PARCIAL 1

SISTEMAS DE IDENTIFICADORES EN LAS COMUNICACIONES

ATAQUES: CSRF

LISTAS: ABAC, RBAC

PRESENTADO POR:

JESUS DELCID

BRANDON SANJUR

ÍNDICE

- Conceptos
- Caracteristicas
- Importancias
- Amenazas
- Prevención

- Ventajas
- Desventajas
- Vídeo Instruccional
- Conclusiones
- Recomendaciones

CONCEPTO: ATAQUE CSRF

Un ataque de falsificación de solicitud entre sitios es un tipo de ciberataque de falsificación por solicitud que engaña a un usuario para que use accidentalmente sus credenciales para invocar una actividad de cambio de estado, como transferir fondos de su cuenta, cambiar su dirección de correo electrónico y contraseña, o cualquier otra acción no deseada.

CONCEPTO: ATAQUE CSRF

Mientras que el impacto potencial que puede tener contra un usuario normal es importante, un ataque CSRF exitoso contra una cuenta administrativa puede poner en riesgo un servidor entero, llegando a provocar potencialmente la toma completa de una aplicación web, API u otro servicio.

CARACTERISTICAS: ATAQUE CSRF

Explotación de Sesiones Activas

- CSRF aprovecha el hecho de que el usuario ya está autenticado en el sitio de destino (es decir, la víctima tiene una sesión activa).
- El ataque se realiza enviando solicitudes HTTP a nombre del usuario autenticado sin su conocimiento.

Acciones No Deseadas

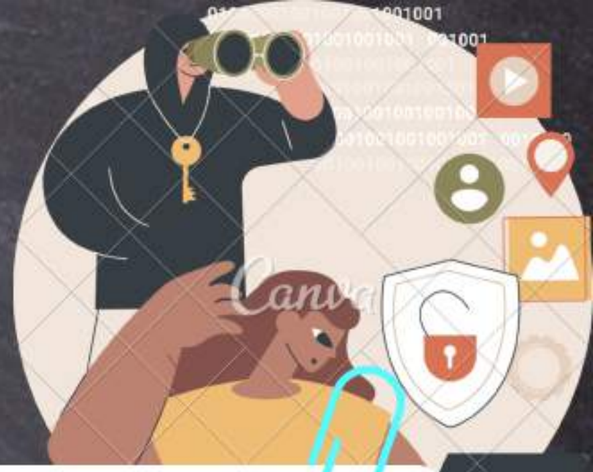
- Los atacantes pueden realizar acciones que la víctima tiene permisos para ejecutar, como cambiar configuraciones, realizar transferencias bancarias o eliminar datos.
- No se puede robar información, pero sí se puede modificarla o alterar el estado de la aplicación.

EJEMPLO: ATAQUE CSRF

Supongamos que una víctima está autenticada en un sitio bancario (ejemplo: banco general) y el atacante envía un enlace malicioso como:

Si banco general no valida adecuadamente la solicitud, el simple hecho de que la víctima cargue esta imagen podría realizar una transferencia de dinero sin su consentimiento.

IMPORTANCIA: ATAQUES CSRF



Un atacante puede realizar acciones en nombre de un usuario autenticado, como transferencias bancarias, cambio de contraseñas o eliminación de información, sin que el usuario se dé cuenta.

Los ataques CSRF son difíciles de detectar porque no requieren robar credenciales ni manipular la comunicación. El atacante aprovecha la sesión ya autenticada del usuario, lo que puede hacer que la actividad maliciosa parezca legítima en los registros de la aplicación.

Un ataque CSRF puede abrir la puerta a otros tipos de ataques, como la inyección de código o la explotación de errores de lógica en la aplicación. La combinación de un ataque CSRF con otras vulnerabilidades podría aumentar el impacto de la intrusión.

Si un ataque CSRF se lleva a cabo contra un usuario con altos privilegios, como un administrador del sistema, el atacante podría obtener control total sobre la aplicación o modificar configuraciones críticas.

VENTAJAS

ATAQUE CSRF

- Facilidad de Ejecución: Son sencillos de llevar a cabo sin necesidad de robar credenciales.
- Dificultad para Detectar: Parecen solicitudes legítimas, lo que dificulta su identificación.

