

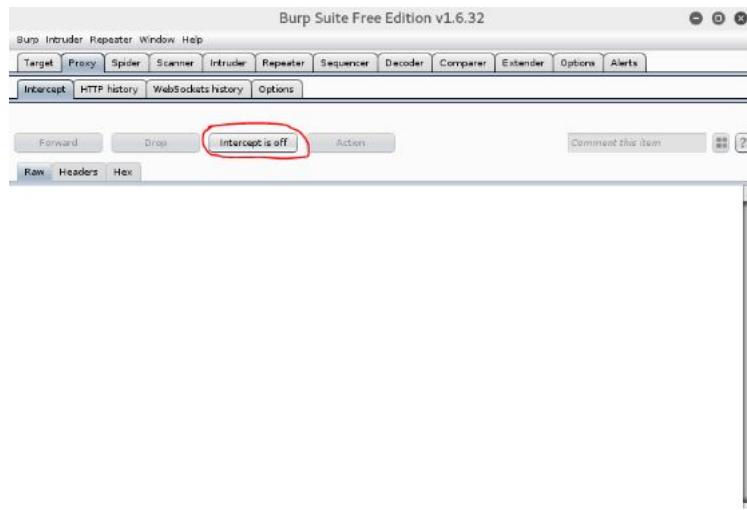
04

Mão à obra: Testando força bruta - Manual

Desabilite momentaneamente a opção **Intercept is On** no Burp Suite.

Vá ao browser no Kali Linux e clique novamente em **Login/Register**.

Volte ao Burp Suite e clique em **Intercept is Off** para que fique **Intercept is On** e o Burp Suite possa assim interceptar a requisição.

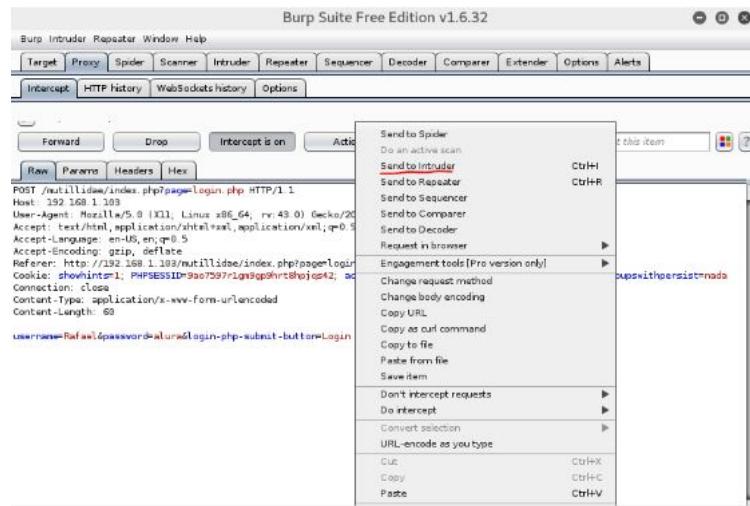


Vá ao browser e coloque em username: [seu nome] e na senha coloque alura. Posteriormente pressione o botão **Login**.

Voltando ao Burp Suite, devemos ver a requisição interceptada.



Clique com o botão direito do mouse na requisição e selecione a opção **Send to Intruder**.



Vá até a aba **Intruder** -> **Positions**. Aperte o botão **Clear** e depois selecione o parâmetro [seu Nome] e clique no botão **Add** e depois selecione o parâmetro alura e clique no botão **Add**. Estamos trabalhando com dois parâmetros, precisamos mudar o tipo de ataque para Cluster Bomb.



Clique na aba **Payloads** e em **Payload Options** vamos colocar os valores do username. Vou fazer o teste com a seguinte lista:

- administrador
- adm
- admin
- administrator
- root
- _admin
- _root
- _administrator
- adm_
- admin_

Mude o **Payload set** para 2. Vou usar para a senha a seguinte lista:

- pass
- senha
- password

- letmein
- autoriza
- logado
- admin
- administrador
- multillidae
- owasp

Uma vez que as duas listas foram selecionadas, pressione o botão **Start Attack** para iniciar o ataque. Qual foi o usuário e senha aceitos pelo sistema? Tente encontrá-los na aba de resultados.