Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

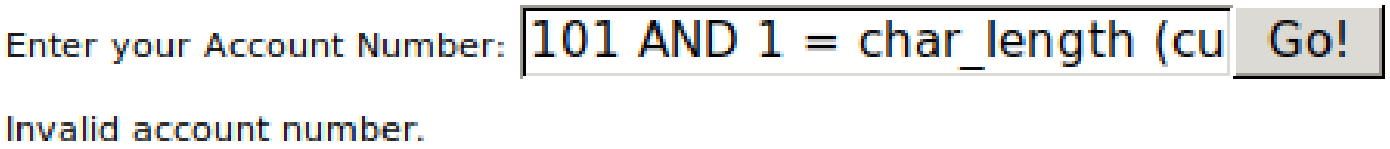
Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Hackeando um Banco de Dados

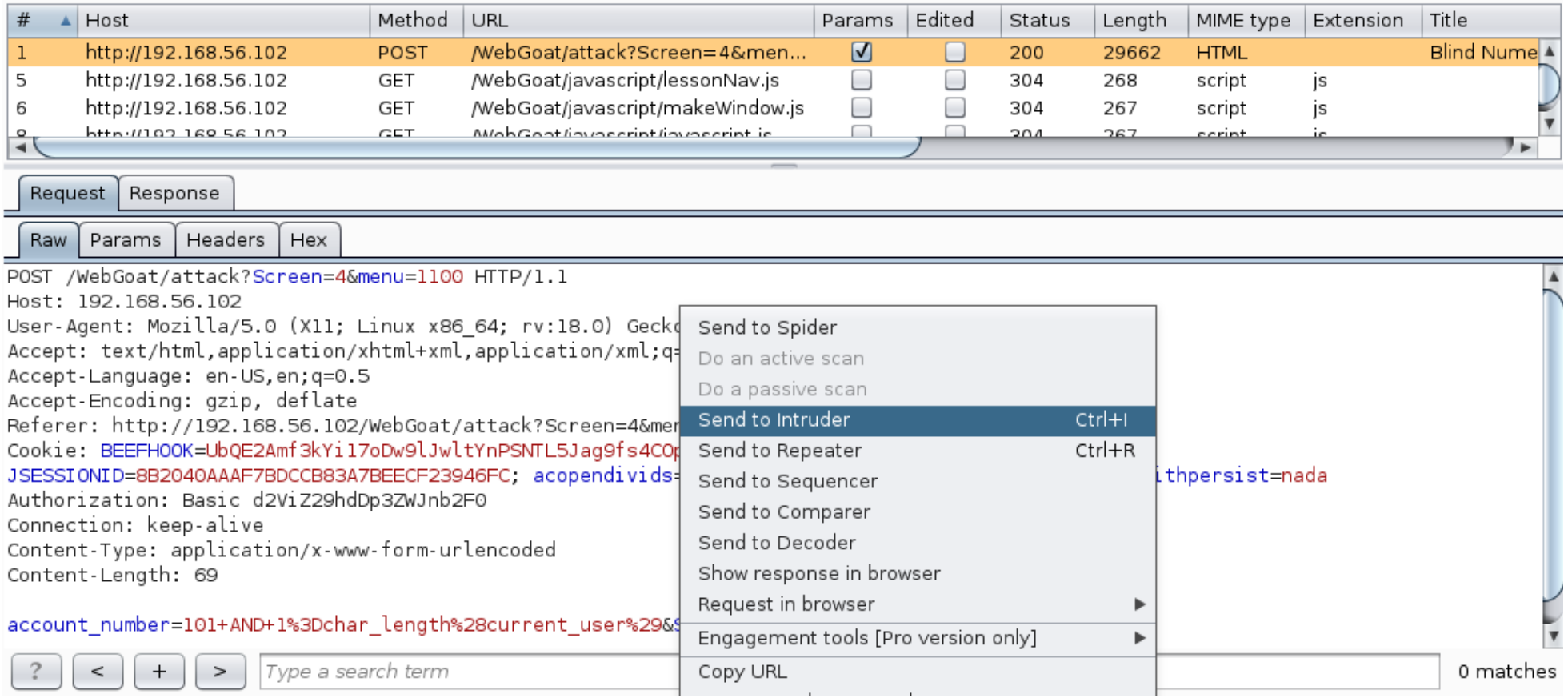
Nessa parte da aula, vamos descobrir o nome do usuário que se conecta ao banco de dados de nosso **WebGoat.** Então primeiro precisamos saber o comprimento do nome de usuário. Vamos tentar injetar a seguinte frase:

