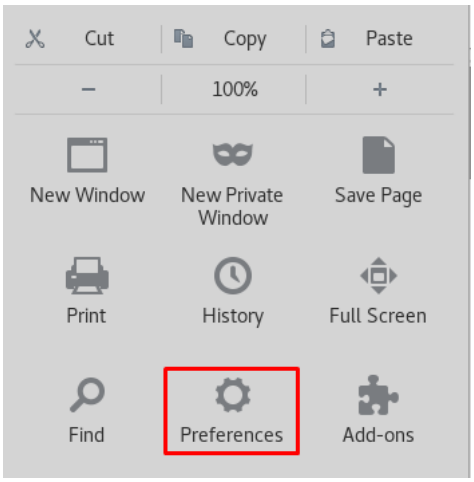
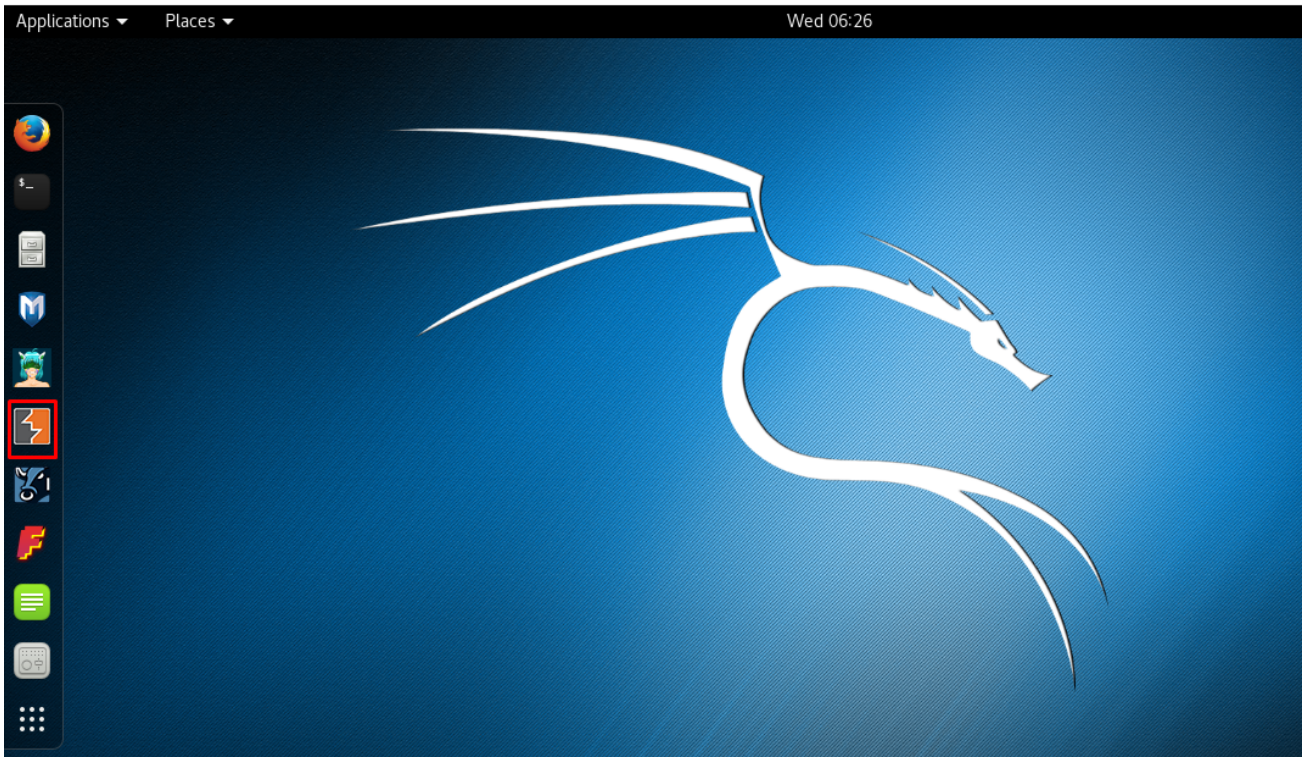
09

Mãos à obra: Forçando senha com o Burp Suite

Agora que implementamos o botão do Google Recaptcha na nossa aplicação, vamos voltar ao Burp Suite para fazermos novamente o ataque automatizado de força bruta. O primeiro passo é ir no browser da máquina do Kali Linux e configurarmos novamente o Proxy para que a requisição passe pelo Burp Suite, para isso, clique na aba **Preferences**

