# A blue and white sign with textSistemas de Segurança de Software

## Mestrado em Engenharia Informática

# Segurança de Software

## Mestrado em Informática

# Class Project: Experiments with WebGoat (class 1)

Gustavo Henriques Nº 64361

Leonardo Monteiro Nº 58250

Maria Figueirinhas Nº 46494

**2. Broken Access Control**

Solving Broken Access Control >> Insecure Direct Object References >> Steps 2 to 5.

Lesson 2: Authenticating as Tom.

Uma imagem com captura de ecrã, texto, file, Retângulo

Descrição gerada automaticamenteDepois de fazer todos os comando no ponto um do pdf fomos à lição referida acima. Ao carregar na lição 2, foi nos pedido para preencher o user com o nome ‘tom’ e a pass como ‘cat’. Deste modo, preenchemos os campos user e pass com ‘tom’ e ‘cat’ e carregamos em ‘Submit’ e apareceu-nos a seguinte imagem:

Lesson 3: Showing the profile attributes that are not listed.

Uma imagem com texto, Tipo de letra, branco, design

Descrição gerada automaticamentePara esta lição o que fizemos foi tratar da configuração do proxy primeiramente. De seguida analisamos no proxy a resposta do servidor, ao carregar em ‘view Profile’ e vimos (no proxy) que os campos escondidos eram o role e o userId como mostra a imagem abaixo:  
Depois disto preenchemos o campo que pedia os atributos que estavam escondidos com ‘role, userId’, obtendo assim a seguinte mensagem de sucesso:

Lesson 4: Finding the path to show user profile.

Uma imagem com texto, Tipo de letra, file, captura de ecrã

Descrição gerada automaticamenteAo analisar o proxy, quando acedemos ao ficheiro <http://localhost:8080/WebGoat/service/lessonoverview.mvc> aparece o path para cada user no formato json.

Com isto foi só preencher o seguinte caminho ‘WebGoat/IDOR/profile/2342384’ no campo de input da lição 4 e completamos assim esta lição:  
  


Lesson 5: See another user’s profile.

Para este exercício usamos a técnica de trial and error. Com isto fomos tentando fazer request com GET em que o user profile era uns valores maiores do que o do Tom. Após algumas tentativas conseguimos ver o perfil de outro user. Para conseguirmos usamos o seguinte GET:

GET [http://localhost:8080/WebGoat/IDOR/profile/2342388 HTTP/1.1](http://localhost:8080/WebGoat/IDOR/profile/2342388%20HTTP/1.1)

Uma imagem com texto, Tipo de letra, Lilás

Descrição gerada automaticamenteCom este GET foi nos dada a seguinte informação:

**3. Path Traversal**

Solving Injection >> Path Traversal >> Steps 2 to 5.

Lesson 2: Upload the file from /home/ss/ptcat.jpg to a location outside the guestss webgoat user.