RESEARCH

by Secure Soft Corp

gtd

SECURESOFT

www.securesoftcorp.com

1. Basic Report Information

Title:

Analysis of the Persistent XSS Vulnerability in ZKTeco WDMS 5.1.3: Implications and Solutions

Researcher	CVE
Miguel Ángel Méndez Zúñiga	CVE-2023–51157

2. Summary:

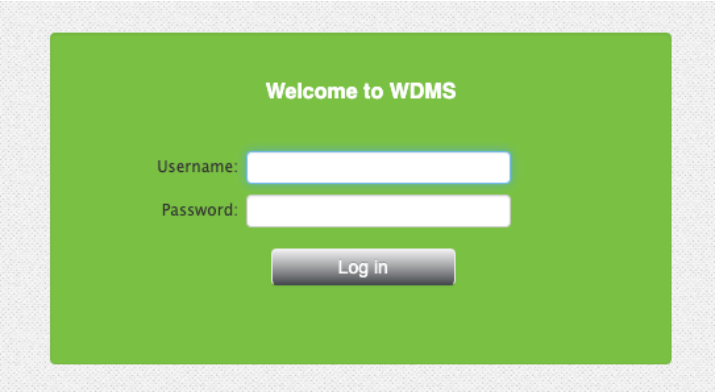
In this report prepared by the Secure Soft Research team, we discovered a critical Persistent Cross-Site Scripting (XSS) vulnerability in the ZKTeco WDMS 5.1.3 platform, which exposes system users and administrators to significant risks. ZKTeco WDMS is a data management system primarily used to control and manage employee access and biometric records, popular in physical security and access control environments.

This report explains how this vulnerability allows attackers to inject malicious scripts into other users' browsers, compromising the security of the platform. Through a detailed technical analysis, we show how attackers can intercept and modify data before it is sent to the server.

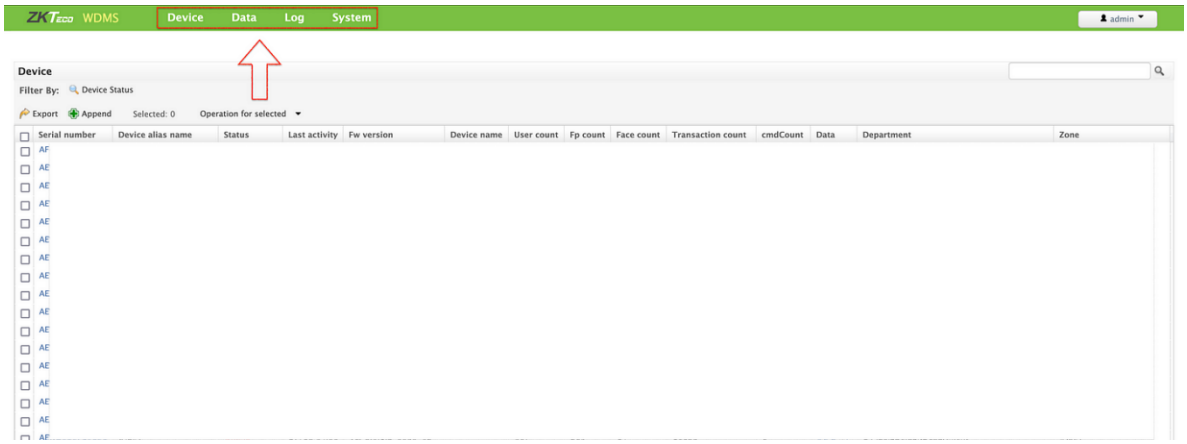
This report is essential for system administrators, software developers, and cybersecurity professionals managing platforms based on ZKTeco WDMS or similar systems, who are looking to protect their systems from emerging threats.

