“The BMI Mystery: Can You Uncover the Clues?”- WRITE-UP

- The BMI Mystery: Can You Uncover the Clues?
- Oh no it looks like you've accidentally broken the register while trying to log in! Your password is all messed up, and you can't seem to remember it. Can you figure out a way to log in despite the broken register and scrambled password?
- Web - easy
- SQL Injection && Path Transversal

Neste desafio não é suposto fornecer os ficheiros aos jogadores, mas sim disponibilizar pistas textuais que possam ser usadas para completá-lo. Quando os jogadores acedem à aplicação web, é apresentada uma página de registo, como mostrado na figura 1:

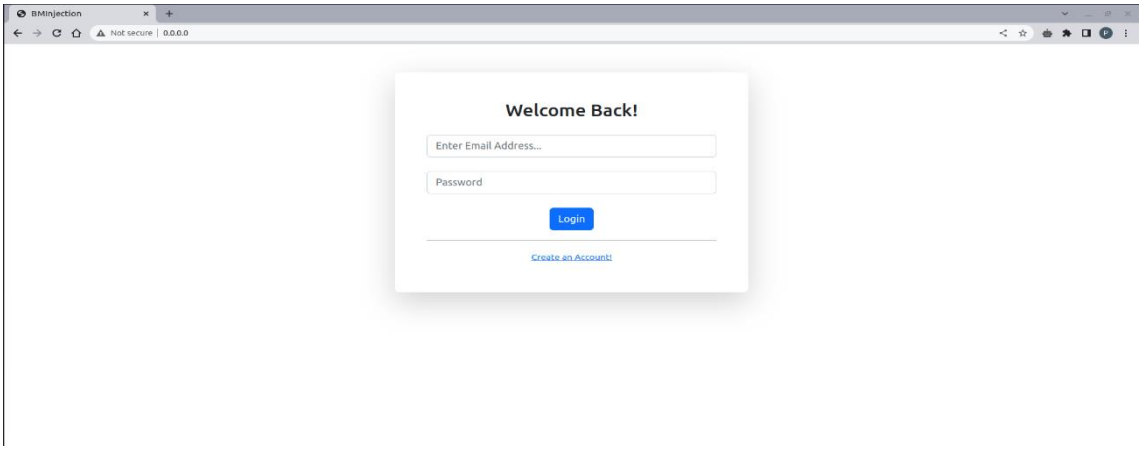


Figura 1 - Página de Login

Ao carregar no botão para criar uma conta e criando a mesma com um nome email e senha, é exibida uma mensagem de alerta a informar que a conta foi criada, mas devido a um erro na gravação dos dados, a senha foi cifrada e não pode ser usada para iniciar sessão, como mostrado na figura 2.

