

Curso DevSecOps

Sábado 22 y Sábado 29 de Noviembre del 2025
De 3:00 pm a 6:00 pm (UTC -05:00)

Las clases en vivo se quedan grabadas en el aula virtual

Presentación

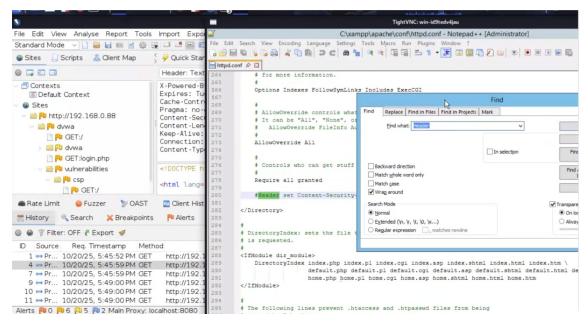
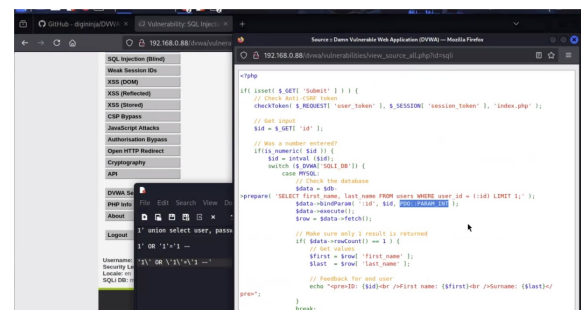
DevSecOps es la abreviatura de las palabras Desarrollo, Seguridad, y Operaciones; también conocido como "Seguridad DevOps", "DevOps Seguro" o "SecDevOps". DevSecOps es una extensión de DevOps el cual codifica la seguridad como parte integral de una estructura de metas más amplia. Para lograrlo DevSecOps concibe la seguridad como una responsabilidad compartida, y algo lo cual debe integrarse perfectamente, en lugar de ser un departamento aislado implementando herramientas engorrosas, soluciones provisionales, u otros medios los cuales dificultan el desarrollo.

Esto requiere la participación de los equipos de seguridad de manera multifacética. Es importante profundizar en esta relación, frecuentemente compleja, entre seguridad y los desarrolladores, aunque es frecuente estas dos áreas parezcan contradictorias. La transición de otras metodologías hacia DevSecOps puede no ser el camino más fácil, pero suele ser el más gratificante.

Este curso proporciona conocimientos y capacidades sobre como la incorporación de prácticas DevSecOps ofrece numerosos beneficios los cuales mejoran la empresa, entre estos, ciclos de desarrollo más rápidos, una mayor seguridad, un mejor desempeño del equipo de desarrollo, y una reducción de costos. Diferenciándose de DevOps, pues representa una mejora integral la cual prioriza la seguridad y la participación de otras unidades de la empresa.

Temario

- DevSecOps: Seguridad como Característica
- El SDLC Tradicional
- El Costo Exponencial de la Corrección
- Integrando "Seguridad" en la Ecuación
- Shift Left
- DevSecOps: Una transformación Profunda
- STRIDE
- Diagramas de Flujo de Datos
- Métricas Clave
- Fase de Codificación: Primera Línea de Defensa
- SAST: Análisis Estático de Código
- Ventajas y Limitaciones de SAST
- Análisis Taint
- Control de Calidad Local
- SCA
- Vulnerabilidades de Componentes
- CVSS
- Integración de SCA en el Proceso de CI
- Gestión de Secretos: Eliminar el "Hardcoding"



