

UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA CAMPUS ZACATECAS



Ingeniería En Sistemas Computacionales

Seguridad Web

Mtra. Sandra Mireya Monreal Mendoza

Proyecto final- Pagina Web.

NOMBRE DEL ALUMNO: Juan Hernández Montalvo
GRUPO AL QUE PERTENEZCO: 4 CM 1
FECHA DE ELABORACIÓN: 3 de Junio del 2019

Tabla de contenido

Introducción	3
Desarrollo	4
Sección 0	4
Sección 1	6
Inicio sesión	6
Registro	7
Sección 2	12
Ver tareas	13
Apuntar tareas	14
Sección 3	17
¿Como se juega?	18
Jugar	21
Error	23
Retos del Proyecto	24
Owasp zap	25
Conclusiones:	33
Referencias	33

Introducción

Meta Wars se desarrolló para poder estar en un mejor contexto en la escuela ya que al mantener un orden con los trabajos, tareas y apuntes de un total descontrol. En el cual Meta Wars tiene la obligación de mejorar estos aspectos al cual tenemos un apartado distinto para la mejora del alumno al cual también se implementa un juego para quitar la aburricion. Ahora en el transcurso de este documento podremos observar que esta página web se elaboró para dos objetivos solamente, uno de ellos es para poder mejorar en la escuela ya que al anotar tareas en un punto llega a ser pesado o simplemente no se hace o en un momento al cual se esté aburrido poder jugar.

El otro objetivo de esta página web es darle la completa seguridad que pueda existir ya que es un requisito para poder pasar la materia de web security.

En el transcurso de este documento observaremos puntos muy importantes que son el cómo utilizar esta página web y hasta las diferentes implementaciones para poder darle seguridad web, también realizaremos una análisis con la herramienta OWASP Zap para poder observar qué tanta seguridad se le dio.

Desarrollo

Podemos decir que que trata esta página al cual podemos decir que La implementación digital de un juego de cartas en un entorno web, estilo “Yu-Gi-Oh!” pero con la temática de bases de la “bioquímica” para facilitar el aprendizaje del alumno en las rutas metabólicas. Esta página al principio se tenía una idea diferente de su elaboración pero con el paso del tiempo se fue modificando esa idea ya que la idea anterior con la nueva se pudo elaborar una fusión y es ahora como tenemos Meta Wars ya que la idea principal solo era tener una página para anotar tareas, y lo pudimos fusionar con el poder jugar. Es así como pudimos fusionar dos grandes ideas.

En este documento será apartado por varias secciones. La primera sección será para el registro y el login, la segunda sección será para el registro de tareas y la tercera sección para el análisis del juego.

Sección 0.

Podemos iniciar con el inicio de la página, se agregó una pequeña introducción al inicio para saber la funcionalidad de la página web y también podremos observar el logo de la empresa al cual fue desarrollado esta página.



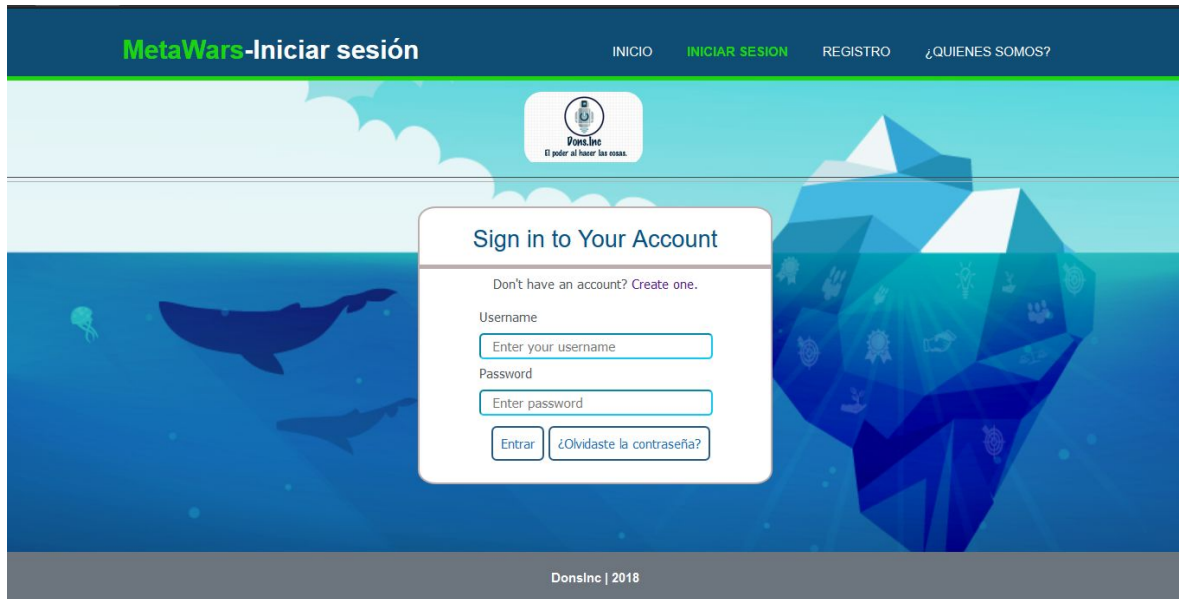
Si podemos observar en la parte de abajo este gran proyecto se empezó a elaborar en el 2018 pero gracias a la clase de seguridad web pudimos retomar la idea y darle un acabado como debe de ser.

Ahora también en la parte superior derecha tenemos diferentes apartados al cual son los siguiente:

1. Inicio(Página en la cual se está en estos momentos)
2. Inicio de sesión- Página para poder dar inicio a las diferentes funcionalidades de dicha página
3. Registro- Pagina donde se puede registrar el usuario con una alta seguridad en todos los aspectos
4. ¿Quienes somos?- Apartado donde se visualizará la visión y la misión de dicha empresa y que es Don sInc.

Sección 1

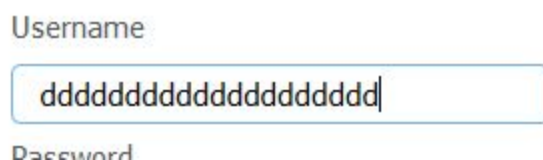
Ahora vamos con la parte de iniciar sesión



En esta parte cómo podemos mencionar al momento de introducir las contraseñas debe ser mayor a 12 caracteres con una mayúscula y un número por lo menos.

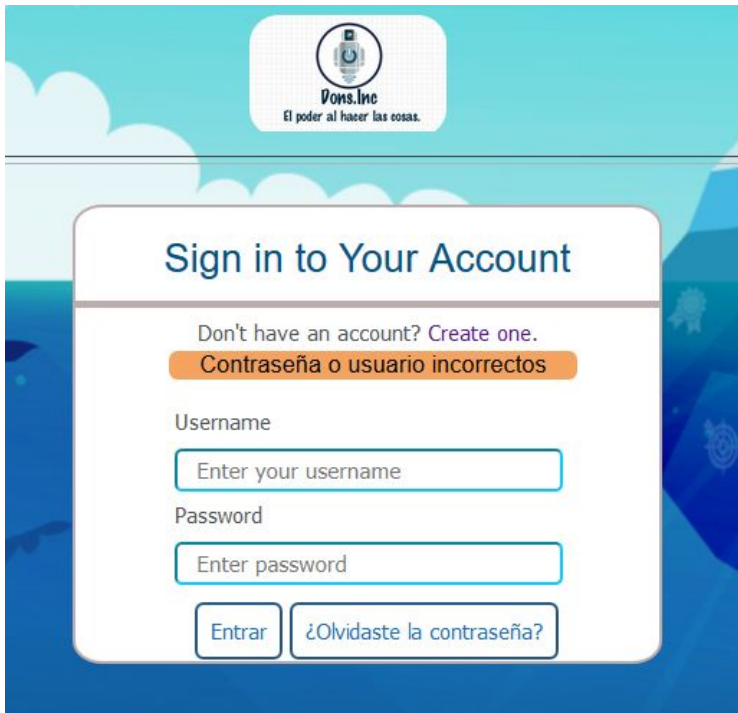
Esta página está restringida para que solo pueda meter el Username Y el Password

Entonces también el username no puede ser tan grande ya que se restringe a cierta cantidad de caracteres.