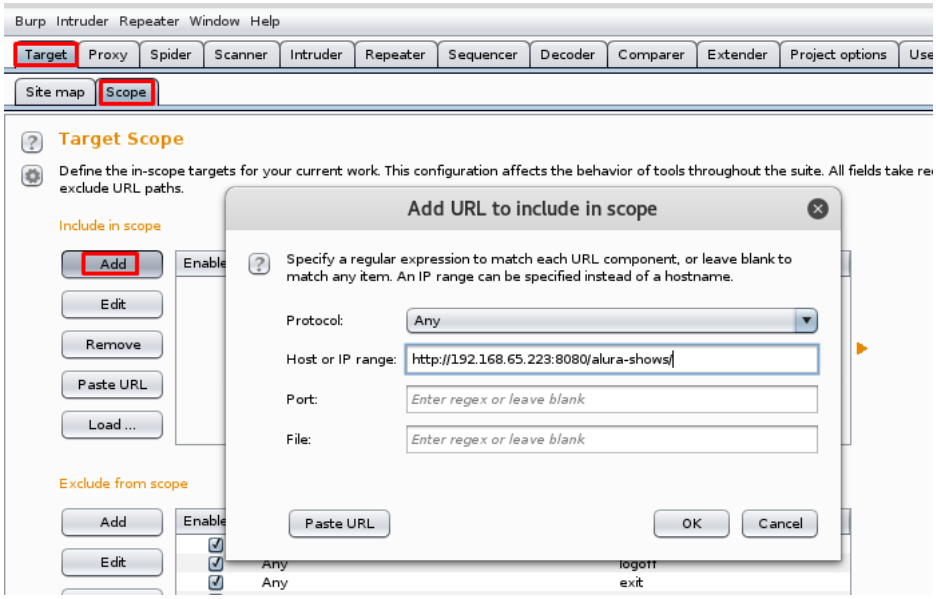


Na sequência, clique na aba **Advanced**->**Network**->**Settings** e configure para ser utilizado o Proxy com o endereço IP 127.0.0.1 e porta 8080, com isso os dados serão passados pelo Burp Suite. Agora vá até o Burp Suite e inicialize-o:



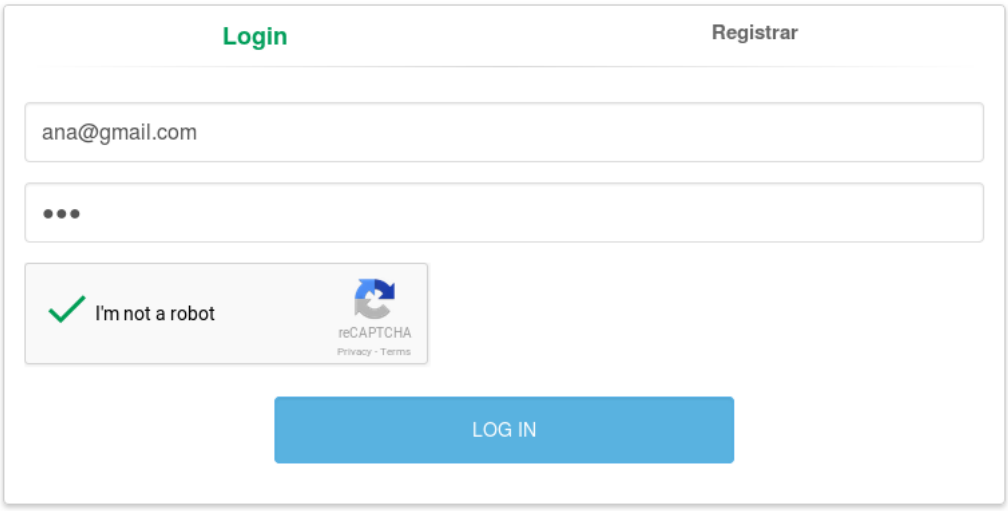
Posteriormente siga os passos até inicializar o Burp Suite. Feito isso, configure a URL das quais queremos interceptar as requisições. Clique na aba **Target**->**Scope**, posteriormente clique no botão **Add** e coloque a URL de acesso da home da Alura Shows:

```
http://[IP da máquina onde o Tomcat está rodando]:8080/alura-shows
```



