RESEARCH

by Secure Soft Corp

gtd

SECURESOFT

www.securesoftcorp.com

1. Datos Básicos del Informe

Titulo: Análisis de la Vulnerabilidad XSS Persistente en ZKTeco WDMS 5.1.3: Implicaciones y Soluciones - CVE-.2023-51157

Investigador	CVE
Miguel Ángel Méndez Zúñiga	CVE-2023–51157

2. Resumen:

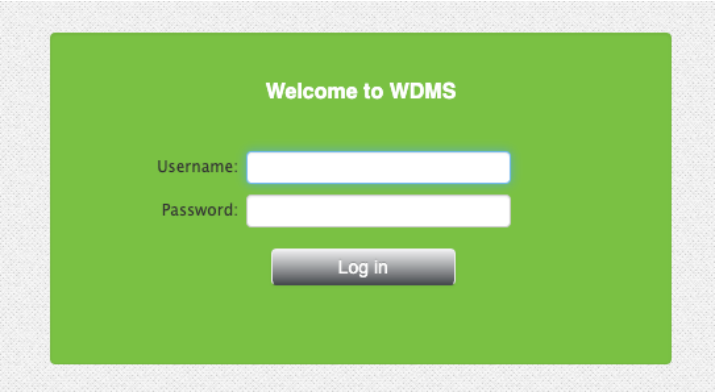
En este informe elaborado por el equipo de Research de Secure Soft, descubrimos una vulnerabilidad crítica de Cross-Site Scripting Persistente (XSS) en la plataforma ZKTeco WDMS 5.1.3 que expone a los usuarios y administradores del sistema a riesgos significativos. ZKTeco WDMS es un sistema de gestión de datos utilizado principalmente para controlar y gestionar el acceso de empleados y registros biométricos, popular en entornos de seguridad física y control de acceso.

Aprenderás cómo esta vulnerabilidad permite a los atacantes inyectar scripts maliciosos en los navegadores de otros usuarios, comprometiendo la seguridad de la plataforma. A través de un análisis técnico detallado, mostramos cómo los atacantes pueden interceptar y modificar los datos antes de enviarlos al servidor.

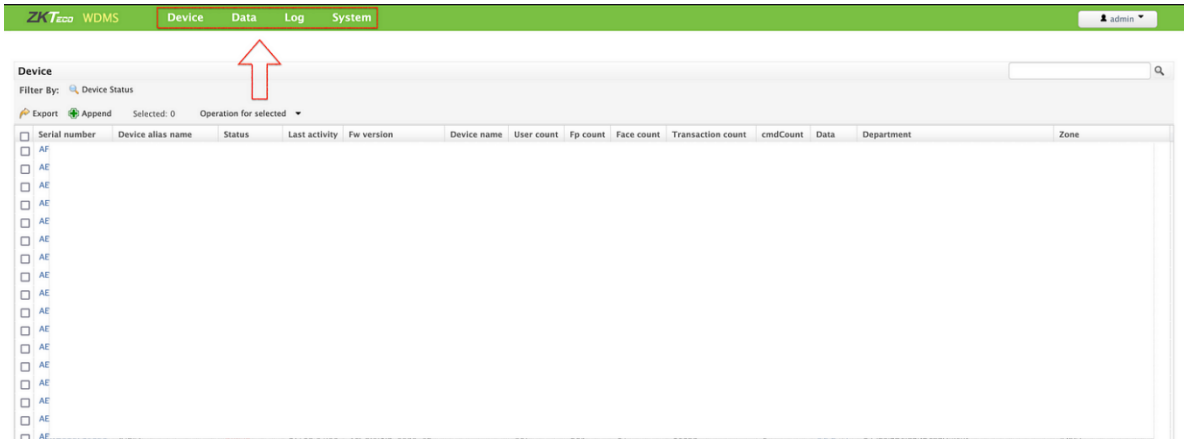
Este informe es esencial para administradores de sistemas, desarrolladores de software y profesionales de ciberseguridad que gestionan plataformas basadas en ZKTeco WDMS o sistemas similares, y buscan proteger sus sistemas de estas amenazas emergentes.

