Modos de Puntuación: Anomaly Scoring vs. Self-Contained
- Entendiendo los Umbrales de Anomalía
- Niveles de Paranoia en CRS
- Descarga y Despliegue de OWASP CRS
- Vinculación del CRS en security2.conf
- Ataques a la Capa de Aplicación: Inyección SQL
- Simulación y Bloqueo de SQLi
- Ataques del Lado del Cliente: Cross-Site Scripting (XSS)
- Simulación y Bloqueo de XSS
- Inclusión Local Archivos
- Simulación y Bloqueo de LFI
- Inyección de Comandos de Sistema
- Simulación y Bloqueo de Inyección de Comandos
- Estructura y Anatomía del Audit Log en ModSecurity
- Lectura y Filtrado del Audit Log
- El Desafío de los Falsos Positivos en Producción
- Mecanismos de Exclusión de Reglas (ctl:ruleRemoveById)
- El Archivo de Exclusiones de Pre-Evaluación
- Creación Paso a Paso de una Exclusión por URI
- Sintaxis Básica de Reglas Propias en ModSecurity
- Acciones de Regla: Control de Flujo y Respuestas
- Regla Personalizada 1: Bloqueo de Archivos Sensibles
- Regla Personalizada 2: Control de User-Agents Maliciosos
- Probar y Validar las Reglas Personalizadas
- Estrategia de Mantenimiento y Parche Virtual
- Buenas Práctica para Producción

Beneficios

- Acceso al aula virtual por sesenta (60) días
- Acceso a las sesiones en vivo
- Videos de las dos (2) sesiones
- Acceso libre a las sesiones en vivo de los siguientes cursos a dictarse
- Material utilizado durante el desarrollo del curso
- Asesoría personalizada y permanente
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 16 horas

Inversión

Perú: S/. 225 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: $ 75 Dólares

- Pago mediante PayPal

Escriba un mensaje al WhatsApp https://wa.me/reydes para proporcionarle los datos pertinentes.

Información

Para obtener más información sobre este curso tiene a su disposición los siguientes mecanismos de contacto.

WhatsApp: https://wa.me/reydes

Correo electrónico: reydes@gmail.com