

Programador WEB



Sessões e Segurança com PHP

Adriel Sales



Segurança em PHP



- Para uma aplicação web, **segurança** é uma palavra indispensável.

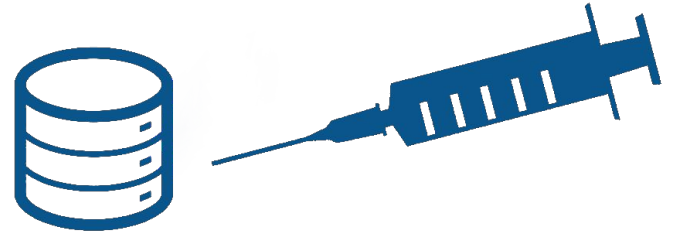
Falhas de segurança mais comuns

- Enviar dados em **texto plano** e não usar **https**.
- Não se proteger da **SQL-Injection**.
- Não diferenciar **páginas restritas** de **páginas públicas** em nosso sistema.



SQL-Injection

- É a inserção de um código SQL em um campo de texto ou parâmetro da URL que será enviado diretamente para o banco.




SQL Injection

SQL-Injection

```
1 <?php
2 // Formato da URL:
3 // http://www.meusite.com.br/produtos.php?id=12
4
5 // Salva o parâmetro da URL numa variável
6 $produto = $_GET['id'];
7
8 // Monta a consulta MySQL
9 $sql = "SELECT * FROM `produtos` WHERE `id` = '". $produto. "' LIMIT 1";
10
11 // Executa a query
12 $query = mysql_query($sql);
13
14 // Salva o resultado (em formato de array) em uma variável
15 $resultado = mysql_fetch_assoc($query);
```

Script
comum
para
consulta de
um
produto.



```
1 SELECT * FROM `produtos` WHERE `id` = '12' LIMIT 1
```

SQL-Injection

```
1 <?php
2 http://www.meusite.com.br/produtos.php?id=' OR 1=1 OR '='
3
4
5 // Salva o parâmetro da URL numa variável
6 $produto = $_GET['id'];
7
8 // Monta a consulta MySQL
9 $sql = "SELECT * FROM `produtos` WHERE `id` = '". $produto. "' LIMIT 1";
10
11 // Executa a query
12 $query = mysql_query($sql);
13
14 // Salva o resultado (em formato de array) em uma variável
15 $resultado = mysql_fetch_assoc($query);
```

Código do mal

```
1 SELECT * FROM `produtos` WHERE `id` = '' OR 1=1 OR '' = '' LIMIT 1
```

SQL-Injection - Solução



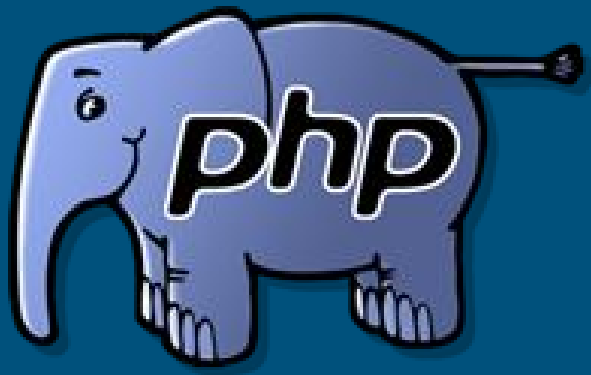
➤ Para dados numéricos:

```
1 // Salva o parâmetro da URL numa variável obrigando-o a ser um valor inteiro
2 $produto = (int)$_GET['id'];
```

➤ Para dados Strings, usar a função:

```
1 <?php
2 $parametro = mysqli_real_escape_string($conexao,$_GET['nome']);
```

Sessões PHP



`$_SESSION`

Sessões PHP

- Recurso que permite armazenar dados entre as requisições no array super global **\$_SESSION**.
- Os valores salvos **podem ser usados** ao longo da visita do usuário, **em qualquer parte do script, mesmo em outras páginas do site.**
- A sessão **estará ativa** e as variáveis **setadas** até o visitante **fechar o browser ou a sessão ser destruída.**

Sessões PHP

- Você **precisa iniciar a sessão** antes de poder **guardar** ou **pegar** valores dela.
- **Não há limite** de valores salvos na sessão.
- **A sessão é pessoal de cada visitante.**



Sessões PHP

```
<?php
```

```
session_start();
```

Iniciando a sessão

```
// Salva o usuário na sessão
```

```
$_SESSION['usuario_nome'] = 'José Maria';
```

Salvando na sessão

```
// Resultado: José Maria
```

```
echo $_SESSION['usuario_nome'];
```

Buscando o dado na sessão

```
// Deleta uma variável da sessão
```

```
unset($_SESSION['usuario']);
```