- Dependencia del Navegador: Los ataques dependen de la configuración del navegador, lo que puede limitar su eficacia.
- Dificultad para Proteger Aplicaciones Antiguas: Aplicaciones sin protección CSRF pueden ser más difíciles de actualizar.

ATAQUE CSRF

DESVENTAJAS

AMANEZAS: ATAQUE CSRF

Los ataques CSRF representan serias amenazas a la seguridad de las aplicaciones web, ya que permiten a los atacantes realizar acciones no autorizadas en nombre de usuarios autenticados. Esto se logra aprovechando la confianza del navegador y el envío automático de credenciales.

- Acciones no autorizadas que pueden comprometer datos sensibles.
- Explotación de la confianza del usuario en la aplicación.
- Escalamiento de privilegios si se compromete un usuario con altos derechos.
- Dificultad de mitigación, ya que requieren medidas específicas como tokens anti-CSRF.

PREVENCION: ATAQUE CSRF

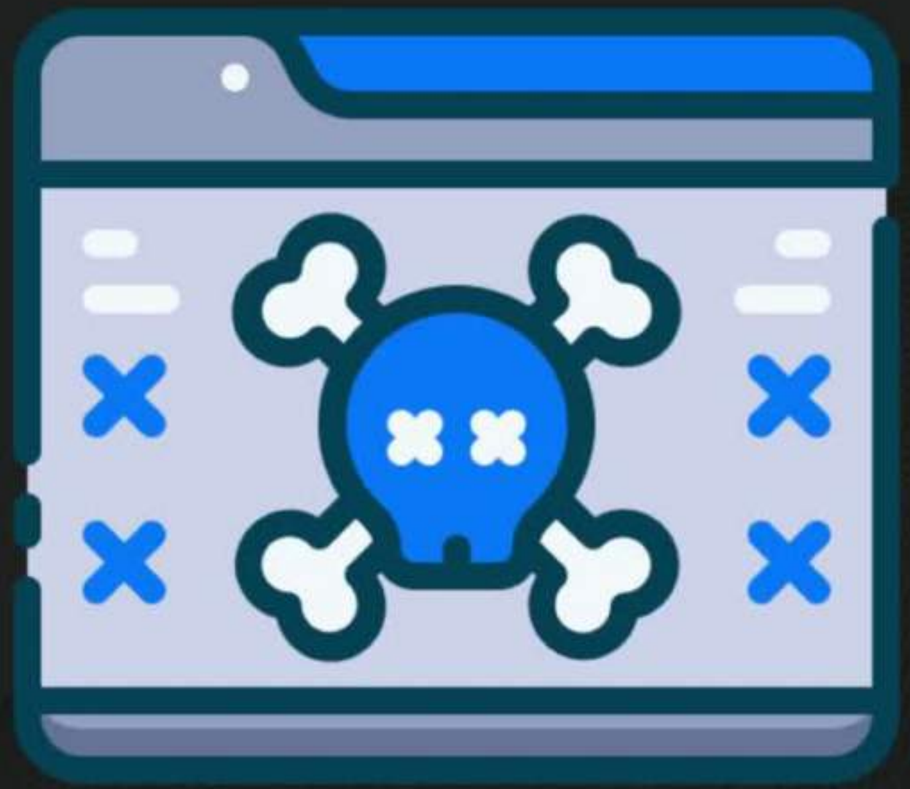
Para prevenir ataques CSRF, se deben implementar tokens anti-CSRF en formularios, verificar las cabeceras Origin y Referer, y limitar acciones sensibles a métodos como POST. Además, las cookies deben configurarse con SameSite, HttpOnly y Secure, y se debe educar a los usuarios sobre los riesgos y mejores prácticas de seguridad. Estas medidas fortalecen la protección de las aplicaciones web.

VIDEO INSTRUCCIONAL

SEGURIDAD CERO

CURSO GRATIS
WEB HACKING

¿QUÉ ES CSRF?



CONCEPTO: ABAC

El control de acceso basado en atributos (ABAC) es un sistema de autorización que define el acceso en función de los atributos asociados a las entidades de seguridad, los recursos y el entorno de una solicitud de acceso. Con ABAC, puede conceder a una entidad de seguridad acceso a un recurso en función de los atributos.

