Thiago "THX" Sena - FireShell Security Team

Mail:thiagosenaribeiro@outlook.com

Sobre o Software:

O Dreambox é um produto da Dream-Multimedia-TV (DMM), que é desenvolvido por receptores baseados em Linux sob o nome Dreambox.

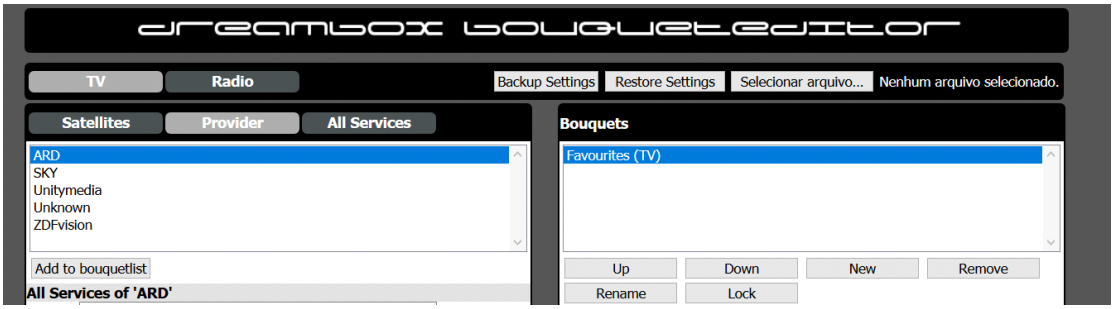
A vulnerabilidade:

O XSS está presente em duas áreas,sendo que na 1 área a vulnerabilidade se encontra em um WebPlugin chamado "BouquetEditor":

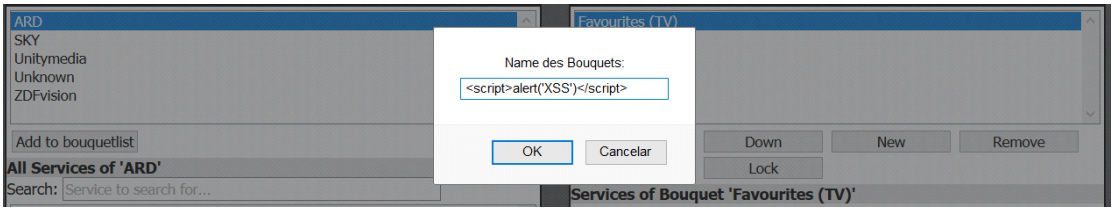
Url: http://IP:PORT/bouqueteditor/

Passos:

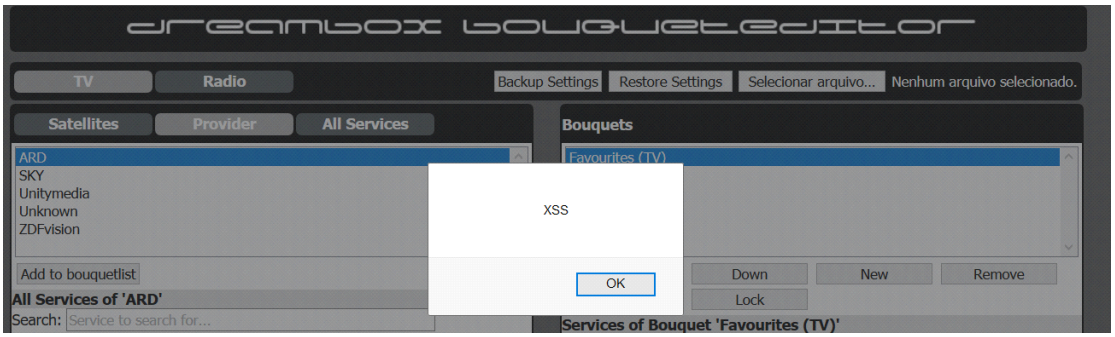
1- Na aba Bouquets, ira adicionar uma nova bouquet



2- Assim, irar colocar o script (<script>alert('XSS')</script>)



3- Vulnerability XSS



A segunda falha consistem em colocar essa variavel depois da url (http://IP:PORT)

Variavel :/file?file=%3CBODY%20ONLOAD=alert(%27XSS%27)%3E