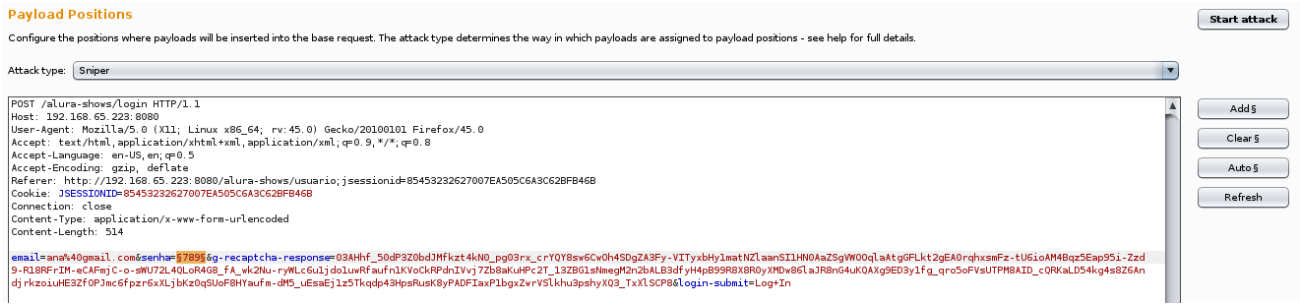
O Burp Suite por padrão já começa a interceptar as requisições. Vamos pausá-la momentaneamente para que possamos ir até a aba de login da nossa aplicação colocar o email e senha, para isso, no Burp Suite vá na aba **Proxy->Intercept** e clique no botão para que ele fique **Intercept is off**, pausando assim momentaneamente as interceptações.

Na sequência, vá até a parte de login da Alura Shows e coloque o email ana@gmail.com, uma senha aleatória, por exemplo 12345 e pressione o botão do Recaptcha do Google. **Antes de pressionar o botão Login** volte no Burp Suite, na aba **Proxy->Intercept** e clique no botão Intercept is off para que ele fique **Intercept is on** reinicializando assim o processo de interceptação das requisições. Agora podemos voltar no browser e pressionar o botão **Login**

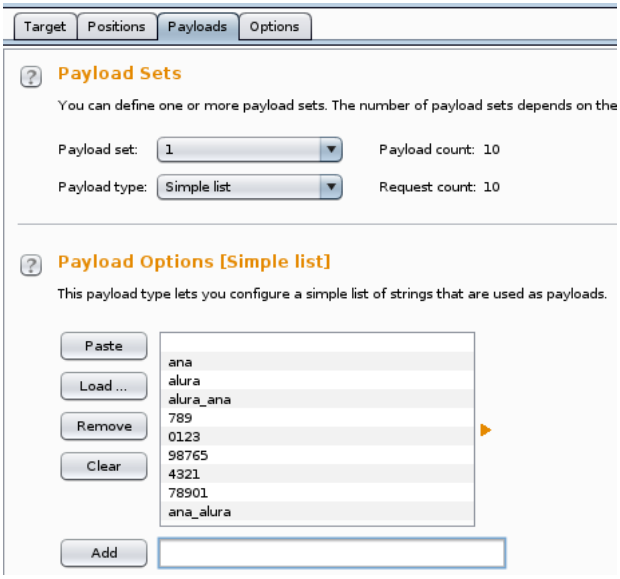


Feito isso, a requisição deve ter sido interceptada pelo Burp Suite, clique com o botão direito do mouse e selecione a opção **Send to intruder**:

Posteriormente, na aba **Intruder**, vá até a aba **Positions** e posteriormente, no lado direito clique em **Clear** para limpar todos os campos, na sequência, selecione o valor da senha 12345 e clique no botão Add.

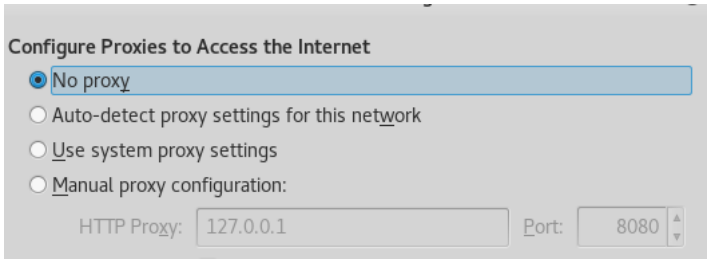


Na sequência, na aba **Payloads** coloque 10 senhas de sua preferência, sendo que uma delas é a senha 789 que a Ana utilizou para se cadastrar na aplicação.



Por fim, clique no botão **Start attack** para inicializar esse ataque. Qual é o resultado? A senha 789 que a Ana havia utilizado para se cadastrar mostrou um status HTTP 200 (OK)?

Importante: Depois do exercício volte no aba **Preferences** no browser, clique na aba **Advanced->Network->Settings** e selecione a opção **No proxy**


Configure Proxies to Access the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration:
HTTP Proxy:
127.0.0.1
Port:
8080