



## Integrantes

Agustín Perez Pesce

Mario Cristian Sánchez

Braian Troncoso

Santiago Mendoza

Franco Sebastián Genre

Sebastián Galván

Mariano Farias

Index.html

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-
scale=1.0">
  <title>Organización Empresarial</title>
  <link rel="stylesheet" type="text/css" href="./index.css" />
</head>
<body>
  <h1 class="title">Debuggin Demons</h1>
  

  <h2>Lista ordenada de objetos:</h2>
  <ol>
    <li>auto</li>
    <li>barco</li>
    <li>avion</li>
  </ol>

  <h2>Lista desordenada:</h2>
  <ul>
    <li>auto</li>
    <li>barco</li>
    <li>avion</li>
  </ul>

  <h2>Tabla de productos:</h2>
  <table>
    <thead>
      <tr>
        <th>Nombre</th>
        <th>Código</th>
```



```

        <th>Precio</th>
        <th>Existencia</th>
        <th>Editar</th>
        <th>Eliminar</th>
    </tr>
</thead>
<tbody>
    <tr>
        <td>Producto 1</td>
        <td>12345</td>
        <td>$10.00</td>
        <td>5</td>
        <td>
            <button onclick="editarFila(1)">Editar</button>
        </td>
        <td>
            <button onclick="eliminarFila(1)">Eliminar</button>
        </td>
    </tr>
    <tr>
        <td>Producto 2</td>
        <td>67890</td>
        <td>$15.00</td>
        <td>10</td>
        <td>
            <button onclick="editarFila(2)">Editar</button>
        </td>
        <td>
            <button onclick="eliminarFila(2)">Eliminar</button>
        </td>
    </tr>
    <tr>
        <td>Producto 3</td>
        <td>54321</td>
        <td>$20.00</td>
        <td>3</td>
        <td>
            <button onclick="editarFila(3)">Editar</button>
        </td>
        <td>
            <button onclick="eliminarFila(3)">Eliminar</button>
        </td>
    </tr>
</tbody>
</table>

<h1>Resultado de examen</h1>
<p>Carlos: <meter value="94" min="0" max="100"></meter></p>

```



```
<p>Ana: <meter value="60" min="0" max="100"></meter></p>
<p>Andres: <meter value="85" min="0" max="100"></meter></p>
<p>Pedro: <meter value="45" min="0" max="100"></meter></p>

<table style="border: 1px;">
  <thead>
    <tr>
      <th>mes</th>
      <th>ahorro</th>
    </tr>
  </thead>
  <tbody>
    <tr>
      <td>Enero</td>
      <td>$100</td>
    </tr>
    <tr>
      <td>Febrero</td>
      <td>$200</td>
    </tr>
  </tbody>
</table>

<h1>Resultado de ventas</h1>
<p>Enero: <progress value="94" min="0" max="100"></progress></p>
<p>Febrero: <progress value="60" min="0" max="100"></progress></p>
<p>Marzo: <progress value="85" min="0" max="100"></progress></p>
<p>Abril: <progress value="45" min="0" max="100"></progress></p>
</body>
</html>
```

Index.css

```
body {
  font-family: Arial, sans-serif;
  margin: 20px;
  padding: 0;
}

.title {
  font-family: Arial, Helvetica, sans-serif;
  color: red;
  text-align: center;
}

h2 {
  color: #333;
}
```



```
table {
  border-collapse: collapse;
  width: 50%;
  margin-bottom: 20px;
}

table, th, td {
  border: 1px solid #333;
}

th, td {
  padding: 10px;
  text-align: left;
}

ol, ul {
  margin-bottom: 20px;
}

button {
  padding: 5px 10px;
  background-color: blue;
  color: #fff;
  border: none;
  cursor: pointer;
}

