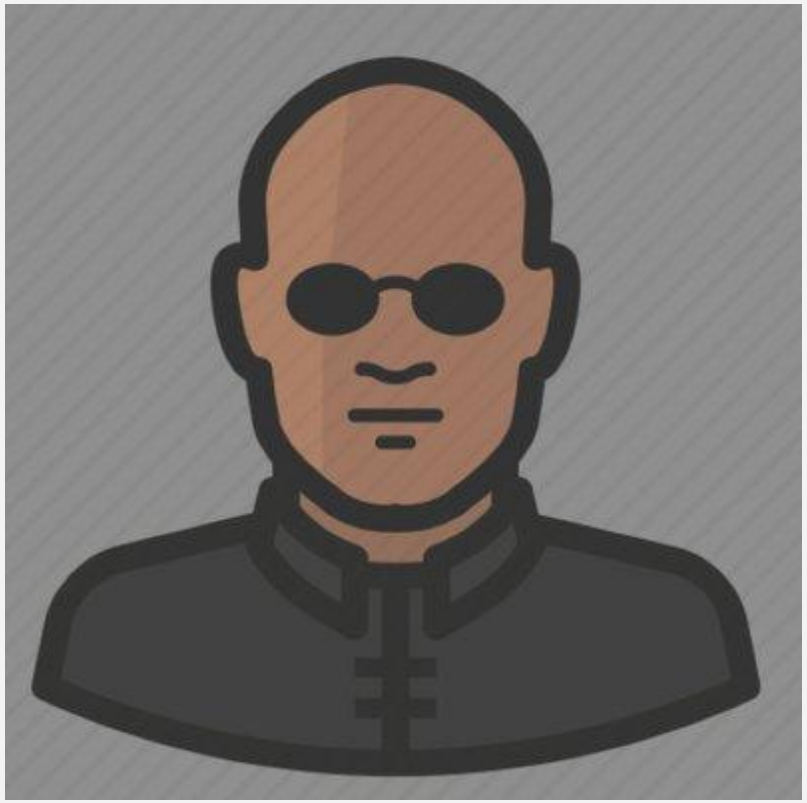
# Web App Pentesting

# BIO



- Raga también c.c. Luis Diego Raga
- Sr. Penetration Tester
- Cloud Security, DDoS, WAF, Bot Management, CDN, Networking (FWs, VPN, IPS), Incident Response
- LinkedIn: Luis Diego Raga
- Discord: dc506.org
- Twitter: @Ragab0t
- Blog: blog.ragab0t.com

