

Sistema Integrado de Soporte para Análisis de Vulnerabilidades en Sistemas Web (SISAVSW)

Problemática

En el ámbito del desarrollo de software existen los denominados entornos de desarrollo integrado (IDE, Integrated Development Environment) siendo programas de mucha utilidad por la considerable reducción de tiempo que brindan al programador al momento de desarrollar un sistema, sin embargo en lo concerniente a seguridad informática sólo existen aplicaciones diferentes, cada una enfocada en un único aspecto de seguridad.

Funciones

- Verificar si el sitio es vulnerable a ataques de Cross-Site Scripting, SQL Injection, Remote File Inclusion.
- Extraer información sobre la tecnología usada en el sistema web objetivo.
- Permitir la consulta y modificación de peticiones HTTP.
- Probar el nivel de acceso de los recursos del sitio.
- Permitir el seguimiento de metodologías de pentesting provistas por organismos como OWASP.
- Generar reportes y estadísticas sobre vulnerabilidades encontradas.
- Validar el código fuente HTML con el estándar de la W3C.
- Verificar la interoperabilidad del código del lado del cliente entre navegadores.
- Permitir ofuscación del código fuente visible por el cliente, así también la eliminación de comentarios del mismo.

Contexto

El proyecto se desarrolla dentro del Laboratorio de Sistemas de la UTN - FRC. En el marco del grupo de investigación en Seguridad Informática.

Solución

Desarrollar una herramienta de software libre que permita ejecutar múltiples pruebas de seguridad para identificar vulnerabilidades sobre sistemas web, y cumplimentar con los estándares de seguridad informática. La misma está destinada a profesionales de informática a quienes brindará soporte en procesos de auditorías de sitios web.

