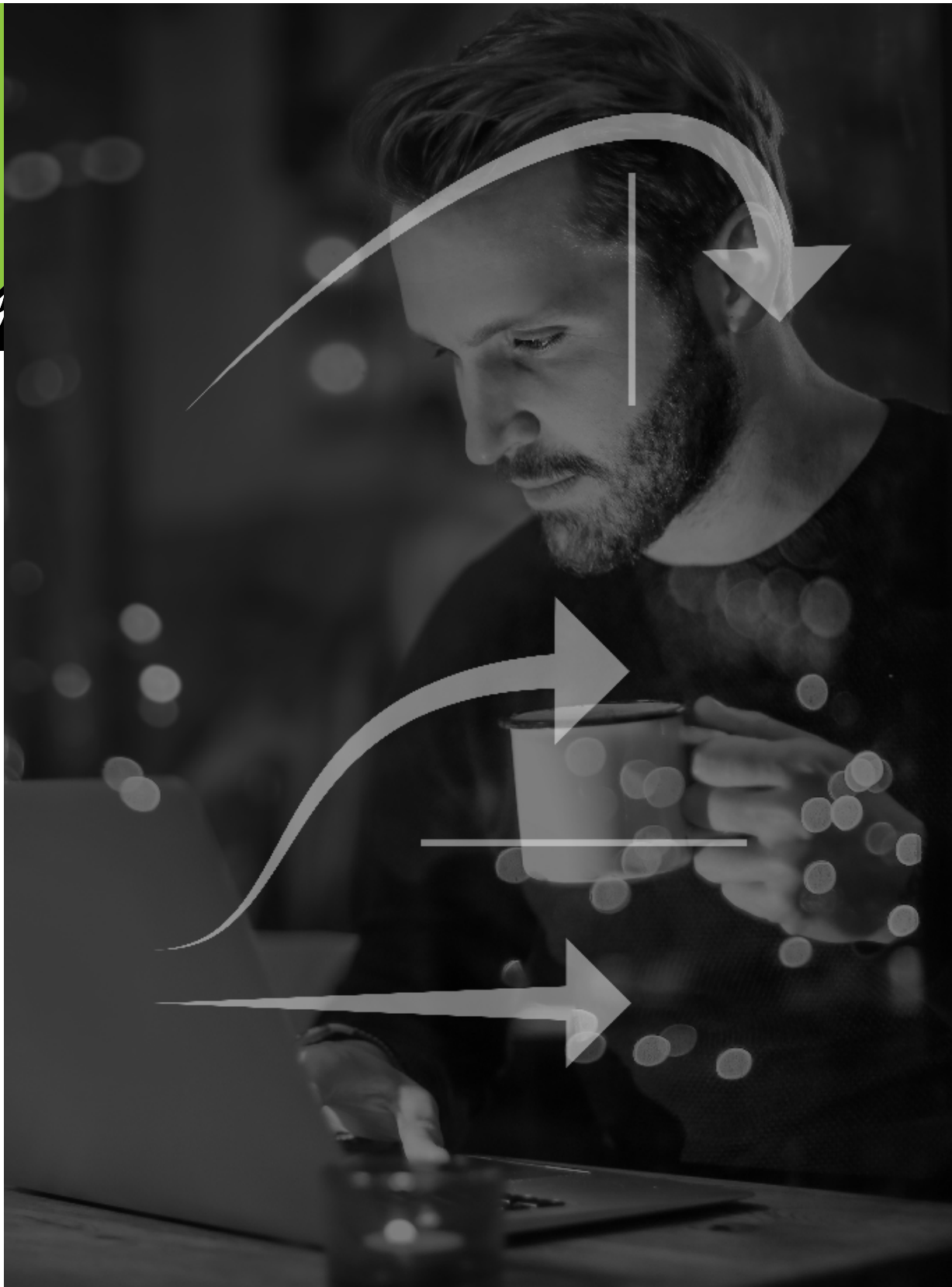
RidgeHAD

Detección Top de Acceso Horizontal

RIDGE SECURITY



Antecedentes

Control de Acceso Roto y Escalada de Privilegios Horizontales

El Control de acceso interrumpido se refiere a la capacidad de un usuario final, ya sea mediante la manipulación de una URL, cookie, token o contenido de una página, para acceder virtualmente a datos donde no deberían tener acceso. Comúnmente se encuentran controles de acceso rotos y vulnerabilidades críticas de seguridad.

Estas vulnerabilidades ocupan el puesto número 5 en los 10 riesgos de seguridad de aplicaciones web más importantes de OWASP (Proyecto de seguridad de aplicaciones web abiertas)2017.

