INFORME - REVISIÓN DE SEGURIDAD

audit.auraquantic.com

Métodos y Tecnología de Sistemas
y Procesos S. L.

Versión 1.0 - 21/03/2024

Tabla de contenido

1. INTRODUCCIÓN

1.1. Objetivo de la auditoría

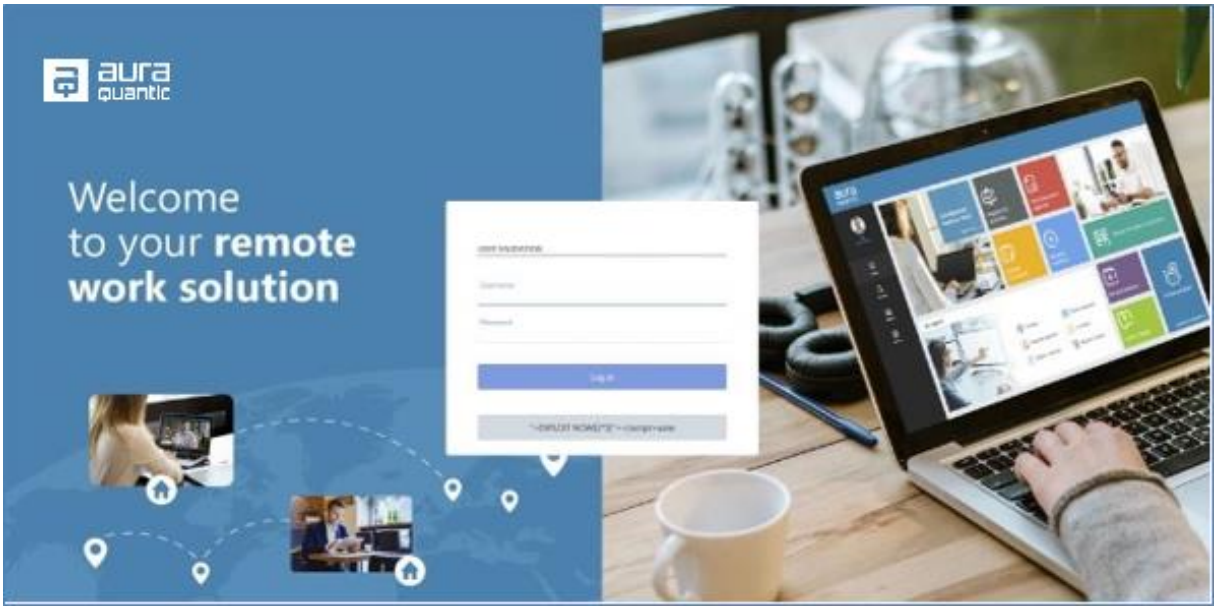
Los objetivos esenciales de la auditoría practicada sobre el portal web **AuraQuantic (audit.auraquantic.com),** son:

- Verificación del aplicativo en funcionamiento (análisis de seguridad del aplicativo en ejecución sobre entorno de pruebas)
- Evaluación del nivel de seguridad de la aplicación a raíz de las vulnerabilidades identificadas

El presente informe recoge los resultados de las pruebas de seguridad realizadas. El propósito del presente documento es mostrar, dentro de un contexto técnico detallado, los resultados obtenidos en las actividades de Auditoría de Seguridad realizada por MTP sobre el servicio mencionado.

1.2. Contexto y metodología

Se han realizado pruebas de seguridad (*Hacking ético*) sobre los siguientes activos en ejecución, desplegados sobre una instancia *cloud* facilitado por AuraQuantic para la realización de las pruebas: https://audit.auraquantic.com:



Las pruebas de seguridad han sido ejecutadas en modalidad **caja negra** (Sin credenciales ni ningún tipo de información sobre componentes internos/tecnologías) con la finalidad de realizar un bypass en el sistema de login de la aplicación o conseguir acceso mediante un exploit.