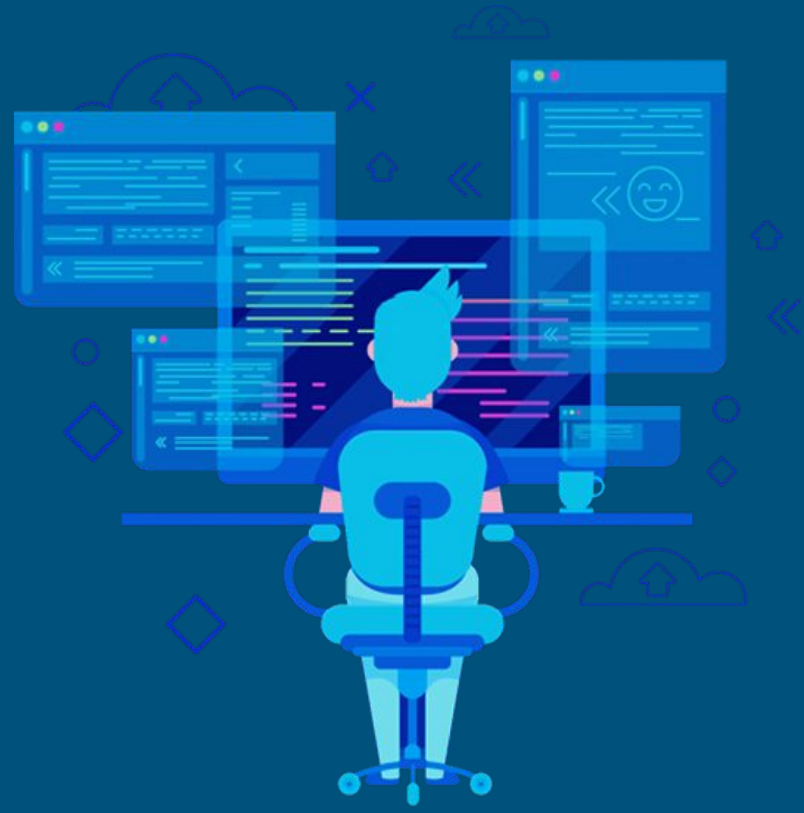
# Agenda

- Objetivos
- Proceso
- Metodología
- Desafíos
- Ética
- Demo
- Recursos

# Web App Pentesting - Objetivos

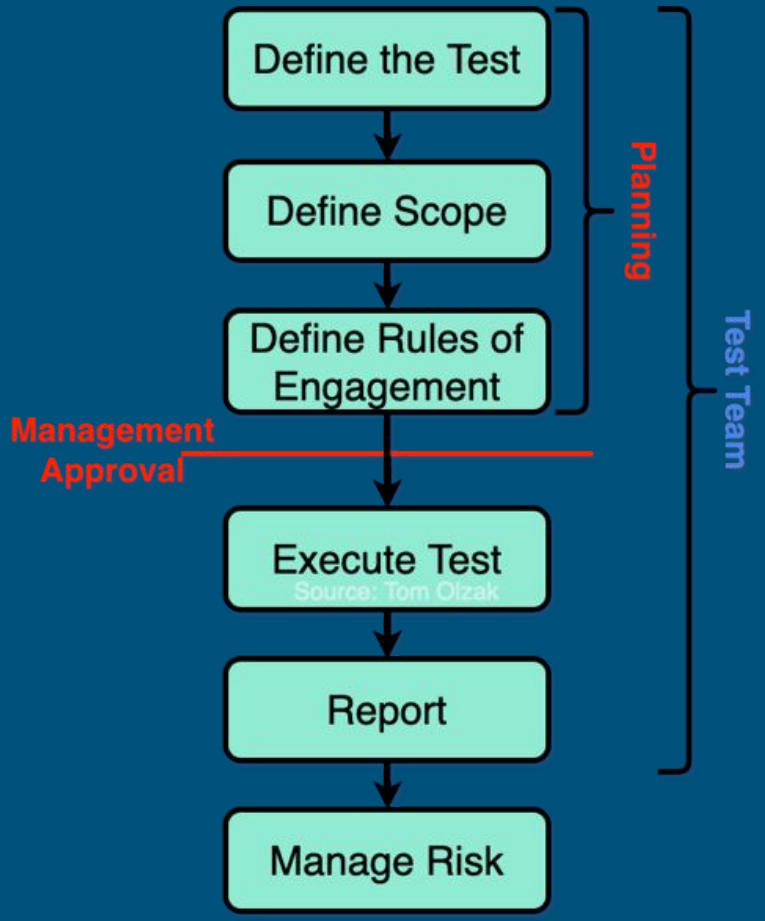
Un Pentest es un proyecto que tiene los siguientes objetivos:

- Identificar vulnerabilidades que podrían ser explotadas por atacantes malintencionados
- Garantizar que las aplicaciones web sean seguras y estén mejor equipadas contra ataques
- Cumplir con requisitos de cumplimiento y certificaciones
- Probar la madurez del programa de seguridad en tema de respuesta a incidentes



