|  | 🞂Análisis de seguridad en página y base de datos  Virtual XP |
| --- | --- |
|  |  |
|  | **Carolina Navarrete M** 🞂FUCAP 🞂 07/09/2024 |
|  |  |
|  | Rol en el proyecto: Analista. |
|  |  |
|  | Nombre del curso: Redes seguras y ciberseguridad. |
|  |  |
|  | Grupo de trabajo 7: Agencia de desarrollo de Aplicaciones Móviles, Smart TV, Wearables y Proyectos IoT |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Contenido

[3. Introducción 2](#_heading=h.gjdgxs)

[4. Análisis de requisitos en página web 2](#_heading=h.30j0zll)

[4.1 Identificación de datos sensibles en la Arquitectura de página 2](#_heading=h.1fob9te)

[4.2 Evaluación de riesgos en la Arquitectura de página Web. 2](#_heading=h.3znysh7)

[4.3 Propuestas de medidas de seguridad en la Arquitectura de página 3](#_heading=h.2et92p0)

[5. Análisis de requisitos en la base de datos. 3](#_heading=h.tyjcwt)

[5.1 Identificación de datos sensibles en la base de datos. 3](#_heading=h.3dy6vkm)

[5.2 Evaluación de riesgos en la base de datos 3](#_heading=h.1t3h5sf)

[5.3 Propuestas de medidas de seguridad en la base de datos 3](#_heading=h.4d34og8)

[6 Propuestas adicionales de medidas de seguridad para la base de datos. 3](#_heading=h.2s8eyo1)

[Compra de certificados SSl para los datos más sensibles 3](#_heading=h.17dp8vu)

[Accesos controlados de manera escalonado a diferentes participantes del sistema 3](#_heading=h.3rdcrjn)

[Bibliografía 5](#_heading=h.26in1rg)

Análisis de seguridad en página y base de datos

Virtual XP

# 3. Introducción

El presente informe tiene como objetivo hacer observaciones con respecto a vulnerabilidades y amenazas que pueden afectar a la página web y base de datos de la empresa Virtual XP. Empresa dedicada a entregar servicios de vigilancia por medio de cámaras IP, que integra domótica y wearables.

En cuanto a la base de datos, se llevará a cabo por medio de MySQL Workbench, para fines explicativos.

Se detallarán las indicaciones de posibles vulnerabilidades en sus distintas entradas.

Por último, se realizarán las recomendaciones de seguridad correspondientes a cada etapa de su implementación y puntos de vulnerabilidades.

# 4. Análisis de requisitos en página web

## 4.1 Identificación de datos sensibles en la Arquitectura de página

La descripción de datos sensibles manejados en el sistema corresponde a información de clientes como nombre, dirección, teléfono, datos de tarjetas bancarias; sin duda, los datos que pueden ser más controversiales son los provenientes de las grabaciones de las cámaras de seguridad, debido a los procesos legales que pudiesen apoyar, siendo parte de pruebas en casos.

Ejemplos específicos de vulneración de acceso a estos datos sensibles podrían ser la sustracción de cualquiera de estos datos para venta, extorsión o para anular procesos legales.

## 4.2 Evaluación de riesgos en la Arquitectura de página Web.

Identificación de posibles amenazas y vulnerabilidades: la página web puede estar expuesta a gran cantidad de vulnerabilidades. Los peligros que frecuentemente sufren son:

Malware o “Software malicioso” que puede interrumpir el funcionamiento de la página, o acceder al sistema informático de la empresa.

Tipo: Virus y gusanos, troyanos, programas espía.

Evaluación del impacto potencial de cada amenaza.

Los **malware** pueden infectar varios computadores rápidamente cuando se propagan a través de archivos adjuntos, pueden auto replicarse de un computador a otro a través de las redes.

Los **troyanos** podrían robar información de computadores en los que se ejecutan. Esto puede afectar a los clientes y poner en riesgo la seguridad de sus datos. Y, sobre todo, los datos de la propia empresa, involucrándola incluso en problemas legales y serias complicaciones financieras.