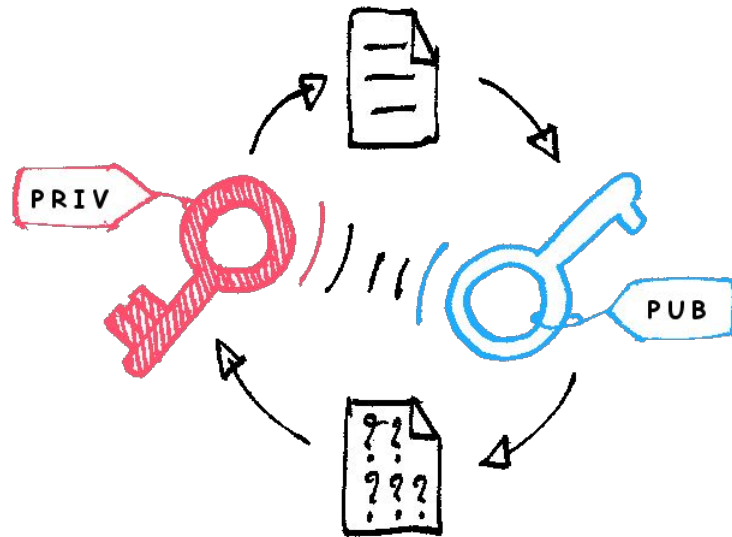
Destruindo apenas uma variável na sessão

```
// Destrói toda sessão
```

```
session_destroy();
```

Destruindo toda a sessão

Algoritmos de Criptografia



Algoritmos de Criptografia

Definição:

criptografia

substantivo feminino

1. conjunto de princípios e técnicas empr. para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; criptologia.
2. em operações políticas, diplomáticas, militares, criminais etc., modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções.

Algoritmos de Criptografia

- **Criptografia de Mão Única: MD5 e SHA1.**
 - Nesse tipo de criptografia, você codifica o texto e, após esse passo, não tem como descobrir o texto original.
- **Criptografia de Mão Dupla: BASE64.**
 - Possibilita a criação de duas funções: uma para codificar e outra para decodificar o texto.

Algoritmos de Criptografia

MD5

Gera uma string alfa-numérica de **32 caracteres**, não importa o tamanho da palavra, o **md5** gerado sempre vai ter **32 caracteres**.

```
$frase1 = 'Curso Programador Web 2017';  
$codificada1 = md5($frase1);  
  
$frase2 = 'números 123';  
$codificada2 = md5($frase2);  
  
echo "Frase 1: $codificada1";  
//Resultado: Frase 1: 242d757f2f4d359e0f65cbca15aa5965  
echo "<br>";  
  
echo "Frase 2: $codificada2";  
//Resultado: Frase 2: 9a739b87falaabcaae073251fcbceab5
```

Algoritmos de Criptografia

SHA1

Praticamente identico ao md5, só que tem 160 bits, o que acaba criando uma string-resultado maior: **40 caracteres alfa-numéricos**.

```
$frase1 = 'Curso Programador Web 2017';  
$codificada1 = sha1($frase1);  
  
$frase2 = 'números 123';  
$codificada2 = sha1($frase2);  
  
echo "Frase 1: $codificada1";  
//Resultado: Frase 1: b34c81ca15b12cf7426d3b7c51beb07af367fa2e  
echo "<br>";  
  
echo "Frase 2: $codificada2";  
//Resultado: Frase 2: 4d54767be4fa01bf9eb720cff625a461da29a198
```


Algoritmos de Criptografia

BASE64

É uma codificação de mão
dupla, e usando uma segunda
função você pode descobrir a
string original de uma string
codificada.

```
$string = 'Curso Programador Web 2017';  
$codificada = base64_encode($string);  
echo "Codificado: $codificada";  
//Resultado: Codificado: Q3Vyc28gUHJvZ3JhbWFKb3IgV2ViIDIwMTc=  
echo "<br>";  
$original = base64_decode($codificada);  
echo "Decodificado: $original" ;  
//Resultado: Decodificado: Curso Programador Web 2017
```

Manipulando Strings

Antes de salvar informações no banco de dados, é importante aplicar alguns padrões de formatação para strings:

strtolower — Converte uma string para minúsculas.

strtoupper — Converte uma string para maiúsculas.

substr_count — Conta o número de ocorrências de uma substring.

substr_replace — Substitui o texto dentro de uma parte de uma string.

substr — Retorna uma parte de uma string.

Manipulando Strings

Antes de salvar informações no banco de dados, é importante aplicar alguns padrões de formatação para strings:

trim — Retira espaço no início e final de uma string.

ucfirst — Converte para maiúscula o primeiro caractere de uma string.

ucwords — Converte para maiúsculas o primeiro caractere de cada palavra.

str_pad — Preenche uma string para um certo tamanho com outra string.



Fontes de Pesquisa



- <http://www.devmedia.com.br/manipulando-datas-com-php/32966>
 - <http://www.php.net/>
 - Principais falhas de segurança no PHP:
<http://blog.thiagobelem.net/principais-falhas-de-seguranca-no-php>
- 