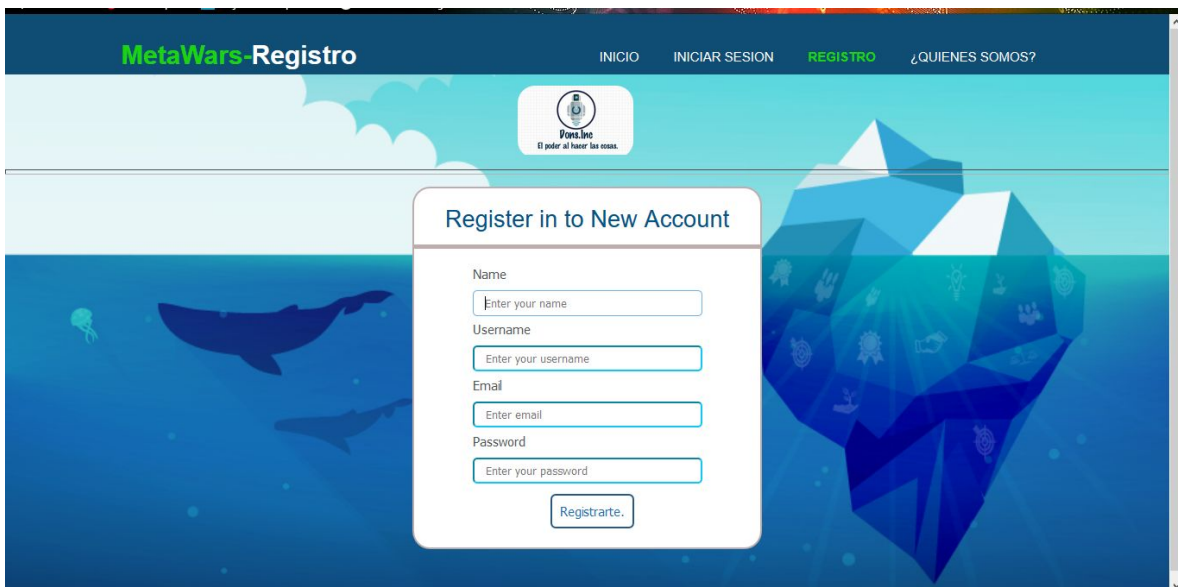
Después de cierta cantidad ya no se puede escribir más.

Si la contraseña o el usuario son incorrectos se manda un mensaje de error.



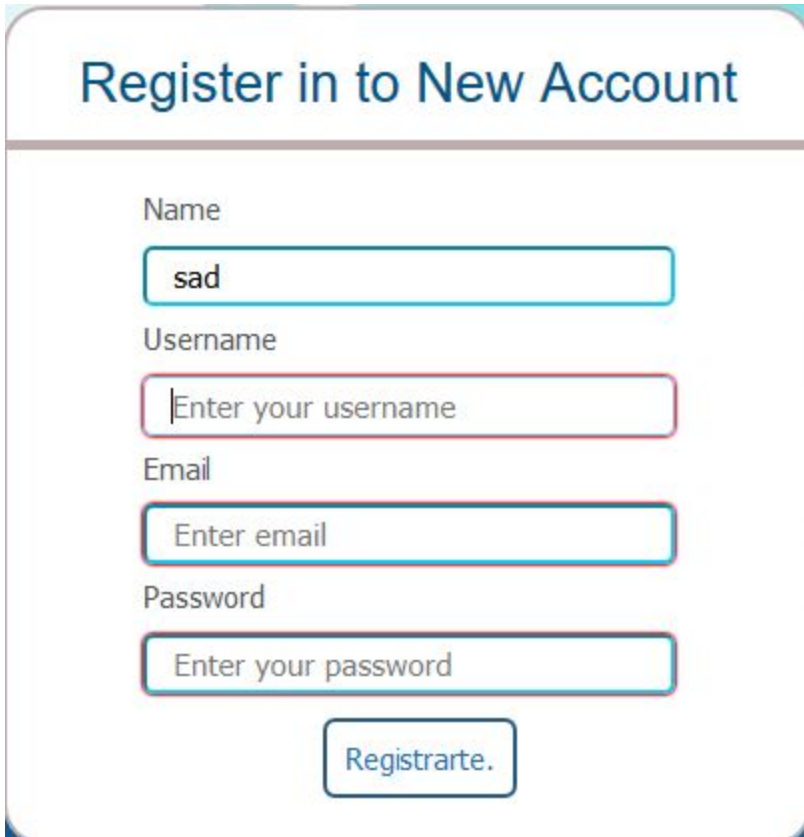
The image shows a login form titled "Sign in to Your Account" on a blue background with a stylized ocean scene. At the top left is the Pons.Inc logo with the tagline "El poder al hacer las cosas.". Below the title, there is a link "Don't have an account? Create one." and an orange error message box that says "Contraseña o usuario incorrectos". The form includes input fields for "Username" (placeholder: "Enter your username") and "Password" (placeholder: "Enter password"). At the bottom are two buttons: "Entrar" and "¿Olvidaste la contraseña?".

Ahora vamos a la parte de **Registro**.



The image shows a registration form titled "Register in to New Account" on a blue background with a stylized ocean scene. At the top left is the Pons.Inc logo with the tagline "El poder al hacer las cosas.". The form includes input fields for "Name" (placeholder: "Enter your name"), "Username" (placeholder: "Enter your username"), "Email" (placeholder: "Enter email"), and "Password" (placeholder: "Enter your password"). At the bottom is a button labeled "Registrarte.". The top navigation bar includes links for "INICIO", "INICIAR SESION", "REGISTRO" (highlighted in green), and "¿QUIENES SOMOS?".

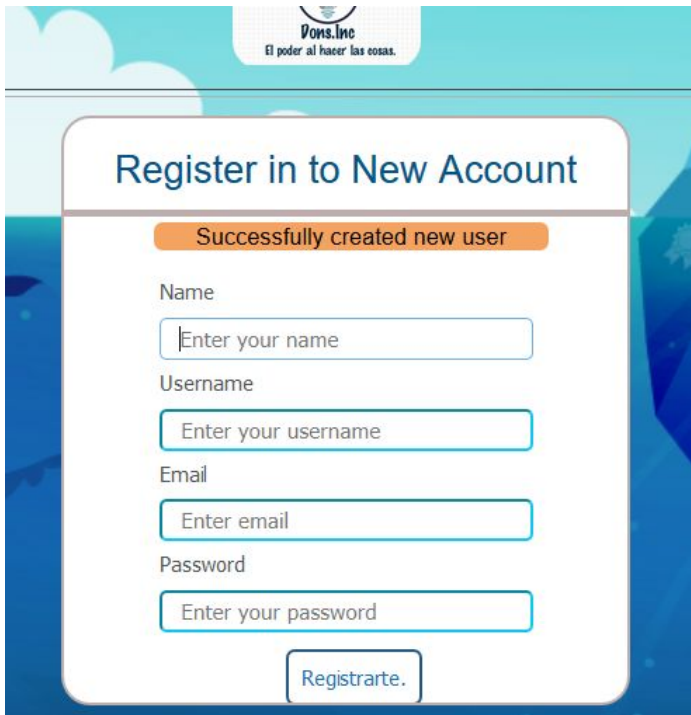
Como mencionamos en antiguos reportes si marcamos algún campo o con otras cosas que no son la casilla se marca en rojo y nos manda un error.



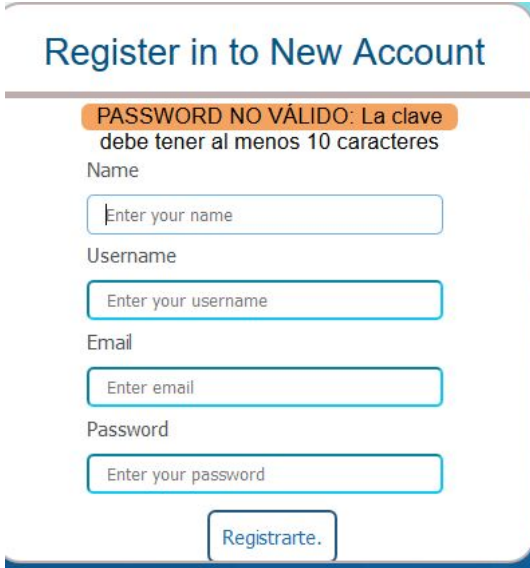
The image shows a registration form titled "Register in to New Account". It contains four input fields: "Name" with the text "sad", "Username" with the placeholder "Enter your username", "Email" with the placeholder "Enter email", and "Password" with the placeholder "Enter your password". Below these fields is a button labeled "Registrarte.". The form is styled with a light blue header and a white body with rounded corners.

