**ATIVIDADE TI7 REC FRANCISLEY FERNANDES DE SOUZA**

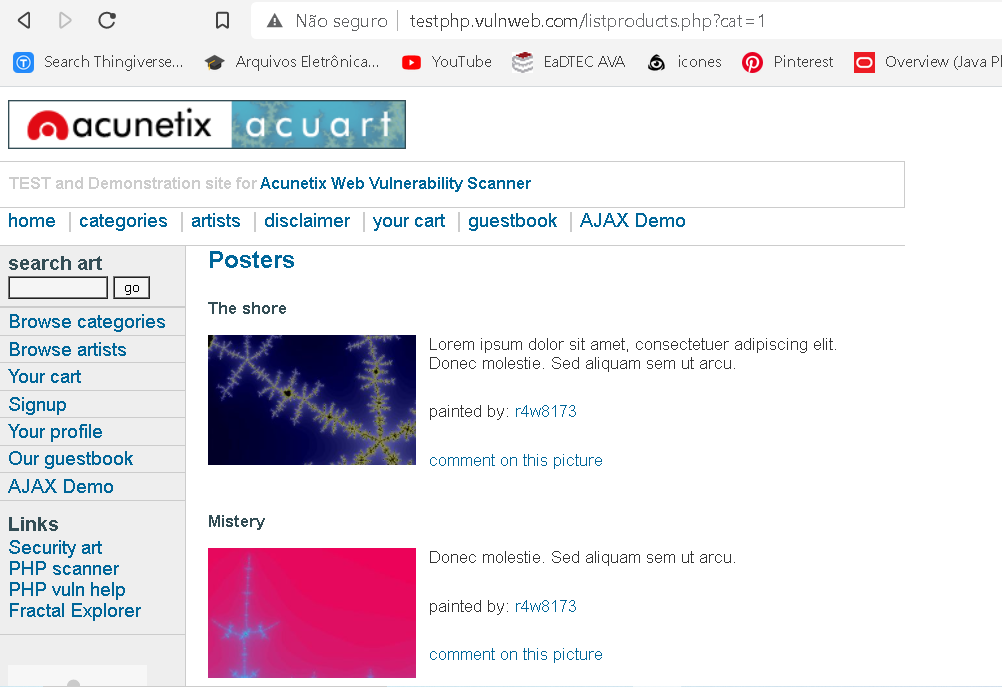
O exercício deve ser entregue em documento do formato Word no ambiente virtual de aprendizagem. Observação: explique como cada comando em SQL se comporta ao ser executado

SQL INJECTION é uma técnica de invasão de sistemas web, que consiste em enviar comando em sql no formulários, e estes comando são executados no banco de dados, onde o invasor consegue realizar comandos de pesquisas, de inserção ou modificação diretamente no banco da aplicação.

um exemplo que demonstrarmos esta vulnerabilidade e o site <http://testphp.vulnweb.com/index.php> e um site feito para testar tipos de ataques, somente para aprendizado academico.



para começar vou entrar na aba categorias



pelo endereço da url e possivel verificar que e feito uma pesquisa no banco de dados solicitando as categorias do tipo 1