101 AND 1 = char_length (current_user)



Hackeando um Banco de Dados

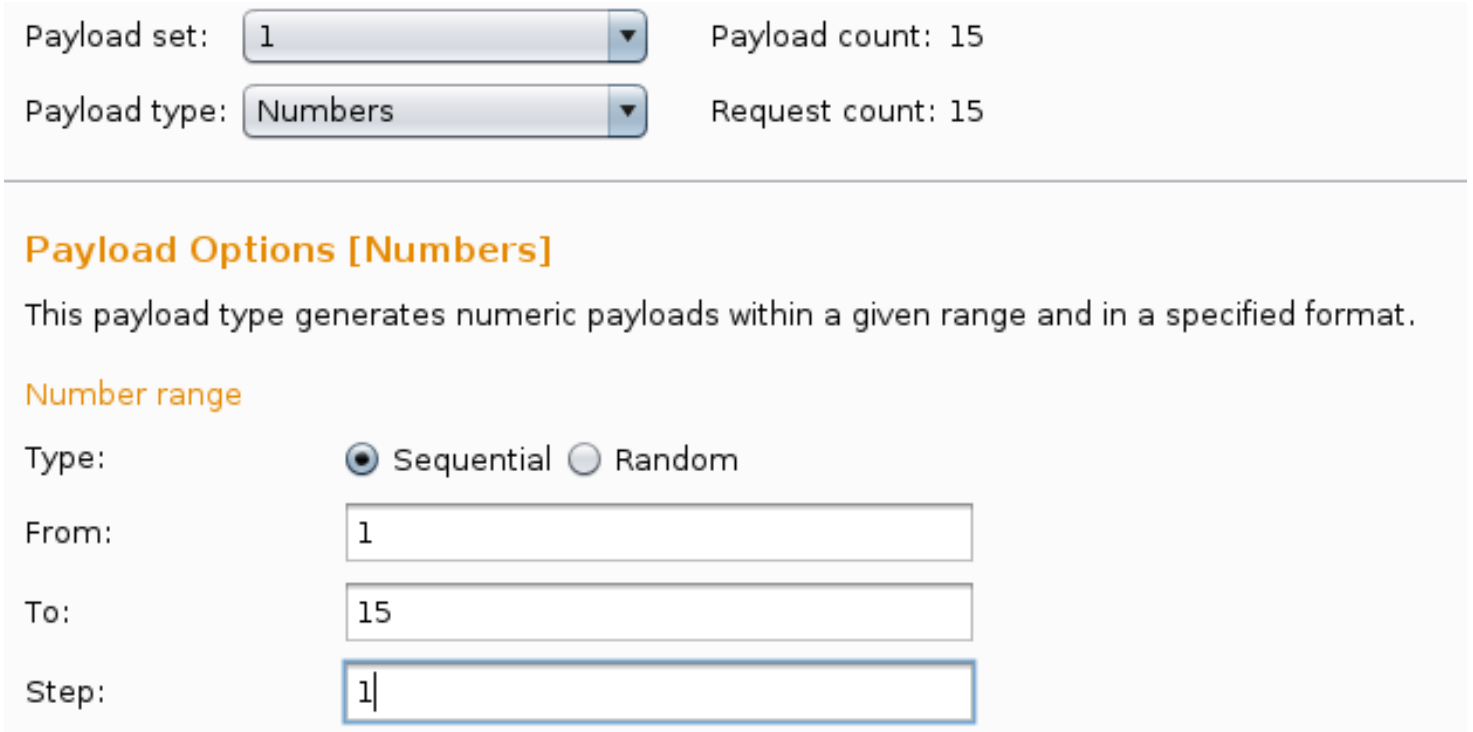
O próximo passo é encontrar este último pedido no histórico de proxy do **BurpSuite** e enviá-lo para o **intruder**, como mostrado:



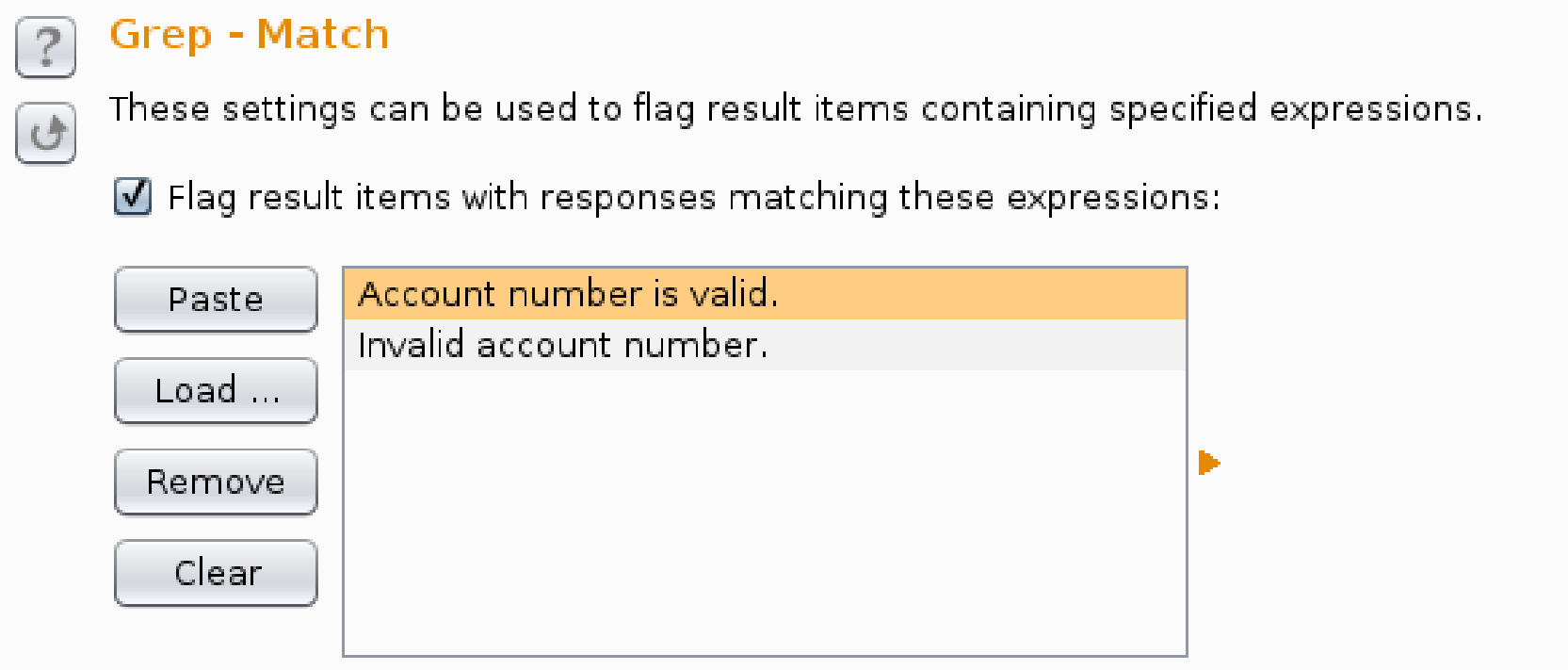
Uma vez enviado ao **intruder**, podemos limpar todos os marcadores com o botão Clear e adicionar um novo no caractere 1 e após o AND, como mostrado:

```
account_number=101+AND+§1§%3Dchar_length%28current_user%29&SUBMIT=Go%21
```

