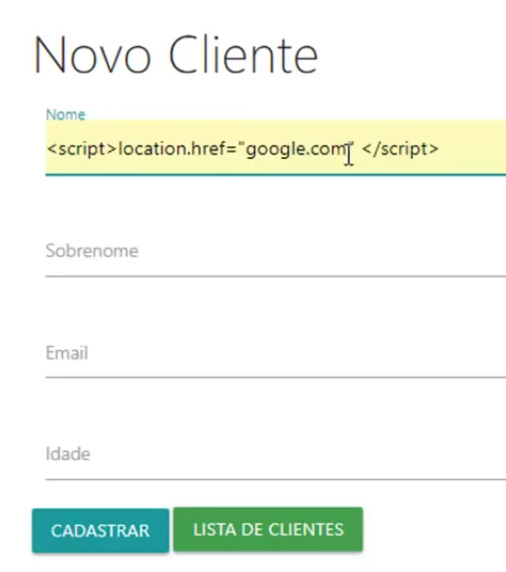
Já vi aprendi sobre "MySQL\_Injection" que é quando hackers se aproveitam de falhas no sistema

para inserir códigos SQLs através dos nossos Inputs sem tratamento.

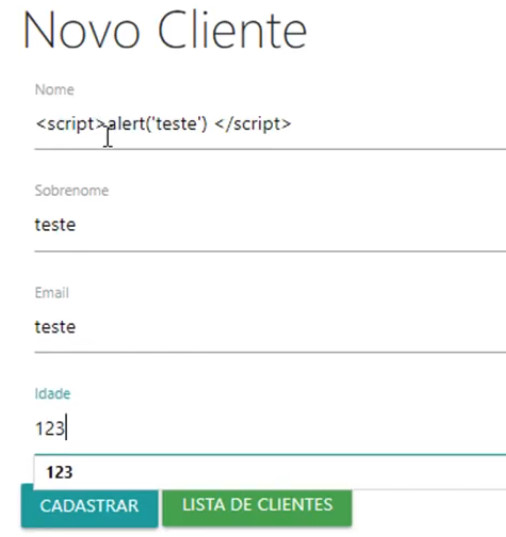
E vi como se previnir que é usando a função: mysqli\_escape\_string().

Outro tipo de ataque é o Cross\_Site\_Scripting que é semelhante ao MySQL\_Injection,

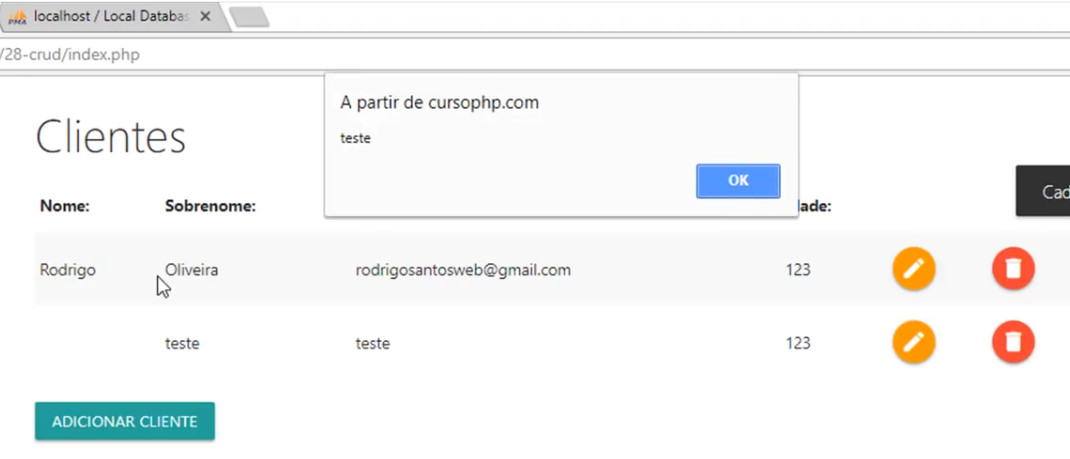
só que em vez de insirir comandos "SQL" o invasor inseri "Scripts" nos inputs.



