

# FRANCISCO ESCALANTE DUEÑAS

Cybersecurity Analyst | Web Application Security | Penetration Testing

---

## CONTACTO

- Telefono: 999 486 2981
  - Email: fco.escalanted@gmail.com
  - Ubicacion: Ciudad de Mexico, CDMX
  - GitHub: [github.com/Paxx16/cybersecurity-journey](https://github.com/Paxx16/cybersecurity-journey)
  - LinkedIn: [En desarrollo]
- 

## PERFIL PROFESIONAL

Profesional en transicion hacia ciberseguridad con solida experiencia en gestion operativa y liderazgo de equipos. Actualmente en formacion intensiva en seguridad web, con enfoque practico en identificacion y explotacion de vulnerabilidades OWASP Top 10. Experiencia demostrada en SQL Injection, Cross-Site Scripting, Command Injection, CSRF, Path Traversal y Access Control a traves de laboratorios practicos en DVWA y PortSwigger Academy.

---

## HABILIDADES TECNICAS

**Seguridad Web** - OWASP Top 10: SQL Injection, XSS, Command Injection, CSRF, Path Traversal - Analisis de vulnerabilidades en aplicaciones web - Pruebas de penetracion (Penetration Testing)

**Herramientas** - Burp Suite Community Edition - Parrot OS / Kali Linux - Nmap, SQLMap - Firefox Developer Tools - Git / GitHub

**Plataformas de Practica** - PortSwigger Web Security Academy (12 labs completados) - DVWA (Damn Vulnerable Web Application) - TryHackMe (en progreso)

**Idiomas** - Espanol: Nativo - Ingles: Intermedio (lectura tecnica, documentacion)

---

## FORMACION EN CIBERSEGURIDAD

**Programa de Ciberseguridad** | UTEL | 2026 - Diploma en fundamentos de ciberseguridad - Enfoque en seguridad de aplicaciones web

**PortSwigger Web Security Academy** | 2026 - 12 laboratorios completados -  
SQL Injection, XSS, Command Injection - CSRF, Path Traversal, Access Control

**Formacion Autodidacta** | 2026 - Laboratorios practicos en DVWA - Documentacion tecnica de vulnerabilidades - Reportes profesionales bilingues (ES/EN)

---

## PROYECTOS DE CIBERSEGURIDAD

**Portafolio de Seguridad Web** | [github.com/Paxx16/cybersecurity-journey](https://github.com/Paxx16/cybersecurity-journey)  
- Writeups tecnicos de vulnerabilidades explotadas - Documentacion bilingue (Espanol/Ingles) - Analisis de impacto en entornos fintech - Recomendaciones de remediacion con codigo

**Vulnerabilidades Documentadas:** - SQL Injection: Extraccion de credenciales, bypass de autenticacion - XSS: Reflected, Stored, DOM-based, session hijacking - Command Injection: Ejecucion remota de codigo - CSRF: Falsificacion de solicitudes - Path Traversal: Acceso a archivos del sistema - Access Control: Escalacion de privilegios, IDOR

---

## EXPERIENCIA PROFESIONAL

**Gerente General** | Club Privado | 2021 - 2024 - Gestion integral de operaciones y equipo de trabajo - Administracion de presupuestos y recursos - Implementacion de procesos de seguridad fisica - Atencion y resolucion de incidentes

**Gerente de Operaciones** | Hotel | 2021 - 2024 - Supervision de operaciones diarias - Coordinacion de equipos multidisciplinarios - Gestion de sistemas de reservaciones - Control de accesos y seguridad de instalaciones

---

## EDUCACION

**Licenciatura en Relaciones Institucionales** | Universidad La Salle | 2 anos cursados - Desarrollo de habilidades de comunicacion y negociacion - Analisis estrategico y toma de decisiones

---

## CERTIFICACIONES EN PROGRESO

- CompTIA Security+ (planificado)
  - eJPT - eLearnSecurity Junior Penetration Tester (planificado)
  - TryHackMe Learning Paths (en curso)
-

## **COMPETENCIAS ADICIONALES**

- Redaccion de reportes tecnicos
- Documentacion bilingue
- Aprendizaje autonomo
- Resolucion de problemas
- Trabajo bajo presion
- Liderazgo de equipos