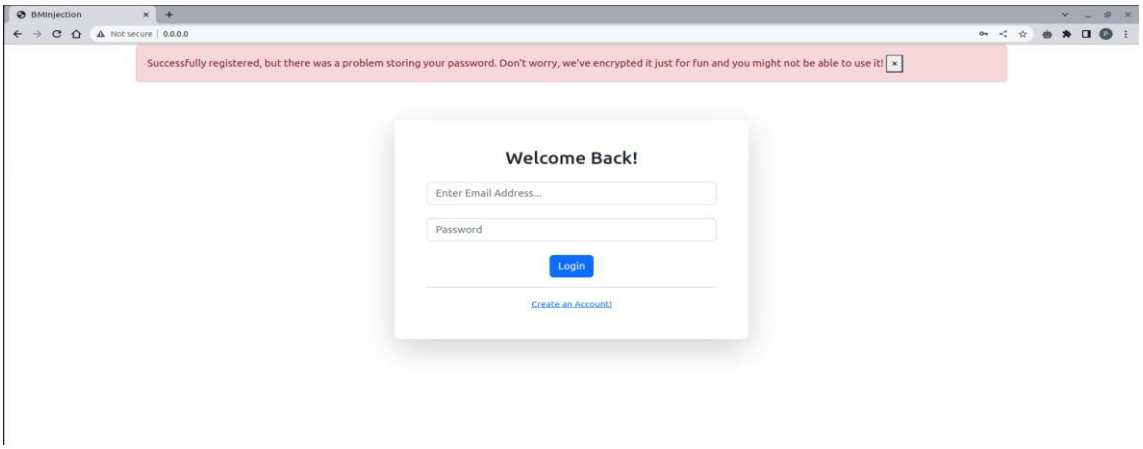
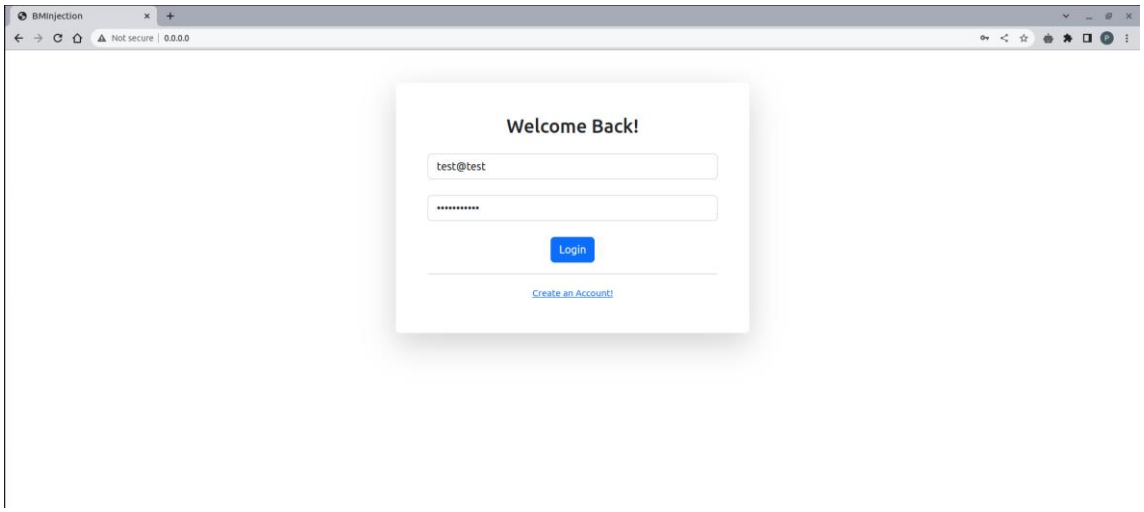
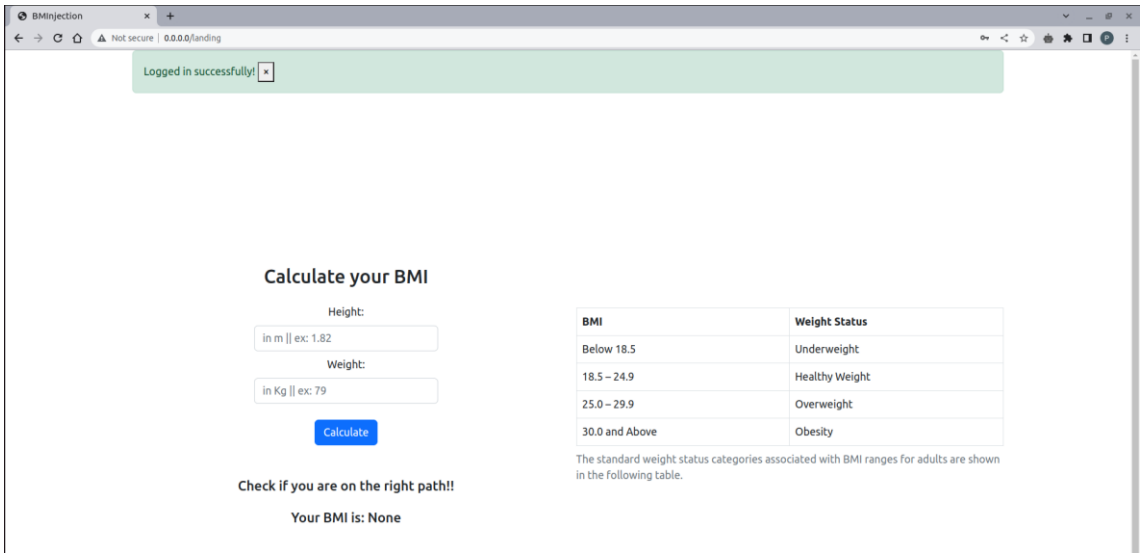


Figura 2 - Página de Login após registo

Para entrar na aplicação agora, o utilizador precisa de inserir o nome de utilizador de uma conta existente na base de dados e realizar uma injeção SQL no campo da senha. Um payload possível para conseguir iniciar sessão seria " ' OR ‘1’=’1 ", como mostrado na figura 3. Dessa forma, a aplicação irá primeiro buscar o utilizador e, caso ele exista, vai executar uma query SQL vulnerável que, ao retornar true, fará com que a sessão seja iniciada com esse utilizador.



Ao iniciar sessão, é apresentada a página mostrada na figura 4, onde é possível ver uma tabela com os diferentes níveis de índice de massa corporal e vários campos que podem ser preenchidos para calcular esse índice. Há também uma frase que revela uma pista "Check if you are on the right path".



Essa frase tem um segundo significado que sugere que é possível alterar o URL para tentar aceder à flag. Ao colocar "localhost:/flag" no url, é apresentada a flag (meter aqui a flag), como mostrado na figura 5.

Referências:

Link repositório: https://github.com/Torrakanor611/BMInjection.git