CARACTERISTICAS: ABAC

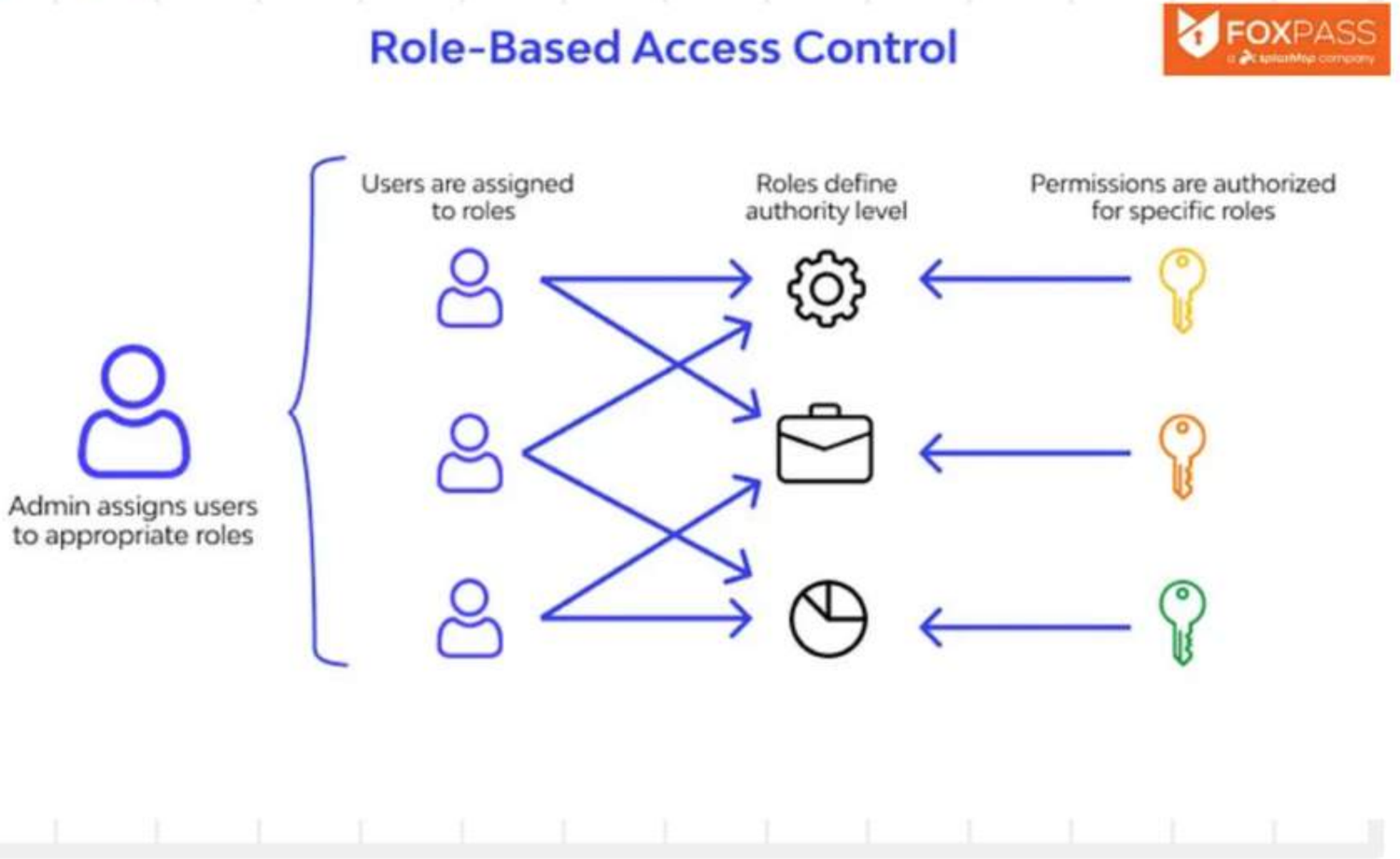
Decisiones de Acceso Basadas en Atributos:

- Las decisiones se basan en atributos relacionados con el usuario (rol, cargo, ubicación), el recurso (tipo, propiedad, confidencialidad) y el contexto (hora, ubicación, dispositivo).