Está protegido para que no se hagan ataques así no podemos registrarnos ahora la nueva seguridad que le dimos a esta pagina es que la contraseña debe de ser mínima de 12 caracteres, también debe de incluir una mayúscula o un número, En el nombre solo debe de existir letras y no numeros y tambien nos marca cuando el nombre tiene numeros, al igual que en otras ocasiones si se quiere realizar un registro con etiquetas html lo que hará este registro simplemente es quitarlas y seguir trabajando como debería de ser.

Cuando se registra correctamente un usuario se muestra de la siguiente forma



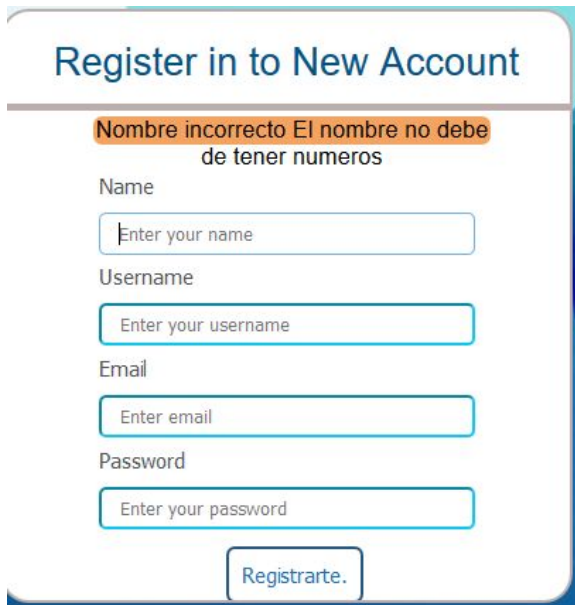
The screenshot shows a registration form for 'Vons Inc.' with the tagline 'El poder al hacer las cosas.' at the top. The form is titled 'Register in to New Account'. Below the title, an orange banner displays the message 'Successfully created new user'. The form contains five input fields: 'Name' (placeholder: 'Enter your name'), 'Username' (placeholder: 'Enter your username'), 'Email' (placeholder: 'Enter email'), and 'Password' (placeholder: 'Enter your password'). A 'Registrarte.' button is located at the bottom right of the form.



The screenshot shows the same registration form as above, but with an error message. An orange banner at the top of the form area displays the text 'PASSWORD NO VÁLIDO: La clave debe tener al menos 10 caracteres'. The input fields and the 'Registrarte.' button are still visible below the error message.

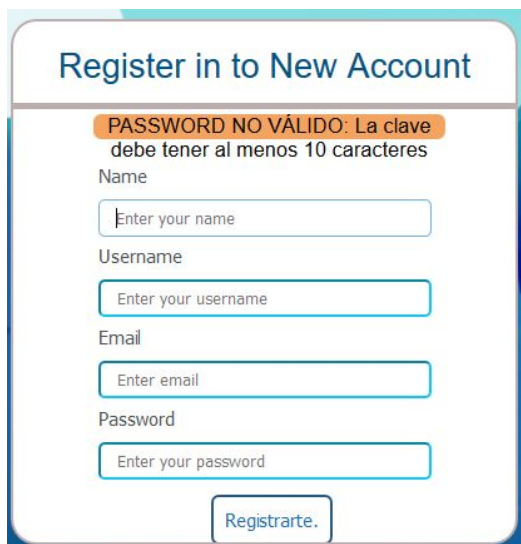
La clave este caso sería el password.

Aquí podemos observar lo siguiente



The image shows a web registration form titled "Register in to New Account". It contains five input fields: "Name", "Username", "Email", and "Password", each with a placeholder text "Enter your [field name]". Below the fields is a button labeled "Registrarte.". An orange error message is displayed above the "Name" field, stating: "Nombre incorrecto El nombre no debe de tener numeros".

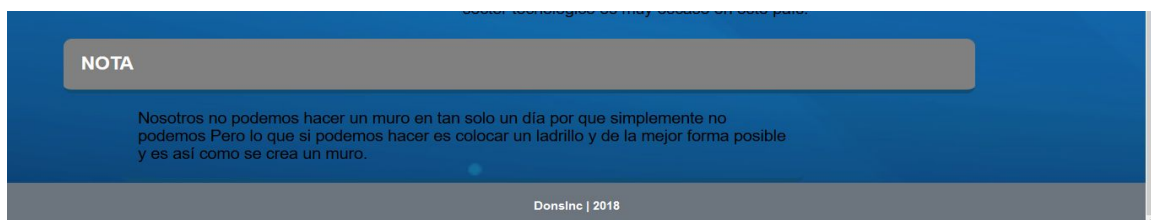
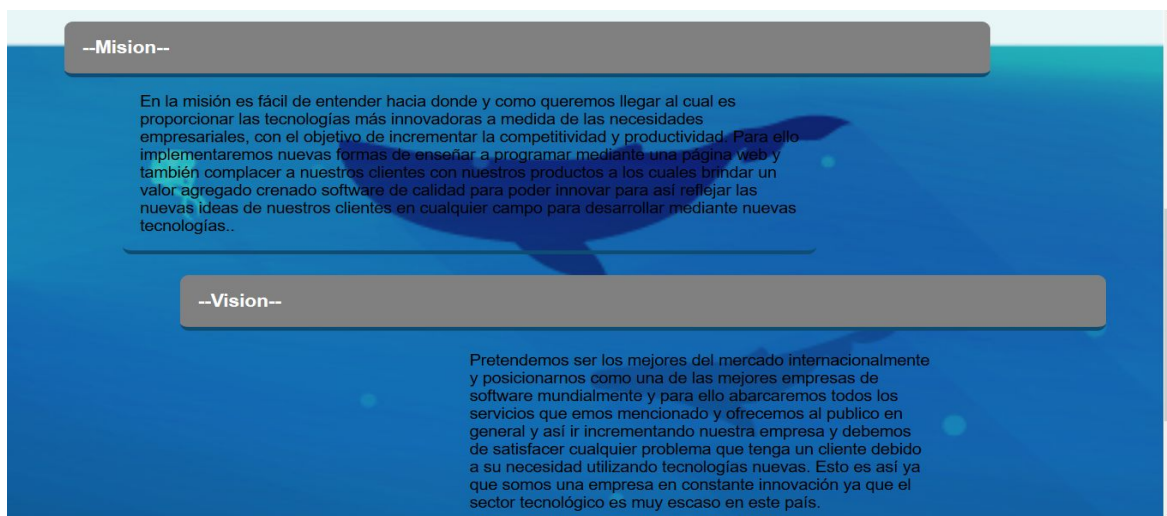
En la parte de name se introdujo un nombre con números y el resultado fue el de la imagen anterior. Ahora si observamos la siguiente imagen



The image shows the same web registration form as before. An orange error message is now displayed above the "Password" field, stating: "PASSWORD NO VÁLIDO: La clave debe tener al menos 10 caracteres". The other fields and the "Registrarte." button remain the same.

En el apartado de password se introdujo una contraseña corta y el mensaje de error es que debe de tener un mínimo de 10 caracteres la contraseña.

Ahora que ya vimos esta parte de seguridad podemos observar lo siguiente página de ¿Quiénes somos?