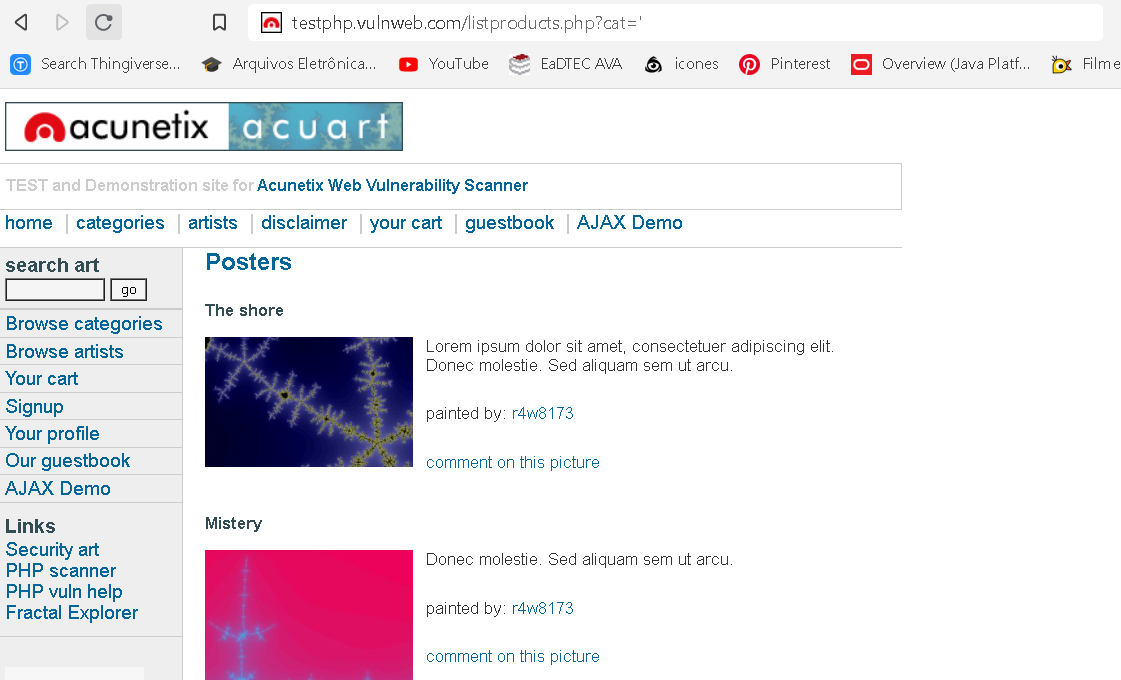
no banco de dados, este comando seria algo do tipo

SELECT CATEGORIA FROM TABELA

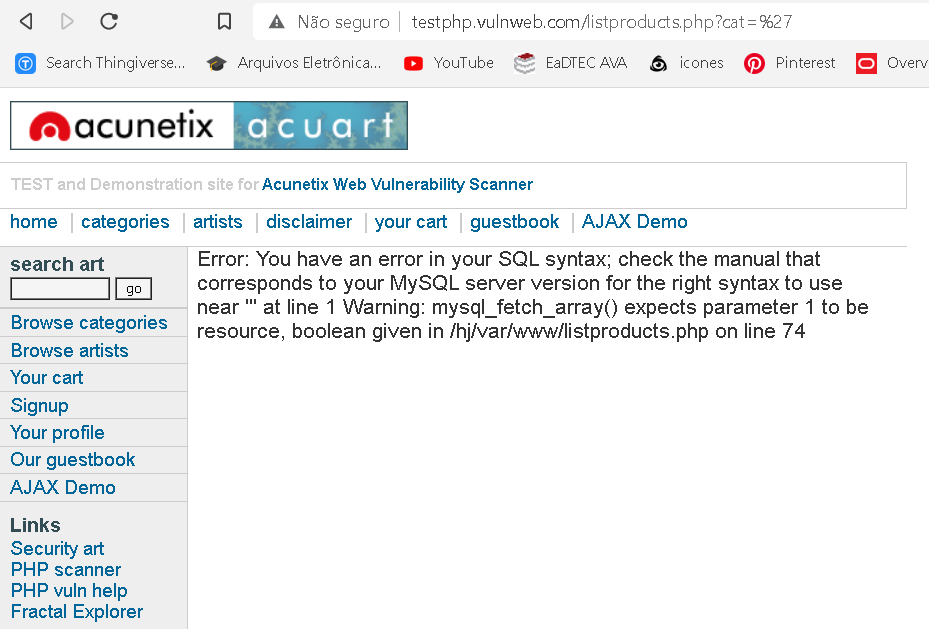
WHERE ID\_CATEGORIA = 1;

esta query realiza uma busca no banco de dados e retorna as categorias que são com o id = 1;