Granularidad y Flexibilidad:

- Permite definir políticas de acceso muy detalladas y precisas, adaptándose a diferentes escenarios y combinaciones de atributos.

RBAC


Role-Based Access Control
FOXPASS
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles
Admin assigns users to appropriate roles

IMPORTANCIA: ATAQUES ABAC

Compromiso de Seguridad: Un atacante puede manipular atributos para obtener acceso no autorizado a recursos sensibles.

Escalamiento de Privilegios: La explotación de vulnerabilidades en el control de atributos puede permitir a un atacante acceder a funciones o datos fuera de sus permisos.

Exposición de Información Crítica: Los ataques ABAC pueden provocar la divulgación de datos confidenciales, afectando la privacidad y la integridad de la información.

Evasión de Políticas de Acceso: Un atacante puede eludir las reglas de acceso definidas, accediendo a recursos restringidos o sensibles sin ser detectado.

AMANEZAS: LISTA ABAC

- Acceso No Autorizado: Manipulación de atributos para obtener acceso a recursos restringidos.
- Escalamiento de Privilegios: Cambio de atributos que permite a atacantes obtener privilegios adicionales.
- Divulgación de Información Sensible: Exposición de datos confidenciales a través de accesos no autorizados.
- Errores de Configuración: Configuraciones incorrectas que facilitan el acceso no autorizado.

PREVENCION: LISTA ABAC

Para prevenir ataques en sistemas ABAC, es esencial validar rigurosamente los atributos de acceso y realizar revisiones periódicas de las políticas. También se debe manejar de manera segura los atributos sensibles y mantener registros detallados para auditorías. La educación y capacitación de usuarios, junto con la seguridad en la infraestructura y la segregación de funciones, son medidas clave para fortalecer la protección.

CONCEPTO: RBAC

El control de acceso basado en roles (RBAC) es un mecanismo de control de acceso que define los roles y los privilegios para determinar si a un usuario se le debe dar acceso a un recurso. Los roles se definen en función de características como la ubicación, el departamento, la antigüedad o las funciones de un usuario.

CARACTERISTICAS: RBAC

Asignación de Permisos Basada en Roles:

- Los permisos se asignan a roles, y los usuarios obtienen estos permisos a través de los roles que tienen. Esto simplifica la gestión de acceso y asegura que los usuarios solo puedan realizar acciones relacionadas con sus responsabilidades.

Jerarquía de Roles:

- Los roles pueden organizarse en una jerarquía, permitiendo que los roles superiores hereden permisos de roles inferiores.

IMPORTANCIA: ATAQUES RBAC

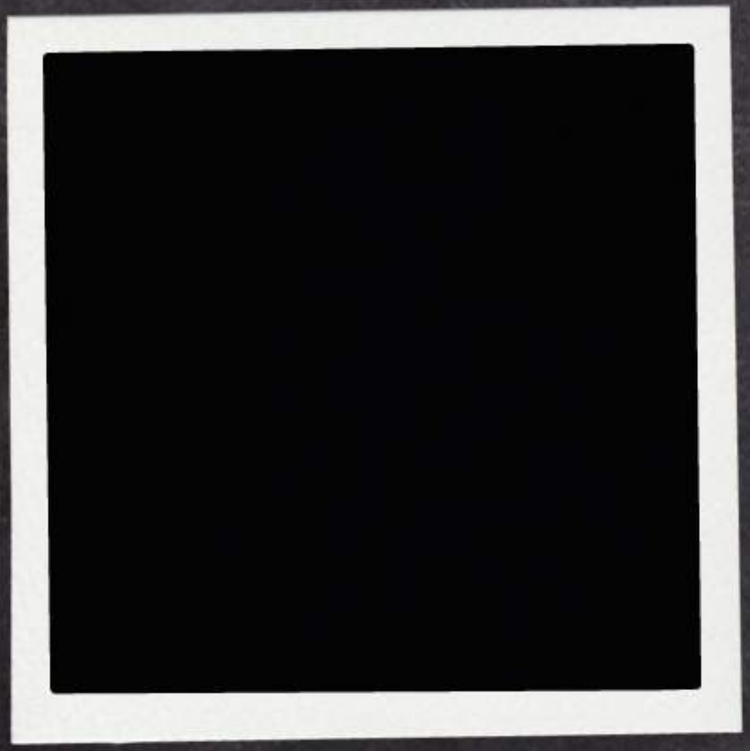
Acceso No Autorizado: Un atacante puede asumir roles que le otorgan privilegios excesivos, accediendo a información sensible.

