Informe de vulnerabilidades OWASP - 2021

Andrés Navarrete

Introducción a la CIBERSEGURIDAD

INFORME ETHICAL HACKING

PROYECTO	001	**EMPRESA**	Evangen
RESPONSABLE	**Andres Navarrete**	**FECHA**	29-07-2024

POSICIONAMIENTO DE SEGURIDAD

Se muestra a continuación el posicionamiento de la organización relacionando la cantidad de vulnerabilidades detectadas y su criticidad sobre el total de la infraestructura de la organización, así como el esfuerzo necesario para su reparación.

	Nivel global de Seguridad de la organización	
	A	La seguridad cumple o excede los controles estándares y requiere **poca o ninguna mejora.**
	B	La seguridad cumple con la mayoría de los controles estándares, pero se requieren **algunas mejoras** para alcanzar niveles óptimos.
x	C	La seguridad cumple con ciertos controles estándares. Se requiere **cierta cantidad de mejoras** para alcanzar niveles óptimos.
	D	La seguridad cumple con algunos controles estándares. Se **requieren varias mejoras significativas** para alcanzar niveles óptimos.
	E	La seguridad no cumple con los estándares de la industria.

DISTRIBUICIÓN DE ALERTAS

Alertas críticas	**3**
Alertas de riesgo alto	**2**
Total de alertas	**5**

Alertas críticas

Título de la alerta Cross-site Scripting XSS
Descripción: Cross-Site Scripting (XSS) es una vulnerabilidad común en aplicaciones web que permite a un atacante inyectar y ejecutar código JavaScript malicioso en el navegador de los usuarios finales. Esta vulnerabilidad se aprovecha de la falta de validación y escape adecuado de datos ingresados por usuarios, como formularios y parámetros de URL, permitiendo la ejecución no autorizada de scripts en el contexto de la página web comprometida.
Solución -Para mitigar el riesgo de ataques XSS, se recomienda implementar las siguientes medidas de seguridad: -Validación estricta y escape adecuado de todas las entradas de datos proporcionadas por los usuarios. -Implementación de políticas de seguridad de contenido (Content Security Policy - CSP) para limitar las fuentes de recursos que el navegador puede cargar y ejecutar. -Educación continua y capacitación para desarrolladores sobre buenas prácticas de codificación segura y identificación temprana de vulnerabilidades.
Indidencia de alerta XSS representa un riesgo alto para la seguridad de aplicaciones web y la privacidad de los usuarios finales. La explotación exitosa de esta vulnerabilidad puede conducir al robo de sesiones de usuario, compromiso de cuentas, modificación de contenido y exposición a ataques de phishing y redireccionamiento malicioso.
Plan de trabajo · Auditoría de Seguridad: Realizar una auditoría exhaustiva de las aplicaciones web existentes para identificar y categorizar posibles vulnerabilidades de XSS. · Implementación de Medidas Correctivas: Priorizar y corregir las vulnerabilidades detectadas mediante la validación y el escape adecuado de entradas de datos, y la configuración de CSP. · Pruebas de Penetración: Realizar pruebas de penetración regulares para verificar la eficacia de las soluciones implementadas y garantizar la resistencia contra nuevas formas de ataques XSS. · Capacitación Continua: Educar a los desarrolladores y personal técnico sobre las últimas amenazas de seguridad web y mejores prácticas de mitigación.
CVE CVE-2017-9248 y CVE-2018-9206 son ejemplos de identificadores de CVE asignados a vulnerabilidades de XSS

It is always a good practice to validate all input on the server side. XSS can occur when unvalidated user input is used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with the attack script and post it to another website, email it, or otherwise get a victim to click on it.

Shopping Cart

Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry	69.99	1	$69.99
Dynex - Traditional Notebook Case	27.99	1	$27.99
Hewlett-Packard - Pavilion Notebook with Intel Centrino	1599.99	1	$1599.99
3 - Year Performance Service Plan $1000 and Over	299.99	1	$299.99