El enfoque de pruebas de seguridad se ha basado en los más de 250 controles propuestos por el estándar de verificación **OWASP Application Security Verification Standard 4.0.3 (ASVS)** y en las recomendaciones de las guías de seguridad de **OWASP Testing Guide 4.2**

Dominio	Prueba	Resultado
Fallo de Identificación o Autenticación	Ataques de fuerza bruta para el reconocimiento de directorios	✓
	Ataques de fuerza bruta al formulario de inicio de sesión	✓
Inyección	Ataques de inyección SQL	✓
	Ataques de ejecución de código	✓
	Ataques de salto de directorios	✓
	Ataques de cross-site scripting (XSS)	✓
Configuración de Seguridad Incorrecta	Implementación de las cabeceras de seguridad	✓
	Configuración correcta de las cabeceras de seguridad	✓
	Ataques de orígenes cruzados	✓
	Ataque de redirecciones abiertas	✓
	Ataque de Cross-Site Request Forgery (CSRF)	✓
Análisis de Infraestructura	Escaneo de Puertos	✓

Herramientas específicas

Para la realización de la actividad se han empleado el siguiente conjunto de utilidades y herramientas específicas para ejecución de verificación y pruebas de vulnerabilidades de seguridad:

- **Suite Kali v2024.1** (Nmap, SSLScan, Metasploit, SqlMap, Nikto, Dirb entre otras)
- **Burp Suite Professional (v2024.1.1)**

2. Resumen de resultados

A continuación, se resumen y detallan los hallazgos de defectos de configuración y vulnerabilidades detectadas en la auditoría, debidamente categorizadas (dominio, CWE, severidad, impacto CVSS 3.1):

- **No se identificaron ocurrencias**

La actividad realizada en colaboración con AuraQuantic **ha contribuido a confirmar el buen nivel de seguridad (confidencialidad, integridad, disponibilidad) de este producto BPMS, sus fortalezas y protecciones contra vectores de ataque específicos** con efectos potencialmente perniciosos para los datos y usuarios del producto.

3. Recomendaciones generales para la mejora continua

Recomendaciones de carácter general para asegurar una mejora continua de la seguridad de la aplicación:

- **Concienciación y formación progresivas** de los desarrolladores en buenas prácticas de desarrollo seguro
- **Realización periódica de auditorías con pruebas de caja blanca/negra/gris** que incluyan tests de penetración manual.
- **Adopción progresiva de herramientas y buenas prácticas, así como mejora de los procedimientos de desarrollo seguros en el SDLC,** con objeto de prevenir potenciales vulnerabilidades en futuras versiones del producto; potenciando aún más si cabe el modelo de desarrollo actual (SSDLC – Secure SW Development Life Cycle).

4. Referencias

- Estándar OWASP. https://owasp.org/
- Top 10 OWASP 2021. https://owasp.org/Top10/
- OWASP Testing Guide v4.2 https://owasp.org/www-project-web-security-testing-guide/v42/
- Open Source Security Testing Methodology Manual (OSSTMM) https://www.isecom.org/OSSTMM.3.pdf
- SANS TOP 25. https://www.sans.org/top25-software-errors/
- PTES technical guidelines. http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- CVSS - Common Vulnerability Scoring System. https://www.first.org/cvss/calculator/3.1

- CVE - Common Vulnerability and Exposures. https://cve.mitre.org/
- CWE – Common Weakness Enumeration. https://cwe.mitre.org

Anexo 1 – Definición y atributos de las categorías OWASP Top 10 2021

La clasificación de los 10 riesgos más críticos en Aplicaciones Web puede encontrarse en el siguiente enlace: OWASP Top 10 – 2021

La clasificación de vulnerabilidades según OWASP Top 10 – 2021 es la siguiente:

- A1 – Control de acceso roto
  El control de acceso hace cumplir la política de modo que los usuarios no pueden actuar fuera de sus permisos previstos. Las fallas generalmente conducen a la divulgación de información no autorizada, la modificación o la destrucción de todos los datos o la realización de una función comercial fuera de los límites del usuario.
- A2 – Fallos Criptográficos
  Conocida en OWASP 2017 como "Exposición de datos sensibles". El enfoque implementado en este punto es sobre los fallos relacionados con la criptografía, que a menudo conduce a la exposición de datos sensibles o al compromiso del sistema.
- A3 – Inyección
  Los fallos de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización. El 94% de las aplicaciones existentes se sometieron a pruebas para detectar alguna forma de inyección, y los 33 CWE asignados a esta categoría son los segundos que más ocurrencias presentan. El Cross-site Scripting pasa a formar parte de esta categoría.
- A4 – Diseño Inseguro
  El diseño inseguro es una categoría amplia que representa diferentes debilidades, expresadas como "diseño de control inexistente o ineficaz". Un diseño inseguro puede tener defectos de implementación que conduzcan a vulnerabilidades que pueden explotarse. Un diseño inseguro no se puede arreglar con una implementación perfecta, ya que, por definición, los controles de seguridad necesarios nunca se crearon para defenderse de ataques específicos. Uno de los factores que contribuye al diseño inseguro es la falta de perfiles de riesgo empresarial inherentes al software o sistema que se está desarrollando.
- A5 – Configuración de Seguridad Incorrecta
  Esta categoría avanza desde el sexto puesto en OWASP 2017. El 90% de las aplicaciones probadas para detectar algún tipo de configuración incorrecta, de las cuales se presenta una tasa de incidencia promedio del 4%. La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión (o directamente por la falta de configuración). La categoría de entidades externas XML (XXE) ahora forma parte de este apartado.
- A6 – Componentes Vulnerables y Obsoletos

Los componentes vulnerables son un problema conocido con gran dificultad en la evaluación de riesgo, debido a que no tiene enumeraciones de debilidades comunes (CWE) asignadas. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.

- A7 – Fallos de Identificación y de Autenticación
  Conocida en OWASP 2017 como "Pérdida de control de autenticación", esta categoría desciende desde la segunda posición en la anterior revisión. Ahora incluye enumeraciones de debilidades comunes (CWE) relacionadas con fallos de identificación. Las funciones de la aplicación relacionadas con autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otros fallos de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).
- A8 – Fallos en la integridad del Software y los Datos
  Nueva categoría en OWASP 2021. Los fallos en la integridad del software y los datos se relacionan con el código e infraestructuras no protegidas contra las violaciones de la integridad. Un ejemplo de esto es cuando una aplicación se basa en complementos, bibliotecas, repositorios y redes de entrega de contenido (CDN) que no son de confianza. Una canalización de CI / CD insegura puede presentar la posibilidad de accesos no autorizados, aplicación de código malicioso o compromiso del sistema.
- A9 – Fallos de Seguridad en Monitorización y Registros
  Conocida en OWASP 2017 como "Registro y monitorización insuficientes". No se dispone de muchos datos CVE / CVSS para esta categoría, pero detectar y responder a este tipo de fallos se considera fundamental. Esta categoría se expande más allá de CWE-778 (utilizada anteriormente), para incluir los tipos CWE-117 (Neutralización de salida inadecuada para los registros), la CWE-223 (Omisión de información relevante para la seguridad) y la CWE-532 (Inserción de información sensible en el archivo de registro). El registro y monitorización insuficientes, junto a la falta de respuesta ante incidentes, permiten a los atacantes mantener el ataque en el tiempo, pivotar a otros sistemas y manipular, extraer o destruir datos.
- A10 – Falsificación de Solicitudes del lado del Servidor (SSRF)
  Nueva categoría en OWASP 2021. Los fallos de SSRF ocurren siempre que una aplicación web obtiene un recurso remoto sin validar la URL proporcionada por el usuario. Esto permite que un atacante manipule a la aplicación para que envíe una solicitud diseñada a un destino inesperado, incluso cuando está se encuentra protegida por un firewall, VPN u otro tipo de lista de control de acceso a la red (ACL). Dado que las aplicaciones web actuales son capaces de proveer a los usuarios finales funciones específicas o determinadas en un marco, la búsqueda de una URL se convierte en un escenario común. Como resultado, la incidencia de SSRF está aumentando. Además, la gravedad de SSRF es cada vez mayor debido a los servicios en la nube y la complejidad de las arquitecturas.