PICKTRAVEL

# SEGURANÇA

| Categoria | Descrição | Resultado | Seguro |
|---|---|---|---|
| Injecting PHP | Introdução do segunte texto na caixa de entrada de uma nova mensagem: <?php echo "olá<br />mundo"; ?> | Os caracteres especiais são convertidos, escrevendo na base de dados o respectivo código html. Na página é apresentado o texto exactamente como foi inserido | ✓ |
| Injecting SQL | Introdução do segunte texto na caixa de entrada de uma nova mensagem: mysql_query("DELETE FROM users WHERE idUser='1'"); | Os caracteres especiais são convertidos, escrevendo na base de dados o respectivo código html. Na página é apresentado o texto exactamente como foi inserido | ✓ |
| Injecting Javascript | Introdução do segunte texto na caixa de entrada de uma nova mensagem: <script>alert('ola')</script> | Os caracteres especiais são convertidos, escrevendo na base de dados o respectivo código html. Na página é apresentado o texto exactamente como foi inserido | ✓ |
| URL | Tentativa de introdução na barra de URL do endereço http://weblab.epaveiro.edu.pt/wtgwws/profile.php | Caso o utilizador não esteja autenticado, o portal é reencaminhado para a página de entrada (index.php) | ✓ |
| Variáveis $_GET | Manipulação da varável idview (directamente na barra de URL) no endereço http://weblab.epaveiro.edu.pt/wtgwws/destinations.php?id=2 | Caso não exista o valor inserido o portal é reencaminhado para a página de entrada (index.php) | ✓ |

| | | | |
|---|---|---|---|
| Variáveis $_GET | Manipulação da varável idview (directamente na barra de URL) no endereço http://weblab.epaveiro.edu.pt/wtgwws/profile.php?idview=2 | Caso não exista o valor inserido o portal é reencaminhado para a página de entrada (index.php) | ✓ |
| Variáveis $_GET | Tentativa de introdução na barra de URL do endereço http://weblab.epaveiro.edu.pt/wtgwws/destinations.php?id=2&action=removePost&result=true&postid=6 | Caso o utilizador não esteja autenticado, o portal é reencaminhado para a página de entrada (index.php) | ✓ |
| Variáveis $_GET | Tentativa de introdução na barra de URL do endereço http://weblab.epaveiro.edu.pt/wtgwws/destinations.php?id=2&action=removeReply&result=true&postid=6 | Caso o utilizador não esteja autenticado, o portal é reencaminhado para a página de entrada (index.php) | ✓ |
| Manipulação de Javascript | Alteração do valor da variavel "str" (campo de pesquisa) para passar pela função de verificação de número mínimo de caracteres, utilizando o Firebug | A validação não é efectuada do lado do servidor, apenas do lado do cliente, sendo portanto vulnerável a esta intrusão | ✗ |
| Manipulação de Javascript | Edição da propriedade "onclick" do elemento "post_submit" (botão de enviar comentário). Removendo esta propriedade a função Javascript de validação não é chamada, passando assim variáveis em branco para o servidor | A validação não é efectuada do lado do servidor, apenas do lado do cliente, sendo portanto vulnerável a esta intrusão | ✗ |

Não testámos a segurança (ecriptação) de variáveis do tipo $_POST (nem foi tecnicamente implementada), pois consideramos que para total segurança a esse nível o ideal será que o site corra sob o protocolo https e não http.