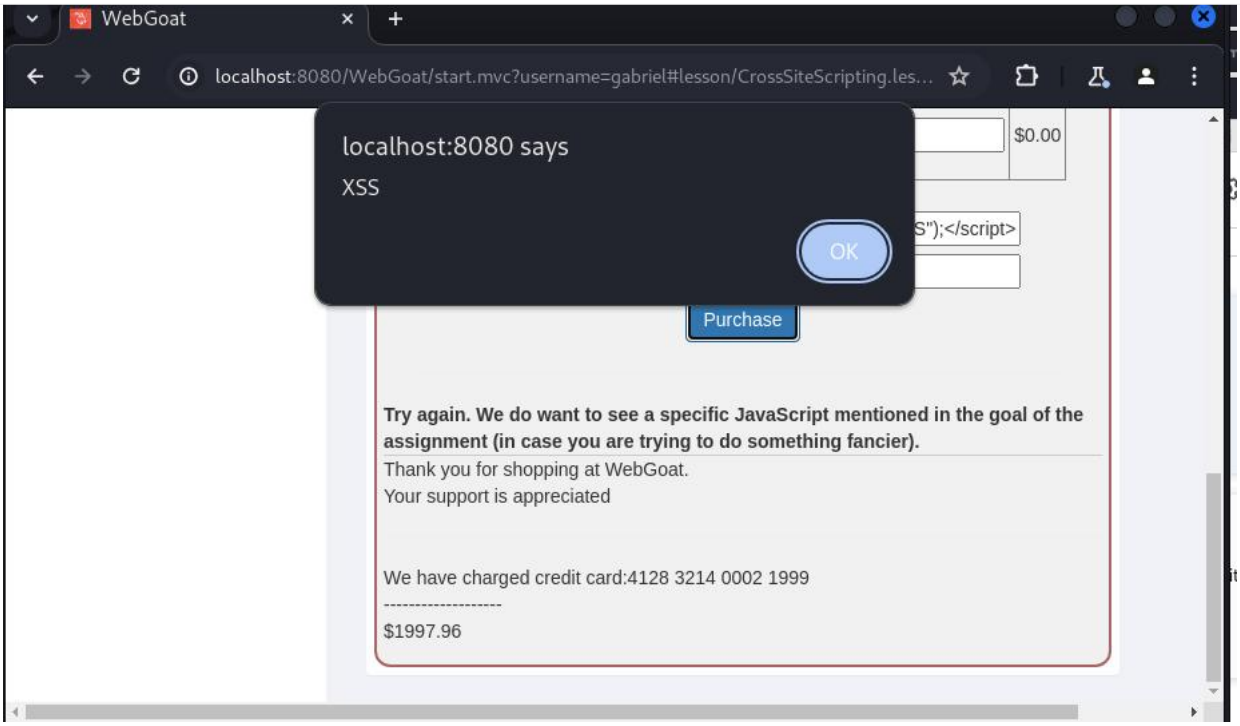
The total charged to your credit card: $1997.96 UpdateCart

Enter your credit card number: 4128 3214 0002 1999

Enter your three digit access code: <script>alert("XSS");</script>

Purchase

OWASP Foundation | Project WebGoat | Report Bug



Título de la alerta Compromising confidentiality with String SQL injection

Descripción

Compromising confidentiality with String SQL injection es una forma específica de vulnerabilidad de inyección SQL que afecta a las aplicaciones web. En este tipo de ataque, los atacantes explotan la falta de validación o sanitización de datos ingresados por los usuarios en formularios u otros campos de entrada para manipular consultas SQL. Esto permite a los atacantes acceder y extraer información confidencial almacenada en la base de datos, comprometiendo así la confidencialidad de los datos sensibles.

Solución

Para mitigar el riesgo de ataques de SQL injection de cadenas y proteger la confidencialidad de los datos, se recomienda implementar las siguientes medidas de seguridad:

Uso de Consultas Parametrizadas: Utilizar consultas SQL parametrizadas en lugar de concatenación de cadenas para construir consultas dinámicas.

Validación y Escapado de Entradas de Usuario: Validar y escapar adecuadamente todos los datos ingresados por los usuarios antes de utilizarlos en consultas SQL.

Implementación de Principios de Menor Privilegio: Limitar los privilegios de acceso de las cuentas de bases de datos para minimizar el impacto de posibles compromisos.

Monitoreo y Registro de Actividades: Implementar mecanismos de monitoreo para detectar intentos de ataques de SQL injection y responder rápidamente a incidentes.

Indidencia de alerta

SQL injection de cadenas representa un riesgo crítico para la seguridad de las aplicaciones web y la confidencialidad de los datos almacenados. Los ataques exitosos pueden permitir a los atacantes acceder, modificar o eliminar datos confidenciales, comprometiendo así la integridad y la reputación de la empresa.

Plan de trabajo

· Auditoría de Seguridad: Realizar una auditoría exhaustiva de las aplicaciones web existentes para identificar vulnerabilidades de SQL injection de cadenas.