3. Root cause analysis

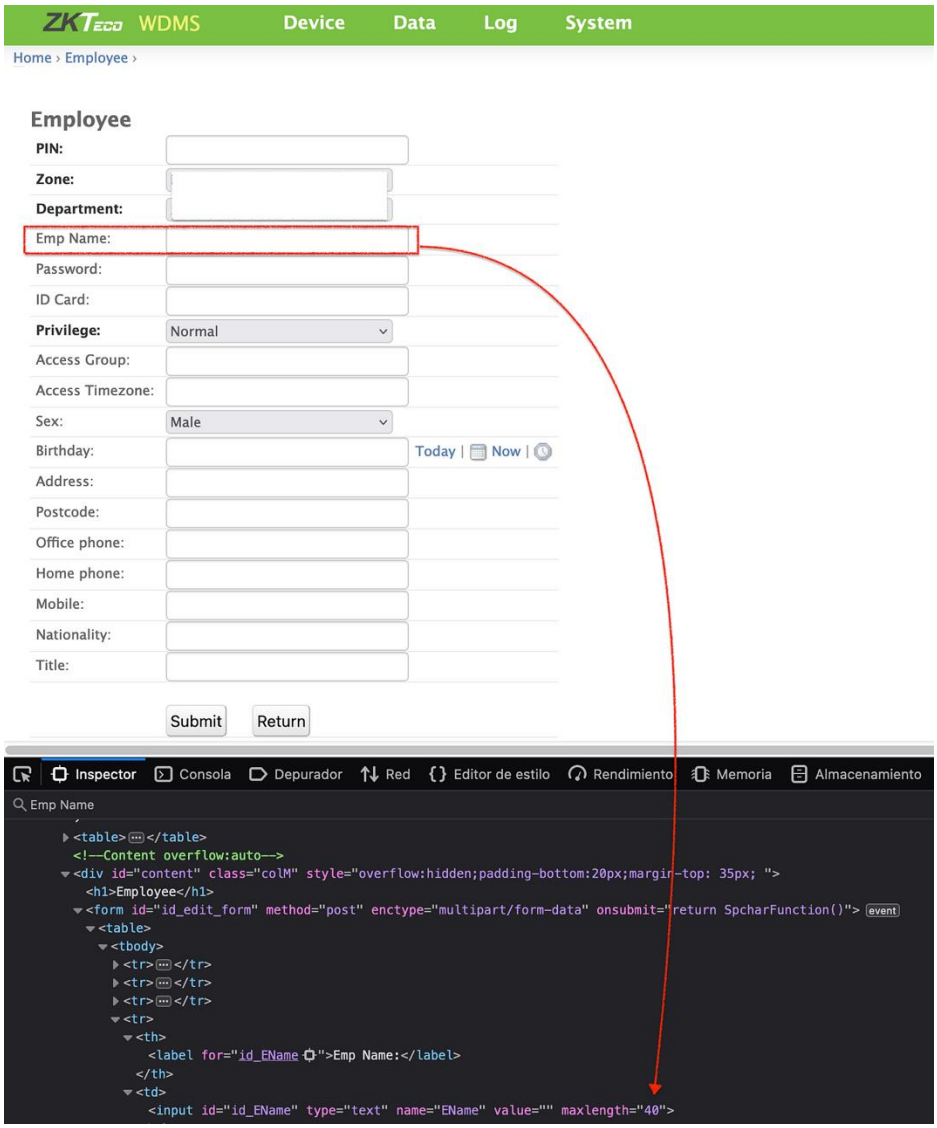
This version highlights login as the user authentication process, briefly mentioning that it is a common step and is omitted to maintain focus on other more critical aspects for the release.



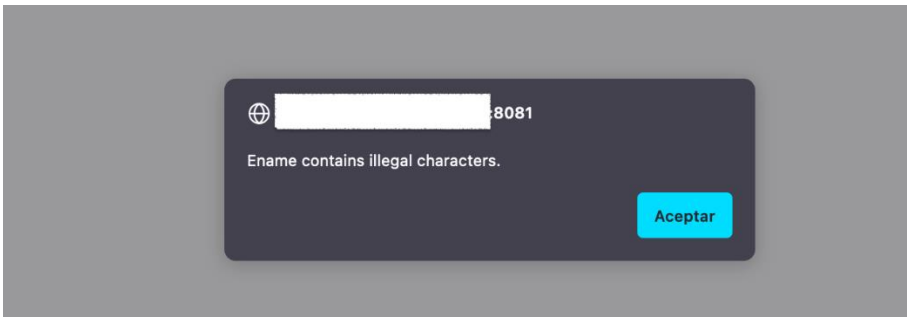
Once logging into the application, a dashboard is displayed with a menu that allows users to view, modify, and delete specific information. This menu acts as a key interface for efficient data management. From here, various functions can be accessed, facilitating the interaction and administration of data within the platform.



