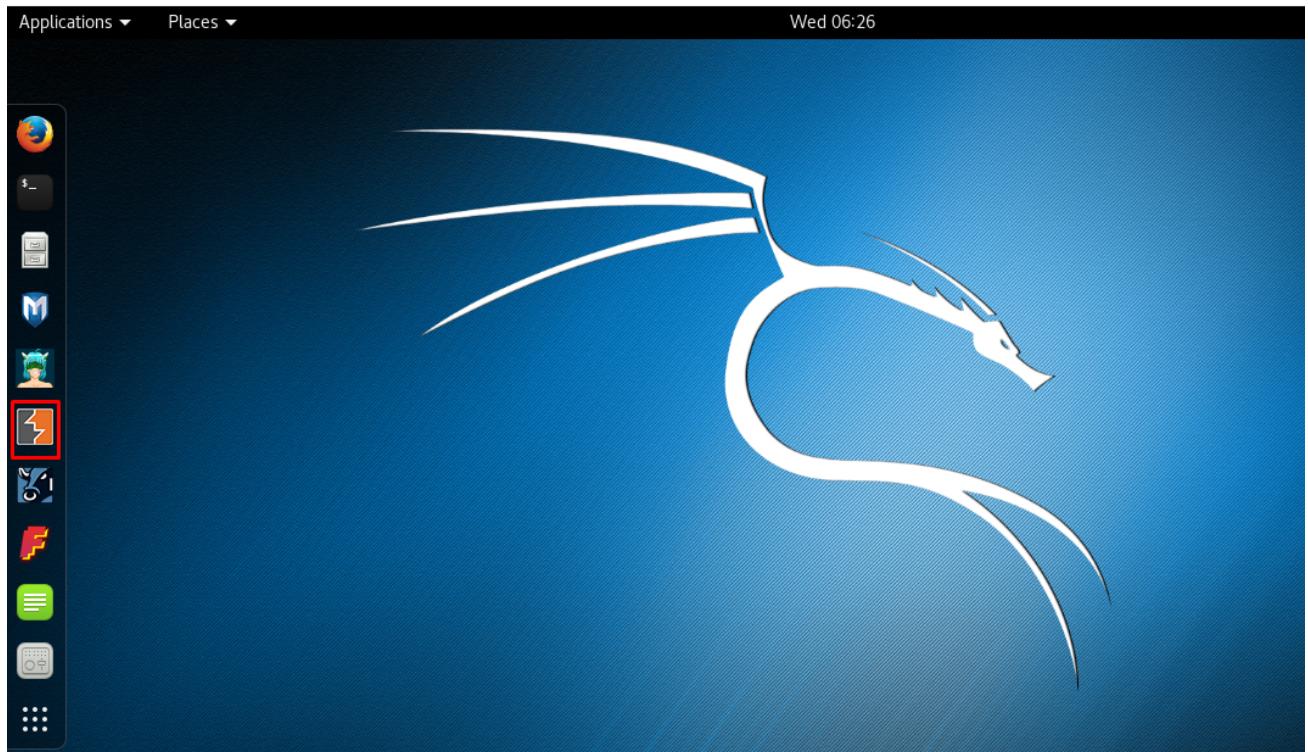


02

Mão à obra: Interceptando a requisição

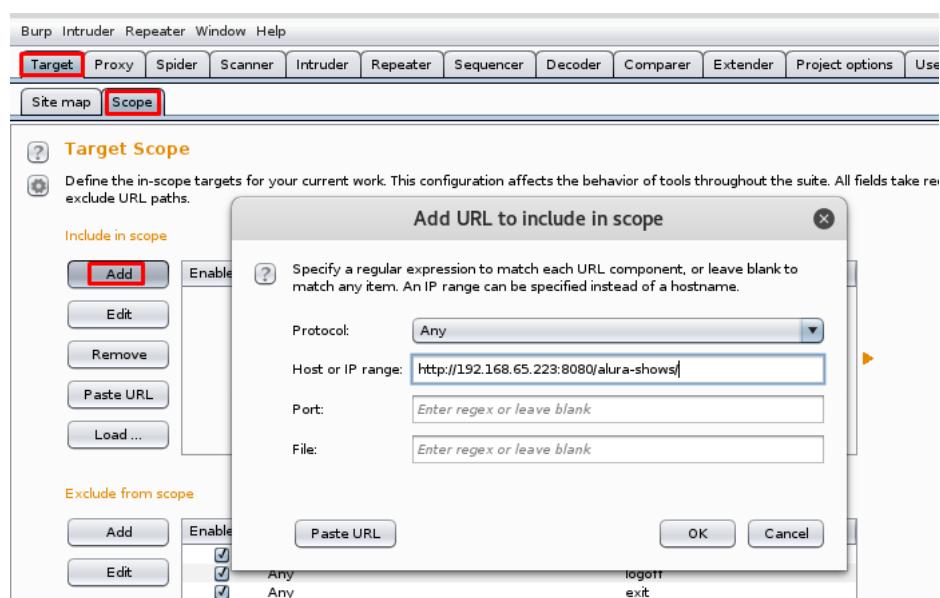
Vamos agora utilizar o Burp Suite para interceptar a requisição do login e forçarmos assim várias senhas com o objetivo de descobrir de forma automatizada a senha que a Ana se cadastrou na aplicação da Alura Shows.