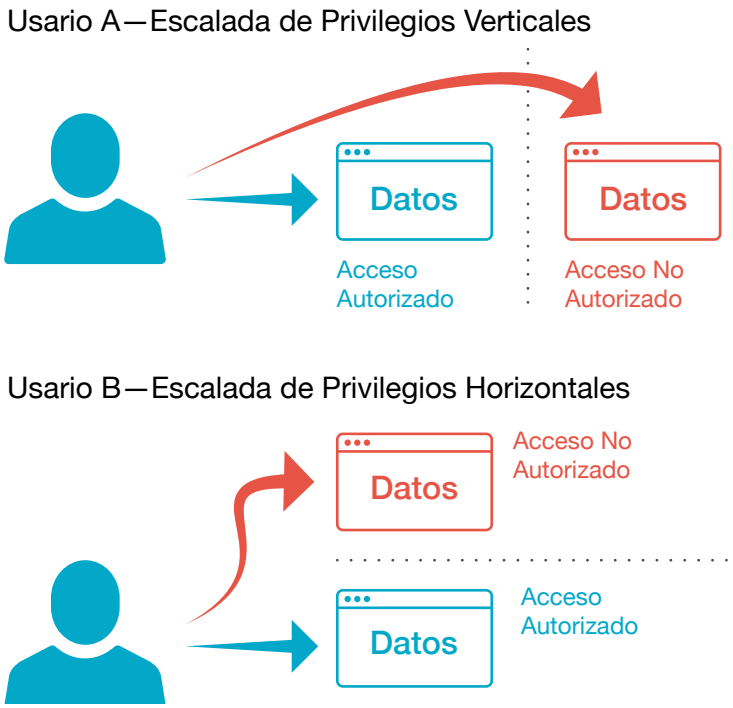
El diseño y la gestión de los controles de acceso pueden ser complicados y dinámicos. Las aplicaciones webs están en constante evolución, y encontramos que las reglas de control de acceso se insertan en varias ubicaciones en diferentes momentos. Es un desafío insidioso detectar controles de acceso defectuosos confiando en la discreción de un desarrollador.

Los controles de acceso defectuosos se explotan para ataques de:

- **Escalada Vertical de Privilegios**
  La escalada de privilegios verticales se refiere a la violación de acceso entre diferentes niveles de privilegios de usuario, como un usuario ordinario para ejecutar como usuario administrador.
- **Escalada de Privilegios Horizontales**
  La escalada de privilegios horizontales se refiere a una operación no autorizada entre usuarios en el mismo nivel, Por ejemplo, si es un empleado solo debe poder, acceder a sus registros de empleo y nómina, pero, de hecho, también puede acceder a los registros de otros empleados, entonces esto es la escalada de privilegios horizontales.

Las escaladas de privilegios verticales y horizontales resultan en consecuencias devastadoras. Como la escalada vertical de privilegios es un paso imprescindible para la mayoría de los ataques sofisticados, su detección es explorada ampliamente y cubierta por muchos sistemas de detección de amenazas. El ataque horizontal merece su tratamiento especial, ya que las fallas son comunes en el código, y es fácil de explotar y se le culpa por muchas violaciones importantes de datos y pérdidas financieras.

El RidgeHAD es un sistema que tiene como objetivo principal detectar y detener los ataques de escalada de privilegios horizontales y ayudar a las organizaciones a aplicar el control de acceso horizontal.



El usuario A y el usuario B pertenecen al mismo rol y tienen el mismo nivel de permiso. Aun así, el sistema de nómina solo verifica el rol que puede acceder a los datos, sin vincularlo a una identidad de usuario específica.

Causas y Consecuencias

Por lo general, durante el desarrollo, la mayoría de los desarrolladores de aplicaciones web diseñan deliberadamente una verificación de permisos estricta para cada función. Sin embargo, a medida que el código simplemente evoluciona, y la aplicación se acerca a la implementación, la colección de reglas ad hoc se vuelve tan difícil de manejar que es casi imposible de entender. Una vez que hay una omisión, puede ocurrir un acceso no autorizado.

Las Vulnerabilidades de Privilegios Causan Daños Devastadores Tanto de las Organizaciones Como de los Usuarios.

Algunas brechas de datos bien conocidas en el pasado culparon a la protección de privilegios defectuosa. Por ejemplo, las infracciones de Home Depot en 2014 comenzaron cuando se robaron las credenciales de un socio externo. El daño real ocurrió cuando el atacante obtuvo la escalada de privilegios a través de esta cuenta robada, lo que le permite acceder al mismo tipo de datos a través de toda la organización.