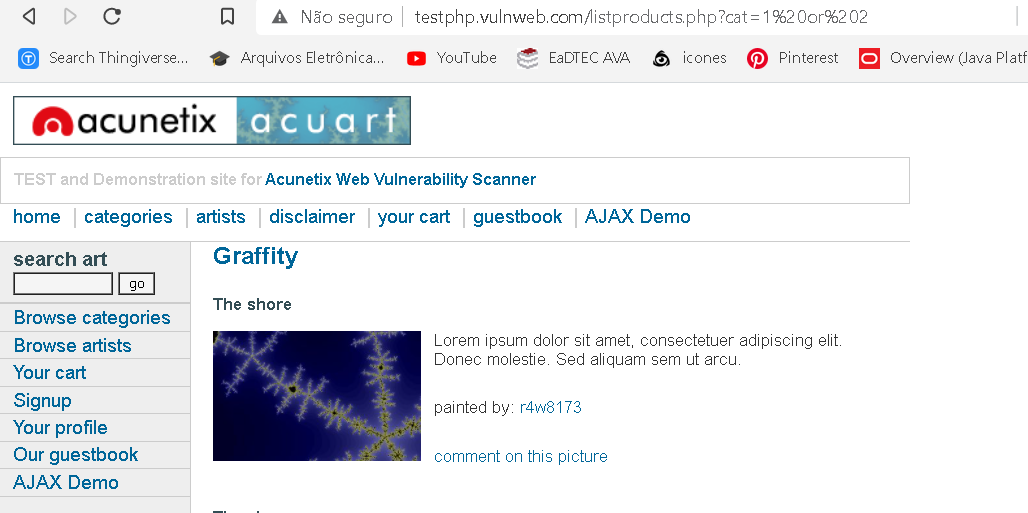
para saber sobre a vulnerabilidade inserimos aspas na pesquisa na url no lugar do numero 1,



lancado isso temos o retorno de erro no banco de dados sobre erro de sinstaxe sql

