



**ESCOLA  
SUPERIOR  
DE TECNOLOGIA  
E GESTÃO**

## **Trabalho Prático**

# **Segurança em Aplicações Web**

Cursos Técnicos Superiores Profissionais (CTeSP)

Cibersegurança, Redes e Sistemas Informáticos

Desenvolvimento para a Web e Dispositivos Móveis

**Docentes:**

Almerindo Oliveira – [ajo@estg.ipp.pt](mailto:ajo@estg.ipp.pt)

Filipe Oliveira – [fvo@estg.ipp.pt](mailto:fvo@estg.ipp.pt)

Hugo Barbosa – [hfab@estg.ipp.pt](mailto:hfab@estg.ipp.pt)

Rui Bento – [rmbs@estg.ipp.pt](mailto:rmbs@estg.ipp.pt)

2025/2026

## 1. Destinatários

Este trabalho destina-se a todos os estudantes inscritos na disciplina de Segurança em Aplicações Web. Os trabalhos devem ser efetuados por grupos de dois estudantes tendo estes a possibilidade de escolha dos elementos do grupo. Excecionalmente, e quando se justifique, poderão ser considerados grupos com outro número de elementos.

Os elementos de um mesmo grupo podem ter classificações diferentes.

## 2. Objetivo

O objetivo do trabalho consiste na elaboração de uma aplicação Web em PHP e MySQL que sirva de apoio à **Gestão de um Stand Automóvel**, contendo o seguinte conjunto de funcionalidades:

- Registo de utilizadores;
- Recuperação da conta (“Forgot me”);
- “Remember me”
- Autenticação
- Três áreas:
  - Uma área pública visível para todos os utilizadores (registados e não registados)
    - Devem ser listadas todos os veículos, mas sem informação do seu estado.
  - Uma área para utilizadores registados (utentes)
    - Contendo um perfil do utilizador
      - Um utilizador pode associar uma imagem ao seu perfil
      - Alterar os seus dados
      - Não pode ter acesso ao perfil dos outros utentes
    - Contendo uma área para consulta dos carros com filtros tais como Marca e Ano de fabrico.
    - Possibilitar requisitar um test drive para um determinado dia e hora. Quando é feita a requisição de um veículo, este deve passar

a indisponível para reserva num determinado dia e hora. Atenção: Só pode ser marcado um test drive por dia/hora, uma vez que só uma pessoa está disponível para acompanhar.

- Deve ser possível ter acesso a uma listagem de todas as reservas já realizadas por si.
- Uma área para Administração
  - Contendo um perfil do Administrador
  - Contendo uma listagem dos utilizadores existentes
  - Uma área que permita fazer a manutenção dos veículos, inserir, alterar, eliminar com indicação do seu estado (disponível, indisponível, brevemente)
  - Deve considerar que são várias as características de um veículo, tais como: Marca, Modelo, Cor, Combustível, Ano de fabrico, Km, NºPortas, Lugares, Fotos, etc.
  - Uma área com a listagem de marcações de test drive por dia/veículo.

A acompanhar o trabalho desenvolvido deve estar um relatório que documente toda a aplicação e onde sejam documentadas todas as ações de segurança, ou outras, que considere relevantes.

No relatório indique quais as técnicas que utilizou para garantir a segurança da plataforma, para além da estrutura do seu site e configurações / permissões que considere necessárias.

### 3. Outras informações:

- ☐ Valide tudo;
- ☐ Parametrize o sistema para ser de fácil alteração e manutenção
- ☐ Crie um sistema de tratamento de erros;
- ☐ Pode e deve complementar o trabalho com funcionalidades extra.

As informações fornecidas no enunciado são propositadamente vagas. Justifique adequadamente as decisões que tomar.

Deverão ser introduzidos dados iniciais (de arranque) de forma a testar a base de dados, devendo estes representar informação verosímil (ex: não é permitido o nome do utente ser “skjdajdk”).

A originalidade assim como a diversidade das funcionalidades será muito valorizada.

Cada grupo deverá cumprir todos os prazos estipulados, podendo ser anulada a avaliação do grupo em caso contrário. Abaixo, na devida secção será abordada toda a informação relativa aos prazos.

**A deteção de trabalhos fraudulentos invalida a nota do estudante. Serão considerados trabalhos fraudulentos, aqueles onde se verifique trabalho desenvolvido por pessoas que não o estudante, na totalidade do trabalho ou apenas em parte deste.**

#### **4. Prazos**

A entrega do trabalho deve seguir o seguinte modelo:

**SAW\_AMT\_8290XXX.zip - alunos de Amarante**

**SAW\_FEL\_8290XXX.zip - alunos de Felgueiras**

**SAW\_LSD\_8290XXX.zip - alunos de Lousada**

O número é o correspondente ao número do estudante, e deverá ser num documento ZIP. A sua entrega será via **Moodle** até à data limite lá indicada. Dentro de cada ficheiro zip, os alunos devem ser responsáveis pela colocação de todos os ficheiros necessários para avaliação do trabalho e também do relatório que deverá estar no formato “PDF”.

## 5. Defesa

Todos os trabalhos estão sujeitos a defesa por parte do aluno que o elaborou. A defesa decorrerá na data para avaliação definida no *Moodle*. A não comparência de um aluno à defesa implica a não consideração do trabalho para a nota do aluno em questão. Durante a defesa poderá ser colocada qualquer questão lecionada na UC assim como a implementação/alteração de funcionalidades do trabalho.

## 6. Outras Situações

Caso o trabalho não seja entregue até à data definida nas regras, o trabalho será considerado como não entregue. Ficará assim impedido comparecer na data de Exame, para realizar a sua defesa.

## 7. Avaliação

Componente	Peso Nota Final
Segurança e utilização da aplicação	45%
Validação de dados introduzidos	15%
Simplicidade e organização do código	5%
Facilidade de utilização	5%
Parte gráfica	5%
Qualidade do relatório	5%
Apresentação e Defesa do Trabalho Prático	20%
<b>Total</b>	<b>100%</b>