

RESILIA

Módulo 1.19: Dados, código, tipos e hacknagem

Tarefa em aula:

- Exemplo de injeção de código durante a aula;
- [Fazer em grupos] 1) Dada a página a seguir:

```
<!DOCTYPE html>
<html lang="pt-BR">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Página top</title>
  </head>
  <body>
    <h1>Página top</h1>
    <h3>Dados do cartão de crédito:</h3>
    <p>0101 1234 5678 9101</p>

    <input/>
    <button onclick="pesquisa()">Comentar</button>

    <script>

      // Não modificar!!!!
      function pesquisa()
      {
        var input = document.querySelector("input");
        var body = document.querySelector("body");
        body.innerHTML += "<br>" + input.value + "<br>";
      }

    </script>
  </body>
</html>
```

Faça um ataque XSS que busca os dados do cartão de crédito na página SEM MODIFICAR O CÓDIGO FONTE DA PÁGINA

- [Fazer em grupos] 2) Dada a página anterior:
 - Edite o código fonte da página para que ele evite ataques XSS

Tarefa de casa (terminar até amanhã 08/10 ANTES da aula):

- Finalizar os exercícios da aula de hoje (não precisa entregar), pois vamos pedir para apresentar amanhã
- Assista [What is cross site scripting](#) (10 min)
- Assista [Hacking Websites with SQL injection](#) (10 min)