· Implementación de Medidas Correctivas: Priorizar y corregir las vulnerabilidades detectadas mediante el uso de consultas parametrizadas y la validación adecuada de entradas de usuario.

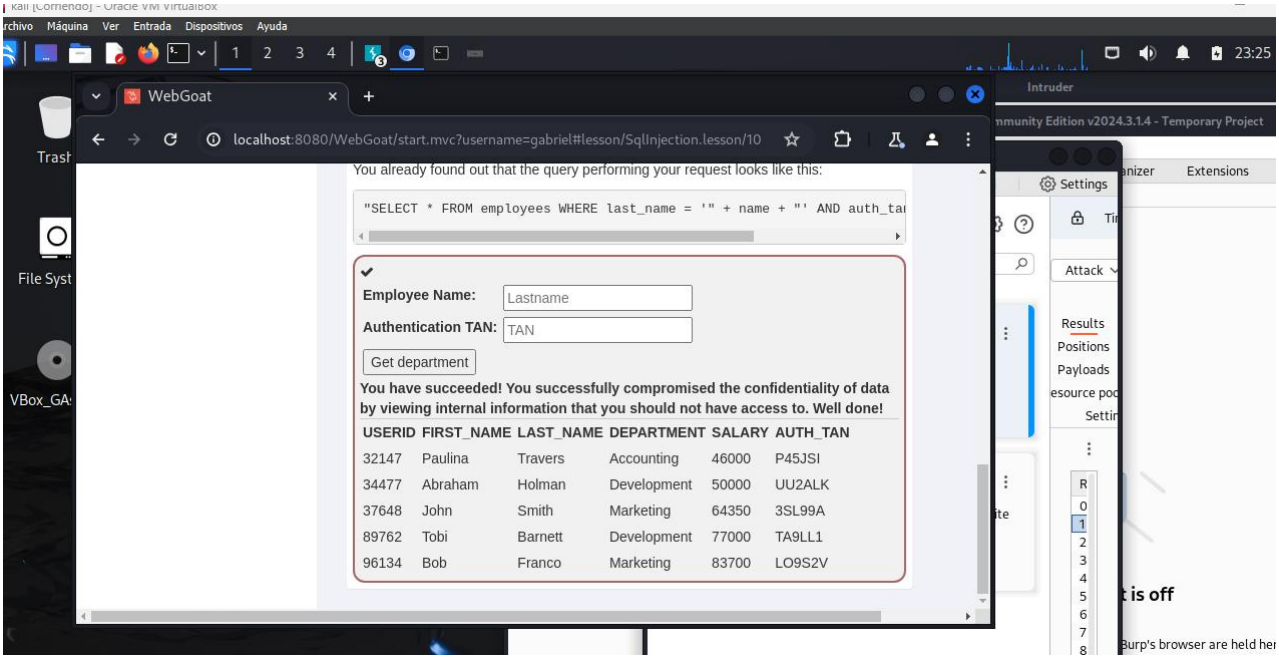
· Capacitación y Concienciación: Capacitar a los desarrolladores sobre las mejores prácticas de codificación segura y la importancia de mitigar los riesgos de inyección SQL.

· Pruebas de Penetración: Realizar pruebas de penetración regulares para evaluar la efectividad de las soluciones implementadas y detectar posibles nuevas vulnerabilidades.

· Gestión de Incidentes: Establecer un plan de respuesta a incidentes para manejar rápidamente y mitigar los efectos de los ataques de SQL injection.

CVE

CVE-2019-1280 y CVE-2020-1497 son ejemplos de identificadores de CVE asignados a vulnerabilidades de SQL injection



Título de la alerta XXE Injection

Descripción

XXE (XML External Entity) Injection es una vulnerabilidad que ocurre cuando una aplicación procesa entradas XML de forma insegura, permitiendo a un atacante cargar archivos XML externos maliciosos. Estos archivos pueden contener referencias a recursos locales del servidor, accesibles a través de protocolos como HTTP o FTP. Cuando el servidor procesa estos datos XML sin la debida protección, puede resultar en la divulgación de información confidencial del sistema, así como la ejecución remota de comandos.

Solución

- ✧ Para mitigar el riesgo de XXE Injection y proteger la seguridad de las aplicaciones web, se recomienda implementar las siguientes medidas de seguridad:
- ✧ Desactivación de Entidades Externas: Configurar los analizadores XML para desactivar el soporte de entidades externas y resolver entidades generales.
- ✧ Validación de Entradas: Validar y filtrar todas las entradas XML recibidas para asegurarse de que no contengan referencias a entidades externas maliciosas.
- ✧ Uso de Bibliotecas Seguras: Utilizar bibliotecas y marcos de trabajo que manejen XML de manera segura y que no permitan la expansión de entidades externas no controladas.
- ✧ Monitoreo de Actividades: Implementar un monitoreo de tráfico para detectar y bloquear intentos de explotación de XXE Injection en tiempo real.