Ou



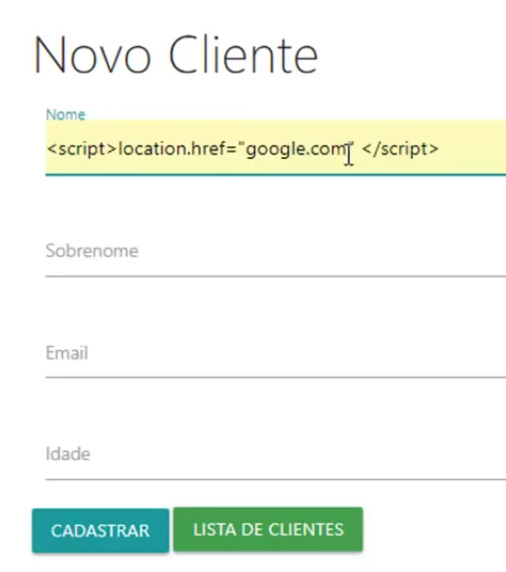
Resultado:



Toda vez que a pagina index ser aberta ela apresentará uma alerta (“Test”). Porque no lugar do nome tem um código ou Script.



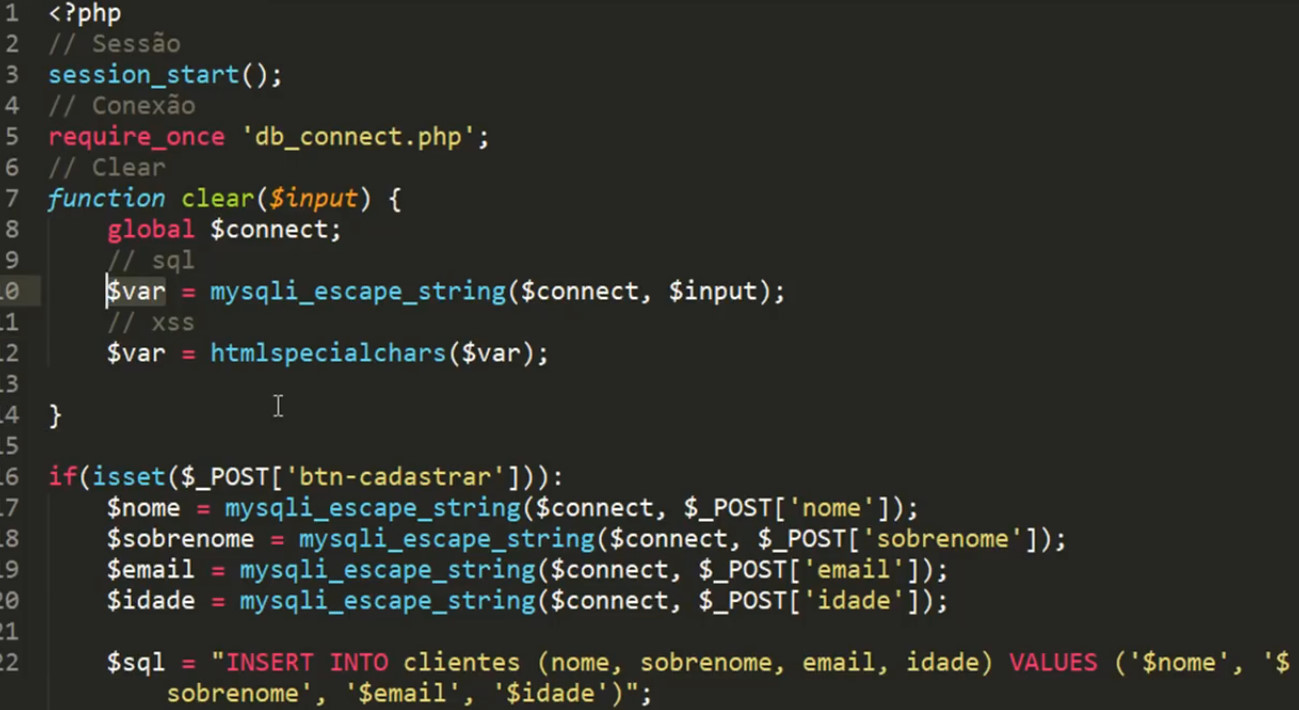
Outro exemplo:



O Script acima fará com que cada vez que a pagina index for actualizada será redirecionada para o google.



COMO RESOLVER ?



Para não fazer htmlspeacialchars(mysqli\_escape\_string($connect, $\_POST[‘’nome’]));

Decidimos criar uma função para fazer as duas ao mesmo tempo.



Ele aparece o script na tabela mas perdeu a ação, porque na BD as tags foram substituidas por characteres;

