Módulo 1.19: Dados, código, tipos e hacknagem

Tarefa em aula:

- **XSS**:
  - Dada a função a seguir:
    - `document.querySelector("tagDoElemento")`: retorna o primeiro elemento que possui essa tag dentro do seu HTML.
      - Exemplo: Buscar o texto de dentro da tag title:

```
var tituloDaPagina = document.querySelector("title");
console.log( tituloDaPagina.textContent );
```

      - O código acima mostrará o título da página no console, caso ele tenha sido definido dentro da tag `<title>` no seu HTML
  - Dada a página a seguir:

```
<!DOCTYPE html>
<html lang="pt-BR">
    <head>
        <meta charset="UTF-8">
        <title>Página muito confiável</title>
    </head>
    <body>
        <h1>Página muito confiável</h1>
        <h3>Dados do cartão de crédito:</h3>
        <p>0101 1234 5678 9101</p>

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

        <script>

            function comenta()
            {
                // Pegamos o elemento input
                var input = document.querySelector("input");
                // Pegamos o corpo da página
```

```
                var body = document.querySelector("body");

                // Adicionamos o conteúdo do input na página
                body.innerHTML += `<br>`
                body.innerHTML += eval( `"` + input.value +
`".toUpperCase();` );
                body.innerHTML += `<br>`
            }

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

- Faça um ataque XSS que busca os dados do cartão de crédito que está na página **SEM MODIFICAR O CÓDIGO FONTE**. Faça o ataque pela página, inserindo dados no input de comentário.
- Discuta possíveis soluções para o problema

Tarefa de casa (terminar até amanhã 18/12 ANTES da aula):

- Finalizar os exercícios da aula de hoje
- Assista What is cross site scripting (10 min)
- Assista Hacking Websites with SQL injection (10 min)

Material complementar:

- MDN - String
- MDN - Template strings
- MDN - eval