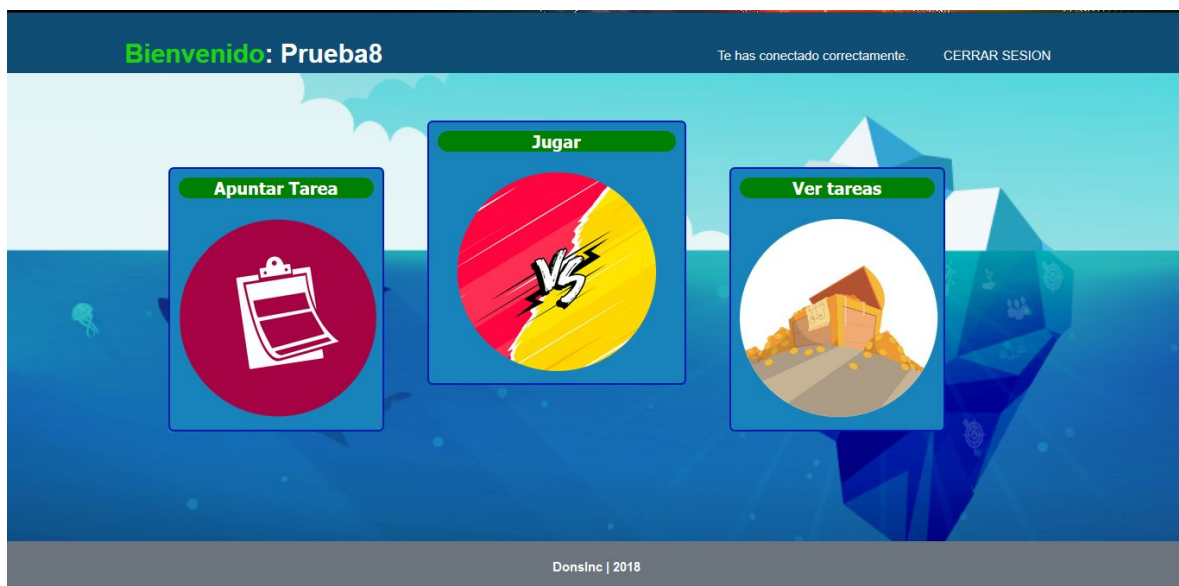


Esta página es solo para observar de dónde es cómo vino la empresa que trabajos se han realizado y entre otras cosas.

Sección 2

En la segunda sección observaremos como se ve la pagina ya cuando se inicia sesion y es la siguiente.

Así es como se ve cuando se inicio sesion



Si podemos observar se toma el username del cliente y se muestra junto con 3 apartados que son:

1. Apuntar tarea.
2. Jugar
3. Ver tareas.

Ver tareas.

Cada apartado tiene diferentes formas de utilizar por ejemplo si nos vamos a la parte de Ver tareas y si aún no se ha agregado ninguno se muestra lo siguiente.



si observamos aún no hay ninguna tarea existente y hasta la propia página nos lo muestra en el siguiente punto podremos observar como se observa esta pagina al guardar una tarea.

Apuntar tareas.

Al introducirnos a la página de apuntar tarea se nos muestra de la siguiente forma:

Usuario: Bejas Te has conectado correctamente. CERRAR SESION

Apuntar Tarea Regresar

Escribe el nombre de la materia.

Escriba la fecha de entrega

dd / mm / aaaa

Escriba la tarea

Guardar Borrar

DonsInc | 2018

Al cual se tiene los siguientes apartados:

1. Nombre de la materia
2. Fecha de entrega
3. Anotación de la tarea

Con 2 botones que son el guardar la tarea y borrar lo escrito por si se equivoca uno.

Esta pagina tambien esta diseñada para que no se realicen ataques de inserción de código entre otras cosas.

También existe un botón de regresarnos a la página anterior y si guardamos una tarea se anotara lo siguiente:

Usuario: Bejas Te has conectado correctamente. CERRAR SESION

Apuntar Tarea Regresar

Escribe el nombre de la materia.
Español

Escribe la fecha de entrega
06 / 06 / 2019

Escribe la tarea
Leer 7 libros

Guardar Borrar

DonsInc | 2018

Usuario: Bejas Te has conectado correctamente. CERRAR SESION

Apuntar Tarea Regresar

Tarea guardada correctamente

Escribe el nombre de la materia.

Escribe la fecha de entrega
dd / mm / aaaa

Escribe la tarea

Guardar Borrar

DonsInc | 2018

Aparece un anuncio de tarea guardada correctamente

y ahora si vamos a panel de ver tareas se muestra lo siguiente:

Usuario: Bejas

Te has conectado correctamente. [CERRAR SESION](#)

Tareas pendientes

Nombre de usuario	Nombre de la materia	Fecha de entrega	Apunte de la tarea.
Bejas	Español	2019-06-06	Leer 7 libros.

Atras

Ahora si queremos introducir un simple `<h1>HOLA</h1>` Se muestra lo siguiente:

Usuario: Bejas

Te has conectado correctamente. [CERRAR SESION](#)

Apuntar Tarea [Regresar](#)

Escribe el nombre de la materia.

`<h1>HOLA</h1>`

Escribe la fecha de entrega

12 / 06 / 2019

Escribe la tarea

`<h1>HOLA</h1>`

Guardar

Borrar

DonsInc | 2018

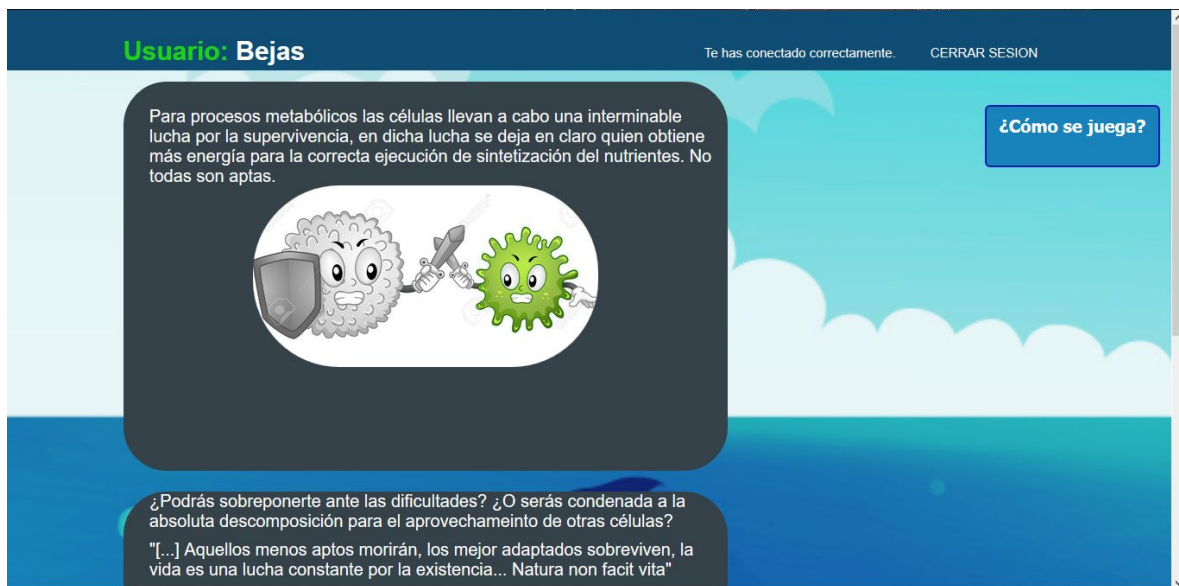
Nombre de usuario	Nombre de la materia	Fecha de entrega	Apunte de la tarea.
Bejas	Español	2019-06-06	Leer 7 libros.
Bejas	HOLA	2019-06-12	HOLA

Atras

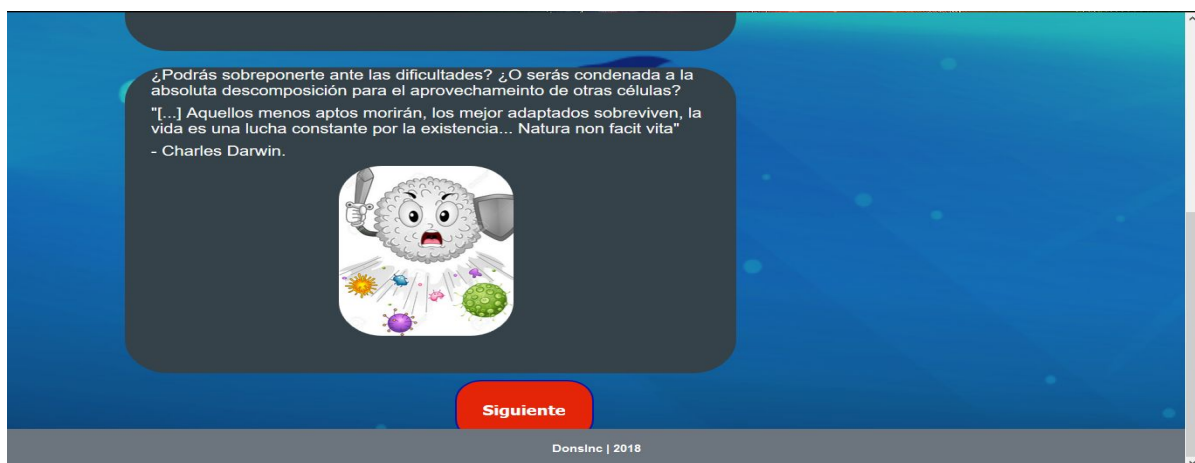
Si observamos la imagen anterior se quita la etiqueta de h1 y se guarda como debe de ser un simple hola en la base de datos.