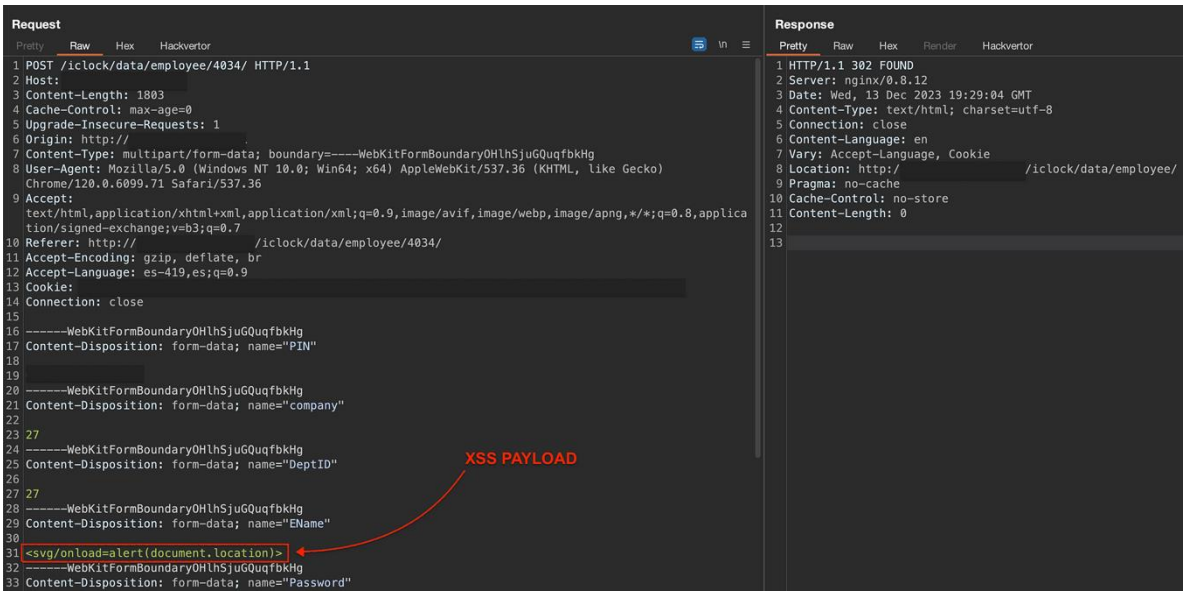
We then attempted to modify employee information in the "Emp Name" (EName) field. Initially, we tested with a small payload; however, the results were unsatisfactory. This was due to the form being validated on the frontend, and the payload being limited to a maximum of 40 characters.



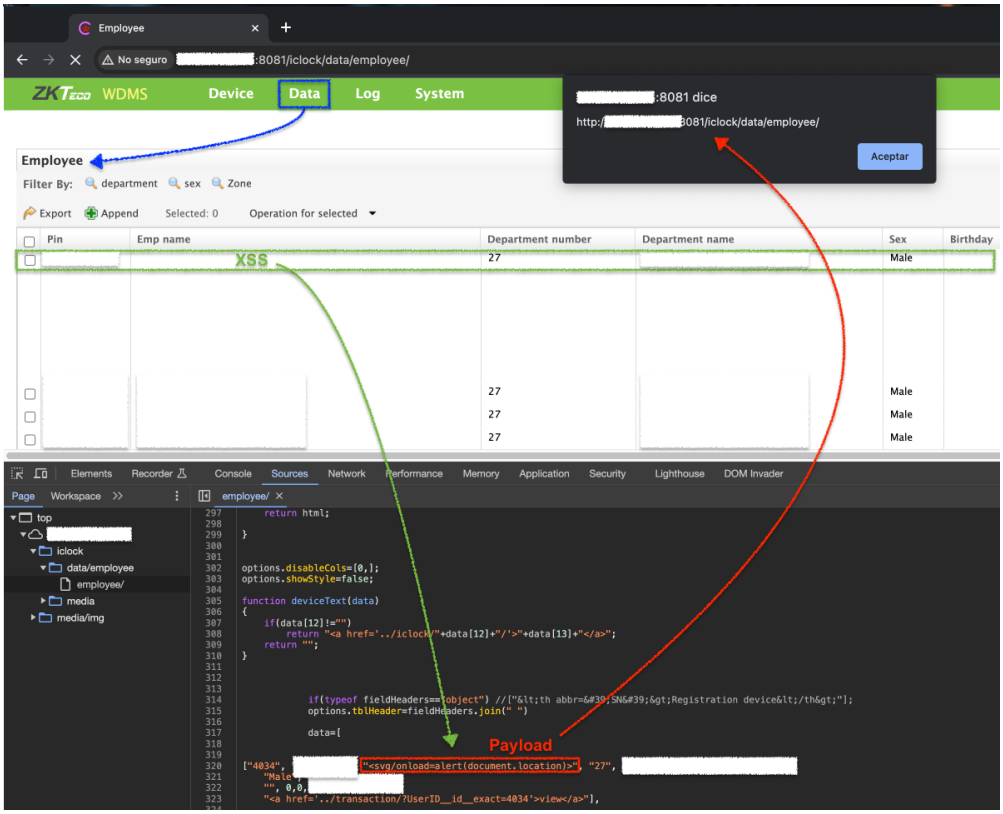
The results obtained from attempting to inject payloads into the form are as follows, indicating the system's behavior in response to these security tests.



The vulnerability in this form lies in the fact that the information is validated only on the frontend, as mentioned earlier. However, this validation is not performed on the backend, which allows the possibility of intercepting the request and modifying the data before it is sent.



After submitting the payload, it can be observed how it is stored in the system, ready to be executed and displayed in the user interface, which highlights the vulnerability in the data handling process.



4. Conclusion: When attempting to modify employee data, a validation vulnerability is revealed, occurring exclusively on the frontend. This allows for the interception and modification of information before it is sent to the backend. The conclusion emphasizes the importance of implementing stronger validation measures on both the frontend and backend to prevent potential security breaches.

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