**Escaneo**: antes de sufrir un ataque de denegación de servicio, suele detectar vulnerabilidades por medio de puertos abiertos.

**Acceso no autorizado:** generalmente, son ejecutados por medio de Ransomware, puede mantener secuestrados los datos de la empresa.

**Phishing**: un engaño que sustrae información de ingreso a la red o a bases de datos, la información sensible queda muy expuesta.

**Spam:** mensajes masivos no solicitados enviados a través de internet.

**Análisis de paquetes:** se puede capturar información, observar el tráfico de red y van en búsqueda de información confidencial.

**El Cross- site scripting** **(XSS):** código malicioso de JavaScript, HTML, Flash u otro código, puede ser almacenado o reflejado[[1]](#footnote-0).

**Desbordamiento de búfer:** sobrecargan el almacenamiento de búfer de datos en búsqueda del robo de datos.

## 4.3 Propuestas de medidas de seguridad en la Arquitectura de página

Recomendaciones para mitigar riesgos identificados

Se recomiendan firewalls y antivirus mixtos de firma y heurísticos para proteger el entorno web, para crear un cerco que evite los ataques que puedan rodear el sistema.

Es necesario implementar un sistema de validación y filtro de todas las entradas de datos provenientes a través de formularios web o URL.

Las medidas sugeridas se justifican en cuanto a la reducción de riesgos que puedan afectar los datos de la empresa y de acuerdo a los ataques del entorno.

También se protege a través de las actualizaciones y aplicaciones del sitio web.

# 5. Análisis de requisitos en la base de datos.

## 5.1 Identificación de datos sensibles en la base de datos.

La descripción de datos sensibles manejados en el sistema corresponde a datos bancarios, videos de las cámaras de seguridad y datos de los clientes.

Ejemplos específicos de vulneración de acceso a estos datos sensibles sería la sustracción de algún video de seguridad que puede contribuir a la obstaculización de alguna prueba legal de robo u otro.

## 5.2 Evaluación de riesgos en la base de datos

Los datos sensibles manejados en el sistema que pueden ser afectados son las informaciones de direcciones, cuentas bancarias, videos o paquetes de información que la empresa maneja.

Ejemplos específicos de vulneración de acceso a estos datos sensibles es la inyección de código malicioso o inyección de SQL puede ingresar por medio de un formulario web, caja de búsqueda o entrada de inicio de sesión.

## 5.3 Propuestas de medidas de seguridad en la base de datos

Se deben filtrar todas las entradas de datos que se reciban a través de formularios web o URL.

Uso de herramientas de escaneo de vulnerabilidades para detectar y corregir vulnerabilidades de XSS[[2]](#footnote-1).

