01

Forçando senhas de forma automática

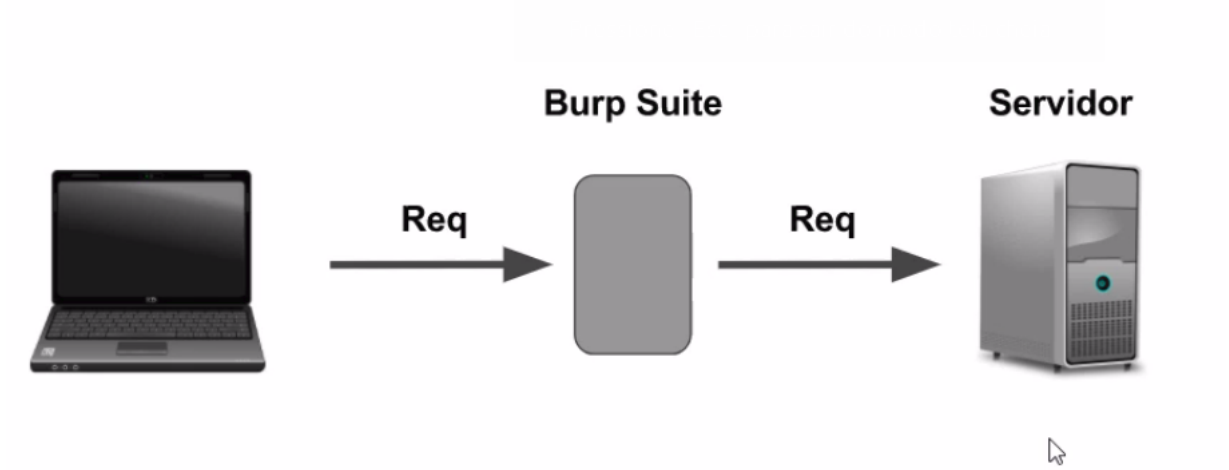
Transcrição

Conseguimos proteger a aplicação contra os ataques de injeção de código SQL, e estamos salvando as senhas dos usuários utilizando o código ***Hash***. Com essas modificações na aplicação, passamos a oferecer uma segurança maior aos usuários do **Alura Shows**.

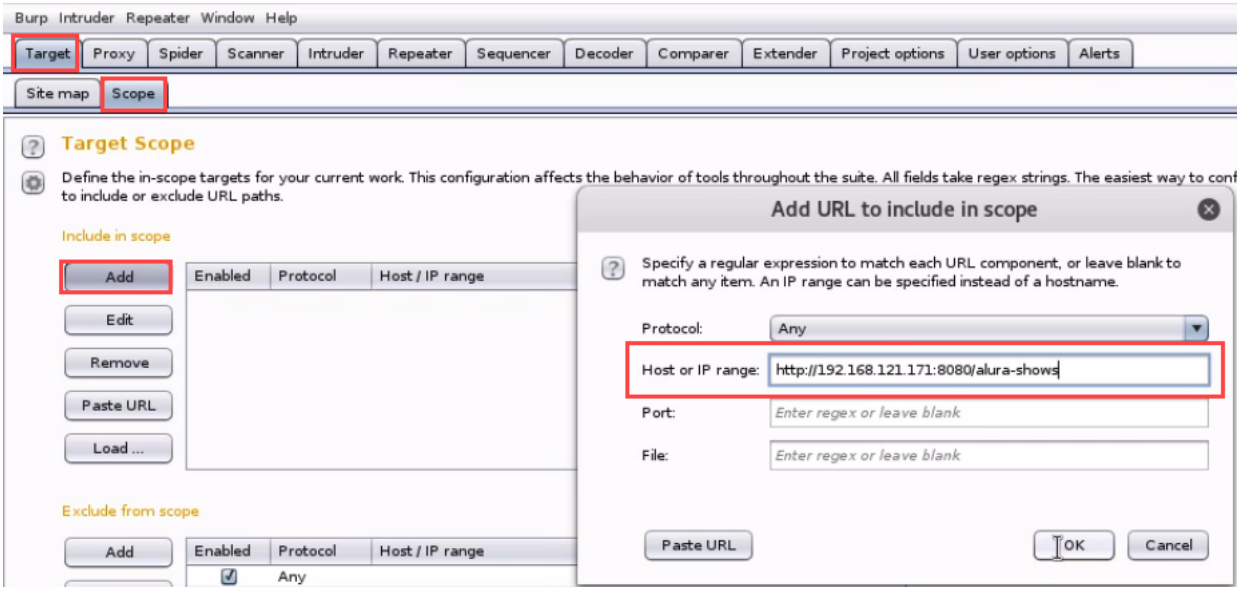
O usuário **Alex** irá realizar mais alguns testes na aplicação. Dessa vez, o Alex tem a intenção de fazer o *Login* como se fosse a **Ana**. Como a aplicação está protegida contra-ataques de injeção de código, o Alex terá que inserir senhas manualmente até conseguir ser autenticado.