Compromiso de Roles: Si un rol se ve comprometido, un atacante puede usarlo para realizar acciones maliciosas dentro del sistema.

Dificultad en la Auditoría: La complejidad en la gestión de roles puede dificultar la identificación de accesos indebidos durante auditorías de seguridad.

Explotación de Errores de Configuración: Configuraciones incorrectas de roles pueden permitir a los atacantes acceder a recursos que deberían estar restringidos.

AMANEZAS: LISTA RBAC



- Acceso No Autorizado: Los atacantes pueden asumir roles y acceder a información restringida.
- Compromiso de Roles: Si un rol es comprometido, se pueden ejecutar acciones maliciosas con esos privilegios.
- Errores de Configuración: Configuraciones incorrectas pueden facilitar accesos indebidos a recursos críticos.
- Dificultad en la Auditoría: La complejidad en la gestión de roles dificulta la identificación de accesos no autorizados.

PREVENCION: LISTA RBAC

Para prevenir ataques en sistemas RBAC, es crucial realizar revisiones regulares de roles y aplicar el principio de menor privilegio al asignar permisos. La configuración segura de roles, junto con el monitoreo y registro de actividades, fortalece la seguridad. Además, la capacitación de usuarios sobre políticas de acceso y la separación de funciones ayudan a reducir el riesgo de abuso.

TABLA COMPARATIVA POR CARACTERÍSTICAS

Característica	RBAC	ABAC
Política de control de acceso	Basada en roles	Basada en atributos
Granularidad	Gruesa	Fina
Flexibilidad	Limitada	Altamente flexible
Complejidad	Más sencilla	Más compleja
Impacto en rendimiento	Mínimo	Puede ser significativo
Gestión de acceso	Gestión de roles	Gestión de políticas
Mejor para	Estructuras de permisos bien definidas	Control de acceso dinámico y consciente del contexto

TABLA COMPARATIVA DE LAS VENTAJAS Y LOS CONTRAS

Ventajas de RBAC	Contras de RBAC
RBAC funciona bien para organizaciones pequeñas y medianas.	Las grandes organizaciones pueden requerir tantas funciones que gestionarlas resulta difícil de manejar.
Puede modelar fácilmente la jerarquía organizacional. Por ejemplo, puede otorgar automáticamente a los gerentes todos los permisos de sus subordinados directos.	Definir los derechos de una gran cantidad de roles puede llevar mucho tiempo y ser complicado.
Los costos necesarios para implementar RBAC son relativamente bajos.	Garantizar que cada usuario tenga todos los derechos que necesita puede requerir la creación frecuente de nuevos roles.
Ventajas de ABAC	**Contras de ABAC**
ABAC puede funcionar mejor para organizaciones grandes.	La implementación de RBAC puede ser compleja y llevar mucho tiempo.
Para agregar o eliminar permisos, los administradores pueden simplemente actualizar los atributos de un usuario, lo cual es mucho más fácil que definir nuevos roles.	Recuperarse de errores durante la implementación puede resultar difícil debido a la complejidad de ABAC.

VIDEO INSTRUCCIONAL

CONCLUSIONES

La seguridad es fundamental para organizaciones y usuarios, ya que los atacantes utilizan sitios web maliciosos para realizar ataques CSRF y tomar control de cuentas. Es crucial verificar que las páginas no tengan rastreadores y cuenten con medidas de seguridad adecuadas antes de ingresar datos. Mantener la precaución en línea protege la información personal y organizativa.

RECOMENDACIONES

- Entre las recomendaciones se puede decir que estar pendiente siempre de
- la URL del sitio visitado.
- Activar la verificación de pasos ya sea por correo electrónico o acceso
- telefónico.
- Reportar cualquier sitio o actividad sospechosa
- Uso de herramientas de seguridad en caso de desconfiar del sitio en
- cuestión muchos antivirus ofrecen una capa extra se seguridad analizando
- los posibles sitios que se desean visitar.

MUCHAS GRACIAS

03 de octubre de 2024