Otros casos comunes son con aplicaciones de comercio electrónico, donde las promociones usan cupones o canje de puntos. Si los sitios web usan alguna forma de identificación, clave o índice como una forma de referenciar a un usuario, pero no validan la identificación que pertenece a ese usuario actual, el atacante puede adivinar estas identificaciones, acceder a datos robados y robar puntos, cupones y otra información. Si esto ocurre, el sitio web no puede lograr el objetivo de sus promociones, sufre pérdidas financieras y pone en riesgo a sus clientes.

Para los usuarios finales, el impacto es directo y desastroso. Una vez que su identidad, domicilio, teléfono y otra información confidencial se filtre al mercado negro, los delincuentes podrían hacer todo tipo de daños con ella: moderar / eliminar cuentas e información, incluso robar sus identidades.

Las Tres Razones más Comunes que Resultan en una “Escalada de Privilegios Horizontales”

1. Función web basada únicamente en el “ID de identidad del usuario.” Cuando se realiza una función, se accede a los datos correspondientes o se manipula a través de una ID única basada en la identidad de un usuario, como la ID de usuario, el número de cuenta, el número de teléfono móvil, el número de identificación, etc.

2. Función web basada únicamente en “el ID del objeto.” Al realizar una función, se accede a los datos correspondientes o se manipula a través de la ID del objeto, como el número de pedido, el número de registro, etc.

3. Función web basada únicamente en el “nombre de archivo.” Cuando se realiza una función, se accede a un archivo utilizando su nombre de archivo, más comúnmente visto cuando un usuario está cargando un archivo.

Ejemplos de Acceso Horizontal Detecció

Un Proveedor de Servicios de Correo Electrónico: Vulnerabilidad de Restablecimiento de Contraseña de Correo Electrónico

Este proveedor de servicios de correo electrónico envió un código de verificación al teléfono móvil de un usuario para restablecer la contraseña del buzón del usuario como lo hacen muchos sitios web. Sin embargo, en su mecanismo de control de acceso, omitieron verificar la relación vinculante entre el buzón y el número de teléfono móvil. Entonces, un atacante restablece la contraseña del buzón modificando la dirección de correo electrónico en la URL de solicitud y recibió el código de verificación con un número de teléfono móvil que especificaron. Con el exploit de restablecimiento de contraseña, un atacante rápidamente obtuvo acceso a los correos electrónicos del usuario. Hoy en día, la mayoría de los usuarios vinculan su dirección de correo electrónico con sus sitios web de comercio electrónico de uso frecuente, a través de la función “Olvidó su contraseña.” El atacante restablece las contraseñas del usuario en todos los sitios web de comercio electrónico con la dirección de correo electrónico comprometida.

Un Sitio Web de Reclutamiento: Acceso No Autorizado a Todos los CV

En este sitio web, al atravesar los parámetros de solicitud de URL, un atacante obtuvo los currículums de otros usuarios, donde encontraron información confidencial y personal como identificación, dirección residencial, número de teléfono móvil, dirección de correo electrónico, educación, etc.

Una Aplicación Movie Ticket: Acceso No Autorizado a las Órdenes de Reserva de Otros Usuarios

Después de comprar un boleto en línea, cuando un usuario abandona su pedido, la ID se muestra en los parámetros de la URL como un texto claro. En el estado de inicio de sesión, al atravesar las ID, un atacante obtuvo toda la información de reserva del otro usuario y el código QR de los tickets.

Un Sitio Web Oficial de Smart Watch: Canje de Puntos No Autorizados

Este sitio web ofrece a los usuarios una función para canjear puntos por productos. Sin embargo, el control de acceso de esta función tenía una falla, y un atacante pudo obtener todos los puntos del usuario al alterar la ID del usuario en los parámetros de URL.

Sistema RidgeHAD

La escalada de privilegios horizontales es una vulnerabilidad de lógica empresarial que es difícil de evitar durante el desarrollo. Las pruebas de seguridad exhaustivas antes de la implementación son la mejor herramienta recomendada por los expertos en seguridad para detectar las violaciones y proteger los controles de acceso.

El mecanismo de control de acceso debe probarse ampliamente para asegurarse de que no hay forma de evitarlo. Esta prueba requiere una variedad de cuentas e intentos extensos de acceder a contenido o funciones no autorizados.

Actualmente, muchas organizaciones adoptaron pruebas manuales; sin embargo, las pruebas manuales no solo son muy costosas, sino que tampoco son factibles para aplicaciones complejas y de gran escala. La detección de escalada de privilegios horizontales es relativamente lenta y requiere mucho trabajo en comparación con otras pruebas, lo que inevitablemente afecta la entrega rápida de los sistemas de aplicación. Se necesita un sistema de detección automatizado eficiente y confiable.

