Pergunta 1.1

SELECT * FROM user_data WHERE last_name = 'Your Name'

Como a *query* é realizada colocando o nome em “your name”, pode-se introduzir uma tautologia na *query*, através de, por exemplo, colocando como último nome, **' or 1=1 or last_name = 'teste.** Assim, é fechada a aspa inicial, colocada a tautologia, e é criada outra condição para fechar a última aspa.

Pergunta 1.2

Visto que, a opção de input agora são opções num *spoiler*, de modo a efetuar a tautologia, teremos de alterar o código HTML. Sendo assim, ao acedermos ao código da página (através da inspeção da página), e inspecionando o spoiler, alteramos o valor da opção “Colombia” para **1 or 1=1.**

Pergunta 1.3

Para atualizar o salário, basta realizar uma *query* “update”, depois de introduzido o id. **101; update employee set Salary=100000 where UserID = 101**

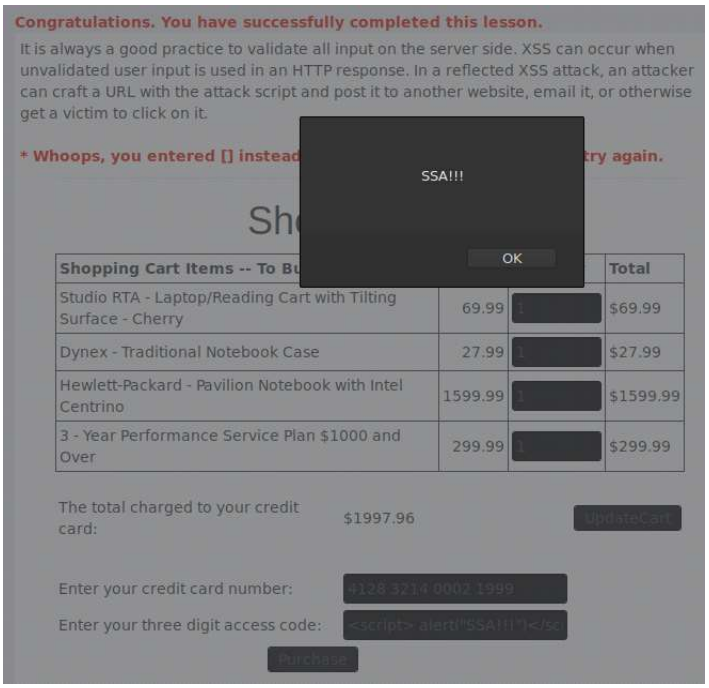
De modo a inserir um backdoor, que neste caso, acrescenta ao salário 10000 por cada utilizador adicionado, realiza-se os mesmos passos realizados anteriormente, mas neste caso, cria-se um “trigger”. **101; CREATE TRIGGER myBackDoor BEFORE INSERT ON employee FOR EACH ROW BEGIN UPDATE employee SET Salary=Salary+10000 WHERE userid = 101**

Pergunta 2.1

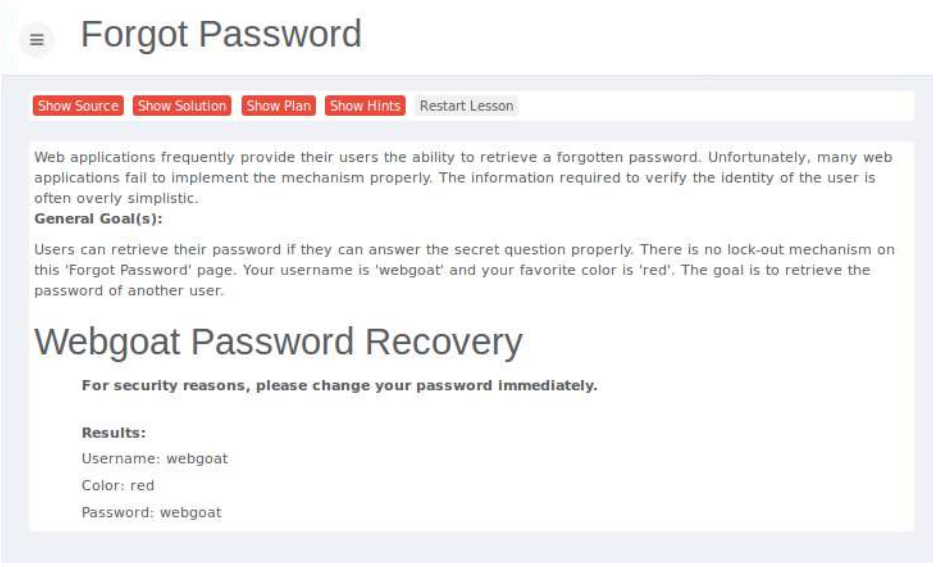
Para demonstrar este ataque tentou-se introduzir letras nos campos “Quantity” mas verificou-se que estes alteravam o valor total para 0. Isto leva-nos a crer que existe uma validação na parte destas mesmas quantidades que force a que este valor seja expresso por um inteiro.

Da mesma maneira verificou-se que o campo relativo aos dados do cartão não está suscetível a este ataque. Depois de várias tentativas, conclui-se que apenas o campo

relativo ao CCV poderá ser utilizado para explorar esta vulnerabilidade, pelo que foi neste que se introduziu a *script* maliciosa. O resultado obtido pela sua execução é o apresentado na imagem seguinte.



Pergunta 3.1



1. Aparece na janela a password do utilizador webgoat, que também é webgoat.

2. Geralmente num sistema existem contas de utilizadores e contas de administradores, quando se tenta invadir e ter acesso a um sistema, o ideal é obter as credenciais de uma conta de administrador devido aos privilégios que esta obtém, sendo assim mais fácil obter dados e comprometer o sistema. Ao tentar aceder a essa, à semelhança da anterior pede a cor favorita do utilizador.

3. Uma vez que o número de cores é um espectro bastante limitado, um simples ataque de força bruta conseguir-se-ia facilmente em pouco tempo obter a password da conta, porém no caso de se conhecer a identidade do administrador em questão utilizando engenharia social, poder-se-ia até saber exatamente qual a sua cor favorita, ou qual a resposta a uma outra qualquer pergunta de segurança do mesmo género.
   Neste caso foi utilizada a força bruta, tendo-se tentado primeiramente com “blue” e de seguida com “yellow” obtendo assim as credenciais do administrador de sistema.