10

Mãos à obra: Quantidade de colunas

Clique na aba:

OWASP 2013 -> A1 - Injection (SQL) -> SQLi Extract Data -> User Info (SQL).

No campo username, peça para que a tabela accounts ordene os valores das colunas 1 e 2.

Depois peça para que a tabela accounts ordene valores de uma coluna que provavelmente não exista, será que por exemplo a tabela accounts tem 50 colunas?

Por fim, vá aumentando gradativamente a numeração a fim de obter qual é o limiar de ordenação que é obtida uma resposta e o limiar de uma coluna inexistente. Qual foi esse valor?

Lembre-se: Eu posso pedir para que uma coluna seja ordenada através do **order by**. Não sabemos qual é a senha do usuário admin, mas isso é um problema?