- Riesgo Persistente del Historial en Git
- Herramientas para Detección de Secretos
- Criptografía Segura
- Principio de Confianza Cero
- Manejo de Errores e Información Sensible
- Pipeline CI/CD
- DAST
- Vulnerabilidades de DAST
- Integración de DAST en el Pipeline
- Herramientas para IaC y PaC
- Integración de Herramientas en Ciberseguridad en CI/CD
- Pruebas de Fuzzing Automatizadas
- Despliegue Seguro: Blue / Green
- SIEM, WAF, Microsegmentación, SOAR
- Bucle de Retroalimentación
- Cumplimiento y Auditoría
- Principio del Mínimo Privilegio
- Código Limpio
- El Éxito de DevSecOps

```

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @davidmiller for the fix.

# Database management system to use
dbms = getenv('DBMS') ? 'mysql' : 'mysql'
dbms = 'mysql' // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DWA.

# If you are using MySQL then you cannot use root, you must use a dedicated DWA user.
# See https://github.com/OWASP/SecWiki/wiki/MySQL for more information on this.
$DWA = {
  db_server = 'localhost'
  db_database = 'dwa'
  db_user = 'root'
  db_password = 'root'
  db_port = '3306'
}

# Recaptcha settings
# Used for the 'Insecure CAPTCHA' module
# Note: you need to generate your own keys at: https://www.google.com/recaptcha/admin
$Recaptcha = {
  recaptcha_public_key = 'recaptcha_public_key'
  recaptcha_private_key = 'recaptcha_private_key'
}
  
```

Host	Strength	Progress	Elapsed	Reqs	Alerts	Status
Cloud Metadata Potentially Exposed	Medium	00:02:244	18	0	✓	
Server Side Template Injection (SSTI)	Medium	00:17:440	98	0	✓	
Remote OS Command Injection (RCE)	Medium	00:01:661	7	0	✓	
Directory Browsing	Medium	00:13:640	80	0	✓	
Buffer Overflow	Medium	00:05:287	46	5	✓	
Format String Error	Medium	00:00:007	0	0	✓	
CRP Injection	Medium	00:07:603	49	0	✓	
Parameter Tampering	Medium	00:08:604	50	0	✓	
ELMAH Information Leak	Medium	00:01:602	1	0	✓	
Trace and Information Leak	Medium	00:02:702	20	0	✓	
Process Information Leak	Medium	00:01:696	20	0	✓	
env Information Leak	Medium	00:02:287	52	0	✓	
Hidden File Finder	Medium	00:00:001	0	0	✓	
Spring Actuator Information Leak	Medium	00:05:542	24	0	✓	
SQL Injection	Medium	00:02:379	1	0	✓	
SQL Injection	Medium	00:39:397	552	264	✓	
Script Active Scan Rules	Medium	00:00:006	0	0	✓	
SOAP Action Spoofing	Medium	00:00:005	0	0	✓	
SQL Injection	Medium	00:00:005	0	0	✓	

Fechas y Horario

El Curso DevSecOps tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de un tres (3) horas de duración cada una.

- **Fechas:**

Sábado 22 y Sábado 29 de Noviembre del 2025

- **Horario:**

De 3:00 pm a 6:00 pm (UTC -05:00).

Beneficios e Inversión:

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las dos (2) sesiones
- Acceso libre a las sesiones en vivo del siguiente curso a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría en vivo personalizada por videoconferencia
- Libro "Fundamentos de Hacking Web" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 16 horas

S/. 225 Soles o \$ 70 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú

Deposito bancario o transferencia interbancaria en la siguiente cuenta. O también YAPE o PLIN.



Escriba por favor un mensaje al WhatsApp <https://wa.me/51949304030> o reydes@gmail.com para proporcionarle los datos pertinente para realizar el pago.

Residentes en Otros Países

Pago a través de PayPal. O también transferencia de dinero mediante Western Union y MoneyGram



Escriba por favor un mensaje al WhatsApp <https://wa.me/51949304030> o reydes@gmail.com para proporcionarle los datos pertinente para realizar el pago.

Confirmado el pago se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia la plataforma, además de toda la información pertinente para su participación en el curso.

Más Información

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

Correo electrónico: reydes@gmail.com

Teléfono: +51 949 304 030 | (WhatsApp): <https://wa.me/51949304030>

Sitio Web: <https://www.reydes.com>

Instructor



**Alonso
Eduardo
Caballero
Quezada**

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). Cuento con más de dieciocho años de experiencia en el área y desde hace catorce años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: <https://www.ReYDeS.com>