Documentacion Proyecto lakich

FLUID

SECURITY WITHOUT MYSTERY

FLUID

FIN.0020. Uso de canal inseguro

Vulnerabilidad

La informacin de los clientes es transmitida por un canal que no usa cifrado, por lo cual puede ser capturada en texto plano credenciales e informacin confidencial.

Amenaza

Un usuario no autorizado puede interceptar el canal HTTP para hacer un Man in the Middle capturando as todo el trfico de red con informacin sensible.

Riesgo

Probabilidad de que un usuario no autorizado intercepte el canal donde se genera el trfico de la aplicacin permitiendo as la lectura de este.

Donde

- http://10.8.69.166/

Recomendacion

Desplegar la aplicacin sobre un canal de comunicacin cifrado, como por ejemplo: HTTPS + TLS. = Documentacion Proyecto lakich

FIN.0066. Tiempo lmite de inactividad inseguro

Vulnerabilidad

La sesin de usuario de la aplicacin no expira despus de 5 minutos de inactividad.

FLUID

Amenaza

Un usuario no autorizado puede tomar control de un equipo desatendido suplantando el usuario que desatendi la mquina.

Riesgo

Probabilidad de que un usuario no autorizado tome control de un sesin desatendida debido a que esta permanece activa por un tiempo indeterminado lo que puede ocasionar que este usuario sea suplantado

Donde

http://10.8.69.166

Recomendacion

Cerrar las sesiones cuando permanezcan inactivas ms de 5 minutos

Documentacion Proyecto lakich

FIN.0060. Sesiones Concurrentes

Vulnerabilidad

La aplicacin no valida el nmero de sesiones por usuario permitiendole a un usuario iniciar sesin con las mismas credenciales en un mismo momento.

Amenaza

Un usuario no autorizado con credenciales de acceso puede suplantar un usuario sin generar ninguna alerta en el usuario autorizado ni en los administradores de la plataforma.

FLUID

Riesgo

Probabilidad de que un usuario no autorizado ingrese a la aplicacin debido a que en la aplicacin se permite establecer mltiples sesiones concurrentes lo que puede ocasionar que no se levante ninguna alerta al momento de suplantar un usuario autorizado .

Donde

http://10.8.69.166

Recomendacion

El sistema debe restringir el nmero de sesiones concurrentes que puede establecer un usuario y a su vez notificar al usuario cuando se inicie sesion en otra ubicacin. = Documentacion Proyecto lakich

FIN.0041. Cabeceras de seguridad HTTP no establecidas

Vulnerabilidad

El servidor carece de algunos encabezados HTTP que le permiten evitar ataques como el clickjacking y Cross site Scripting a las pginas que estn alojadas en ste.

Amenaza

Un usuario en la intranet puede realizar ataques como clickjacking y XSS pudiendo modificar el contenido que se le presenta a los usuarios de la aplicacin debido a que no se est estableciendo las cabeceras de seguridad.

Riesgo

Probabilidad de que un usuario en la intranet pueda modificar el contenido que se le presenta a los usuarios debido a que no se tienen definidas las cabeceras de seguridad, lo que puede ocasionar robo de informacin de los usuarios, as como la

distribucin de software malicioso.

Donde

http://10.8.69.166

Recomendacion

Establecer las cabeceras HTTP de seguridad: - access-control-allow-origin - x-content-security-policy - x-permitted-cross-domain-policies - strict-transport-security (Si usa SSL) - x-frame-options - x-xss-protection - cache-control. = Documentacion Proyecto lakich

FIN.0024. Enumeracin de usuarios

Vulnerabilidad

Debido a una mala prctica en la configuracin se pueden enumerar los usuarios vlidos en la aplicacin.

Amenaza

Un usuario no autorizado desde internet puede realizar un ataque de diccionario a la URL objetivo para enumerar usuarios con privilegios de la aplicacin.

Riesgo

Probabilidad de que un usuario pueda enumerar usuarios con privilegios haciendo un ataque de diccionario sabiendo que el sistema responde de manera diferente cuando el usuario es vlido o y cuando no.

