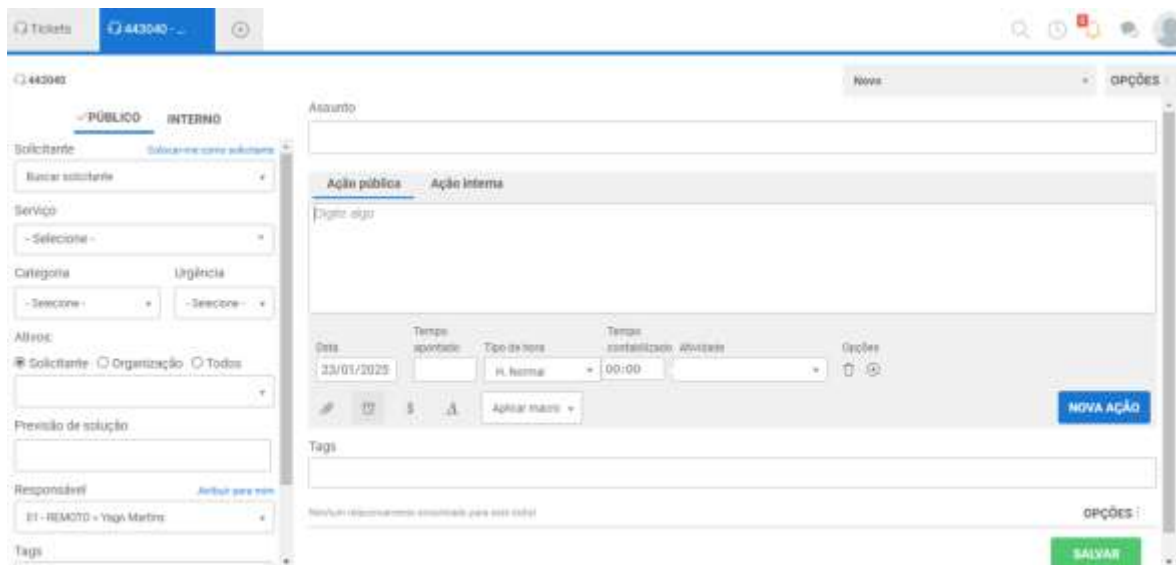


Movidesk - 25.01.22.245a473c54

Stored XSS leads Account take over 0 Click

\*for this exploit, you have to be authenticated\*

first, we can open a new ticket:



The screenshot shows the Movidesk ticket creation form. On the left, there are filters for 'PÚBLICO' and 'INTERNO', a search bar for 'Solicitante', and dropdowns for 'Serviço', 'Categoria', and 'Urgência'. The main form area has a 'Assunto' field, a 'Data' field set to '23/01/2025', and a 'Tipo de hora' dropdown set to 'H. normal'. There are also fields for 'Tempo estimado' and 'Tempo contabilizado'. A 'NOVA AÇÃO' button is visible at the bottom right of the form.

now, we can put the payload in subject field, like this:

"><img src onerror=alert()>

After this, we can save this ticket, in the same time, the alert already shows, but it's a self-xss yet.



The screenshot shows the same Movidesk ticket creation form, but with a self-XSS alert triggered. The 'Assunto' field contains the payload '><img src onerror=alert()>'. A black alert box is overlaid on the form, displaying the URL 'com.br diz' and an 'OK' button. The 'NOVA AÇÃO' button is still visible at the bottom right.

if we come back to visualize all tickets, we can see the stored xss, it can be very dangerous, because its a vulnerability 0 click account takeover.