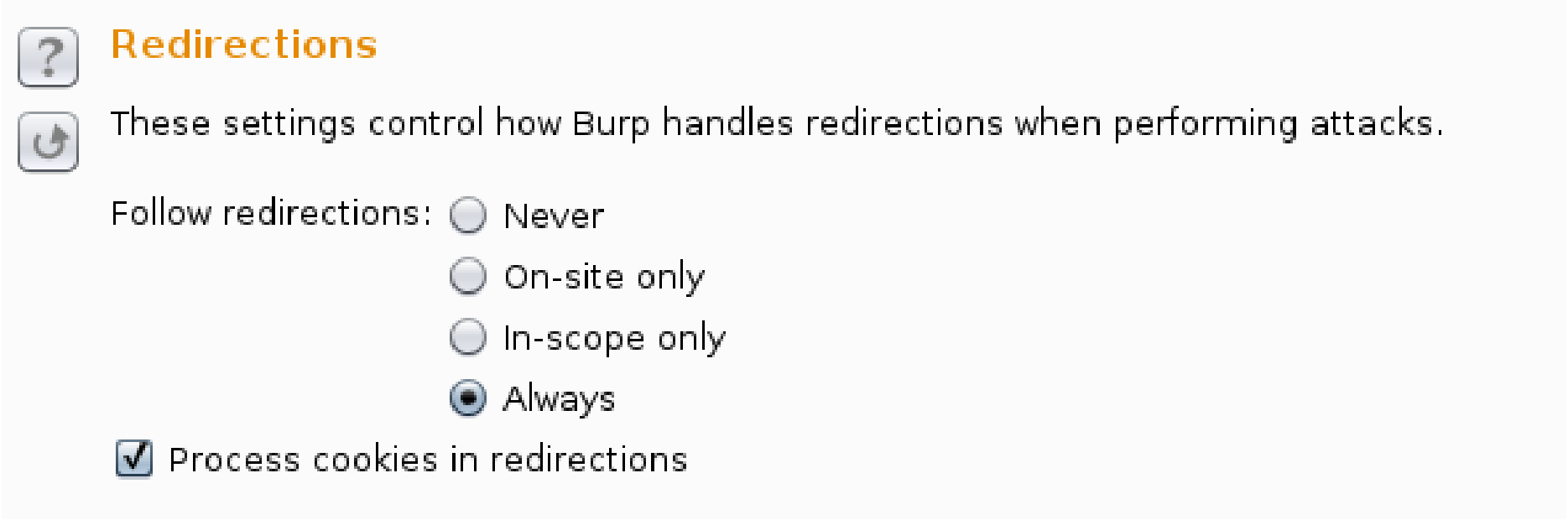
Vá para a seção de **Payload** e defina o tipo de **Payload type** para **Numbers.** Defina o tipo de **Payload** para **Sequential**, de 1 a 15 com um **step** de 1.



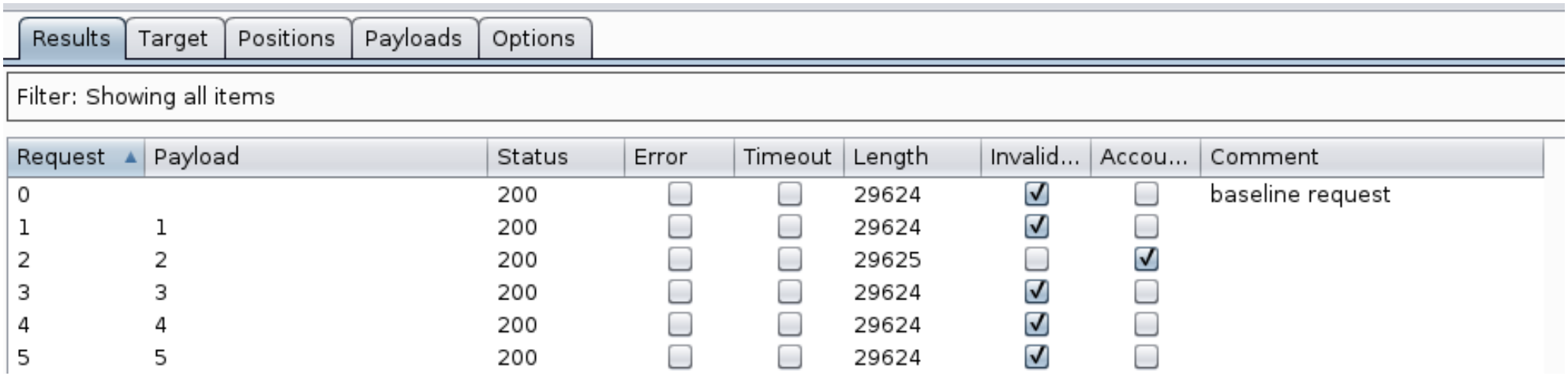
Para ver se uma resposta é positiva ou negativa, vá para as **Options** do **Intruder**, desmarque a lista **Grep-Match** e adicione: **Invalid account number.** e **Account number is valid.** (Com o ponto final!)