# Web App Pentesting: Proceso

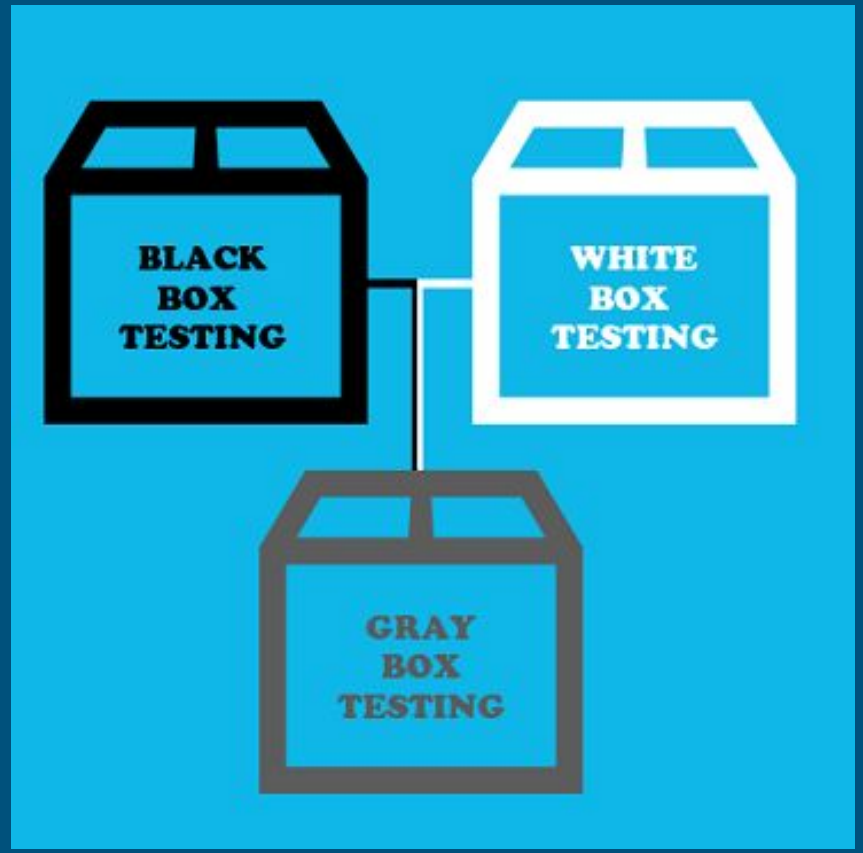
- Definir el motivo del test
- Definir el alcance
- Definir Rules of Engagement
- Kickoff
- Recolección de información
- Identificación de vulnerabilidades
- Explotación de vulnerabilidades
- La generación y presentación de informes
- Re-Tests



