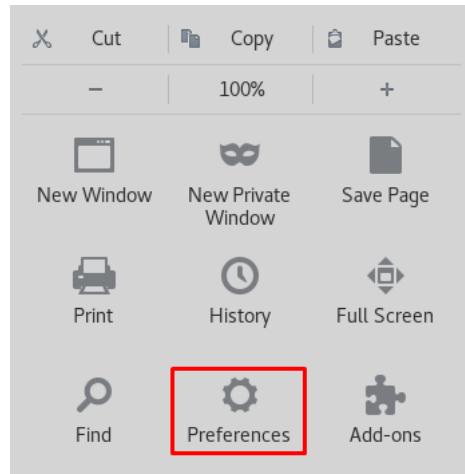


09

Mão 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**

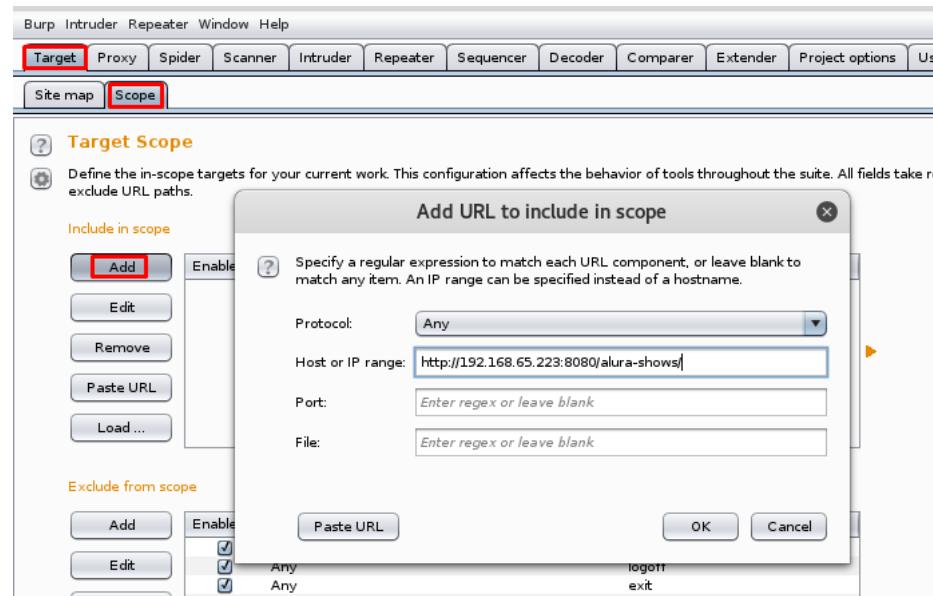


Na sequência, clique na aba **Advanced->Network->Settings** e configure para ser utilizado o Proxy com o endereço IP 127.0.0.1 e porta 8080, com isso os dados serão passados pelo Burp Suite. Agora vá até o Burp Suite e inicialize-o:



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**:

Raw Params Headers Hex

```
POST /alura-shows/Login HTTP/1.1
Host: 192.168.65.223:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.65.223:8080/alura-shows/usuário
Cookie: JSESSIONID=63FC1539E8A14EDB94DFEC36175C715F
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 53

email=ana%40gmail.com&senha=12345&login-submit=Log+In
```

Send to Spider
Do an active scan
Send to Intruder
Send to Repeater
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser ►
Engagement tools [Pro version only] ►
Change request method
Change body encoding
Copy URL

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**.

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

Start attack

Add \$

Clear \$

Auto \$

Refresh

POST /alura-shows/Login HTTP/1.1
Host: 192.168.65.223:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.65.223:8080/alura-shows/usuário
Cookie: JSESSIONID=85453232627007EA505CEA3C62BF846B
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 514

email=ana%40gmail.com&senha=12345&recaptcha-response=03AHnf_50dP820bdJHfkzt4kN0_pg03rx_cryOY8sw6Cw0h45DgZA3Fy-VITybHy1matHzlaanSI1H0AaZSgW00qlsAtgFLkt2gEA0rqhsxmFz-tU6ioAM4Bqz5Eap95i-Zzd9-R18PFrIM-cxFeqjCo-o-wlJ72L40LR4G8_faw_k2Nu-ryML6Uj1doluRfaunKVxckRFDnIVj72baMukPc2T_12ZB01shwegt2n2bALB9dfyH4pB99RB8R0yXM0w66LaJR8n64uK0Xg9ED3y1fg_qr5oFvzUTPM8AID_cQRKAlD54kg4s826An djrkzouuH32fOPjmcf6prz6xLjlk2oqSluP8Htauf-dH5_uEsseEj1z5Tkqdpr3hpsRusK8yPADFIaxP1bgz2xrySlkhu9phyx03_Tx1SCP86Ilogin-submit=Log+In

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.

Target Positions Payloads Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set: 1 Payload count: 10

Payload type: Simple list Request count: 10

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Add

- ana
- alura
- alura_ana
- 789
- 0123
- 58765
- 4321
- 78901
- ana_alura

Por fim, clique no botão **Start attack** para iniciar 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**