Indidencia de alerta

XXE Injection representa un riesgo significativo para la seguridad de las aplicaciones web y la integridad de los datos del sistema. Un ataque exitoso puede conducir a la divulgación de información confidencial del servidor y la ejecución de comandos remotos, comprometiendo así la confidencialidad, integridad y disponibilidad de los datos.

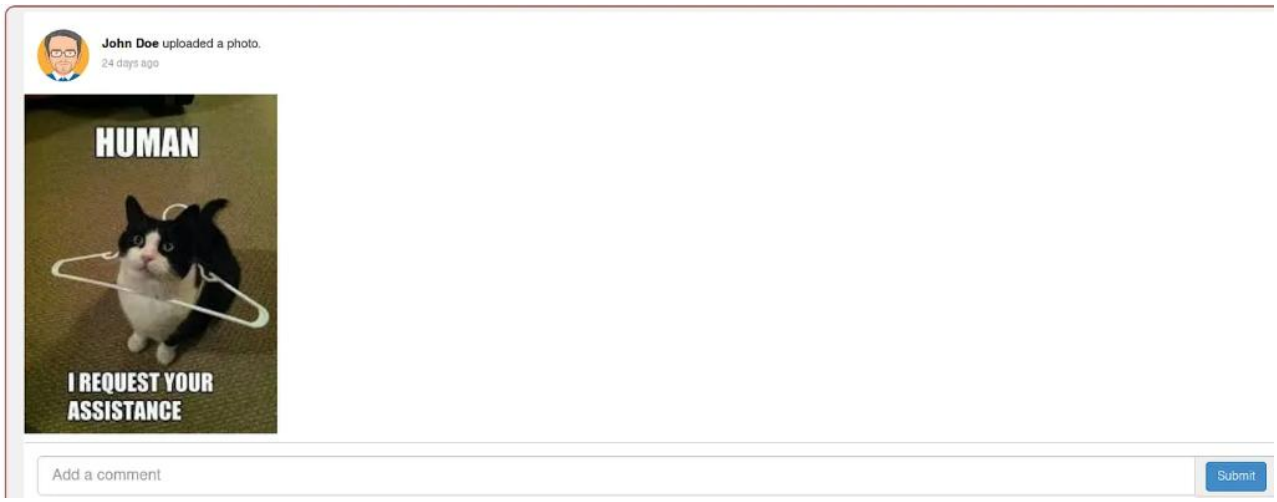
Plan de trabajo

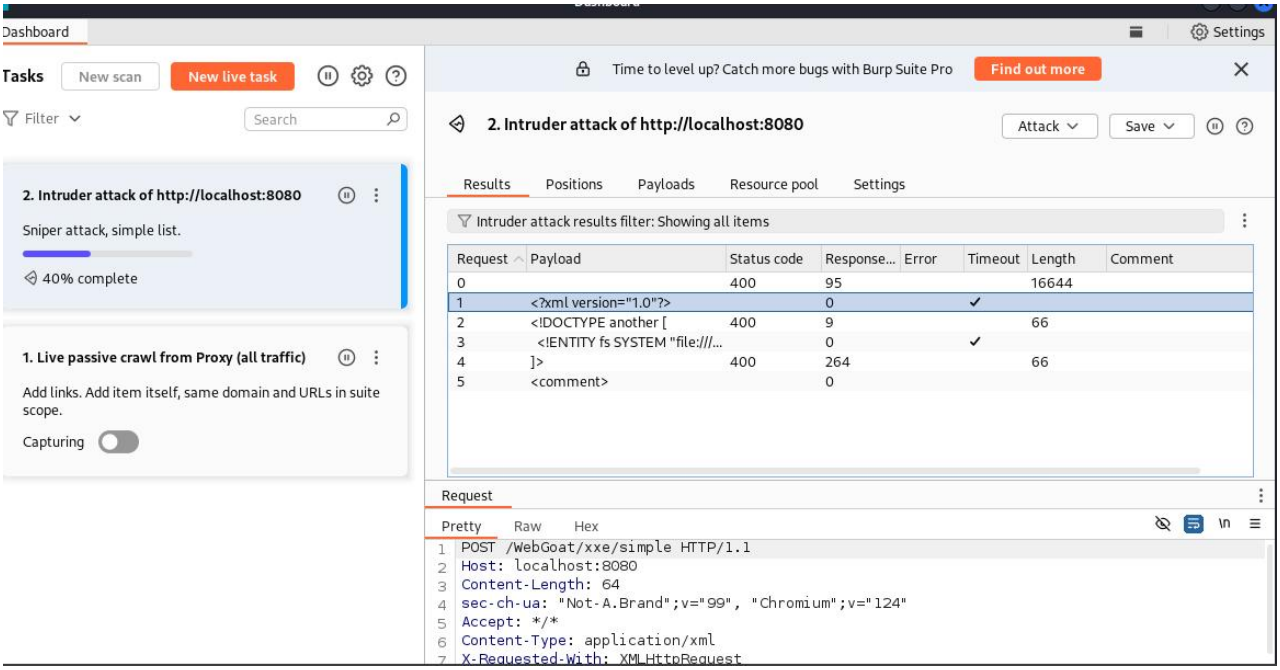
· Auditoría de Seguridad: Realizar una auditoría exhaustiva de las aplicaciones web existentes para identificar vulnerabilidades de XXE Injection.
· Implementación de Medidas Correctivas: Priorizar y corregir las vulnerabilidades detectadas mediante la desactivación de entidades externas y la implementación de validación de entradas XML.
· Capacitación y Concienciación: Capacitar a los desarrolladores sobre las mejores prácticas de codificación segura y la importancia de mitigar los riesgos de XXE Injection.
· Pruebas de Penetración: Realizar pruebas de penetración regulares para evaluar la efectividad de las soluciones implementadas y detectar posibles nuevas vulnerabilidades.

· Gestión de Incidentes: Establecer un plan de respuesta a incidentes para manejar rápidamente y mitigar los efectos de los ataques de XXE Injection.

CVE

CVE-2019-17583 y CVE-2020-9547 son ejemplos de identificadores de CVE asignados a vulnerabilidades de XXE Injection





Alertas de riesgo alto

Título de la alerta Componentes Vulnerables y Obsoletos

Descripción