Para isso vamos até a máquina do hacker, o Kali Linux e clicamos no ícone do Burp Suite:



E posteriormente siga os passos até inicializar o Burp Suite. Feito isso, o primeiro passo será configurar 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:

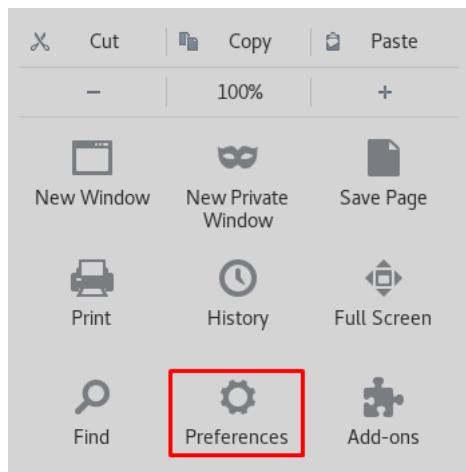
`http://[IP da máquina onde o Tomcat está rodando]:8080/alura-shows`



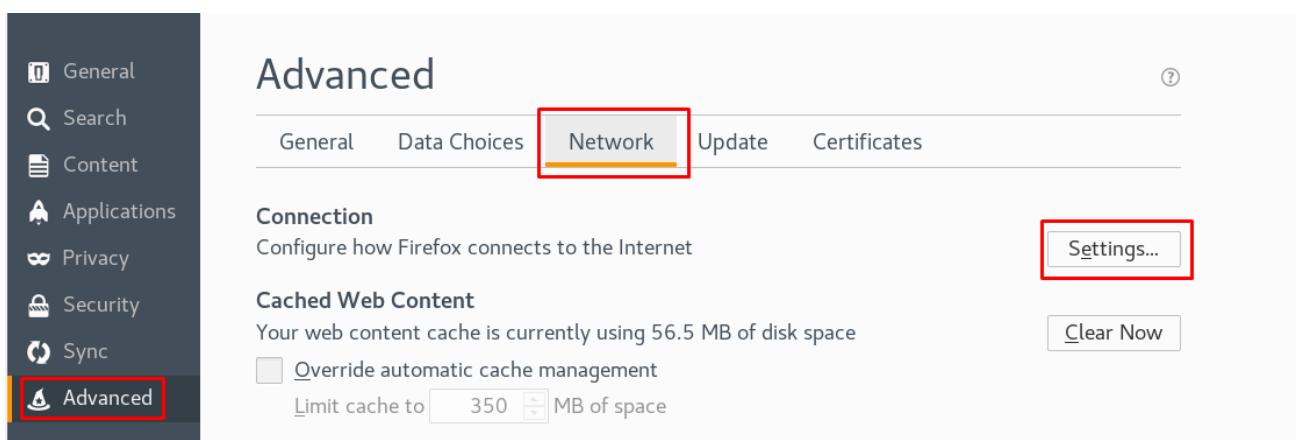
O Burp Suite por padrão já começa a interceptar as requisições. Vamos pausá-la momentaneamente para acessarmos a página de login e fazermos os devidos ajustes no browser. Vá na aba **Proxy->Intercept** e clique no botão para que ele fique **Intercept is off**, pausando assim momentaneamente as interceptações.



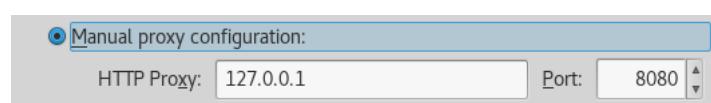
Ainda no Kali Linux, vá até o browser e accese a parte de login da aplicação da Alura-Shows. Na sequência, vamos configurar o browser para enviar as requisições passando pelo Burp Suite. Vá até a aba **Preferences**:



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 que fizemos essa configuração no browser, volte para a aba **Proxy->Intercept** e clique no botão para reativar a interceptação



Faça o login com o e-mail `**ana@gmail.com**` e uma senha aleatória, por exemplo, `12345`, essa requisição deve ser interceptada pelo Burp Suite. Na sequência, clique com o botão direito do mouse e envie para o **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**.

Depois vá na aba **Payloads** e insira 10 senhas de sua preferência, sendo que uma delas deve ser a senha correta que a Ana utilizou para se cadastrar na Alura Shows. No nosso caso, a senha é `789`

Para finalizar clique no botão **Start Attack** no canto superior direito. Qual é o resultado? Alguma delas indicou um status HTTP 200 (OK)?

Importante: Com essa configuração do Proxy, ao fecharmos o Burp Suite, perderemos o acesso à internet. Dessa forma, depois do exercício volte na aba **Preferences** no browser, clique na aba **Advanced->Network->Settings** e selecione a

opção No proxy

