Reporte Ejecutivo

Ataque SQL Injection

No de Folio 00025698

Fecha del Incidente: 15 de agosto de 2024

Fecha del Reporte: 16 de agosto del 2024

Duración del Incidente: 2 horas

Impacto: Se comprometieron los datos sensibles de la organización 4geeksAcademy en la integridad y confidencialidad estudiantes y empleados.

Descripción del Incidente:

El día 15 de agosto de 2024, 4GeeksAcademy detecto que sufrió un ataque de SQL Injection que comprometió la base de datos principal de la organización. Este tipo de ataque permitió al actor o actores maliciosos manipular, editar y extraer consultas SQL que se ejecutaban en el servidor sin autorización.

Alcance

El ataque se ejecutó a través de una vulnerabilidad en el sitio www4geeksacademy.com de la organización. Un atacante logró inyectar código SQL malicioso en los campos de entrada, lo que resultó en la ejecución de comandos SQL arbitrarios por parte del servidor de la base de datos.

Impacto en la Organización:

- **Datos Expuestos:** Información personal de los estudiantes y empleados, incluyendo nombres, direcciones de correo electrónico, y posiblemente datos financieros.
- **Integridad de los Datos:** Los atacantes tuvieron la capacidad de alterar o eliminar registros de la base de datos, lo que podría haber comprometido la precisión y la confiabilidad de la información almacenada.
- **Reputación:** El incidente podría afectar la confianza de los estudiantes, empleados y socios en la capacidad de la organización para proteger la información sensible.

Medidas Ejecutadas:

1. **Contención Inmediata:**
    - Se bloqueó el acceso a la página web comprometida.
    - Se suspendió temporalmente el acceso a la base de datos para evitar más daños.
2. **Investigación Forense:**
    - Un equipo de respuesta a incidentes realizó un análisis completo de los registros del servidor para identificar la naturaleza y el alcance del ataque.
    - Se determinó que la vulnerabilidad se debió a la falta de sanitización de las entradas de usuario.
3. **Remediación:**
    - Se implementaron parches de seguridad para corregir la vulnerabilidad.
    - Se actualizó el código de la aplicación web para incluir medidas de sanitización y validación de entradas.
    - Se llevó a cabo una auditoría de seguridad completa en el sistema para identificar y mitigar cualquier otra posible vulnerabilidad.
4. **Comunicación:**

Los estudiantes, empleados y partes interesadas fueron informados del incidente y de las medidas tomadas para asegurar su información.

Recomendaciones Futuras:

- **Implementación de Controles de Seguridad:**
- Aplicación de procedimientos de validación y sanitización de entradas en todas las interfaces que interactúan con la base de datos.
- Uso de consultas preparadas y parámetros en lugar de concatenar cadenas de consulta SQL.

Capacitación en Seguridad:

- Capacitación continua del personal de desarrollo en prácticas seguras de codificación y gestión de datos.

Auditorías de Seguridad Regulares:

- Realización de auditorías de seguridad periódicas para identificar y corregir posibles vulnerabilidades en las aplicaciones y bases de datos.

Plan de Respuesta a Incidentes:

- Actualización y prueba continua del plan de respuesta a incidentes para mejorar la rapidez y efectividad de la respuesta ante futuros ataques.

Conclusión:

El ataque de SQL Injection contra 4GeeksAcademy puso de manifiesto la importancia crítica de implementar controles de seguridad adecuados en todas las aplicaciones que manejan datos sensibles. Aunque el incidente fue contenido y se tomaron medidas correctivas, es fundamental continuar fortaleciendo las prácticas de seguridad para proteger la integridad y confidencialidad de la información y mantener la confianza de los interesados.

Preparado por: *Abraham Caballero*