Para fazer com que os aplicativos fluam, selecione **Always** na seção **Redirections** e selecione **Process cookies** em **Redirections**.



Agora selecione a opção **Start the attack**



Ele encontrou uma resposta válida no número **2**, isso significa que o nome de usuário de nosso banco de dados é apenas **dois caracteres**.

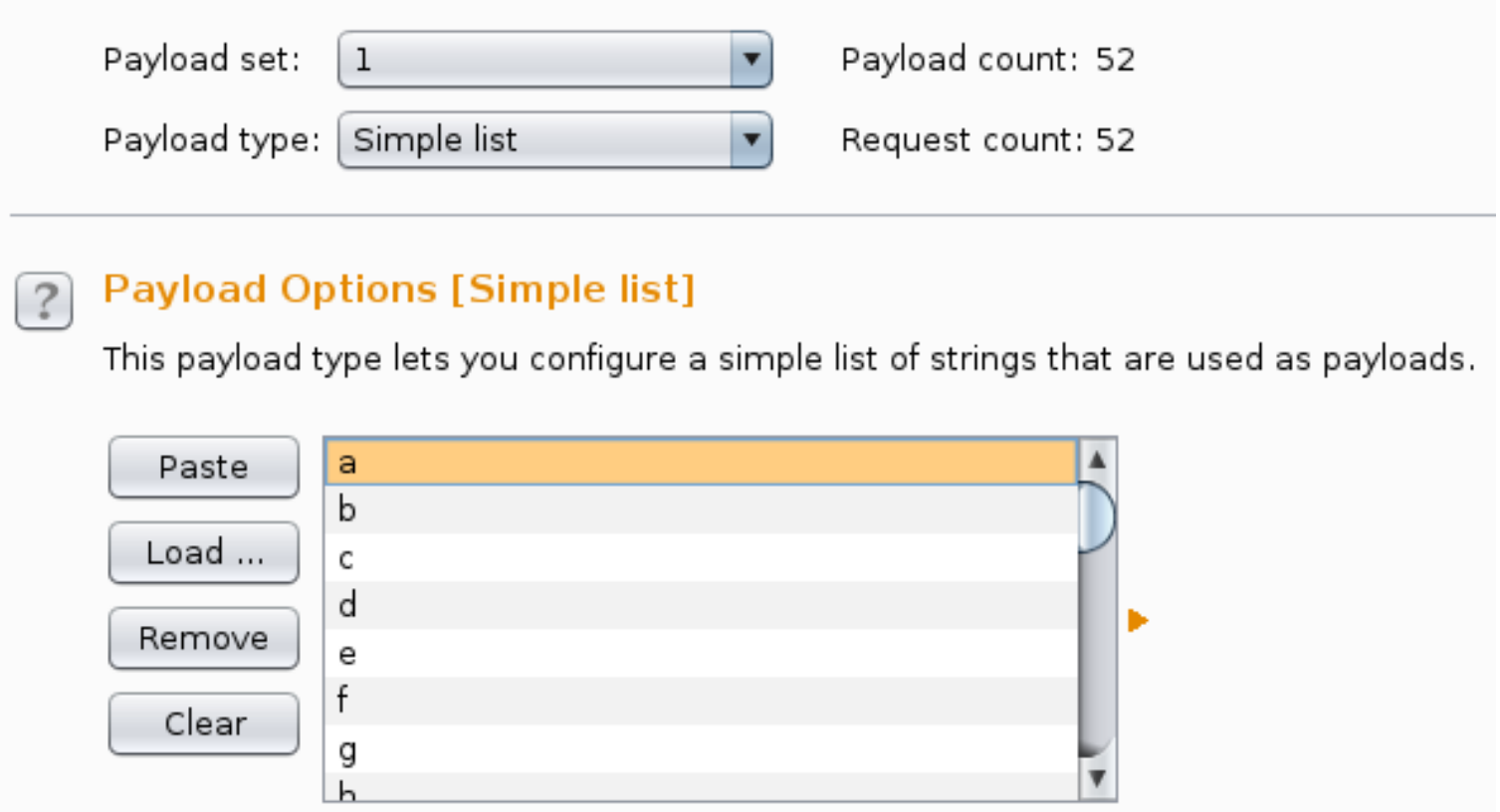
Agora, vamos adivinhar cada caractere no nome de usuário, começando por adivinhar a primeira letra. Envie o seguinte no aplicativo: 101 AND 1 = (current_user LIKE 'b%')