Mas é muito trabalhoso colocar muitas senhas manualmente, por isso o Alex usará uma ferramenta automatizada que forçará diversas senhas, com o objetivo de descobrir qual a senha cadastrada pela Ana. Esse tipo de ação é conhecido como **Força Bruta**. A ferramenta utilizada para isso é o ***Burp Suite***.

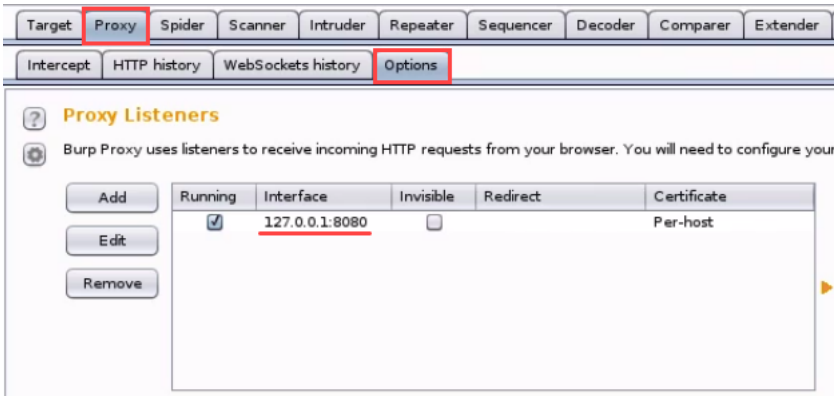
Como funciona o *Burp Suite*? Quando clicamos no botão ***LOG IN***, estamos fazendo uma requisição para o servidor. O *Burp Suite* interceptará essa requisição, onde passa manipular o valor da senha colocando diversas possibilidades. Em seguida ele completa a requisição com o servidor, indicando a possível senha usada pelo usuário alvo.



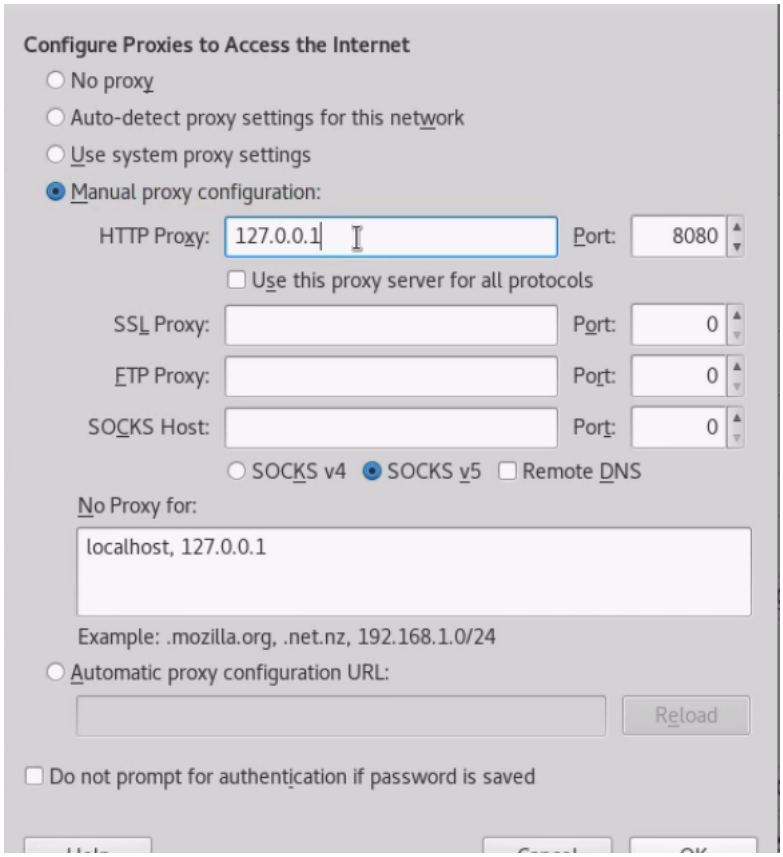
No Kali Linux, abriremos o *Burp Suite* que está na barra lateral esquerda. Com o programa aberto, clicaremos em "Next", em seguida "Start Burp". Precisamos informar qual a URL que o *Burp Suite* irá interceptar, acessaremos o caminho "Target > Scope > Include in scope > Add" e colocaremos em ***Host or IP range*** o endereço `http://192.168.121.171:8080/alura-shows/` , clicaremos em "OK".