button:hover {
  background-color: red;
}

h1 {
  color: #333;
  margin-top: 30px;
}

meter {
  width: 200px;
}

progress {
  width: 200px;
  height: 20px;
}

progress::-webkit-progress-bar {
  background-color: #eee;
}
```



```

}

progress::-webkit-progress-value {
  background-color: #333;
}

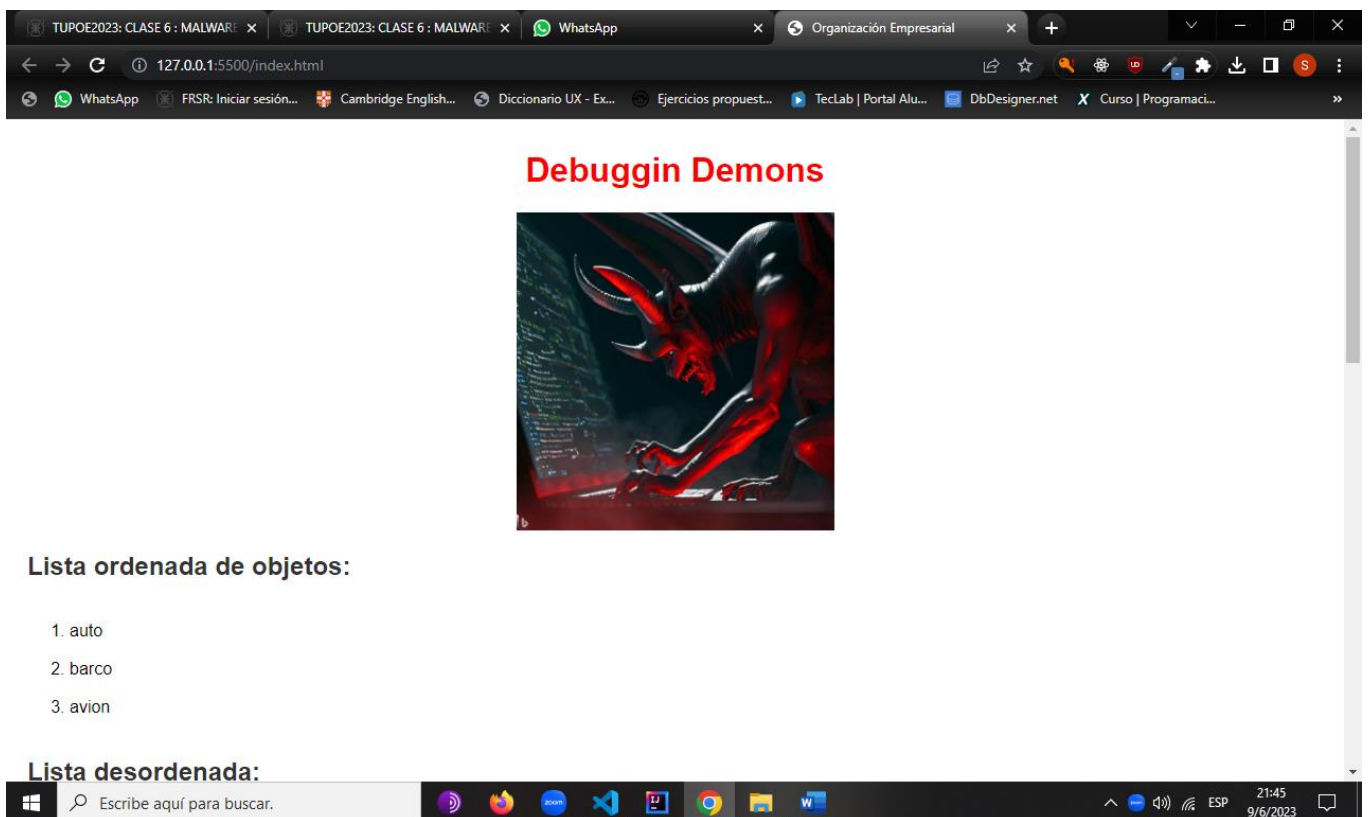
progress::-moz-progress-bar {
  background-color: #333;
}