3. Análisis de Causa Raíz

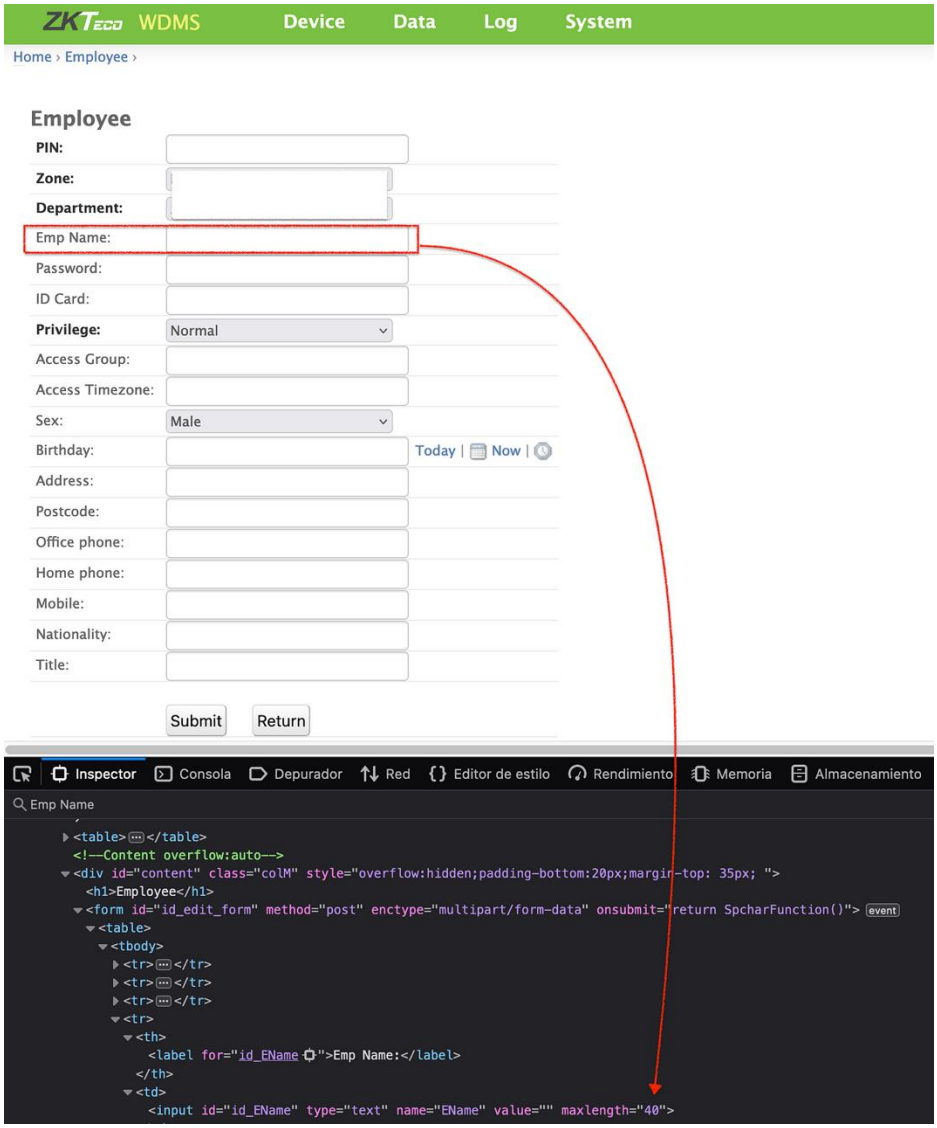
Esta versión resalta el login como el proceso de autenticación de usuario, mencionando brevemente que es un paso común y que se omite para mantener el enfoque en otros aspectos más importantes para la publicación.



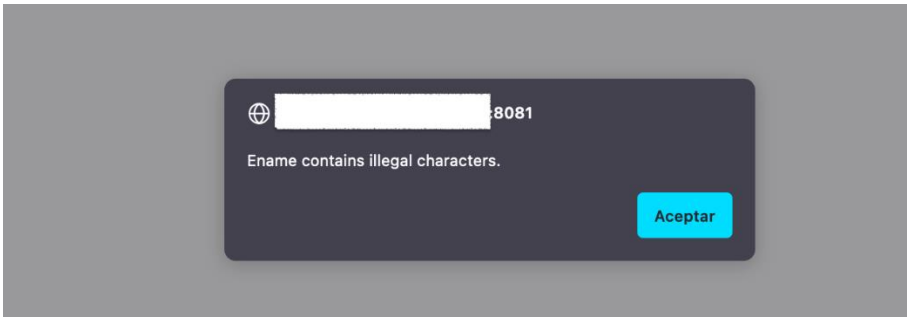
Tras iniciar sesión en la aplicación se muestra un panel que cuenta con un menú que nos permite ver, modificar y eliminar información específica. Este menú sirve como una interfaz clave que permite una gestión eficiente de los datos. Desde aquí se accede a diversas funciones que facilitan la interacción y administración de la información contenida en la plataforma.