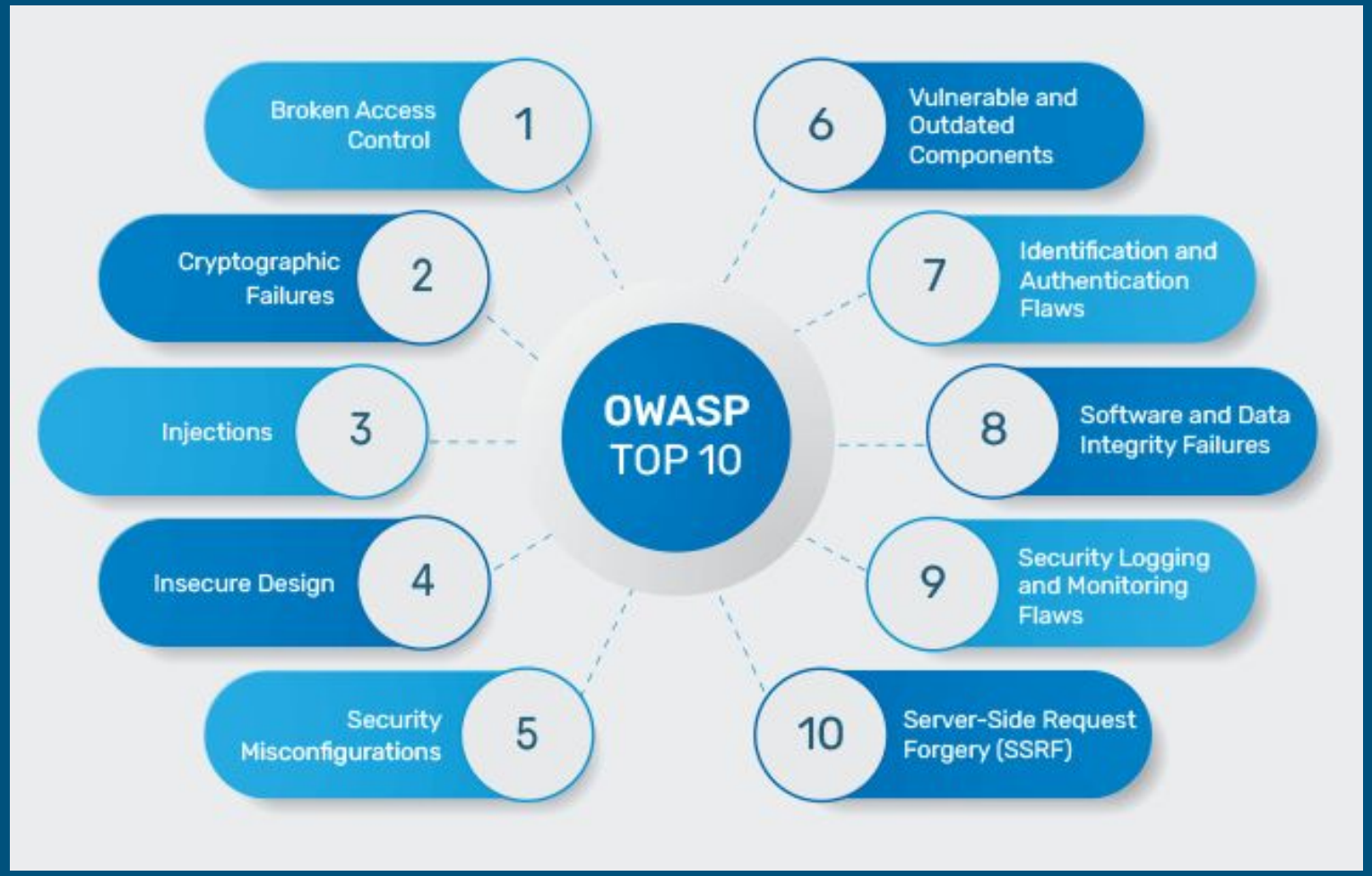
# Web App Pentesting: Tipos

- Basados en la información provista:
  - Black Box
  - Gray Box
  - White Box

- Basados en el alcance
  - Incremental
  - Full

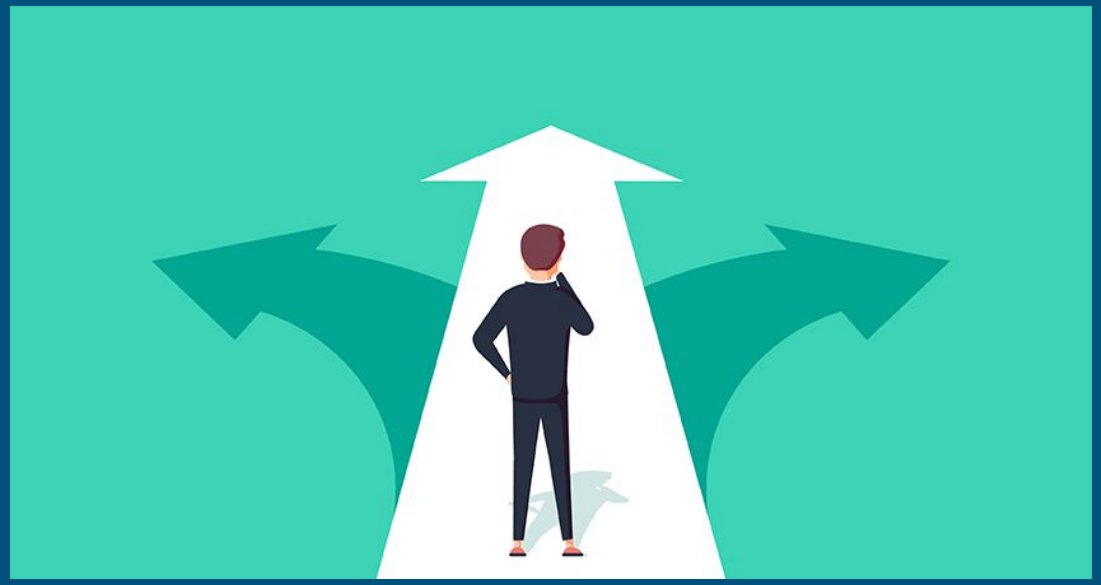


# Tipos de Vulnerabilidades



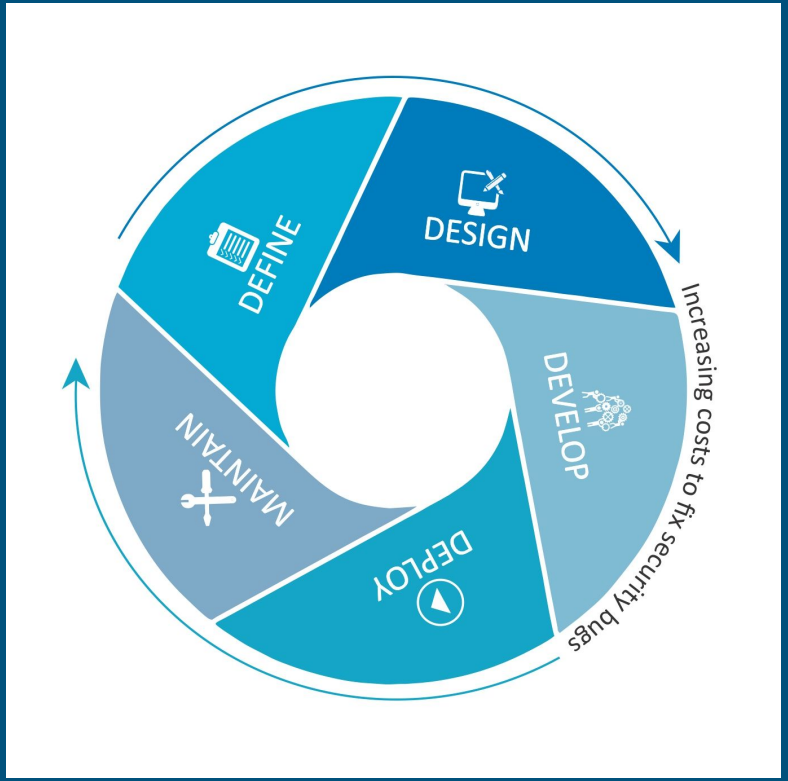
# Metodologías - Marcos de Referencia

- OWASP Top 10
- OWASP Top 10 API
- OWASP Top 10 Mobile
- SANS Top 25
- PCI



# Guías - OWASP Testing Guide

- Guia desarrollada por OWASP
- Proporciona una metodología estructurada
- Incluye mejores prácticas, riesgo, planificacion y ejecucion de pruebas, y presentación de resultados
- Incluye recomendaciones de herramientas y técnicas utilizadas



# Preparación

- Disponer de ambientes de prueba (UAT, QA, DEV) para evitar llevar a cabo la prueba en producción
- Contar con contacto técnico que se encargue del proyecto
- Asegurarse que la aplicación pueda ser accedida de forma segura
- Asegurarse que existen backups de la base de datos (prod)
- Tener listo el plan de respuesta a incidentes