El RidgeHAD es un sistema de este tipo que libera a los evaluadores de seguridad de las pesadas pruebas manuales y mejora la productividad.

Mecanismos de Detección

El RidgeHAD utiliza dos mecanismos de detección: rastreo y proxy.

El **modo de rastreo**, configurado para aplicaciones WEB, utiliza motores Smart Crawler y Bruteforce para obtener todas las URL y datos interactivos de las aplicaciones probadas. El modo de rastreo, configurado para aplicaciones WEB, utiliza motores Smart Crawler y Bruteforce para obtener todas las URL y datos interactivos de las aplicaciones probadas.

El **modo proxy** se usa principalmente para aplicaciones móviles. Un proxy está configurado para capturar todas las URL y los datos interactivos generados por los usuarios desde sus aplicaciones móviles.

Después de recopilar todos los datos a través de Crawler o Proxy, RidgeHAD enciende su motor de inspección de vulnerabilidades, junto con su motor de detección de amenazas alimentado por IA, descubriendo vulnerabilidades ocultas en los controles de acceso horizontal de las aplicaciones bajo prueba. La seguridad en los equipos revisa todos los hallazgos de RidgeHAD para validar. El equipo de desarrollo repara vulnerabilidades validadas antes de la implementación.

El RidgeHAD es una prueba de caja negra. Los probadores no necesitan comprender los detalles de implementación de la aplicación ni ningún lenguaje de programación en particular. La prueba es simple y conveniente, y los resultados son persistentes. Esto libera a los evaluadores de la gran carga de trabajo de la documentación y la preparación de informes, como se requiere en las pruebas manuales.

Ventajas Técnicas

Cinco tecnologías centrales impulsan el sistema RidgeHAD

- Rastreador inteligente
- Motor de fuerza bruta
- Proxy de tráfico
- Motor de inspección de vulnerabilidad
- Motor de detección de amenazas impulsado por IAe

Rastreador Web Inteligente

El rastreador inteligente de seguridad de Ridge simula la acción de “hacer clic”, raspando eficientemente cualquier contenido revisable en las páginas web, como texto, imagen, correo electrónico, dirección, número de teléfono, resultado de búsqueda... Hay dos módulos clave en el rastreador de Ridge: el **Módulo de Control** y el **Módulo de Ejecución**. El Módulo de control controla la estrategia de rastreo, los datos de autenticación de inicio de sesión y personaliza qué y qué no raspar, y el Módulo de ejecución extrae los enlaces de una página y manipula el Modelo de objetos de documento (DOM), una API de programación para documentos HTML y XML.

El Rastreador Inteligente Ridge Se Diferencia de las Siguientes Maneras

1. Alta eficiencia: verifica y filtra las duplicaciones, acortando significativamente el tiempo de raspado.
2. Estrategias de control enriquecidas para filtrar URL no válidas.
3. Soporte de intérprete de JavaScript, capaz de obtener URL del código JavaScript.
4. Soporte para extraer enlaces de un archivo flash.
5. Soporte de rastreo a través de un proxy.
6. Soporte de escaneo a través de autenticación.
7. Soporte de control granular del alcance de escaneo. Los usuarios pueden elegir escanear todo el dominio, subdominios o el directorio actual.
8. Diseño de múltiples hilos en ejecución para mejorar la velocidad de rastreo; y, mientras tanto, puede configurar de manera flexible el número de subprocesos de ejecución en ejecución para evitar una presión excesiva en una sola aplicación por un gran número de sesiones simultáneas.

Motor de Fuerza Bruta

El RidgeSecurity Motor de Fuerza Bruta está basado en la nube, admite el recorrido de la ruta URL y fuerza bruta a una página web para localizar enlaces ocultos. El motor admite un diccionario personalizado de fuerza bruta e identifica automáticamente las páginas de redireccionamiento de URL, directorios no válidos, páginas no válidas y enlaces panorámicos para evitar esfuerzos innecesarios. También logra eficiencia con un alto soporte de sesiones concurrentes.

Proxy de Tráfico

En el caso de que Smart Crawler no pueda reconocer todos los parámetros o simular con precisión los parámetros de entrada, el Proxy de tráfico es útil. Como intermediario entre el cliente y el servidor, El Proxy de tráfico captura con precisión todos los valores de entrada del usuario mientras el usuario realiza una prueba funcional estándar. Intercepta, almacena y analiza el flujo de datos original en dos direcciones.

