

Creado por Colin Watson

Version WebApp-1.02-ES (Classic)

OWASP Serpientes y Escaleras - Aplicaciones Web -

Serpientes y Escaleras es un juego con propósitos educativos relacionados con seguridad en aplicaciones web. Esta versión representa a el proyecto "OWASP Top Ten Proactive Controls" (OWASP Top Diez Controles Proactivos) como escaleras, mientras que el conocido proyecto "OWASP Top Ten Most Critical Risks" (OWASP Top Diez Riesgos Más Críticos) como serpientes. Agradecemos a los líderes y contribuidores a estos dos proyectos.

OWASP Top Diez Controles Proactivos en Aplicaciones Web (2014)

El proyecto Top Diez Controles Proactivos en Aplicaciones Web es una lista de técnicas de seguridad que deberían ser incluidos en todo proyecto de desarrollo de software.

- C1 Parametrización de Consultas
- C2 Cifrado/Codificación de Datos
- C3 Validación de Toda Entrada
- C4 Implementación de Controles de Acceso Apropriados
- C5 Establecer Controles de Identidad y Autenticación
- C6 Protección de Datos y Privacidad
- C7 Implementar Registros de Auditoría, Manejo de Errores y Detección de Intrusiones
- C8 Utilizar las Funciones Nativas de Seguridad de las Librerías y Frameworks
- C9 Incluir Requerimientos Específicos de Seguridad
- C10 Diseñar e Implementar Arquitectura de Seguridad Desde Adentro

https://www.owasp.org/index.php/OWASP_Proactive_Controls

El archivo fuente de esta página, material y otros temas relacionados con seguridad en aplicaciones, así como versiones de diferentes idiomas, y más información relacionada con el Proyecto se puede encontrar en el siguiente sitio https://www.owasp.org/index.php/OWASP_Snakes_and_Ladders

OWASP Top Diez Riesgos Más Críticos en Aplicaciones Web (2013)

El OWASP Top Diez representa un amplio consenso acerca de las fallas de seguridad más comunes en aplicaciones web.

- A1 Inyección
- A2 Pérdida de Autenticación y Gestión de Sesiones
- A3 Secuencia de Comandos en Sitios Cruzados (XSS)
- A4 Referencia Directa Insegura a Objetos
- A5 Configuración de Seguridad Incorrecta
- A6 Exposición de Datos Sensibles
- A7 Ausencia de Control de Acceso a las Funciones
- A8 Falsificación de Peticiones en Sitios Cruzados (CSRF)
- A9 Uso de Componentes con Vulnerabilidades Conocidas
- A10 Redirecciones y Reenvíos No Validados

<https://www.owasp.org/index.php/TopTen>

Antecedentes

Serpientes y Escaleras es un juego de mesa popular importado de Gran Bretaña por los Victorianos y ésta basado en un juego Asiático. El juego original mostraba los efectos del bien y el mal, virtudes y vicios. El juego es conocido en algunos lugares de América como toboganes y escaleras. En esta versión de OWASP, las actitudes virtuosas están relacionadas con prácticas de desarrollo de software y código seguro (los controles proactivos) y los vicios son los riesgos de seguridad en aplicaciones.

Advertencia

OWASP Serpientes y Escaleras está pensado para ser utilizado por programadores de software principiantes y experimentados. Este juego de mesa no es dañino, pero si escoges utilizar tu propio dado de plástico o de madera, entonces estos podrían tener riesgos de sofocar a niños menores de 4 años de edad.

No cuentas con dados ni jugadores para jugadores? Corte los bordes de los círculos coloreados de abajo y utilízalos como marcadores para los jugadores. Adicionalmente escribe un programa en computadora para simular un dado de seis caras, o utiliza una función aleatoria ya sea de tu teléfono o computadora para generar números enteros entre 1 y 6. Revisa si la función aleatoria trabaja apropiadamente!

Para hacer un dado, corta cuidadosamente la forma de dado de ésta hoja, dobla los bordes de las líneas punteadas y pega las pestañas hasta que formes un cubo.

Debe de haber 7 marcadores, pero la codiciosa serpiente se ha comido uno. Lo podrías identificar?

Lider de Proyecto

Colin Watson

Traductores / Otros Contribuidores

Manuel Lopez Arredondo, Fabio Cerullo, Tobias Gondrom, Martin Haslinger, Yongliang He, Cédric Messeguer, Rirotaro Okada, Ferdinand Vroom, Ivy Zhang

OWASP Serpientes y Escaleras es libre de uso. Está bajo la licencia de Creative Commons Attribution-ShareAlike 3.0, por lo que éste trabajo lo puedes copiar, distribuir y transmitir, también lo puedes adaptar y utilizarlo comercialmente, pero todo está proporcionado para que el trabajo lo puedas atribuir y si lo alteras, transformas, o construyes algo sobre éste trabajo, el trabajo resultante lo deberías compartir bajo la misma licencia o una similar a ésta. © OWASP Foundation 2014.

Final (100) → **Inicio** (1)

OWASP-A1 Inyección (96)

OWASP-A9 Uso de Componentes con Vulnerabilidades Conocidas (92)

OWASP-A10 Redirecciones y Reenvíos No Validados (82)

OWASP-A6 Exposición de Datos Sensibles (84)

OWASP-A5 Configuración de Seguridad Incorrecta (89)

OWASP-A8 Falsificación de Peticiones en Sitios Cruzados (CSRF) (76)

OWASP-A4 Referencia Directa Insegura a Objetos (78)

OWASP-C10 Diseñar e Implementar Arquitectura de Seguridad Desde Adentro (65)

OWASP-C9 Incluir Requerimientos Específicos de Seguridad (53)

OWASP-C8 Utilizar las Funciones Nativas de Seguridad de las Librerías y Frameworks (42)

OWASP-A7 Ausencia de Control de Acceso a las Funciones (37)

OWASP-A2 Pérdida de Autenticación y Gestión de Sesiones (35)

OWASP-C7 Implementar Registros de Auditoría, Manejo de Errores y Detección de Intrusiones (36)

OWASP-C6 Protección de Datos y Privacidad (34)

OWASP-A3 Secuencia de Comandos en Sitios Cruzados (XSS) (27)

OWASP-C5 Establecer Controles de Identidad y Autenticación (30)

OWASP-C4 Implementación de Controles de Acceso Apropriados (19)

OWASP-C3 Validación de Toda Entrada (12)

OWASP-C1 Parametrización de Consultas (5)

OWASP-C2 Cifrado/Codificación de Datos (8)