

## INTRODUCCIÓN

Es la metodología de trabajo que desarrolla técnicas de evaluación de seguridad y rendimiento en contextos específicos de su infraestructura. Esta metodología fue desarrollada por Shellcode® a partir del Standard Penetration Test, el cual, luego de un análisis minucioso y desde nuestra vasta experiencia desarrollándolo, ha sido fragmentado en módulos para ampliarse en alcances operativos acordes con la realidad de los avances tecnológicos.



- ➔ **WebApplications/Databases**; evaluación de seguridad y rendimiento de aplicaciones WEB de NEGOCIO, desarrollando técnicas de Pre-authentication y Post-Authentication utilizadas por potenciales atacantes externos.
- ➔ **Wifi**; evaluación de seguridad de los controles de acceso inalámbrico de la compañía, en búsqueda de accesos no autorizados.
- ➔ **VoIP**; evaluación de seguridad de la plataforma de telefonía IP de su compañía, detectando fallas desde Internet y desde la red local.

**Nuestros servicios incluyen presentaciones gerenciales, reportes técnicos y ejecutivos, con resultados, y criterios concensuados que muestran conclusiones claras.**

El servicio continúa hermanado con los clásicos conceptos de Penetration Testing y Ethical Hacking, por consiguiente las fases operativas de este servicio poseen estructuras similares, donde en un modelo acorde con los estándares conocidos incluimos las siguientes comprobaciones de seguridad:



### Detección de vulnerabilidades en aplicativos WEB y Base de Datos

- ▶ SQL Injection
- ▶ Remote File Inclusion
- ▶ Local File Inclusion
- ▶ Authentication bypass
- ▶ File Upload
- ▶ Cross Site Scripting
- ▶ LDAP Injection
- ▶ Session Fixation
- ▶ X-Path Injection
- ▶ Inyection Header
- ▶ XML Injection
- ▶ HTTP Response Splitting



### Detección de vulnerabilidades en su infraestructura de red

- ▶ Port Scanning
- ▶ Servidores de correo electrónico
- ▶ Servidores de dominio de nombres

- ▶ Validación de certificados SSL
- ▶ Contraseñas débiles.



#### **Detección de riesgos de pérdida o manipulación de información**

- ▶ Debilidades de CAPTCHA
- ▶ Errores de diseño
- ▶ Vulnerabilidades funcionales aplicativas.

La metodología de seguridad aplicada por Shellcode presenta importantes diferencias respecto de estos tipos de evaluaciones aplicadas habitualmente en el mercado, que deberán tenerse en cuenta durante la cotización del servicio. Lea, "[Como elegir el proveedor de evaluaciones de seguridad](#)"

Servicios profesionales de evaluación de seguridad		
Ethical hacking / Security Modular Test / Penetration Testing		
Descripción del servicio	SHELLCODE	OTROS
Se entrega informe ejecutivo ?	si	n/c
El informe técnico explica el detalle de las vulnerabilidades descubiertas ?	si	no
Incluye el detalle de las vulnerabilidades descubiertas un Roadmap para su resolución ?	si	no
Coordinación de las pruebas de Negación de Servicio ?	si	si
Se entregan ejemplos de los reportes ejecutivos/técnicos que forman el producto final?	si	no
La metodología tiene base en el movimiento OWASP y OSSTMM ?	si	si
Existe un procedimiento para alinear las operaciones a procesos ITIL ?	si	no
El criterio aplicado en el análisis de riesgo es desarrollado en conjunto con el cliente ?	si	no
Se utilizan herramientas automatizadas y de desarrollo interno ?	si	si
Es una empresa libre de intereses comerciales con proveedores de soluciones de seguridad ?	si	n/c
Ante la urgencia de una caso se entregan "informes de descubrimiento" parciales?	si	no
Se contempla el análisis de vulnerabilidades 0days ?	si	n/c

#### **Contáctenos**

Por teléfono al: +54 0(11) 59.17.52.31

Vía e-mail a: [seguridad@shellcode.com.ar](mailto:seguridad@shellcode.com.ar)

Tucumán 1441 piso 9 oficina A - C1050AAC

Ciudad Autónoma de Buenos Aires – República Argentina

FAX: +54 0(11) 59.17.52.32

#### **SECURITY MODULAR TEST**

© 2010 SHELLCODE S.R.L – <http://www.shellcode.com.ar>