RidgeSecurity Proxy de Tráfico es totalmente compatible con los protocolos HTTP y HTTPS. Se puede aplicar en aplicaciones específicas (especificar por web o dirección IP) mientras permite que otras aplicaciones fluyan libremente sin pasar por el proxy. La configuración es simple y directa, sin necesidad de conocimientos de red para los administradores.

Motor de Inspección de Vulnerabilidad

El motor de inspección de vulnerabilidades de seguridad de Ridge identifica de forma inteligente los puntos a inspeccionar en una solicitud web. Las solicitudes generalmente incluyen rutas de URL, parámetros de URL, parámetros en el cuerpo de la solicitud y el encabezado, y el valor clave en una cookie, etc., mientras se analizan todos los puntos de control posibles.

El motor de inspección, basado en tecnología de verificación cruzada multiusuario, utiliza varios algoritmos, como algoritmos de coincidencia difusa y algoritmos de similitud para realizar una inspección cruzada e identificar vulnerabilidades de privilegios y generar informes de prueba.

Motor de Detección de Amenazas Impulsado por IA

La base del motor de detección de amenazas impulsado por IA es el aprendizaje automático, más las tecnologías de aprendizaje profundo, bajo un modelo de aprendizaje supervisado. El motor impulsado por IA determina si una página web tiene una escalada de privilegios horizontales que se basa en algoritmos y mapa de conocimiento construido con experiencia experta. Luego envía las páginas sospechosas al equipo de pruebas de penetración. El equipo de pruebas de penetración valida aún más y confirma los hallazgos. De esta manera, mejora drásticamente la productividad de la prueba de penetración y reduce el costo. Este método abandona la forma tradicional de detectar la escalada de privilegios horizontales, en función del valor de retorno de diferentes inicios de sesión de usuario. El motor impulsado por IA puede identificar páginas exactas donde existe vulnerabilidad de privilegios de una manera mucho más rápida y precisa.

Resumen

Con el aumento de la conciencia de seguridad de la organización y el uso extensivo de varios sistemas de seguridad (como el marco de desarrollo de seguridad, el sistema de prevención de intrusiones, el software de protección de seguridad, etc.), se predice que las vulnerabilidades comunes como la inyección de SQL, XSS, la ejecución de comandos y CSRF serán mínimas... Sin embargo, las “vulnerabilidades en la lógica del código” no muestran signos de declive. Incluso puede convertirse en el campo de batalla principal, ya que la lógica del código es un producto del pensamiento humano, que es propenso a errores.

Actualmente, la detección de escalada de privilegios horizontales está cubierta únicamente por pruebas de penetración manual, durante las cuales un probador debe procesar manualmente todas las URL y solicitar parámetros para encontrar las páginas problemáticas. Las pruebas manuales tienen las siguientes limitaciones:

1. Requerir profesionales altamente calificados que puedan realizar pruebas de penetración y que comprendan bien la lógica de programación. Además, las pruebas manuales requieren una gran cantidad de documentos y preparación de informes. Todo lo anterior eventualmente se traduce en costos más altos y tiempos más largos para las organizaciones.
2. A menudo, no es factible realizar una prueba exhaustiva debido a la fecha de lanzamiento del software, el costo de desarrollo, los recursos de personal, etc.
3. La calidad de la prueba es inconsistente. En muchos casos, el probador tiene que cambiar el rigor de la prueba con el tiempo de comercialización.

RidgeHAD, el sistema de prueba automatizado para la escalada de privilegios horizontales, es una solución viable. Es esencial usar computadoras para manejar el trabajo repetitivo y liberar el tiempo de los evaluadores. Ayuda a las organizaciones a reducir el trabajo de 2 o 3 semanas a 1hora 30 minutos por computadora. Además, RidgeHAD es altamente portátil. Puede realizar varias pruebas de aplicaciones en una organización, ya que es independiente del lenguaje del programa.

Notas

Perfil de la Compañía

RidgeSecurity está transformando la Validación de Seguridad con sistemas inteligentes automatizados modelados usando las técnicas utilizadas literalmente por millones de hackers que penetran en los sistemas. Cuando se implementan dentro de un sistema, las herramientas de RidgeSecurity son implacables en su búsqueda para localizar, explotar y documentar sus hallazgos. Trabajan dentro de un alcance definido y se replican instantáneamente para abordar estructuras altamente complejas. RidgeSecurity permite que los equipos de aplicaciones web y empresariales, los ISV, los gobiernos, la educación o cualquier persona responsable de garantizar la seguridad del software prueben sus sistemas de manera económica y eficiente.

Ridge Security Technology Inc.
www.ridgesecurity.ai