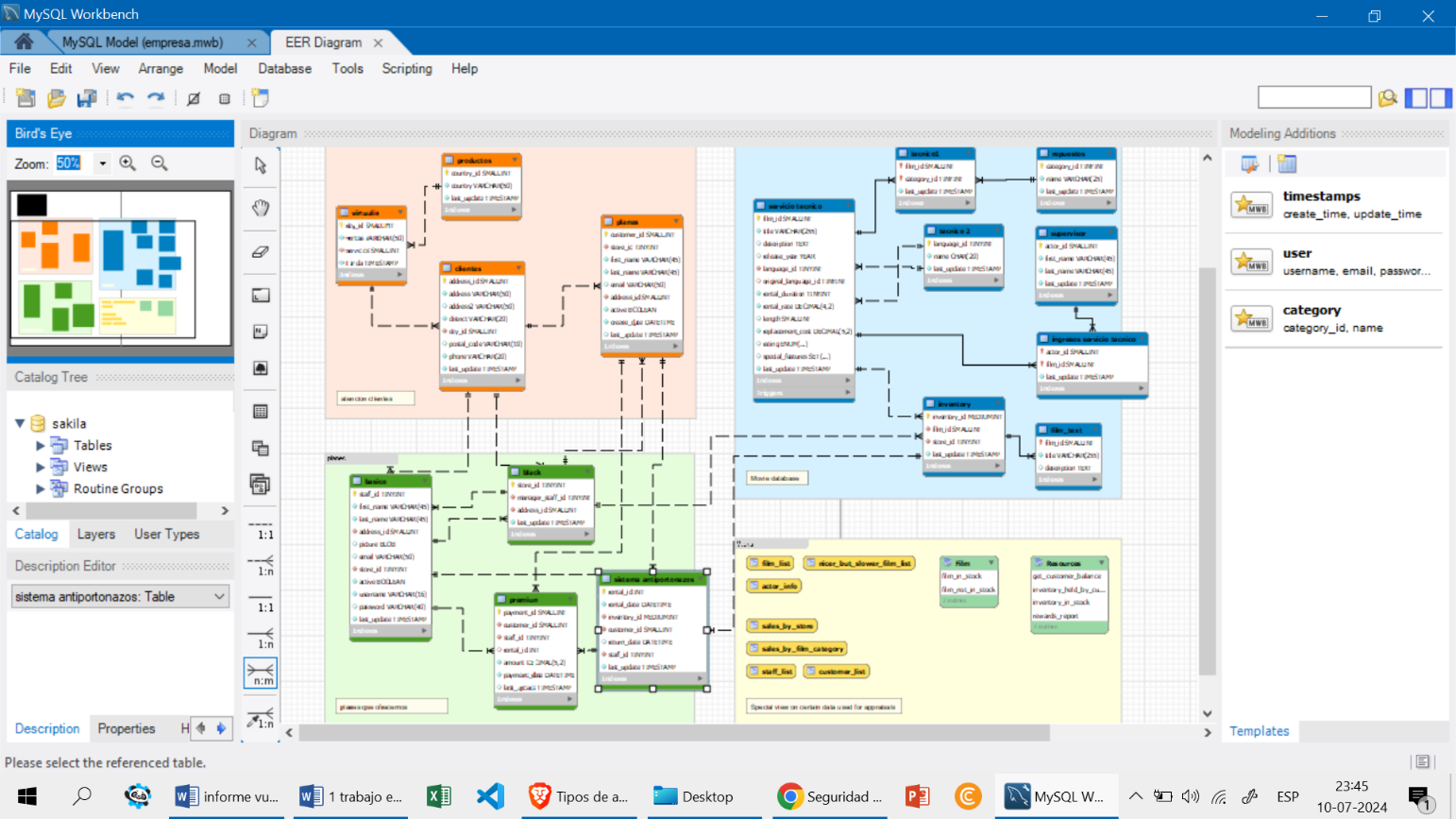
Los Login deben estar protegidos por medio de Captcha y bloqueos al tercer intento, de preferencia por 24 horas en caso de la información más delicada.

Para evitar ataques de fuerza bruta, se deben implementar las autenticaciones de múltiples factores, en lo posible con la comprobación en el celular para los clientes; en los empleados, las contraseñas robustas y cambiadas cada un mes.

# 6 Propuestas adicionales de medidas de seguridad para la base de datos.

Compra de certificados SSL para los datos más sensibles[[3]](#footnote-2)

Accesos controlados de manera escalonado a diferentes participantes del sistema[[4]](#footnote-3).



# Bibliografía

CDMON. (s.f.). Obtenido de https://www.cdmon.com/es/ssl

CSRIT. (s.f.). Obtenido de https://csirt.gob.cl/servicios/escaneo-de-vulnerabilidades/

Hacknoid. (s.f.). Obtenido de https://www.hacknoid.com/?gad\_source=1

Programación Web, V. M. (s.f.). *Youtube*. Obtenido de https://www.youtube.com/watch?v=EWGUznyQIhE

1. (Programación Web, s.f.) [↑](#footnote-ref-0)
2. (CSRIT, s.f.) [↑](#footnote-ref-1)
3. (CDMON, s.f.) [↑](#footnote-ref-2)
4. (Hacknoid, s.f.) [↑](#footnote-ref-3)