Escolhemos o **b** como a primeira letra para obter **BurpSuite** para obter o pedido, poderia ter sido qualquer letra.

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 31

account_number=101 AND 1=(current_user LIKE '§b§%')&SUBMIT=Go%21
```

Nossa **payload** será uma lista simples contendo todas as letras minúsculas e maiúsculas (de a para z e de A para Z):



Hackeando um Banco de Dados

Repita os dois ultimos passos nesta nessa aula e inicie o ataque, como mostrado aqui:

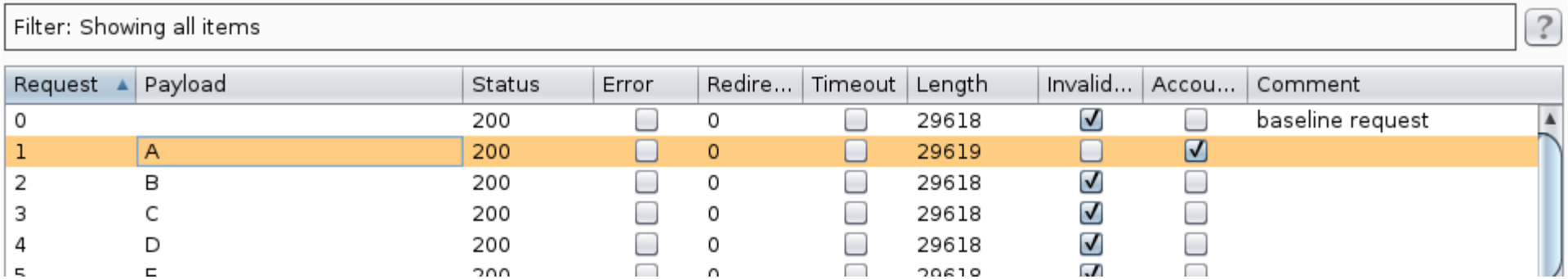
Request	Payload	Status	Error	Redire...	Timeout	Length	Invalid account ...	Account number is valid.	C
15	O	200	☐	0	☐	29624	☑	☐	
16	P	200	☐	0	☐	29624	☑	☐	
17	Q	200	☐	0	☐	29624	☑	☐	
18	R	200	☐	0	☐	29624	☑	☐	
19	S	200	☐	0	☐	29625	☐	☑	
20	T	200	☐	0	☐	29624	☑	☐	
21	U	200	☐	0	☐	29624	☑	☐	
22	V	200	☐	0	☐	29624	☑	☐	

A primeira letra do nosso nome de usuário é **S.** Agora, precisamos encontrar o segundo caractere do nome, então enviamos:

101 AND 1=(current_user='Sa') para a caixa de texto do aplicativo e enviamos o pedido para o intruder.

```
account_number=101+AND+1%3D%28current_user%3D%27S§a§%27%29&SUBMIT=Go%21
```

Repita as etapas as outras etapas. No nosso exemplo, só usamos letras maiúsculas na lista, pois se a primeira letra for uma letra Maiúscula, há uma alta chance de ambos os caracteres no nome serem maiúsculas também.



O segundo caractere do nome é o **A,** então o usuário do banco de dados que o aplicativo usa para fazer consultas é **SA**. SA significa Administrador do Sistema(System Administrator) nos bancos de dados **SQL Server da Microsoft**.