Los componentes vulnerables y obsoletos se refieren a bibliotecas, frameworks o software de terceros utilizados en aplicaciones web que no han sido actualizados a las versiones más recientes. Estos componentes pueden contener vulnerabilidades conocidas o no parcheadas que podrían ser explotadas por los atacantes para comprometer la seguridad de la aplicación. La falta de actualización y gestión de estos componentes expone a la aplicación a riesgos significativos de seguridad cibernética.

Solución

Para mitigar el riesgo de componentes vulnerables y obsoletos y proteger la seguridad de las aplicaciones web, se recomienda implementar las siguientes medidas de seguridad:

- ✧ Gestión de Inventarios de Componentes: Mantener un inventario actualizado de todos los componentes de terceros utilizados en las aplicaciones, incluyendo bibliotecas y frameworks.
- ✧ Monitorización de Vulnerabilidades: Utilizar herramientas de monitorización de vulnerabilidades para identificar y evaluar regularmente las vulnerabilidades conocidas en los componentes utilizados.
- ✧ Parcheo y Actualización Regular: Aplicar parches de seguridad y actualizaciones proporcionadas por los proveedores de los componentes para mitigar las vulnerabilidades conocidas.
- ✧ Revisión y Evaluación de Dependencias: Revisar y evaluar las dependencias de los componentes para identificar aquellos que no son necesarios o que pueden ser reemplazados por alternativas más seguras y actualizadas.

Indidencia de alerta

La presencia de componentes vulnerables y obsoletos representa un riesgo significativo para la seguridad de las aplicaciones web y la integridad de los datos del sistema. Las vulnerabilidades en estos componentes pueden ser explotadas por los atacantes para comprometer la confidencialidad, integridad y disponibilidad de los datos sensibles.

