BY:

Lucas Andrés Belmonte

VULNERABILIDAD GENERADOR DE PASSWORDS

PUNTOS

01 Idea de la aplicación

La aplicación a desarrollar consiste en un generador de contraseñas robustas a partir de dos campos que rellene el usuario, uno con letras y otro con números.

02 Tecnología de la aplicación web

Ésta, será desarrollada en formato de aplicación web con lenguaje html, css y javascript.

03 Especificar la vulnerabilidad a subsanar

En este caso, el tipo de vulnerabilidad a subsanar será el cross site scripting, que es una vulnerabilidad común en aplicaciones web que permite a los atacantes insertar y ejecutar scripts maliciosos en páginas web vistas por otros usuarios. Estos scripts se ejecutan en el navegador de la víctima, lo que puede dar lugar a ataques como robo de información confidencial, manipulación de contenido, redireccionamiento a sitios maliciosos, entre otros.

04 Vulnerabilidad subsanada

Los navegadores admiten Políticas de Seguridad de Contenido que permiten al autor de una página web controlar desde dónde se pueden cargar y ejecutar JavaScript (y otros recursos). Los ataques XSS se basan en que el atacante pueda ejecutar scripts maliciosos en la página web de un usuario, ya sea mediante la inserción de etiquetas <script> en línea en algún lugar dentro de la etiqueta <html> de una página, o engañando al navegador para que cargue JavaScript desde un dominio malicioso de terceros.

Al establecer una política de seguridad de contenido en el encabezado de respuesta, puedes indicarle al navegador que nunca ejecute JavaScript en línea y que restrinja los dominios desde los cuales se pueden hospedar los archivos JavaScript para una página:

Content-Security-Policy: script-src 'self' https://apis.google.com

Al enumerar las URI desde las cuales se pueden cargar los scripts, estás declarando implícitamente que no se permite JavaScript en línea.
La política de seguridad de contenido también se puede establecer en una etiqueta <meta> dentro del elemento <head> de la página:

<meta http-equiv="Content-Security-Policy"
content="script-src 'self' https://apis.google.com">

¡Este enfoque protegerá muy eficazmente a tus usuarios! Sin embargo, puede requerir una considerable disciplina para preparar tu sitio para ese encabezado. Las etiquetas de scripts en línea se consideran una mala práctica en el desarrollo web moderno, ya que mezclar contenido y código dificulta el mantenimiento de las aplicaciones web, pero son comunes en sitios antiguos o heredados.

05 Códigos html, css y javascript

```
<!DOCTYPE html>
<html>
<head>
  <title>Generador de Contraseña</title>
  <meta http-equiv="Content-Security-Policy" content="script-src 'self'
https://apis.google.com">

  <style>
    body {
      font-family: Arial, sans-serif;
    }
    label {
      display: block;
      margin-bottom: 5px;
    }
  </style>
  <script>
    function generarContrasena() {
      var palabra = document.getElementById("wordField").value;
      var numero = document.getElementById("numberField").value;

      if (palabra.length <= 6 && /^\d{1,4}$/.test(numero)) {
        var caracteresEspeciales = "!@#$%^&*()";
        var contrasena = palabra + numero + caracteresEspeciales.charAt(0) +
caracteresEspeciales.charAt(1);

        contrasena = shuffleString(contrasena);

        document.getElementById("passwordField").value = contrasena;
      } else {
        alert("Por favor, ingresa una palabra de máximo 6 letras y un número de
máximo 4 dígitos.");
      }
    }

    function shuffleString(string) {
      var array = Array.from(string);
      var currentIndex = array.length;
      var temporaryValue, randomIndex;

      while (currentIndex !== 0) {
        randomIndex = Math.floor(Math.random() * currentIndex);
```

```
    temporaryValue = array[currentIndex];
            array[currentIndex] = array[randomIndex];
            array[randomIndex] = temporaryValue;
        }

        return array.join("");
    }

    function enviarCorreo() {
        var email = document.getElementById("emailField").value;

        // Aquí puedes agregar tu código personalizado para enviar el correo electrónico

        alert("El correo electrónico ha sido enviado a: " + email);

        // Limpiar los campos después de aceptar el alert
        document.getElementById("wordField").value = "";
        document.getElementById("numberField").value = "";
        document.getElementById("passwordField").value = "";
        document.getElementById("emailField").value = "";
    }
  </script>
</head>
<body>
  <h1>Generador de Contraseña</h1>

  <form id="passwordForm">
    <div>
      <label for="wordField">Palabra (máximo 6 letras):</label>
      <input type="text" id="wordField" maxlength="6" required>
    </div>

    <div>
      <label for="numberField">Número (máximo 4 dígitos):</label>
      <input type="text" id="numberField" maxlength="4" pattern="[0-9]{1,4}" required>
    </div>

    <button type="button" onclick="generarContrasena()">Generar Contraseña</button>

    <div>
      <label for="passwordField">Contraseña Generada:</label>
      <input type="text" id="passwordField" readonly>
    </div>
```

```
    <div>
        <label for="emailField">Tu dirección de correo:</label>
        <input type="email" id="emailField" required>
    </div>

    <button type="button" onclick="enviarCorreo()">Enviar por correo</button>


  </form>
</body>
</html>
```

```
body {
    font-family: "Roboto", Arial, sans-serif;
    text-align: center;
    padding-top: 50px;
    background-color: #f2f2f2;
}

form {
    display: flex;
    flex-direction: column;
    align-items: center;
}

label {
    margin-top: 10px;
    margin-bottom: 5px;
}

input[type="text"],
input[type="email"] {
    padding: 5px;
    width: 200px;
    margin-bottom: 10px;
    background-color: #fff;
    border: 1px solid #ccc;
}
    cursor: pointer;
}

button:hover {
    background-color: #d4d4d4;
}

#passwordField {
    font-weight: bold;
    margin-bottom: 10px;
}
```

```javascript
function generarContrasena() {
    var palabra = document.getElementById("wordField").value;
    var numero = document.getElementById("numberField").value;

    if (palabra.length <= 6 && /^\d{1,4}$/.test(numero)) {
        var caracteresEspeciales = "!@#$%^&*()";
        var contrasena = palabra + numero + caracteresEspeciales.charAt(0) + caracteresEspeciales.charAt(1);

        contrasena = shuffleString(contrasena);

        document.getElementById("passwordField").value = contrasena;
    } else {
        alert("Por favor, ingresa una palabra de máximo 6 letras y un número de máximo 4 dígitos.");
    }
}

function shuffleString(string) {
    var array = Array.from(string);
    var currentIndex = array.length;
    var temporaryValue, randomIndex;

    while (currentIndex !== 0) {
        randomIndex = Math.floor(Math.random() * currentIndex);
        currentIndex--;

        temporaryValue = array[currentIndex];
        array[currentIndex] = array[randomIndex];
        array[randomIndex] = temporaryValue;
    }

    return array.join("");
}
```

```javascript
}

function enviarCorreo() {
    var email = document.getElementById("emailField").value;

    // Aquí puedes agregar tu código personalizado para enviar el correo electrónico

    alert("El correo electrónico ha sido enviado a: " + email);

    // Limpiar los campos después de aceptar el alert
    document.getElementById("wordField").value = "";
    document.getElementById("numberField").value = "";
    document.getElementById("passwordField").value = "";
    document.getElementById("emailField").value = "";
}
```