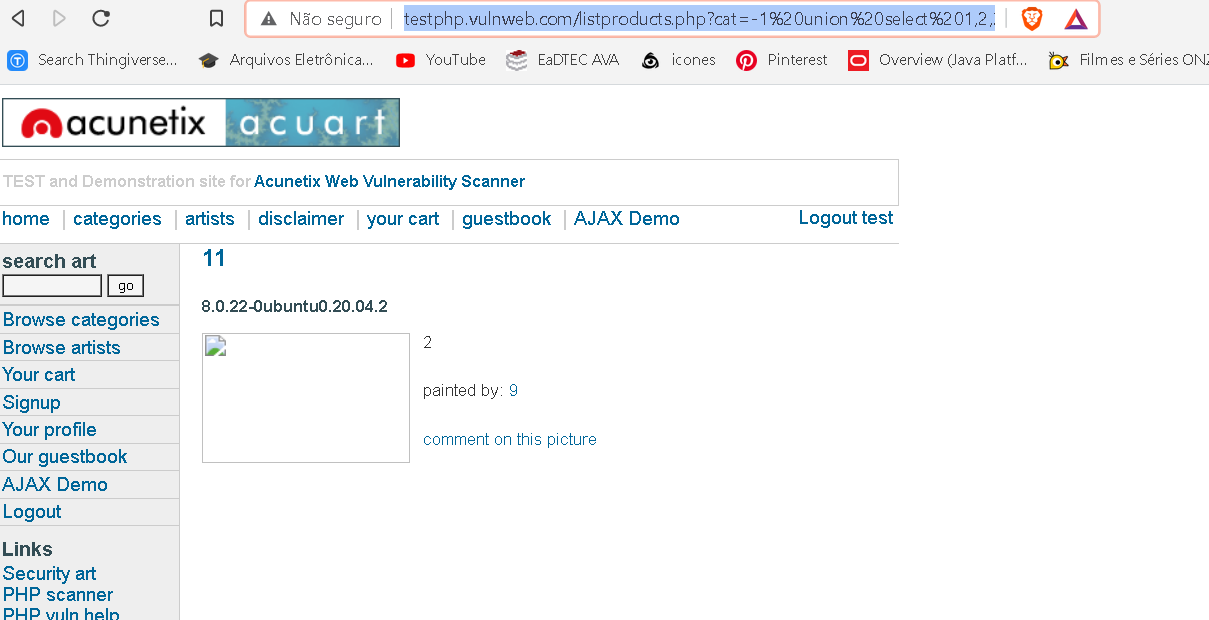


se lançarmos por exemplo na url o valor 1 or 2 conseguirmos as duas categorias.



ou seja estamos manipulando o banco de dados do site.

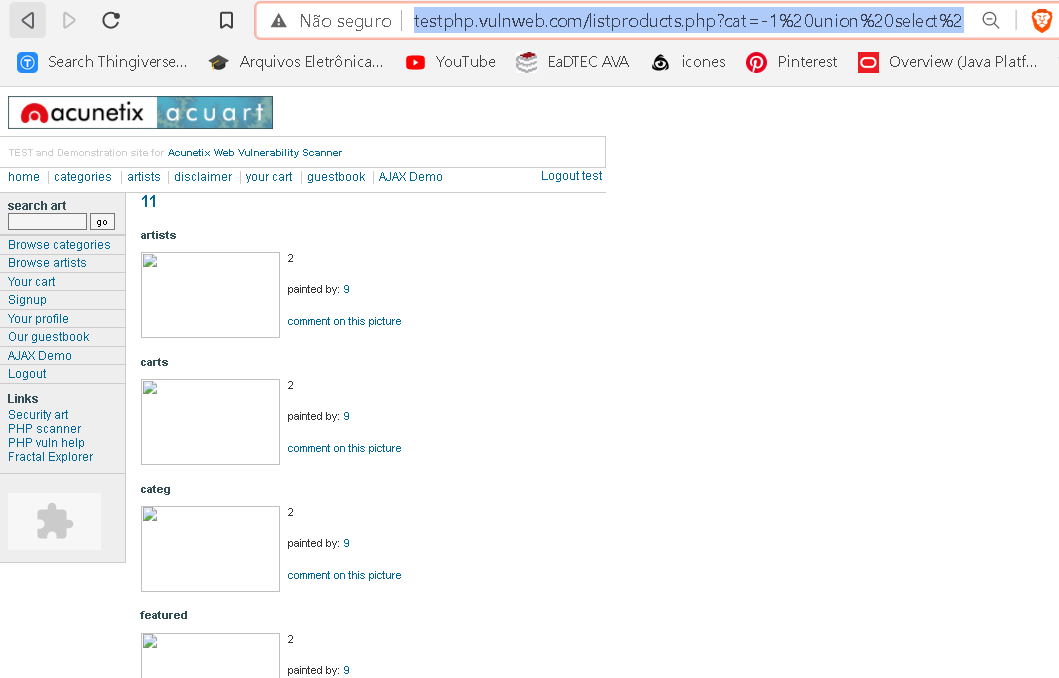
<http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,version(),8,9,10,11> inserir o -1 para não voltar os dados do primeiro select e na segunda solicito a versão do banco de dados



e exibido na tela a versão 8 e que esta usando linux ubuntu 20.04.2

desta forma consigo inserir varios comando na propria url que ela e executada direto no banco de dados, posso tmb ficar um describe das tabelas, descobrir o nome das colunas, inclusive a coluna usuario e senha.

<http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,table_name,8,9,10,11%20from%20information_schema.tables> com esta query ela retorna o nome de todas as tabelas.



desta forma temos nos prevenir contra estas vulnerabilidades, não permitindo os comandos sql direto via string ao banco de dados.