Sección 3

Ahora observamos al momento de dar jugar y se nos muestra lo siguiente:



Si observamos hay un botón en la parte superior derecha para saber como jugar este juego y también se nos muestra una gran historia.



Ahora vamos al apartado de

¿Como se juega?

En este apartado se nos muestra las instrucciones para poder jugar este maravilloso juego al cual se muestra de la siguiente forma.

Manual de usuario.

Metawars es un juego de cartas coleccionables que tiene por objetivo destruir las células enemigas a través de la utilización de Genes para obtener energía. Cada jugador deberá escoger un GEN del cual la célula obtendrá la energía. Para cada gen existen 10 guerreros y 10 defensores asociados los cuales se pueden combinar en parejas para realizar un ataque a la célula enemiga.

--Contenido--

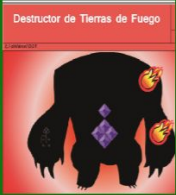
Cada jugador cuenta con 106 cartas de las cuales:

- 55 corresponden a guerreros (rojas).
- 51 corresponden a defensores (azules).

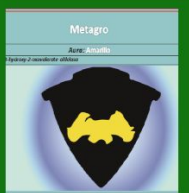
Un tablero.

--- Clasificación de cartas ---

--- Clasificación de cartas ---



Guerreros.
Los guerreros son los encargados de disminuir la vida de la célula enemiga.



Defensores.
Los defensores repelen a los guerreros enemigos y protegen a la célula.

--- Atributos ---

Carta de Guerreros.

Nombre del guerrero ←

Nombre metabolito del ←

Símbolo del guerrero del ←

Defensor compatible ←

Puntos de Ataque ←

Destructor de Especies en Llamas 5

Atributo: Cañón Ácido
Destruye las cartas ocultas.

Defensor requerido para la reacción: Escudero Trágl
Producto de la reacción: PAM 449, Pequeño Asaltador, PRD 270

Número de compatibilidades →

Gen/Ruta →

Atributo (s) y descripción. →

Puntos de reacción →

Guerrero formado →

Carta de Defensores.

Nombre del defensor ←

Escudero del mar de indias 4

Carta de Defensores.

Nombre del defensor ←

Color de Aura ←

Nombre la enzima ←

Símbolo del defensor ←

Puntos de Defensa ←

Escudero del mar de indias 4

Atributo: Fuerza/Persuadir
Aumenta el ataque de los guerreros.
Disminuye su vida.

Guerrero requerido: PDC 105, PRD 30, PVE 9601

Número de compatibilidades →

Gen/Ruta →

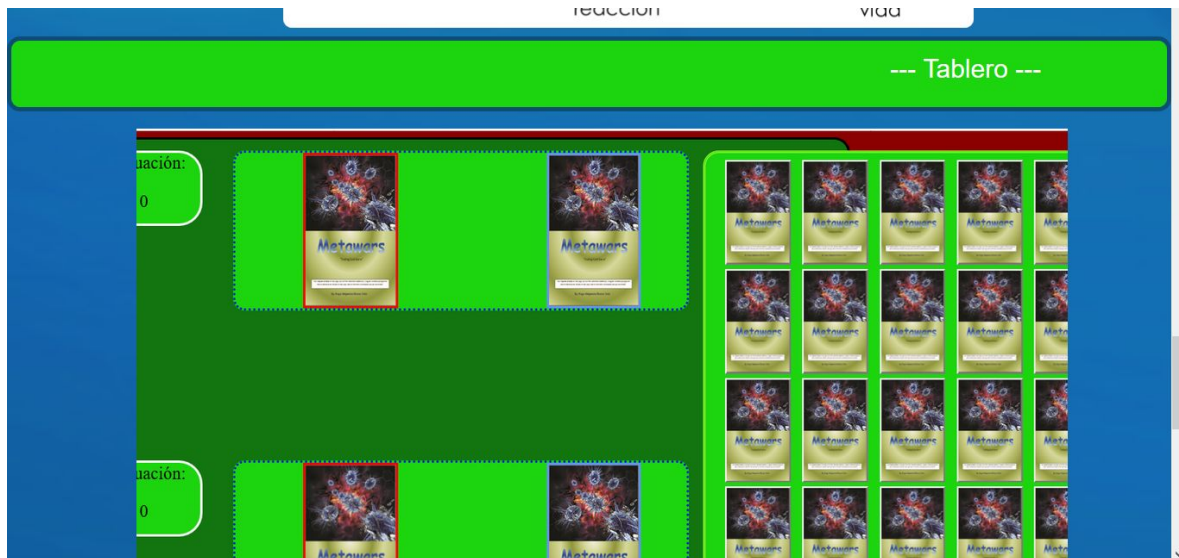
Atributo (s) y descripción. →

Guerrero compatible →

Puntos de vida →

Puntos de reacción

--- Tablero ---



--- ¿Cómo se juega? ---


El Objetivo de juego es terminar con los puntos de vida de la célula contraria.
Dentro del juego hay 2 tipos de cartas básicas:

- Guerreros
- Defensores

Al comienzo de cada juego se entregarán 10 cartas, que pertenecen a un gen en específico que tu podrás elegir (CDK, DDT, GLU, MET, TOL).
En cada turno seleccionarás las mejores cartas que creas ganaran contra las de tu contrincante, podrás ganar la ronda si tu equipo obtiene una mayor cantidad de puntos que la de tu adversario.
y podrás perder si:

- Te quedas sin puntos
- Se rinde
- Se agota el tiempo y no consigues más puntos que tu adversario

Finalmente, gana quién obtiene más puntos al finalizar la partida.



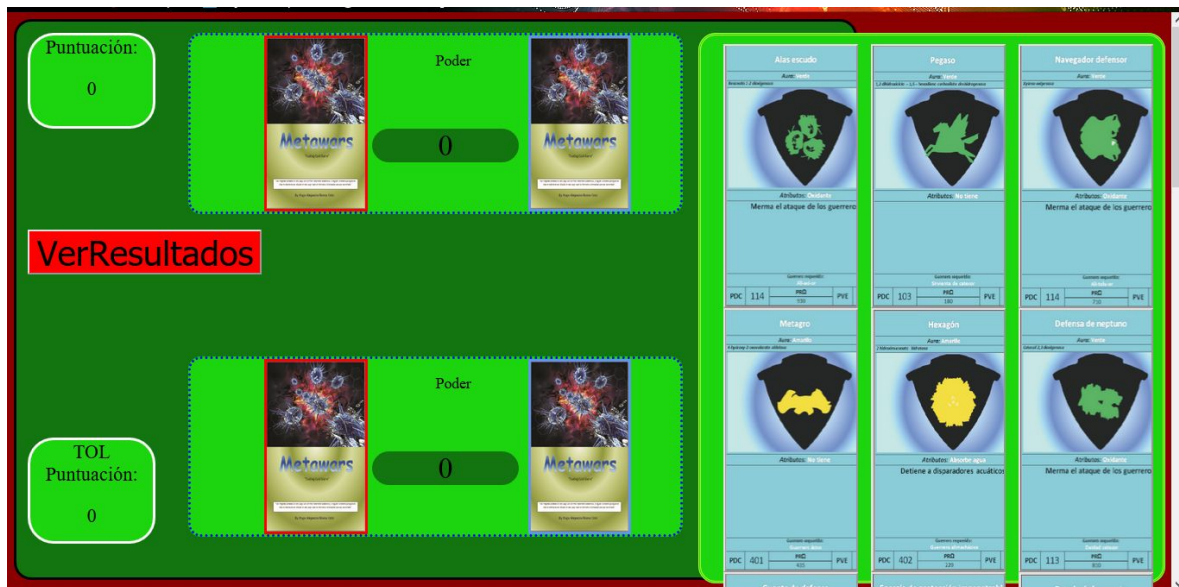
Donsinc, Copyright © 2018

Ahora sí observamos es un gran instructivo pero se da detalle de todo lo que se debe de saber para por jugar perfectamente.

