08

Order By

Transcrição

A *query* que foi direcionada para o banco de dados durante a *exception* é a seguinte:

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

Analisando o código acima, temos certeza de que a tabela `accounts` tem pelo menos duas colunas, a *username* e a *password*. Mas, será que só existem essas duas colunas?

Vamos fazer com que o banco informe o valor máximo de colunas existentes sem que ocorra uma exception e tentaremos descobrir a partir de qual valor elas acontecem. Primeiro, acessamos o site e clicamos no "OWASP 2013 > A1 - Injection(SQL) > SQLi - Extract Data > User Info (SQL)". Chegamos no momento em que é preciso inserir usuário e senha. O usuário nós já sabemos por meio de uma dica é `admin` . Vamos retornar a *query* que estivemos utilizando:

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

Na *query* abaixo, vamos inserir o `username` que será igual ao `'admin'` e também vamos ordenar por colunas, `order 1,2` . Não podemos deixar o `AND password` atrapalhando, portanto, para resolver a situação inserimos um comentário que anula a funcionalidade dessa parte do código, o `--` . Teremos o seguinte:

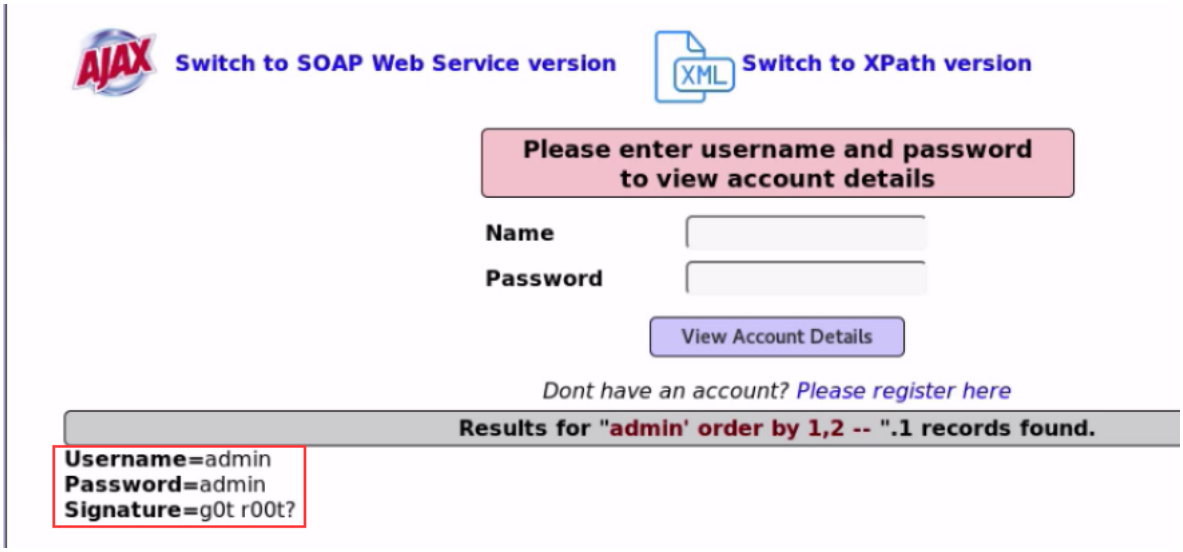
```
SELECT username FROM accounts WHERE username='admin' order by 1,2 -- ' AND password=''
```

O que faremos é selecionar apenas:

```
admin' order by 1,2 --
```

O que acrescentamos ao `Name` da página:

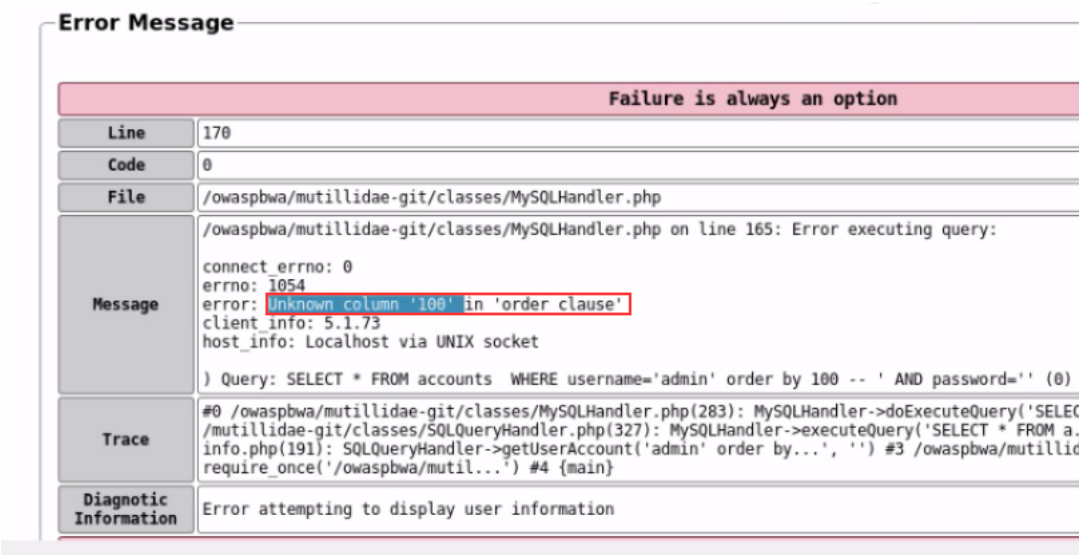
Ao clicar no *View Account Details* teremos uma *exception* e a seguinte informação:



Com isso, descobrimos que além do *username* e *password* também existem as colunas 1 e 2. Vamos fazer um teste, nós acrescentamos junto ao `Name` o seguinte:

```
admin' order by 100 --
```

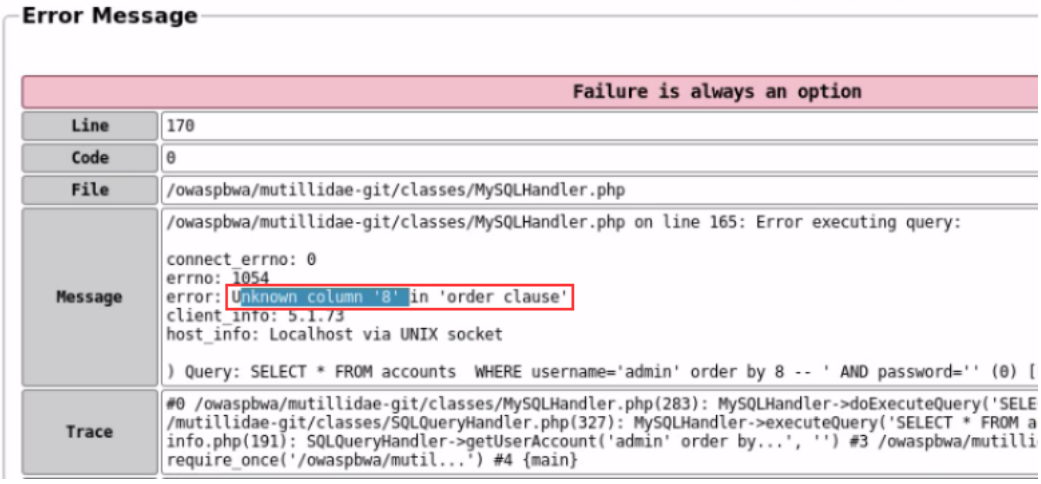
Escrevendo isso nós pedimos para o sistema ordenar a partir do número 100. Esperamos que não exista uma coluna de número 100, portanto, a resposta desejada ao clicar em *View Account Details* é uma *exception*. Ao rolarmos a página para baixo, teremos o seguinte:



Ele nos informa que não conhece a coluna de número 100. Desta maneira, podemos intuir que temos uma coluna entre `2 e 100`. E para descobrir o número máximo de colunas? É preciso chegar em um limiar onde comecem as *exception*. Vamos testar manualmente isso utilizando os números 3, 4, 5 , 6, 7 um de cada vez e, por fim, chegaremos ao seguinte:

```
admin' order by 8 --
```

Teremos no navegador:



Ao recebermos a mensagem `Unknown column '8' in 'order clause'`, temos a certeza de que a tabela possui 7 colunas.