Vulnerability Report

Archivo: ClassUsuario.php

Code Analyzed:

```php
<?php

 class Usuario{

  private $strNombre;
  private $strEmail;
  private $strTipo;
  private $strClave;
  protected $strFechaRegistro;
  static $strEstado = "Activo";

  function __construct(string $nombre, string $email, string $tipo)
  {
   $this->strNombre = $nombre;
   $this->strEmail = $email;
   $this->strTipo = $tipo;
   $this->strClave = rand();
   $this->strFechaRegistro = date('Y-m-d H:m:s');
  }

  public function getNombre():string
  {
   return $this->strNombre;
  }

  public function getEmail():string
  {
   return $this->strEmail;
  }

  public function gerPerfil() {
   echo "<div style='border: 1px solid #ccc; padding: 10px; font-family: sans-serif;'>"; // Contenedor con estilos
   echo "<h2 style='color: #333;'>Datos del usuario</h2>"; // Encabezado

   echo "<p><strong>Nombre:</strong> " . $this->strNombre . "</p>";
   echo "<p><strong>Email:</strong> " . $this->strEmail . "</p>";

   // ¡Nunca muestres la clave real!
   echo "<p><strong>Clave:</strong> " . $this->strClave . "</p>";

   echo "<p><strong>Fecha de registro:</strong> " . $this->strFechaRegistro . "</p>";
   echo "<p><strong>Estado:</strong> " . self::$strEstado . "</p>";

   echo "</div>"; // Cierre del contenedor
  }

  public function setCambiarClave(string $pass){
   $this->strClave = $pass;
  }

 }//End class usuario

 ?>
```

Analysis: ```html

Security Vulnerabilities

Information Disclosure: Sensitive Data Exposure

Type: Information Disclosure - Exposing sensitive information.

Line: Approximately line 31 (`echo "<p><strong>Clave:</strong> " . $this->strClave . "</p>";`)

Description: The `gerPerfil()` method directly outputs the user's password (`$this->strClave`). This is a critical vulnerability, as it exposes sensitive information to anyone who can access the user's profile. The password, even if seemingly random, should never be displayed directly.

Mitigation: Never display the actual password. Instead, display a message like "Password: *******" or remove the password field entirely from the profile output. The actual password should only be used for authentication and stored securely (hashed and salted).

Predictable Password Generation

Type: Weak Password Generation.

Line: Approximately line 15 (`$this->strClave = rand();`)

Description: The password generation uses the `rand()` function, which is not cryptographically secure and produces predictable "random" numbers, making it easier for attackers to guess the password.

Mitigation: Use a cryptographically secure random number generator, such as `random_int()` or `random_bytes()`, to generate stronger passwords. After generating the password, hash it using a strong hashing algorithm like \`password_hash()\` with \`PASSWORD_DEFAULT\` (or PASSWORD_ARGON2I in PHP 7.2+).

Lack of Input Validation/Sanitization in setCambiarClave

Type: Lack of Input Validation/Sanitization.

Line: Approximately line 36 (`$this->strClave = $pass;`)

Description: The `setCambiarClave()` method directly assigns the input `$pass` to `$this->strClave` without any validation or sanitization. This could allow users to set arbitrary values as their password, potentially including malicious code or overly simple passwords.

Mitigation: Implement input validation to ensure the new password meets certain complexity requirements (e.g., minimum length, character types). Also, hash and salt the password before storing it. Consider also rate limiting password change attempts.

Code Quality Metrics

Readability

Issue: The inline CSS in the `gerPerfil()` method reduces readability. Mixing code and presentation logic makes the code harder to understand and maintain.
Improvement: Move the CSS styles to a separate CSS file or use CSS classes instead of inline styles. This promotes separation of concerns and makes the code easier to read and modify. Furthermore the misspelled function name `gerPerfil` also hurts readability.

Coupling

Issue: The `gerPerfil()` method directly outputs HTML, which tightly couples the class to the presentation layer.
Improvement: Separate the data retrieval and presentation logic. The `gerPerfil()` method should return the user data as an array or object, and a separate view or template should be responsible for rendering the HTML. This reduces coupling and makes the code more flexible and testable.

Duplication

Issue: There isn't significant duplication within the provided code snippet, but the concept of a User profile often appears in other locations and should be handled consistently.
Improvement: Ensure that similar output patterns follow DRY principles (Don't Repeat Yourself) and utilize Templates.

Proposed Solution

1. **Never Display the Password:** Remove the line that outputs the password in the `gerPerfil()` method (line 31). Replace it with a generic message, like "Password: *******" or omit the field entirely. 2. **Secure Password Generation and Storage:** * Replace `$this->strClave = rand();` with a cryptographically secure method using `random_bytes()` or `random_int()` and then hash using `password_hash()`. * Example: ```php $this->strClave = password_hash(random_bytes(16), PASSWORD_DEFAULT); ``` 3. **Input Validation and Sanitization:** In the `setCambiarClave()` method, validate the input password `$pass` to ensure it meets complexity requirements (e.g., minimum length, character types, prevent common passwords). Then, hash and salt the password before storing it. ```php public function setCambiarClave(string $pass){ if (strlen($pass) 8) { throw new Exception("Password must be

at least 8 characters long."); } // More validation logic as needed... $this->strClave = password_hash($pass, PASSWORD_DEFAULT); } ``` 4. **Decouple Presentation Logic:** Modify the `gerPerfil()` method to return an array or object containing the user data instead of directly outputting HTML. Create a separate view or template to render the HTML based on this data. 5. **Improve Readability:** Move the inline CSS in the `gerPerfil()` method to a separate CSS file or use CSS classes. Rename the function `gerPerfil` to `getPerfil`.

```
```