Ahora vamos a la parte

Jugar

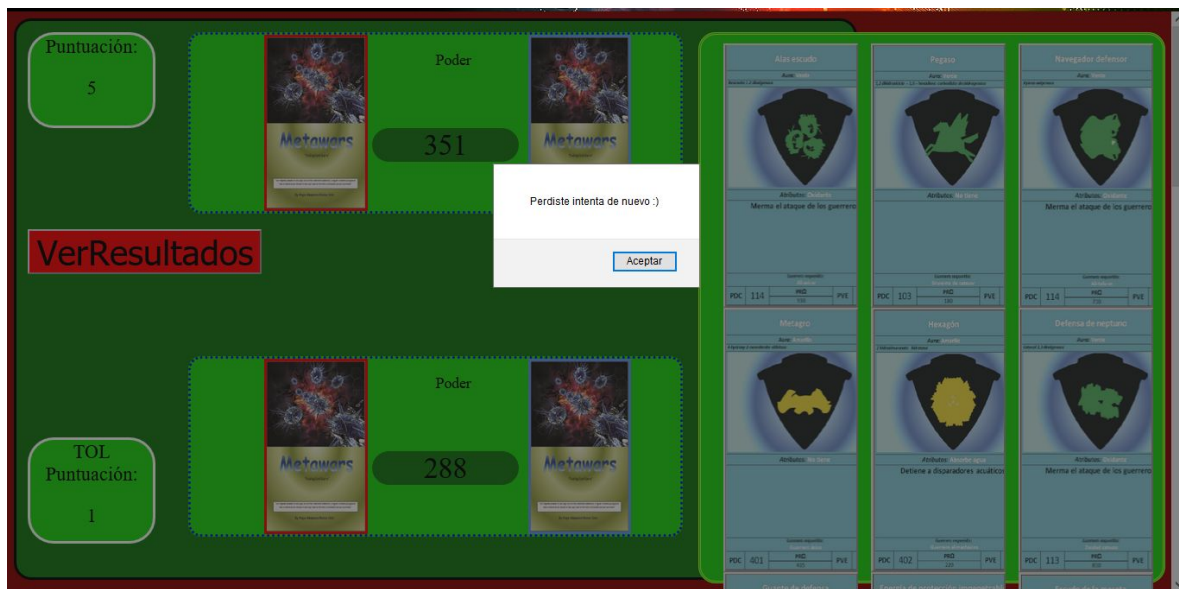
En este apartado es un simple juego y la pantalla principal se muestra de la siguiente manera:



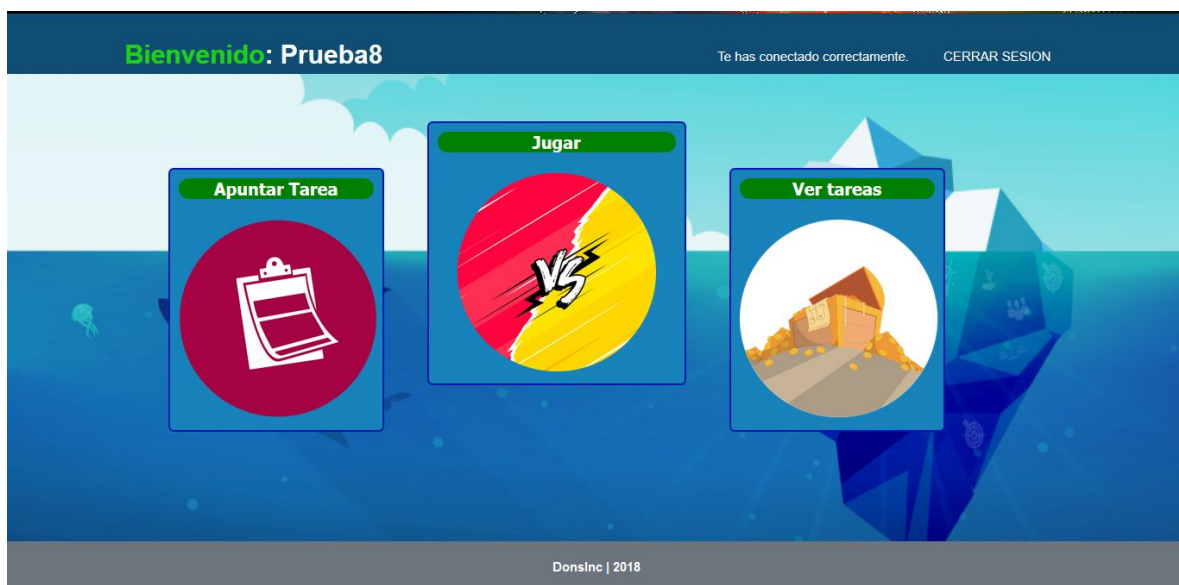
En la parte izquierda tenemos las cartas utilizadas y en la derecha nuestro mazo, ahora al escoger dos cartas y dar en el botón de ver resultados se mostrará lo siguiente:



Si observamos al introducir dos cartas se nos da un ataque pero el otro usuario(PC) tuvo un ataque más grande al cual perdimos y ahí se nos da un punto en este caso gana el que tenga 5 puntos y se muestra así:

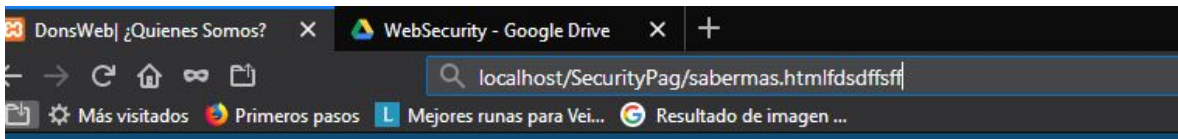


y al dar aceptar nos redirige a la página de inicio de sesión que es la siguiente:

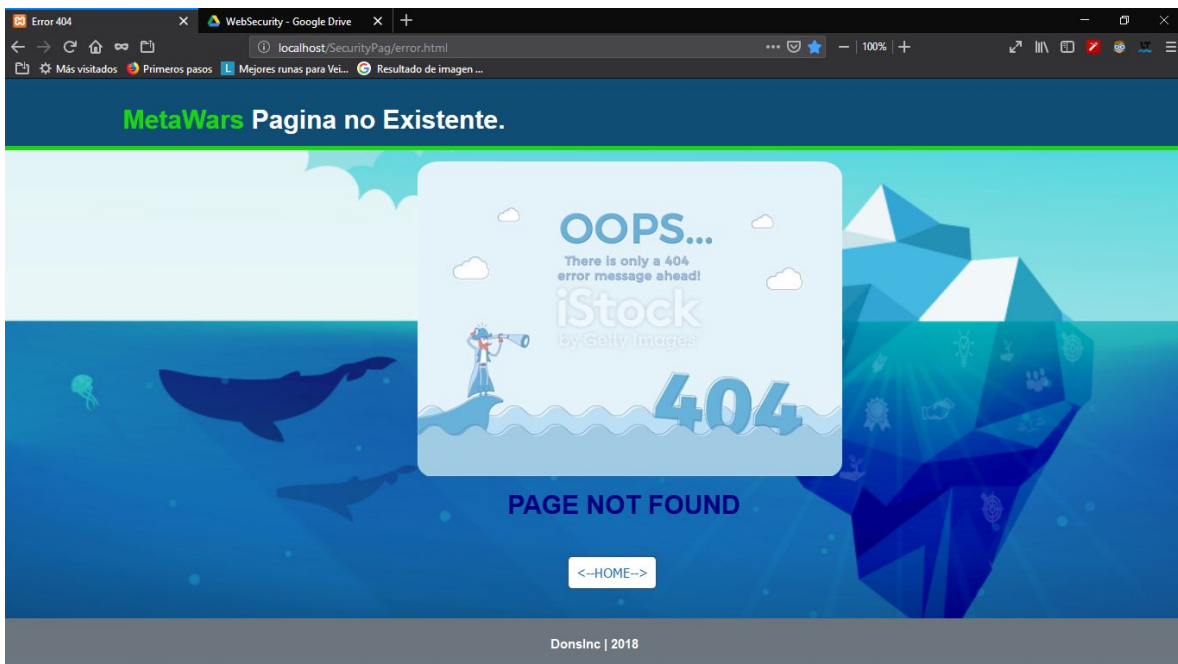


Error

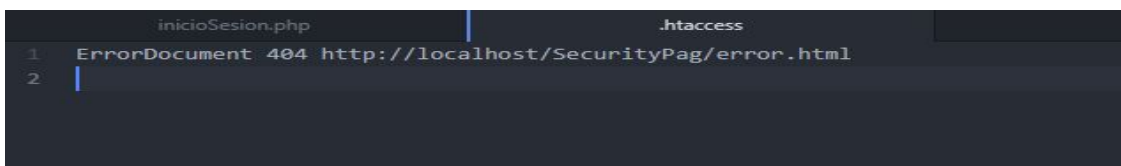
Ahora si el usuario atacante quiere ver que se muestra modificando el url nos muestra lo siguiente.



Y nos muestra lo siguiente:



Página de error con un botón de regresar al inicio, el url se cambia por sí solo. Esto se hizo agregando el .htaccess y se muestra así:



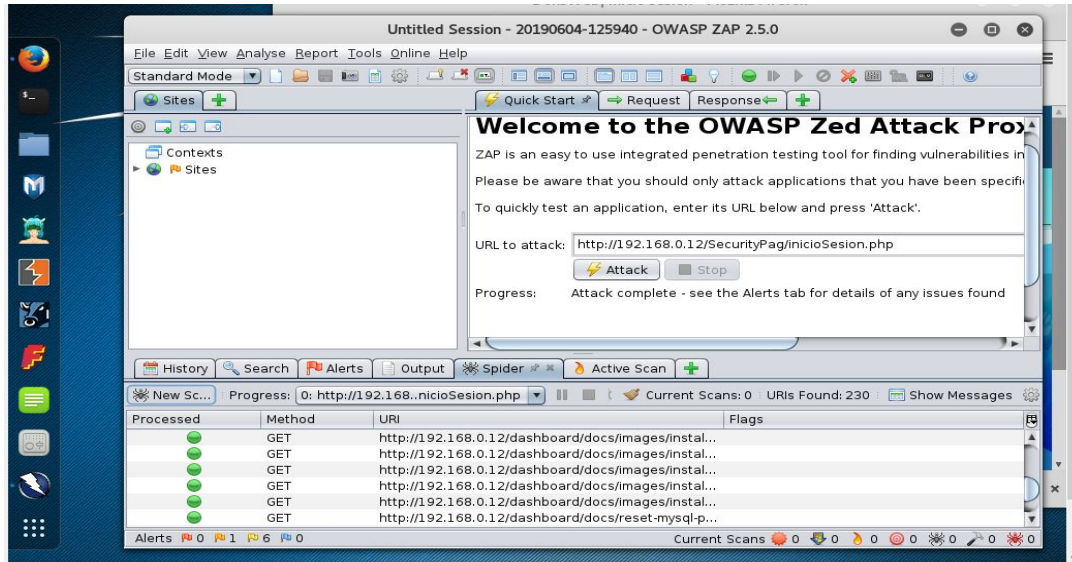
Retos del proyecto

Podemos mencionar que los retos fueron muchos desde el no saber cómo utilizar objetos con PHP que se tuvo que aprender hasta el manejo de la seguridad en todos los aspectos, tal vez lo más difícil en esta cuestión es el manejo de sesiones ya que no se supo cómo implementar algunas cosas, podemos dejar en claro que se implementaron algunas acciones para el manejo de sesión y el seteo de las cookies al igual que quitar caracteres extraños, podemos mencionar que quitar las etiquetas de un input y también la elaboración de funciones para la contraseña y nombre no fue una tarea sencilla pero con el paso del tiempo y con la perfecta disciplina de poder seguir mejorando podemos dejar en claro que todos estos retos que se impusieron fueron controlados y dimos solución a cada uno de ellos.

También puedes dejar en claro que al momento de que el cliente pidió cosas extras que no estaban en la planeación del proyecto se tuvo que hacer una replantación del proyecto y volverlo a estructurar.

Para dar concluido este punto podemos mencionar la parte más difícil fue que se tuvo que dar seguridad a las peticiones al cual necesitamos hacer objetos para hacer una petición, se tuvo que aprender y llevar a cabo pero en otros aspectos no hubo tanta complicación.

OWASP ZAP



Así es como se muestra la página de inicio.

Y ahora haremos un análisis al login y este es el resultado

http://192.168..nicioSesion.php Scan Progress					
Progress Response Chart					
Host: http://192.168.0.12					
Plugin	Strength	Progress	Elapsed	Reqs	St...
Path Traversal	Medium	<div></div>	00:00.023	0	✓
Remote File Inclusion	Medium	<div></div>	00:00.037	0	✓
Server Side Include	Medium	<div></div>	00:00.018	0	✓
Cross Site Scripting (Reflected)	Medium	<div></div>	00:00.026	0	✓
SQL Injection	Medium	<div></div>	00:00.015	0	✓
Server Side Code Injection	Medium	<div></div>	00:00.029	0	✓
Remote OS Command Injection	Medium	<div></div>	00:00.017	0	✓
Directory Browsing	Medium	<div></div>	00:00.088	1	✓
External Redirect	Medium	<div></div>	00:00.019	0	✓
Buffer Overflow	Medium	<div></div>	00:00.031	0	✓
Format String Error	Medium	<div></div>	00:00.021	0	✓
CRLF Injection	Medium	<div></div>	00:00.012	0	✓
Parameter Tampering	Medium	<div></div>	00:00.028	0	✓
Cross Site Scripting (Persistent) - P...	Medium	<div></div>	00:00.027	0	✓
Cross Site Scripting (Persistent) - S...	Medium	<div></div>	00:00.051	1	✓
Cross Site Scripting (Persistent)	Medium	<div></div>	00:00.028	0	✓
Script Active Scan Rules	Medium	<div></div>	00:00.004	0	✗
Totals			00:00.650	2	

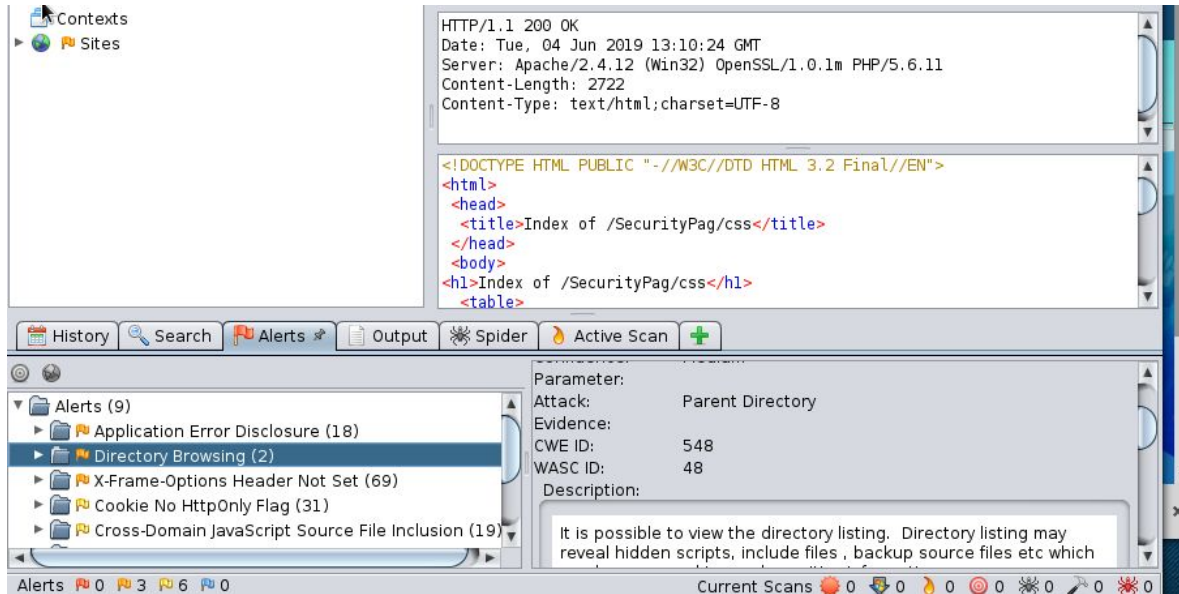
Ahora se hace un análisis general de la página y tenemos el siguiente resultado:

http://192.168...12/SecurityPag Scan Progress					
<div>ProgressResponse Chart</div>					
Host: http://192.168.0.12					
Plugin	Strength	Progress	Elapsed	Reqs	St...
Path Traversal	Medium	<div></div>	00:10.832	225	✓
Remote File Inclusion	Medium	<div></div>	00:04.125	90	✓
Server Side Include	Medium	<div></div>	00:01.743	36	✓
Cross Site Scripting (Reflected)	Medium	<div></div>	00:01.901	27	✓
SQL Injection	Medium	<div></div>	00:07.945	214	✓
Server Side Code Injection	Medium	<div></div>	00:02.870	72	✓
Remote OS Command Injection	Medium	<div></div>	00:11.243	288	✓
Directory Browsing	Medium	<div></div>	00:02.869	11	✓
External Redirect	Medium	<div></div>	00:02.448	81	✓
Buffer Overflow	Medium	<div></div>	00:00.866	9	✓
Format String Error	Medium	<div></div>	00:01.527	27	✓
CRLF Injection	Medium	<div></div>	00:01.239	63	✓
Parameter Tampering	Medium	<div></div>	00:01.269	63	✓
Cross Site Scripting (Persistent) - P...	Medium	<div></div>	00:00.830	9	✓
Cross Site Scripting (Persistent) - S...	Medium	<div></div>	00:03.063	27	✓
Cross Site Scripting (Persistent)	Medium	<div></div>	00:00.345	0	✓
Script Active Scan Rules	Medium	<div></div>	00:00.004	0	✗
Totals			00:56.589	1242	
<div>Copy to ClipboardClose</div>					

Registro.php

http://192.168..ag/registro.php Scan Progress					
<div>ProgressResponse Chart</div>					
Host: http://192.168.0.12					
Plugin	Strength	Progress	Elapsed	Reqs	St...
Path Traversal	Medium	<div></div>	00:00.024	0	✓
Remote File Inclusion	Medium	<div></div>	00:00.023	0	✓
Server Side Include	Medium	<div></div>	00:00.020	0	✓
Cross Site Scripting (Reflected)	Medium	<div></div>	00:00.026	0	✓
SQL Injection	Medium	<div></div>	00:00.020	0	✓
Server Side Code Injection	Medium	<div></div>	00:00.015	0	✓
Remote OS Command Injection	Medium	<div></div>	00:00.005	0	✓
Directory Browsing	Medium	<div></div>	00:00.046	1	✓
External Redirect	Medium	<div></div>	00:00.017	0	✓
Buffer Overflow	Medium	<div></div>	00:00.007	0	✓
Format String Error	Medium	<div></div>	00:00.018	0	✓
CRLF Injection	Medium	<div></div>	00:00.012	0	✓
Parameter Tampering	Medium	<div></div>	00:00.006	0	✓
Cross Site Scripting (Persistent) - P...	Medium	<div></div>	00:00.014	0	✓
Cross Site Scripting (Persistent) - S...	Medium	<div></div>	00:00.043	1	✓
Cross Site Scripting (Persistent)	Medium	<div></div>	00:00.021	0	✓
Script Active Scan Rules	Medium	<div></div>	00:00.011	0	✗
Totals			00:00.443	2	
<div>Copy to ClipboardClose</div>					

Aquí vemos el análisis de la página



Si observamos la mayoría de los errores es por que se puede ver el codigo pero nada de lo inusual.

Ahora observamos el reporte que nos manda Owasp zap y es el siguiente:

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	6
Informational	0

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://192.168.0.12/SecurityPag/inicioSesion.php
URL	http://192.168.0.12/sitemap.xml
URL	http://192.168.0.12/robots.txt

Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Other information	At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15

UPIIZ
Seguridad web - Metawars

URL	http://192.168.0.12/SecurityPag/css/
Parameter	N/A
Evidence	Parent Directory
URL	http://192.168.0.12/SecurityPag/js/
Parameter	N/A
Evidence	Parent Directory
URL	http://192.168.0.12/SecurityPag/js/?C=N;O=D
Parameter	N/A
Evidence	Parent Directory
URL	http://192.168.0.12/SecurityPag/css/?C=N;O=D

URL	http://192.168.0.12/SecurityPag/js/?C=D;O=D
Parameter	N/A
Evidence	Parent Directory
URL	http://192.168.0.12/SecurityPag/js/?C=S;O=D
Parameter	N/A
Evidence	Parent Directory
URL	http://192.168.0.12/SecurityPag/css/?C=D;O=D
Parameter	N/A
Evidence	Parent Directory

Medium (Medium)	Directory Browsing
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files , backup source files etc which can be accessed to read sensitive information.
URL	http://192.168.0.12/SecurityPag/css/
Attack	Parent Directory
URL	http://192.168.0.12/SecurityPag/js/
Attack	Parent Directory
Instances	2
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html

Este error solo es ocultar las carpetas raíz pero nada porqué preocuparse.

Low (Medium)	Web Browser XSS Protection Not Enabled
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://192.168.0.12/SecurityPag/inicioSesion.php
URL	http://192.168.0.12/sitemap.xml
URL	http://192.168.0.12/robots.txt
URL	http://192.168.0.12/SecurityPag/index.html
URL	http://192.168.0.12/SecurityPag/sabermas.html
URL	http://192.168.0.12/SecurityPag/registro.php

UPIIZ

Seguridad web - Metawars

Instances	69
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	<p>The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:</p> <p>X-XSS-Protection: 1; mode=block</p> <p>X-XSS-Protection: 1; report=http://www.example.com/xss</p> <p>The following values would disable it:</p> <p>X-XSS-Protection: 0</p> <p>The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).</p> <p>Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).</p>
Reference	<p>https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet</p> <p>https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/</p>

Low (Medium)	Password Autocomplete in Browser
Description	The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.
URL	http://192.168.0.12/SecurityPag/inicioSesion.php
Parameter	input
Evidence	<input type="password" name="pass" class="input1" placeholder="Enter password" required autofocus>
URL	http://192.168.0.12/SecurityPag/registro.php
Parameter	input
Evidence	<input type="password" name="password" placeholder="Enter your password" required autofocus title="Introduce tu contraseña">
Instances	2

Este error se soluciona rapido solo es quitar el autocompletamiento de contraseñas y de hecho ahí mismo nos da la solución que es la siguiente:

Instances	2
Solution	Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'.
Reference	<p>http://www.w3schools.com/tags/att_input_autocomplete.asp</p> <p>https://msdn.microsoft.com/en-us/library/ms533486%28v=vs.85%29.aspx</p>
CWE Id	525
WASC Id	15

Conclusiones.

Podemos dar por terminado con este proyecto llamado Meta Wars podemos concluir que se seguirá con la mejora de este proyecto ya que el objetivo general es llevarlo a cabo en la vida general será subido a una plataforma web y gracias a la clase de web security sera una pagina mas segura y evitará los ataques ddos y también tendrá un certificado SSL que en el reporte no se implementó pero se elaboró uno. el único problema que se tuvo es que en los requisitos que se muestran(Los de la maestra) piden cosas que no se tenían contempladas en el proyecto, pero como mencionamos anteriormente se tuvo que reestructurar el proyecto para dar una mejora a este y aunque los tiempos estimados no fueron en todo lo correcto se pudo acabar el proyecto en tiempo y forma como lo quería el cliente. En otros aspectos todo salio como debia de haber salido.

Con el análisis de OWASP ZAP encontramos errores que a veces no está en nuestras manos o en por ejemplo en las contraseñas solo es poner un poco de código que tal vez ya en este reporte no se genera pero se puede hacer una mejora.

Fuentes bibliográficas.

En esta parte no hay fuentes ya que las imágenes se sacaron desde hace mucho tiempo y no se perdieron las fuentes de dichas imágenes.