O *Burp Suite* fica ouvindo as requisições por meio de uma porta específica, e só por ela que poderá ocorrer a interceptação. Podemos verificar qual porta ele está ouvindo acessando o caminho "Proxy > Options > Proxy Listeners", veremos que ele está escutando na porta `127.0.0.1:8080`.



Configuraremos o browser Firefox para enviar as informações ao proxy do *Burp Suite*. No Firefox, vamos em "Menu > Preferences > Advanced > Network > Connection > Settings". Na janela de configurações, colocaremos a opção ***Manual proxy configuration***, em seguida na seção ***HTTP Proxy*** colocaremos `127.0.0.1` e na seção ***Port*** colocaremos `8080`. Clicaremos em "OK".



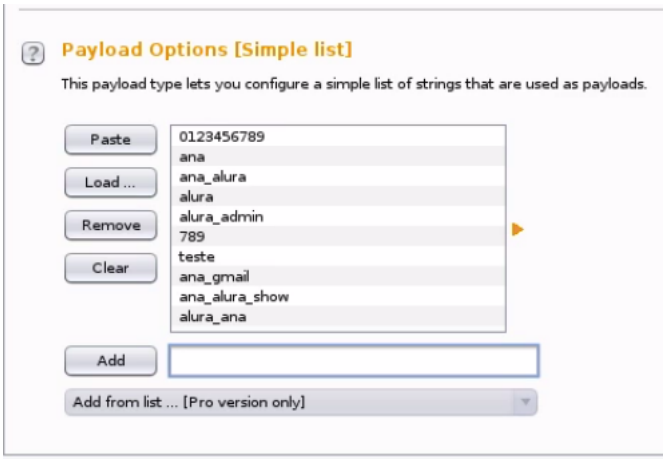
No *Burp Suite*, acessaremos "Proxy > Intercept" e veremos que a sinalização ***Intercepts is on*** está disponível, isso significa que o programa já está ativo para fazer as interceptações. Acessaremos o formulário de *Login* da Alura Shows, no campo **E-mail** colocaremos `ana@gmail.com e no campo **Senha** colocaremos 012345`, clicaremos em "LOG IN".

Após enviar as informações para a autenticação, a interceptação da requisição foi efetuada. De volta ao *Burp Suite*, em "Proxy > Intercept > Raw" veremos a requisição. Enviaremos para o campo de intrusão clicando com o botão direito do mouse, e selecionando a opção ***Send to Intruder***.

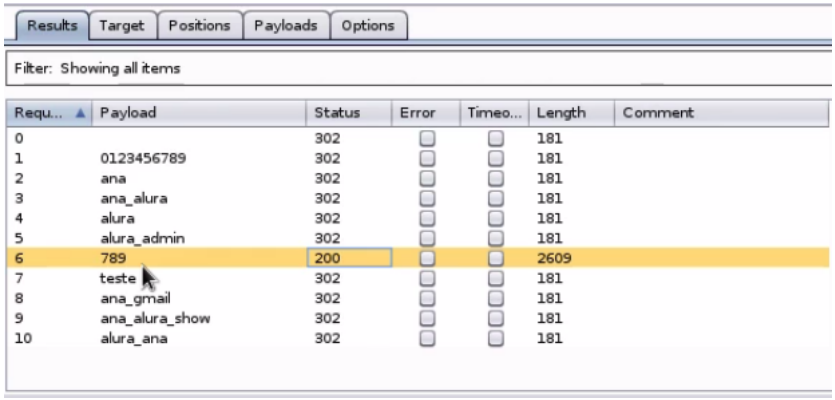
Em "Intruder > 2 x > Positions" veremos todos os parâmetros que podem ser alterados, como queremos apenas a senha clicaremos em "Clear" para limpar os campos. Em seguida, selecionaremos apenas a senha e clicaremos em "Add".

Em "Intruder > 2 x > Payloads > Payloads Options" adicionaremos a lista das senhas que serão testadas. Basta escrever a senha no campo e clicar em "Add". Testaremos as seguintes senhas:

- 0123456789
- ana
- ana_alura
- alura
- alura_admin
- 789
- teste
- ana_gmail
- ana_alura_show
- alura_ana



Iniciaremos o ataque pressionando "Start attack". Após o término do processo de força bruta, veremos o resultado de todas as senhas tentadas. Repare que a senha `789` foi a única que apresentou o *status* **HTTP 200**. A aplicação não está preparada para esse tipo de ataque.



Veremos como resolver esse problema.