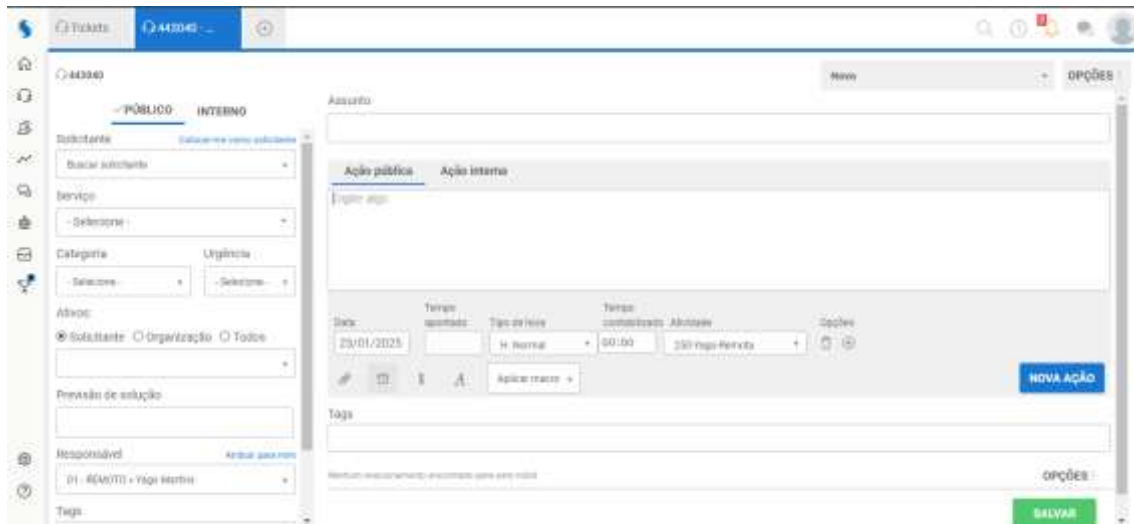


Movidesk - 25.01.22.245a473c54

Stored XSS leads Account take over 0 Click

for this exploit, you have be authenticated

first, we can open a new ticket:



The screenshot shows the Movidesk ticket creation form. The left sidebar contains filters for ticket status (PÚBLICO, INTERNO), subject, service, category, urgency, and assignee. The main form area has fields for 'Assunto' (Subject), 'Data' (Date), 'Tipo de atendimento' (Type of service), 'Tempo estimado' (Estimated time), and 'Opções' (Options). The 'Assunto' field is highlighted with a blue border. The 'Data' field is set to 23/01/2025. The 'Tipo de atendimento' field is set to Normal. The 'Tempo estimado' field is set to 60:00. The 'Opções' field is set to 250 mgps Fibra. A 'NOVA AÇÃO' button is visible at the bottom right of the form.

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

">

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 Movidesk ticket creation form with a self-XSS alert. The 'Assunto' field contains the payload '>'. A black alert box is displayed over the form, showing the URL 'service.sigmatelecom.com.br diz' and an 'OK' button. The 'Data' field is set to 23/01/2025. The 'Tipo de atendimento' field is set to Normal. The 'Tempo estimado' field is set to 60:00. The 'Opções' field is set to 250 mgps Fibra. A 'NOVA AÇÃO' button is visible at the bottom right of the form.

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.