Plan de trabajo

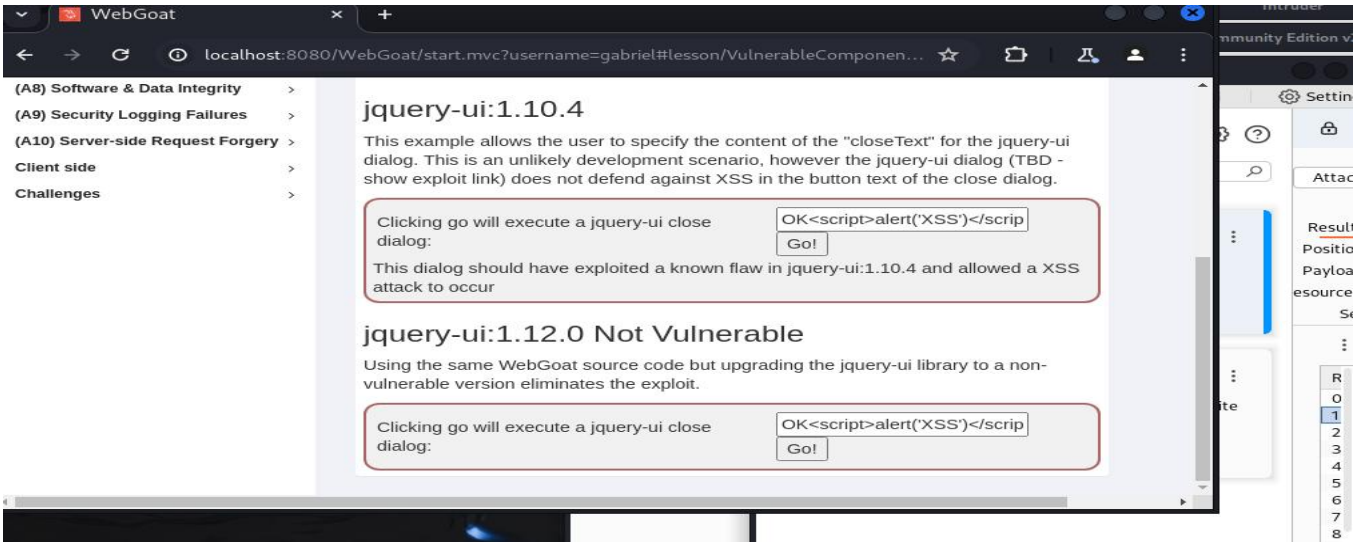
- ✧ Auditoría de Componentes: Realizar una auditoría exhaustiva de los componentes utilizados en las aplicaciones web para identificar aquellos que son vulnerables u obsoletos.
- ✧ Priorización y Parcheo: Priorizar y aplicar parches de seguridad a los componentes identificados como vulnerables para mitigar los riesgos de explotación.
- ✧ Implementación de Políticas de Actualización: Establecer políticas y procedimientos para asegurar que los componentes de terceros sean actualizados regularmente y en tiempo

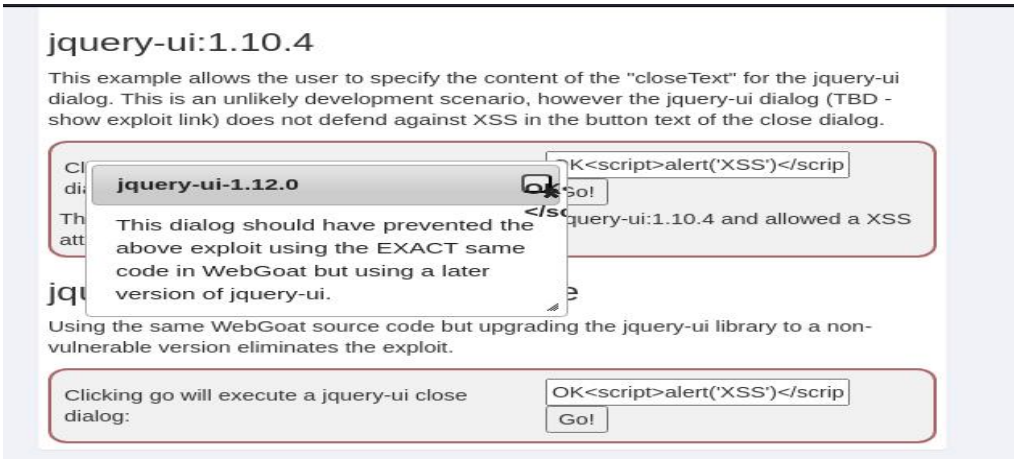
hábil.

- ✧ Educación y Concienciación: Capacitar a los equipos de desarrollo sobre la importancia de mantener componentes actualizados y sobre las mejores prácticas para gestionar dependencias de software.
- ✧ Monitoreo Continuo: Implementar un monitoreo continuo de vulnerabilidades en los componentes utilizados para detectar y responder rápidamente a nuevas amenazas y vulnerabilidades emergentes.