# Ejecución - Herramientas

Burp Suite

ZAP

Postman

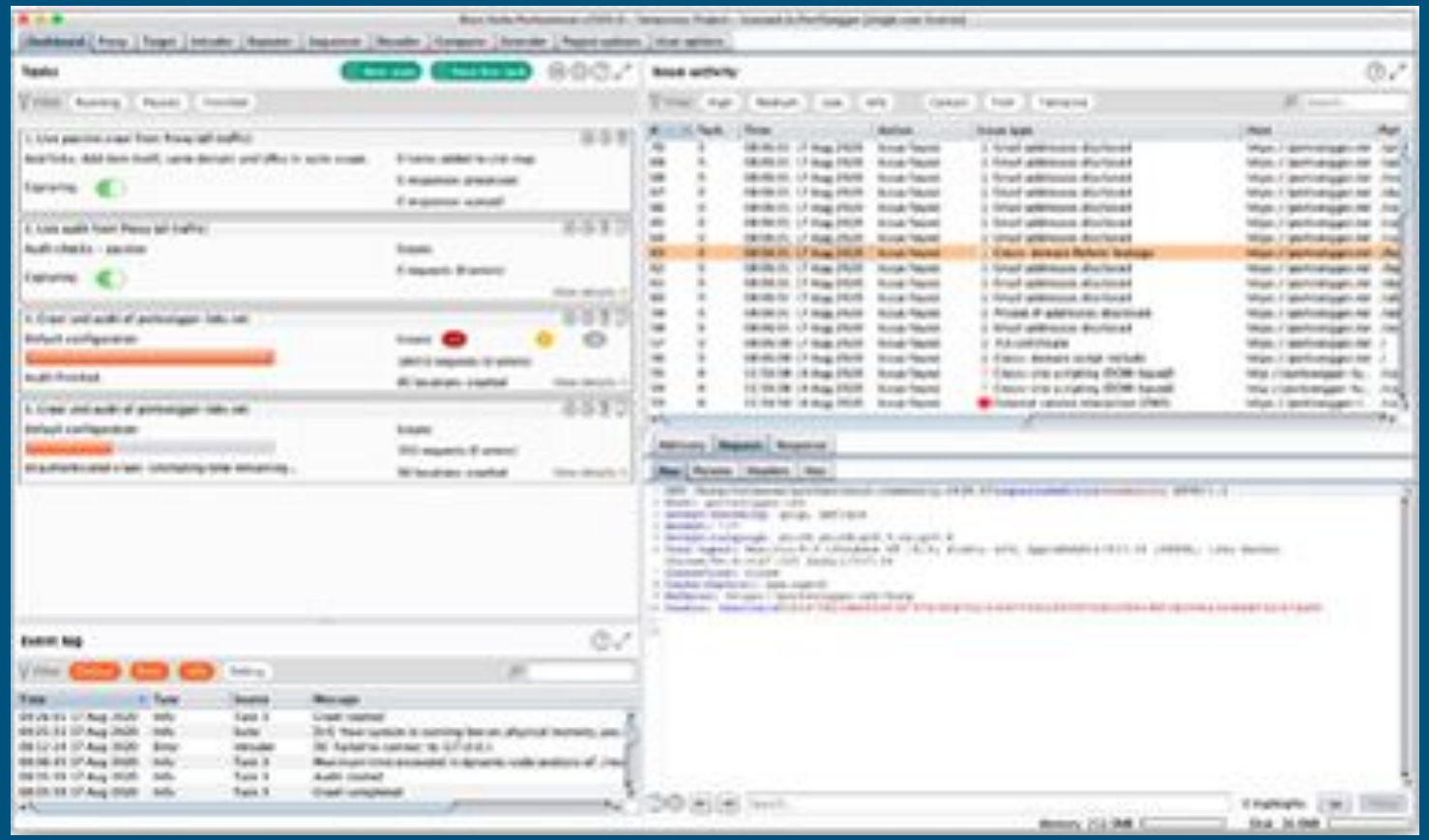
SQLMap

Accunetix

WPScan

Curl

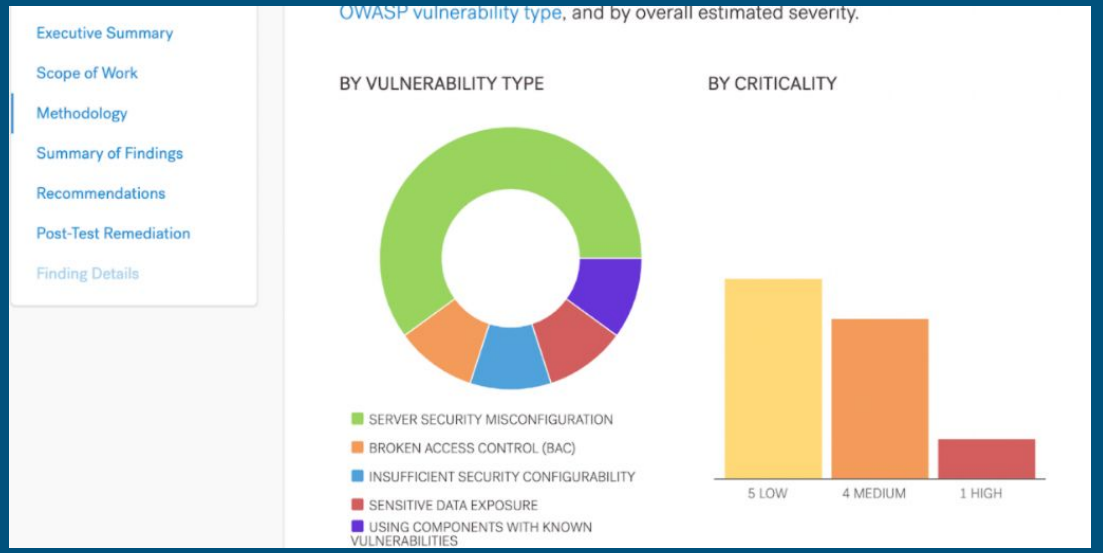
Metasploit



# Reporte

- “Nos pagan por hacer reportes, no por hackear cosas”

- Debe incluir cuando mínimo:
  - Resumen ejecutivo
  - Alcances y metodología
  - Detalles técnicos de cada vulnerabilidad encontrada
  - Recomendaciones



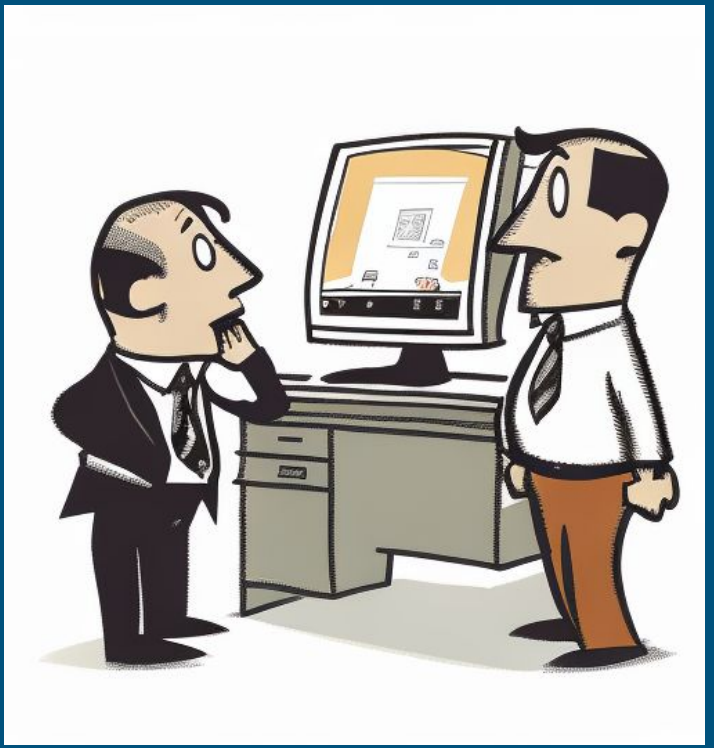
# Mitigación

- Uno de los principales elementos a tomar en cuenta a la hora de mitigar es la severidad de la vulnerabilidad.
- Las soluciones pueden variar desde parches de seguridad y actualizaciones de software hasta cambios en la configuración de la aplicación
- Es importante probar que la mitigación sea efectiva

| Rating | CVSS Score |
|---|---|
| None | 0.0 |
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |

# Desafíos

- Acceso a la información solicitada (credenciales, ambientes, conectividad)
- Disponibilidad del cliente para responder consultas a lo largo del test
- Limitación con respecto a herramientas en ambientes muy seguros
- Mantenerse al día en tema de técnicas, ataques y metodologías

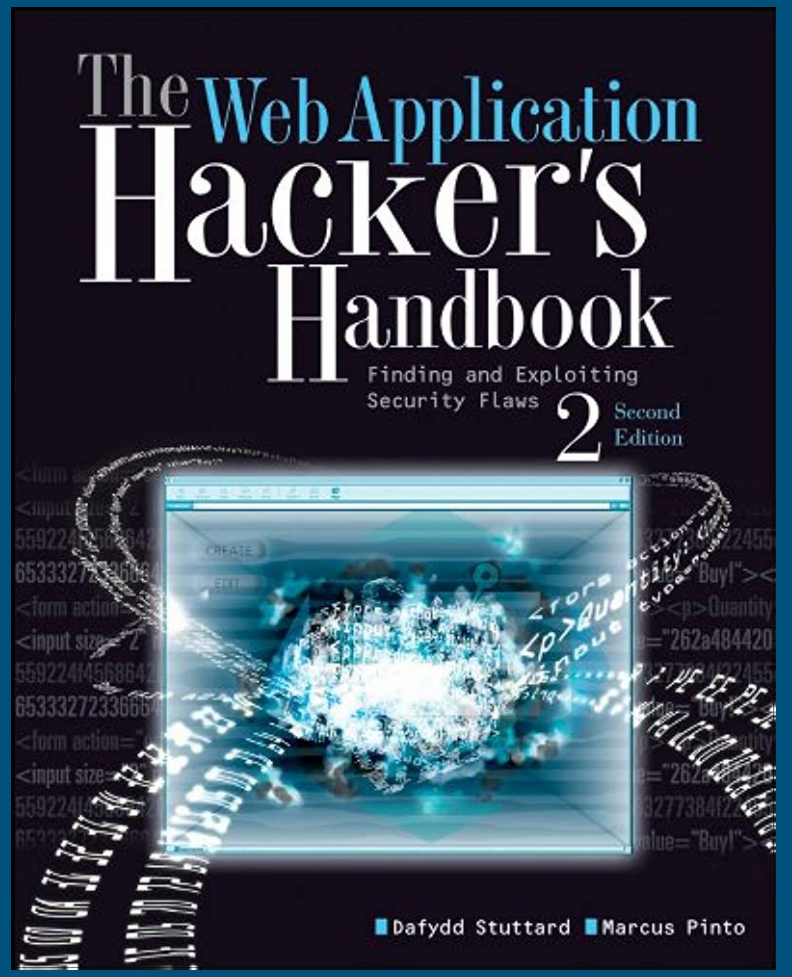


# Ética y Pentesting

- Las pruebas solo deben llevarse a cabo con el permiso del propietario de la aplicación
- En caso de que “accidentalmente” se descubra una vulnerabilidad debe reportarse por medio de los canales adecuados
- De ser posible revisar si la empresa cuenta con programa de Bug Bounty

# Recursos

- Online Labs:
  - Web Security Academy
  - Try Hack Me
  - Pentester Lab
- Vulnerable Web Apps:
  - Juice Shop
  - Web Goat
  - DVWA
- Youtube:
  - InsiderPHD
  - NahamSec
  - The Cyber Mentor
  - The XSS Rat
  - S4vitar
  - DC506



# Certificaciones

- SANS: GWAPT
- eLearn:
  - eWPT
  - eWPTX
- Offsec:
  - OSCP
  - OSWA
  - OSWE
- Portswigger: Burp Suite Certified Practitioner
- Hack the Box: Bug Bounty Hunter

# Preguntas?