progress::-ms-fill {
  background-color: #333;
}

.center-image {
  display: block;
  margin: 0 auto;
  max-width: 300px;
  margin-bottom: 20px;
}

```

Vista de la página con Live Server:



**Debuggin Demons**

Lista ordenada de objetos:

1. auto
2. barco
3. avion

Lista desordenada:



• avion

### Tabla de productos:

Nombre	Código	Precio	Existencia	Editar	Eliminar
Producto 1	12345	\$10.00	5	<a href="#">Editar</a>	<a href="#">Eliminar</a>
Producto 2	67890	\$15.00	10	<a href="#">Editar</a>	<a href="#">Eliminar</a>
Producto 3	54321	\$20.00	3	<a href="#">Editar</a>	<a href="#">Eliminar</a>

### Resultado de examen

Carlos:

Ana:

Andres:

Pedro:

Carlos:

Ana:

Andres:

Pedro:

mes	ahorro
Enero	\$100
Febrero	\$200

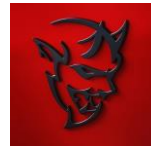
### Resultado de ventas

Enero:

Febrero:

Marzo:

Abril:



## ROOTKIT:

Un ejemplo famoso de un caso en el que se utilizó un rootkit es el del "rootkit Sony BMG". En 2005, Sony BMG, una importante compañía discográfica, decidió utilizar tecnología de protección contra copias en algunos de sus CDs de música para evitar la piratería.

Sin embargo, el método que eligieron fue controvertido y causó un gran revuelo. El CD incluía un rootkit llamado "Extended Copy Protection" (XCP), desarrollado por la empresa de software de protección contra copias First 4 Internet. Este rootkit se instalaba en secreto en las computadoras de los usuarios cuando reproducían el CD en un reproductor de música en sus computadoras.

El rootkit XCP estaba diseñado para ocultar los archivos del CD y cualquier actividad relacionada con ellos, lo que incluía la capacidad de ocultar archivos maliciosos o programas dañinos. Además, XCP se instalaba de forma furtiva y no revelaba su presencia a los usuarios, lo que generaba preocupaciones en cuanto a la privacidad y la seguridad de las computadoras afectadas.

Una vez que se descubrió la existencia del rootkit XCP, se desató una gran controversia y Sony BMG se enfrentó a fuertes críticas por su uso no autorizado de software de vigilancia en las computadoras de los usuarios. La compañía tuvo que retirar los CDs afectados del mercado y enfrentó múltiples demandas legales por violación de privacidad y daños causados a las computadoras de los usuarios.

El caso del rootkit Sony BMG fue un hito en cuanto a la concientización sobre la legalidad y ética del uso de rootkits y la importancia de proteger la privacidad y seguridad de los usuarios. Además, puso de relieve la necesidad de transparencia y consentimiento en la instalación de software en las computadoras de los usuarios.

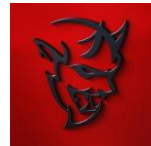
## RANSOMWARE:

Un ejemplo notable de un caso de ransomware es el ataque "WannaCry" que ocurrió en mayo de 2017. Este ataque afectó a miles de organizaciones en todo el mundo, incluyendo hospitales, empresas y organismos gubernamentales.

El ransomware WannaCry se propagó rápidamente utilizando una vulnerabilidad en el protocolo SMB (Server Message Block) de Windows. Una vez que infectaba una computadora, cifraba los archivos del sistema y mostraba una nota de rescate exigiendo un pago en Bitcoin para desbloquear los archivos.

Este ataque fue especialmente notable debido a su alcance y su impacto en los servicios críticos, como el sistema de salud. Muchos hospitales tuvieron que cancelar cirugías y retrasar tratamientos debido a la pérdida de acceso a los registros médicos y a la incapacidad para operar con normalidad.

El ataque WannaCry demostró la capacidad de los ransomware para propagarse rápidamente a través de vulnerabilidades conocidas y la importancia de mantener los sistemas operativos y el software actualizados con los últimos parches de seguridad. También destacó la



necesidad de contar con copias de seguridad regulares y sistemas de seguridad robustos para prevenir y mitigar el impacto de los ataques de ransomware.

## TROYANO:

Un caso famoso de un ataque que utilizó troyanos es el incidente conocido como "Zeus Trojan" o "Zbot". Zeus es un troyano bancario que se hizo notorio por su capacidad para robar información financiera y credenciales de acceso a cuentas bancarias en línea.

El troyano Zeus se propagaba principalmente a través de correos electrónicos de phishing, donde los atacantes enviaban mensajes aparentemente legítimos, pero con archivos adjuntos maliciosos o enlaces a sitios web comprometidos. Cuando los usuarios hacían clic en esos archivos o enlaces, el troyano se instalaba sigilosamente en sus sistemas.

Una vez infectada la computadora, Zeus monitoreaba las actividades del usuario y capturaba información confidencial, como nombres de usuario, contraseñas y números de tarjetas de crédito, mientras la persona realizaba transacciones en línea o ingresaba a sitios bancarios.

La información robada por Zeus se enviaba a los servidores de los atacantes, quienes luego podían utilizarla para cometer fraude financiero o venderla en el mercado negro. Este troyano fue especialmente problemático debido a su capacidad para evadir las medidas de seguridad tradicionales y su enfoque específico en el robo de información bancaria.

Zeus Trojan fue responsable de numerosos ataques exitosos a lo largo de los años y se estima que ha infectado a millones de computadoras en todo el mundo. Este caso destaca la importancia de ser cauteloso al abrir correos electrónicos y hacer clic en enlaces desconocidos, además de mantener actualizados los sistemas operativos y utilizar soluciones de seguridad confiables para protegerse contra este tipo de amenazas.