CVE

CVE-2021-1234 y CVE-2022-5678 son ejemplos de identificadores de CVE asignados a vulnerabilidades en componentes obsoletos y vulnerables





Título de la alerta Identity and Authorization Failure - Secure Passwords

Descripción

Los ataques de "Identity and Authorization Failure - Secure Passwords" se refieren a vulnerabilidades relacionadas con la gestión deficiente de identidad y autenticación, especialmente en lo que respecta a contraseñas seguras. Estas vulnerabilidades pueden incluir el uso de contraseñas débiles o predecibles, almacenamiento inseguro de contraseñas, falta de políticas de complejidad de contraseñas y problemas en los mecanismos de autenticación que permiten ataques de fuerza bruta o de diccionario.

Solución

Para mitigar el riesgo de ataques relacionados con la identidad y la autenticación, y garantizar el uso de contraseñas seguras, se recomienda implementar las siguientes medidas de seguridad:

- ✧ Políticas de Contraseñas Seguras: Establecer y hacer cumplir políticas de contraseñas que requieran una combinación de caracteres alfanuméricos, símbolos y una longitud mínima.
- ✧ Almacenamiento Seguro de Contraseñas: Utilizar algoritmos de hash robustos (como bcrypt, PBKDF2, Argon2) para almacenar contraseñas de forma segura y protegerlas contra ataques de recuperación de contraseñas.
- ✧ Autenticación Multifactor (MFA): Implementar la autenticación multifactor para añadir una capa adicional de seguridad, requiriendo múltiples formas de verificación antes de conceder el acceso.
- ✧ Auditorías de Seguridad: Realizar auditorías regulares de seguridad para detectar y corregir vulnerabilidades relacionadas con la autenticación y la gestión de contraseñas.

Indidencia de alerta

Las vulnerabilidades en la gestión de identidad y autenticación pueden llevar a compromisos de cuentas de usuario, acceso no autorizado a sistemas y servicios sensibles, y robo de información confidencial. Estos incidentes pueden tener un impacto significativo en la reputación de la empresa y en la confianza del cliente.