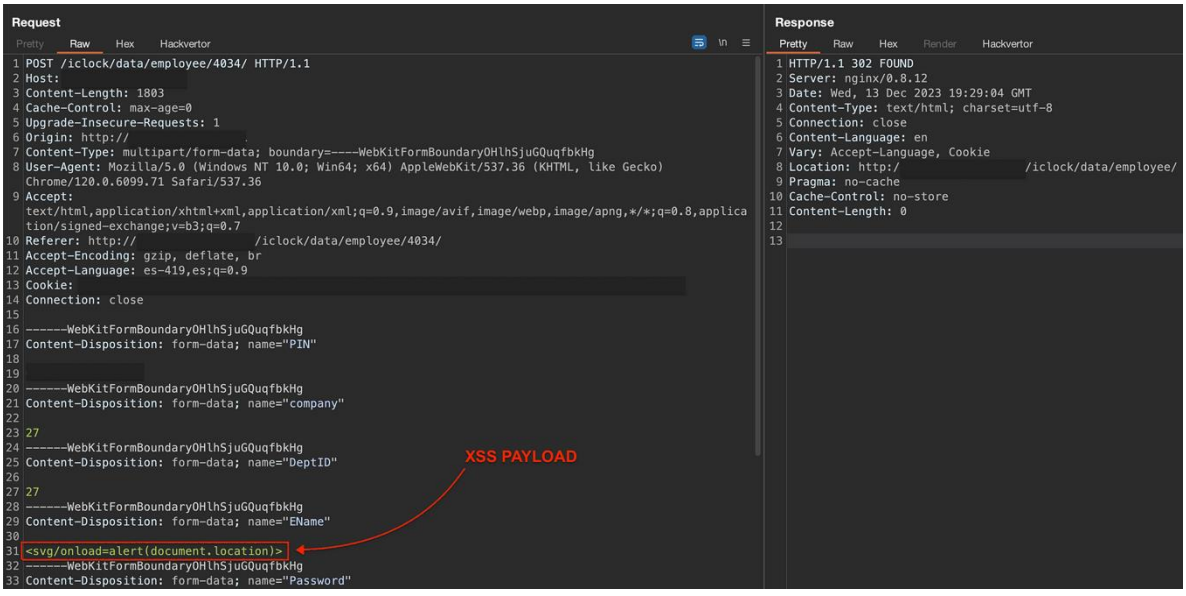
Ahora, procedemos a intentar modificar la información del empleado en el campo “Emp Name” (EName). Inicialmente, probamos con una carga útil pequeña; sin embargo, los resultados no fueron satisfactorios. Esto se debe a que el formulario se valida en la interfaz y la carga útil debe tener un máximo de 40 caracteres.



