Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Exploiting um Blind SQLi

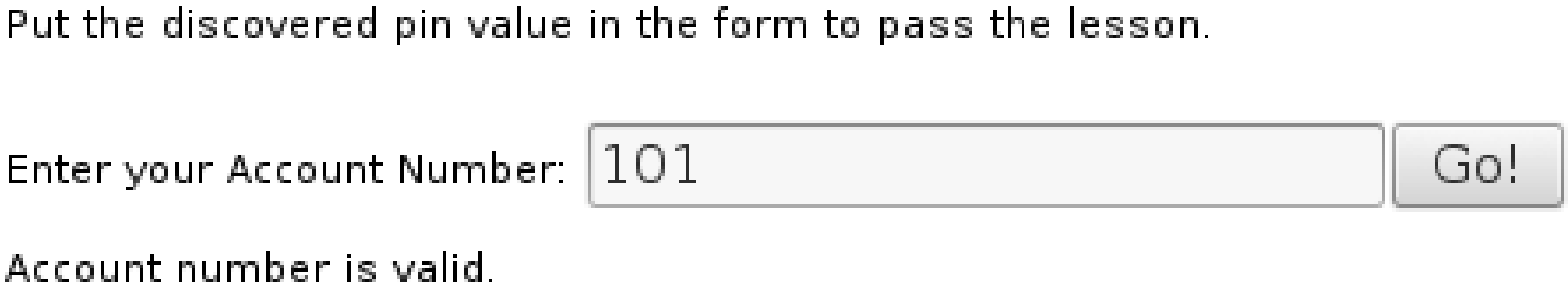
Vamos agora, explorar uma injeção de Blind SQL usando Burp Suite Intruder como nossa principal ferramenta de pentest em banco de dados. Precisaremos do nosso navegador para usar o Burp Suite como um proxy ativado.

Exploiting um Blind SQLi

Navegue até http://192.168.1.163/WebGoat/ e faça login com o webgoat como nome de usuário e senha. Clique em **Start WebGoat** para ir para a página principal do WebGoat. Ir para **Injection Flaws | Blind Numeric SQL Injection**.

Exploiting um Blind SQLi

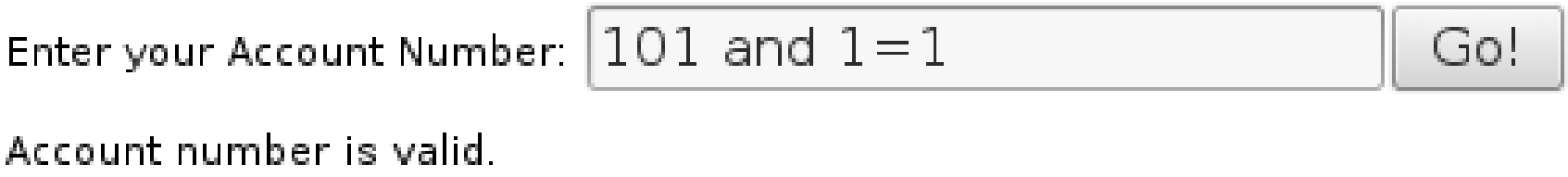
A página diz que o objetivo do exercício é encontrar o valor de um determinado campo em uma determinada linha. Vamos fazer as coisas um pouco diferente, mas vamos primeiro ver como ele funciona: Deixe 101 como o número da conta e clique em **Go !**.



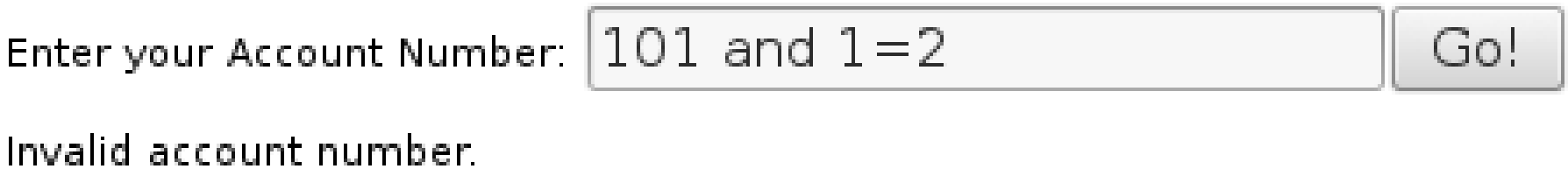
Agora tente com o 1011.

Exploiting um Blind SQLi

Até agora, vimos o comportamento do aplicativo, ele só nos diz se o número da conta é válido ou não. Vamos tentar uma injeção, pois ela está procurando números e provavelmente usá-los como números inteiros para pesquisar. Não vamos usar o apóstrofo neste teste para apresentar: 101 and 1=1



Agora tente: 101 and 1=2



Exploiting um Blind SQLi

Parece que temos um *blind injection* aqui, injetando resultados de declaração verdadeira em uma conta válida, como um falso, aparece a mensagem **Invalid account number**.