Donde

- http://10.8.69.166

FLUID

Recomendacion

Implementar mensajes de error genricos que no le permitan a un atacante discernir la existencia del usuario en el sistema a travs de los errores HTTP (500 o 404) . = Documentacion Proyecto lakich

FIN.0051. Ausencia de proteccin contra ataques de fuerza bruta

Vulnerabilidad

La aplicacin no tiene proteccin contra ataques de automatizados para adivinar credenciales validas.

Amenaza

Un usuario no autorizado con acceso a la intranet puede enumerar cuentas y claves de usuarios vlidos a travs de un robot elaborado que ejecute ataques de fuerza bruta y diccionario.

Riesgo

Probabilidad que una o varias cuentas de la aplicacin sean robadas o enumeradas por un robot debido que el sistema no valida que quien se intenta autenticar sea un humano, lo que puede afectar la disponibilidad de las cuentas vulneradas y la trazabilidad de sus acciones en el sistema.

Donde

- http://10.8.69.166 wtUsernameInput wtPasswordInput

Recomendacion

Implementar un control para evitar este tipo de ataques y que garantice que el acceso no sea de un robot. Ej captcha, bloqueo por retardo en el nmero de intentos fallidos, etc. = Documentacion Proyecto lakich

FLUID

FIN.0009. Software desactualizado y con vulnerabilidades conocidas

Vulnerabilidad

Se encuentra software desactualizado y con vulnerabilidades crticas existentes.

Amenaza

Un usuario no autorizado desde la red interna puede abusar del software no estable o desactualizado y explotar vulnerabilidades pblicas con las cuales pueda tener acceso a informacin contenida en los servidores

Riesgo

Probabilidad de que un usuario no autorizado desde la red interna explote vulnerabilidades pblicas y consiga acceso a informacin sensible almacenada en los servidores de la solucin

Donde

http//10.8.69.166

Recomendacion

Actualizar el software afectado a sus versiones recomendadas por el fabricante (JBOSS EAP 7.0). = Documentacion Proyecto lakich

FIN.0061. Falta de validacin de datos

Vulnerabilidad

La aplicacin no controla del lado de servidor el formato de ciertos datos que son

procesados por el WebService.

Amenaza

Un usuario puede aprovecharse de que el servidor no valida el tipo de carcter en los campos y obtener informacin sensible generando errores en los WebSevices.

Riesgo

Probabilidad de que un usuario inyecte en uno de los campos en el cual no se valida el tipo de carcter permitiendo al atacante obtener informacin sensible de lo XML que son procesados por el WebService.

Donde

http//10.8.69.166

Recomendacion

Validar en el lado del cliente los tipos de datos que se ingresan a distintos tipos de campos en la aplicacin. = Documentacion Proyecto lakich

FIN.0037. Uso de web services sin autorizacin

Vulnerabilidad

Es posible consumir los webservice de la aplicacin sin estar autenticado.

Amenaza

Un empleado de la organizacin o de la red interna del servidor de aplicaciones puede utilizar directamente a los webservices sin estar autenticado en la aplicacin.

FLUID

Riesgo

Probabilidad que un empleado consuma los webservices de la aplicacin debido que el sistema no requiere autenticacin para su uso, lo cual afecta la trazabilidad de las acciones que se realizan en el sistema sistema y genera una fuga de informacin.

Donde

http://10.8.69.166

Recomendacion

Obligar una autenticacin o una cookie de sesin para el consumo de los webservices. = Documentacion Proyecto lakich

FIN.0040. Cookies generadas de forma insegura

Vulnerabilidad

Las Cookies son generadas en la aplicacin sin la bandera Secure lo que facilita el compromiso de la sesin del usuario a travs de ataques tipo Man in the middle.

Amenaza

Un usuario no autorizado en el mismo dominio de broadcast puede capturar la informacin enviada entre el cliente y el servidor con el objetivo de robar informacin de los usuarios de la aplicacin.

Riesgo

Probabilidad de que un usuario no autorizado intercepte la informacin enviada entre el cliente y el servidor o inyecte secuencias de comandos debido a que las cookies no tienen definidos los parmetros de seguridad lo que puede ocasionar robo de informacin de los clientes

FLUID

Donde

pageLoadedFromBrowserCache OSSESSIONID osVisit osVisitor

Recomendacion

Agregar el atributo Secure s se est usando SSL en la aplicacin.