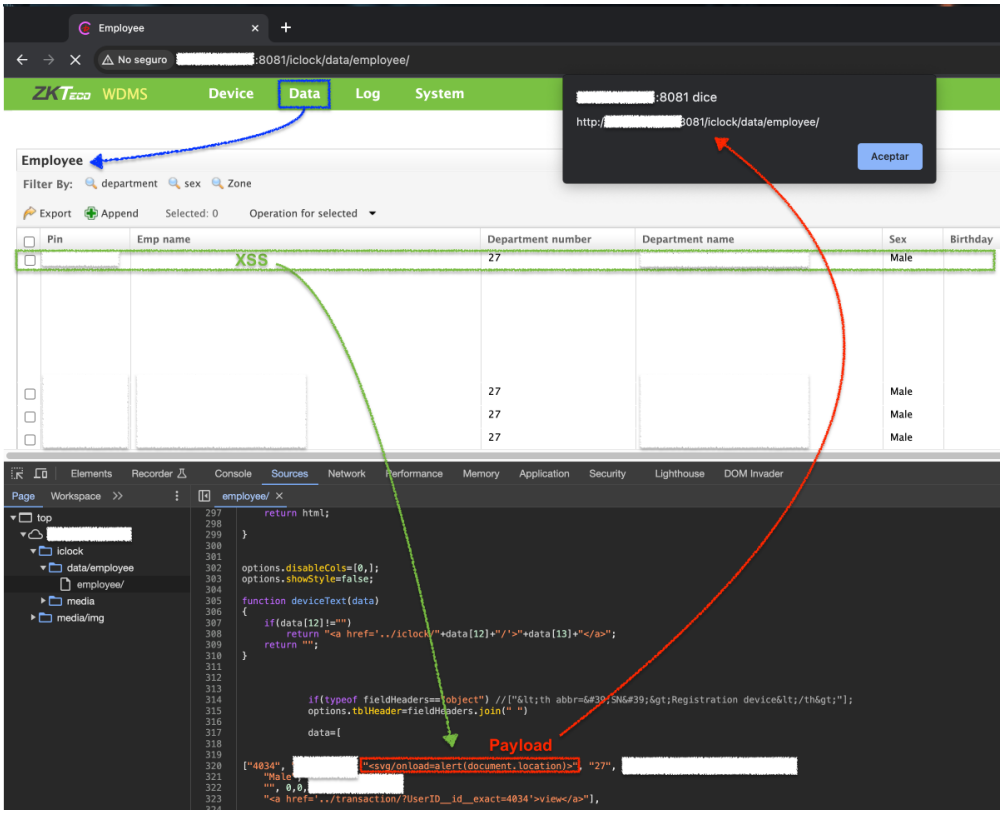
Los resultados obtenidos al intentar inyectar cargas útiles en el formulario son los siguientes, lo que indica el comportamiento del sistema frente a estas pruebas de seguridad.



Ahora bien, la vulnerabilidad de este formulario radica en el hecho de que la información sólo se valida en el frontend, como se mencionó anteriormente. Sin embargo, esta validación no se realiza en el backend, lo que permite la posibilidad de interceptar la solicitud y modificar la información antes de enviarla.



Después de enviar la carga útil, se puede observar cómo queda almacenada en el sistema, lista para ser ejecutada y mostrada en la vista del usuario, lo que demuestra la vulnerabilidad en el proceso de manejo de datos.



4. Conclusión: Al intentar modificar los datos de los empleados se revela una vulnerabilidad en la validación, que ocurre exclusivamente en el frontend. Esto permite la interceptación y modificación de información antes de enviarla al backend. La conclusión subraya la importancia de implementar medidas de validación más sólidas tanto en el frontend como en el backend para evitar posibles violaciones de seguridad.

PERÚ
LIMA
Av. Manuel Olguín 325, Piso 14.
Santiago de Surco. Lima 15023
Telf.: (+511) 711-2900
E-mail:
ventas@securesoftcorp.com

COLOMBIA
BOGOTÁ
Carrera 69, N° 25B - 44, Ofic. 502
Edificio World Business Port
Telf.: (+57) 300 761 26 84
E-mail:
ventas_co@securesoftcorp.com

ECUADOR
QUITO
Martín Carrión E7-61 y Av
República, Edf. Titanium Plaza,
Piso 5, Ofic. 5-2.
Telf: (+593) 2 241 4650
E-mail:
ventas_ec@securesoftcorp.com

GUAYAQUIL
Av. Del Bombero Km 6.5 Plaza
Comercial La vista San Eduardo
Ed 100 A, Ofic.710
Telf.: (+098) 438 8092
E-mail:
ventas_ec@securesoftcorp.com

MÉXICO
CDMX
Montes Urales 425, piso 1, Col.
Lomas de Chapultepec C.P. 11000,
Miguel Hidalgo, Ciudad de México
Telf.: (+55) 4762 1362
E-mail: ventas_mx@securesoftcorp.com

GTD CHILE
SANTIAGO
Av. Del Valle 819, Huechuraba,
Región Metropolitana
Ciudad empresarial
Telf.: (+56) 9 6761 9001
E-mail: ventas@gtd.cl