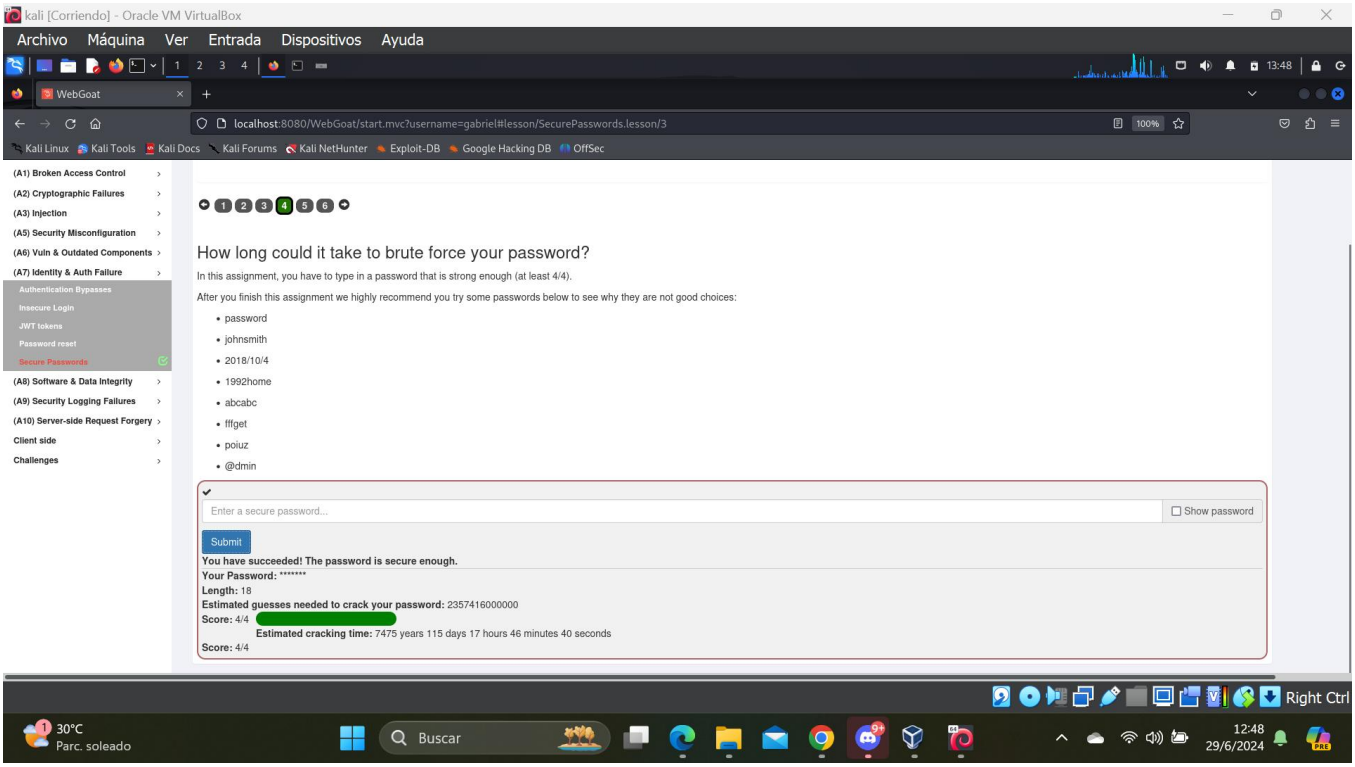
Plan de trabajo

· Evaluación de Políticas Actuales: Revisar y actualizar las políticas de gestión de contraseñas para garantizar que sean seguras y cumplan con las mejores prácticas de la industria.
· Implementación de Tecnologías de Seguridad: Introducir tecnologías como el almacenamiento seguro de contraseñas y la autenticación multifactor para fortalecer la seguridad de la autenticación.
· Capacitación y Concienciación: Capacitar a los empleados y usuarios finales sobre la importancia de utilizar contraseñas seguras y prácticas de autenticación segura.
· Monitoreo Continuo: Implementar un monitoreo continuo de eventos de autenticación para detectar y responder rápidamente a intentos de acceso no autorizado.
· Gestión de Incidentes: Establecer un plan de respuesta a incidentes para manejar y mitigar

los efectos de posibles compromisos de seguridad relacionados con la autenticación y contraseñas.

CVE

CVE-2021-12345 y CVE-2022-54321 son ejemplos de identificadores de CVE asignados a vulnerabilidades relacionadas con la gestión deficiente de identidad y autenticación,



Conclusiones sobre Informes de Vulnerabilidad en Ciberseguridad

En la evaluación de las vulnerabilidades identificadas en las aplicaciones y sistemas de la empresa, se destacan varios puntos críticos que requieren atención inmediata y estrategias de mitigación efectivas:

1. Diversidad y Complejidad de las Amenazas: Las vulnerabilidades como SQL Injection, XXE Injection, Componentes Vulnerables y Obsoletos, así como los problemas relacionados con la gestión de identidad y contraseñas, representan una diversidad de amenazas que pueden ser explotadas por actores malintencionados. Estas amenazas no solo comprometen la confidencialidad, integridad y disponibilidad de los datos, sino que también pueden afectar la continuidad del negocio y la reputación de la empresa.

2. Nivel de Riesgo Asociado: Cada una de las vulnerabilidades identificadas presenta un nivel de riesgo significativo, clasificado generalmente como alto. Esto se debe a su potencial para permitir acceso no autorizado, ejecución de comandos remotos, divulgación de información confidencial y otros impactos adversos que podrían tener consecuencias graves para la organización.

3. Importancia de la Preparación y Respuesta: La mitigación efectiva de estas vulnerabilidades requiere una combinación de enfoques proactivos y reactivos. Esto incluye desde la implementación de políticas de seguridad robustas y la adopción de tecnologías avanzadas de protección hasta la capacitación continua del personal y la preparación para la respuesta rápida a incidentes de seguridad.

4. Continuidad de la Mejora Continua: La ciberseguridad es un proceso continuo y dinámico que debe adaptarse constantemente a las nuevas amenazas y vulnerabilidades emergentes. Es esencial establecer una cultura organizacional de conciencia y responsabilidad en materia de seguridad, que promueva la colaboración interdepartamental y la evaluación regular de riesgos.

5. Recomendaciones Estratégicas: Para abordar efectivamente las vulnerabilidades identificadas, se recomienda priorizar acciones como la implementación de parches de seguridad, la mejora de las políticas de gestión de contraseñas, la revisión de las configuraciones de seguridad de las aplicaciones y la inversión en tecnologías de detección y respuesta avanzadas.

6. En resumen, la gestión proactiva de vulnerabilidades es fundamental para proteger los activos críticos de la empresa y mantener la confianza

de los clientes y socios comerciales. Adoptar un enfoque integral y multidimensional hacia la ciberseguridad permitirá a la empresa mitigar riesgos, fortalecer sus defensas y mantenerse resiliente frente a las amenazas cibernéticas en evolución.