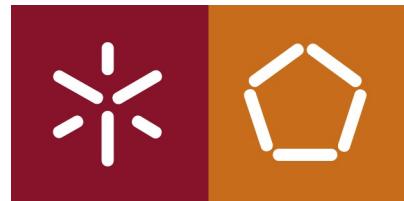


Universidade do Minho



Mestrado Integrado em Engenharia Informática
Engenharia de Segurança

Aula 12

Grupo 8



João de Macedo
A76268



João Aloísio
A77953



Nelson Gonçalves
A78173

24 de Maio de 2020

1 Injection

Inicialmente foi pedido para ser obtido o departamento do trabalhador "Bob Franco". Para isso foi feito o comando **SELECT DEPARTMENT FROM Employees WHERE first_name = 'Bob';**

No passo 3 foi pedido para alterar o valor de "DEPARTMENT" para "Sales" do empregado "Tobi". Para isso foi feito o comando **UPDATE Employees SET DEPARTMENT = 'Sales' WHERE first_name = 'Tobi';**

No passo 4 foi pedido para adicionar a coluna "phone" a tabela "employees". Para isso foi feito o comando **ALTER TABLE employees ADD phone varchar(20);**

No passo 5 foi pedido para alterar as permissões do grupo "UnauthorizedUser" e permitir que este alterem a tabela. Para isso foi deito o comando **GRANT ALTER TABLE TO UnauthorizedUser;**

No passo 9 foi dada hipóteses para obter a lista completa de utilizadores e para isso foi escolhida a opção "Smith' or '1' = '1".

No passo 10 foi pedido para descobrir que campo era vulnerável dos dois fornecidos. Foi descoberto através do 0, sendo o segundo campo o vulnerável inserindo assim os campos **0, 0 or 1=1**

No passo 11 foi pedido para obter a lista de empregados e para isso foram introduzidos os campos "s, ' or '1' = '1" tal como nos exercícios anteriores, sendo após a query ser analisada.

No passo 12 é pedido para alterar o valor do salário do empregado, sendo que após fechar ';' é possível introduzir uma query à tabela e alterar assim os valores **UPDATE employees SET salary=9999999 WHERE first_name='John'**

No passo 13 é pedido para eliminar a tabela "access_log" e para isso foi usado como anteriormente ';' e feita a query **DROP TABLE access_log;**

2 XSS

Ponto 2:

- Abrir 2 separadores na pagina do webgoat
- Abrir a consola do browser e inserir `alert(document.cookie);`
- Verificar que ambas as cookies são iguais e responder "yes"

ponto 7:

- Inserimos `<script>alert()</script>` na box do cartao de credito
- Obtemos um pop-up alert

- Obtemos tb a seguinte mensagem "Well done, but alerts are not very impressive are they? Please continue."

ponto 10:

- Abrir o debugger
- Ir par a diretoria View
- Abrir GoatRouter.js
- Ver as rotas : 'welcome': 'welcomeRoute', 'lesson/:name': 'lessonRoute', 'lesson/:name/:pageNum': 'lessonPageRoute', 'test/:param': 'testRoute', 'reportCard': 'reportCard'

ponto 11:

- Aceder a rota test
- colocar como parametro o webgoat.customjs.phoneHome()
- substituis o "/"em </script> por %2f
- aceder a "http://localhost:8080/WebGoat/start.mvc#test/ <script>webgoat.customjs.phoneHome()%2Fscript</script>".
- Na consola do browser obetmos a seguinte resposta "phoneHome Response is 661119233"

3 Quebra na Autenticação

4 Componentes vulneráveis

Ponto 5:

Neste ponto conseguimos ver que usando o mesmo código fonte do *WebGoat* mas diferentes versões do componente *jquery-ui*, uma é explorável e outra não. Apenas foi copiado o comando *OK<script>alert('XSS')</script>* para a janela de diálogo.

Ponto 12:

Aqui foi adicionado o comando *<java.lang.Integer>96</java.lang.Integer>*