**Informe de Seguridad**

|  |  |
| --- | --- |
| Título del informe: Análisis ético de un caso hipotético | |
| Autor(es): Sebastián Hernández Téllez | Entidad o cliente evaluado: Caso práctico: “La prueba sorpresa” |
| Clasificación del documento: información pública - libre acceso | Fecha de elaboración: 21 de agosto de 2025 |

1. **Resumen Ejecutivo**

Durante una auditoría de seguridad, un pentester junior identificó una base de datos interna expuesta sin autenticación. En lugar de notificar de inmediato a la empresa y limitarse a registrar evidencia mínima, descargó la totalidad de los datos sensibles y desarrolló un script en Python para extraerlos, exponiéndolos posteriormente en su portafolio personal sin un proceso de anonimización adecuado. Esta conducta vulneró principios fundamentales del hacking ético, como la confidencialidad, el respeto al alcance del contrato y el uso responsable de la información. Desde el punto de vista técnico, la extracción masiva y la impresión en consola de datos confidenciales representan una práctica insegura que aumenta el riesgo de fuga. Las acciones correctas debieron incluir la documentación controlada del hallazgo, la notificación inmediata y recomendaciones de mitigación. El incidente evidencia posibles consecuencias legales por uso indebido de información y destaca la necesidad de reforzar la formación ética y profesional en pruebas de seguridad.

**2. Principios del hacking ético vulnerados**

* Confidencialidad y manejo responsable de la información:  
  El pentester accedió y descargó información sensible (usuarios) sin necesidad de hacerlo por completo y luego la usó en un portafolio personal. Esto viola el principio de “usar la información solo para fines del contrato” y no exponer datos confidenciales.
* Consentimiento y alcance definido (Scope):  
  Un pentester debe ceñirse estrictamente al alcance del acuerdo con la empresa. Descargar la base entera y usarla fuera del proyecto excede el alcance y rompe el principio de autorización explícita.

**3. ¿Es válida la justificación de “fue para demostrar mis habilidades”?**

Respuesta: No, no es válida.

* La ética profesional indica que no se pueden usar datos reales de clientes para fines personales, aunque se intente anonimizar.
* Existen medios alternativos como laboratorios (HackTheBox, TryHackMe, entornos propios, datasets ficticios) para demostrar habilidades.
* Según (ISC)² Código de Ética, “Proteger la sociedad, la infraestructura común y los bienes” tiene prioridad sobre cualquier beneficio personal.

**4. Problema técnico del código presentado**

* Exposición total de datos confidenciales: el script extrae toda la tabla usuarios y muestra información en consola sin enmascarar ni proteger.
* Mala práctica de logging: mostrar datos sensibles (usuarios, posiblemente contraseñas o PII) en consola aumenta el riesgo de fuga.
* Uso irresponsable: aunque técnicamente funcional, el código no aplica controles de seguridad como:
  + Filtrado de campos (ej. solo contar registros o mostrar metadatos).
  + Cifrado o anonimización de resultados.
  + Registro seguro de hallazgos (ej. en un informe cifrado, no en consola).

**5. Medidas adecuadas que debió tomar el pentester**

1. Detener la extracción masiva: validar la vulnerabilidad sin descargar la base completa (ej. acceder a un único registro como prueba de concepto).
2. Documentar la falla: registrar la evidencia mínima (captura de pantalla, error de configuración, query de ejemplo).
3. Notificación inmediata: reportar el hallazgo al cliente/empresa, siguiendo el ciclo de Responsible Disclosure.
4. Recomendación técnica: sugerir medidas como restringir el acceso a la API, aplicar autenticación y cifrado, reforzar controles de acceso (ISO 27001 A.9, OWASP API Security Top 10).

**6. Implicancias legales si se filtra la información**

* Para el pentester:
  + Puede enfrentar cargos por uso indebido de información confidencial, violación de contratos de confidencialidad (NDA) y hasta delitos informáticos (según legislación local, ej. Ley de Delitos Informáticos en Chile, GDPR en Europa, HIPAA en EE.UU.).
  + Pérdida de credibilidad profesional y posibles sanciones de certificadoras (ej. revocación de CEH, CISSP).
* Para la empresa:
  + Responsabilidad legal por fuga de datos personales (GDPR, Ley 19.628 en Chile, ISO 27701).
  + Posibles sanciones económicas, demandas de clientes y daño reputacional.

**7. Conclusiones**

Desde el analisis realizado podemos señalar que, el pentester o auditor no actuó de forma ética ni legal, pues usa datos sensibles fuera del alcance del contrato. Lo correcto sería informar de inmediato, registrar evidencia mínima, y nunca reutilizar datos reales con fines personales.