# 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 2)

Gustavo Henriques Nº 64361

Leonardo Monteiro Nº 58250

Maria Figueirinhas Nº 46494

**2. Broken Autentication**

Solving Identity & Auth Failures >> Password Reset >> Steps 4.

Lesson 4: Retrieving the password.

1. Entre os utilizadores "tom," "admin" e "larry," a conta "admin" é a mais relevante para comprometer, pois geralmente possui os maiores privilégios e controlo sobre o sistema, tornando-a a mais suscetível e valiosa num ataque.
2. Para este exercício fizemos brute force para a cor do admin e descobrimos que era a verde.

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

Descrição gerada automaticamente

1. As perguntas que estão no passo 5 são as seguintes:  
     
   Uma imagem com texto, captura de ecrã, número, software

   Descrição gerada automaticamente

Muitas dessas perguntas de segurança apresentam vulnerabilidades porque as respostas podem ser descobertas através de informações públicas ou deduzidas por pessoas próximas. Dados como o nome do teu primeiro emprego, o apelido de infância ou a cidade onde nasceste são, muitas vezes, partilhados em redes sociais ou acessíveis por conhecidos. Este tipo de perguntas, ao depender de respostas que podem ser obtidas ou adivinhadas, reduz a eficácia das perguntas de segurança, tornando-as um alvo fácil para ataques de engenharia social.

Solving Identity & Auth Failures >> Secure Passwords >> Step 4.

Uma imagem com texto, captura de ecrã, software, número

Descrição gerada automaticamente  
**R:** Primeiro começamos por testar umas das passwords sugeridas e observamos que eram muito fracas:  
  
Ao metermos a pass ‘Oteugato\_123’ conseguimos chegar a uma password que é 4/4 segura.

Uma imagem com texto, captura de ecrã, software

Descrição gerada automaticamente

Solving Sensitive Data Exposure >> Insecure Login >> step 2

Uma imagem com texto, software, número, Ícone de computador

Descrição gerada automaticamente**R:** Para esta lição o que fizemos foi pôr um break entre a aplicação e o servidor e, ao carregar no botão de login foi feita, desta forma, uma request para o servidor. Depois disto fomos avançando passo a passo até aparecer os dados do user no proxy, como é possível ver abaixo:

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

Descrição gerada automaticamenteCom isto foi só pôr estes dados nos campos de input que apareciam na lição e completamos assim a mesma:  
  
Solving Identity & Auth Failure >> Authentication Bypasses >> step 2

1. Uma imagem com texto, Tipo de letra, captura de ecrã

   Descrição gerada automaticamenteComeçarmos por responder às perguntas da seguinte maneira:
   1.  Para este exercício o que fizemos foi apanhar a request ao carregar no botão Submit no proxy. De segui alteramos o nome dos campos, desta maneira é gerado um erro do servidor que nos deixa fazer o login à mesma, porque os campos não foram apagados, mas sim foram alterados os seus nomes:

Uma imagem com texto, file, captura de ecrã

Descrição gerada automaticamenteCom isto conseguimos completar esta passo:

Solving Identity & Auth Failure >> JWT tokens >> step 4

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

Descrição gerada automaticamenteLesson 4: Finding out the username.  
  
Para isto abrimos o WebWolf fizemos login com username guestss e pass guestss. De seguida abrimos o JWT e metemos para lá o token e conseguimos assim obter o username:  
  
Uma imagem com texto, captura de ecrã, Tipo de letra, file

Descrição gerada automaticamente Depois disto metemos o username no input pedido e completamos assim mais uma lição:

**3. XML External Entities (XXE)**

Solving Security Misconfigurations >> XXE >> step 4.

Lesson 4: Listing all the files in the root directory.

Uma imagem com captura de ecrã, texto, software, Página web

Descrição gerada automaticamenteNesta lição começamos por enviar um simples comentário e obtivemos a seguinte conversa:

Depois disto intercetamos a request no proxy e mudamos para o seguinte:

<?xml version="1.0"?>

<!DOCTYPE foo [

<!ENTITY xxe SYSTEM "file:///">

]>

<comment>

<text>&xxe;</text>

Uma imagem com texto, captura de ecrã, mamífero, Página web

Descrição gerada automaticamente</comment>  
  
Com isto conseguimos obter a lista dos ficheiros que estão na root, como mostra a imagem abaixo:

**4. Server-Side Request Forgery (SSRF)**

Solving Security Misconfigurations >> XXE >> step 4.

Lesson 2: Retrieving the jerry picture.

Uma imagem com texto, captura de ecrã, software, Ícone de computador

Descrição gerada automaticamenteNesta lição intercetamos mais uma vez o request no proxy e alteramos o nome de tom para jerry, como mostra a imagem:

Depois disto voltamos ao WebGoat e conseguimos ver a imagem do jerry:  
Lesson 3: Getting information from <http://ifconfig.pro>.

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

Descrição gerada automaticamentePara esta lição, mais uma vez intercetamos a request no proxy e alteramos o url para o que mostra a imagem:

Depois disto voltamos ao WebGoat e vimos que que conseguimos obter informação do <http://ifconfig.pro>, como mostra a imagem:  
  
