Nombre del Grupo
DanielFP-IgnacioBN-PaulaSC
13 de junio de 2021
Programación Integrativa

Miembros del grupo
Daniel Feito Pin (daniel.feito.pin@udc.es)
Ignacio Borregán Naya (ignacio.borregan@udc.es)
Paula Serrano Chans (p.serrano@udc.es)

`https://github.com/orgs/IntegrativeProgramming/teams/danielfp-ignaciobn-paulasc`

Resumen

El proyecto consistirá en una aplicación web realizada mediante el *framework* Django. Se tratará de una aplicación de OSINT que permitirá a un usuario realizar actividades de *information gathering* sobre un dominio o dirección IP.

Listado exhaustivo de las funcionalidades a implementar

- **F1**. Descubrir subdominios. **Entrada**: Dominio. **Salida**: Listado de subdominios y las direcciones IP asociadas a ellos.
- **F2**. Geolocalizar dominio o IP. **Entrada**: Dominio o IP. **Salida**: Geolocalización del dominio o IP introducido.
- **F3**. Descubrir servidores DNS. **Entrada**: Dominio. **Salida**: Listado de servidores DNS.
- **F4**. Descubrir servidores de correo. **Entrada**: Dominio. **Salida**: Listado de servidores de correo asociados al dominio.
- **F5**. Descubrir direcciones de correo. **Entrada**: Dominio. **Salida**: Listado de direcciones de correo asociadas al dominio.
- **F6**. Realizar resolución inversa. **Entrada**: IP. **Salida**: Nombre asociado a la IP.
- **F7**. Obtener rango de IPs. **Entrada**: Domino. **Salida**: Rango de IPs del dominio.
- **F8**. Buscar vulnerabilidades. **Entrada**: Dominio o IP. **Salida**: Lista de vulnerabilidades y puertos abiertos en el servidor al que pertenece la IP o en el que está alojado el dominio.

Bocetos de las pantallas de la aplicación

Pantalla de Inicio: Inicio de la página. Se muestra un resumen de las funcionalidades de la página y descripciones breves de los datos que se mostrarán utilizando cada opción. En la parte superior se ubica una barra de navegación que permite el cambio en entre las distintas vistas (esta es una característica que será común a todas las pantallas). En la parte inferior se mostrará un botón cuyo texto pondrá *Login* y que mostrará un formulario que permitirá iniciar sesión con un usuario registrado, o registrar a un usuario nuevo en la aplicación.

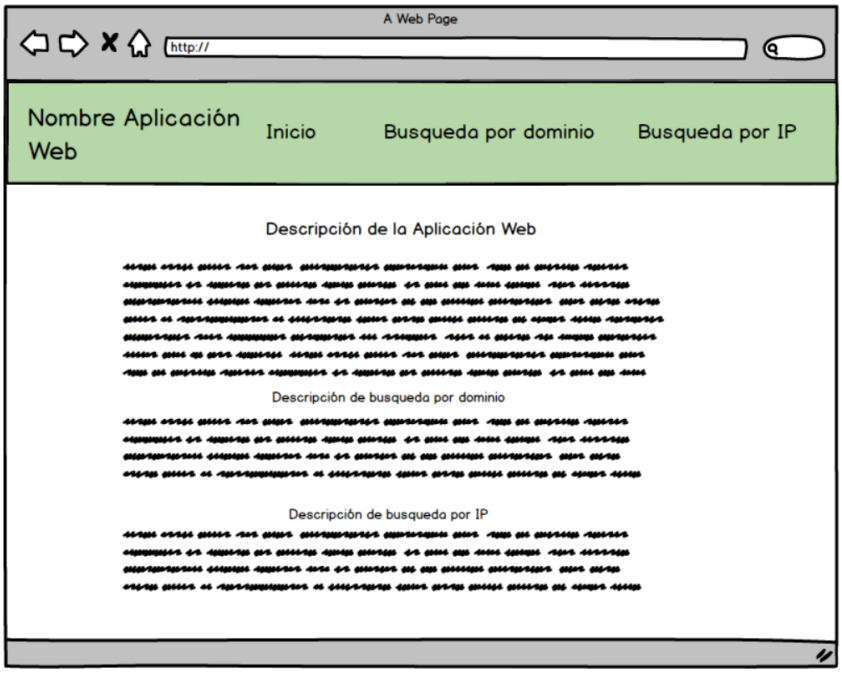

Figura 1: Pantalla de Inicio

Pantalla de Búsqueda de Dominios: Se muestra un *text field* en el que el usuario deberá introducir el dominio. Bajo la caja de búsqueda, se sitúan varios botones entre los que el usuario deberá elegir según el tipo de búsqueda sobre el dominio que quiera realizar. Al seleccionar uno, la página reaccionará mostrándose el resultado. Desde la misma pantalla, el usuario podrá seleccionar otra opción, en cuyo caso, se reemplazará el resultado previo por el nuevo.

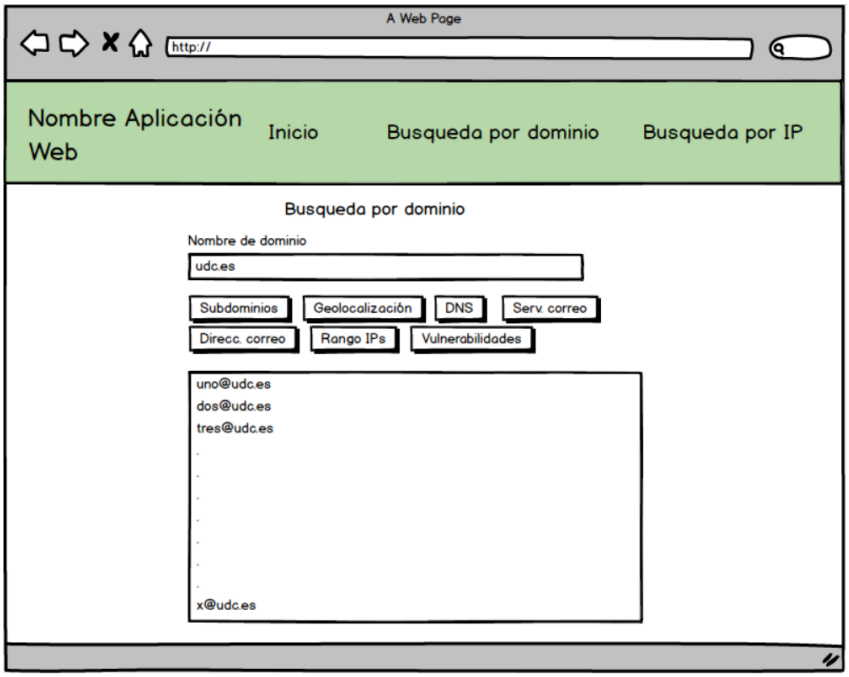

Figura 2: Pantalla de Búsqueda de Dominios

Pantalla de Búsqueda de IP: Se muestra un *text field* en el que el usuario deberá introducir la dirección IP. Bajo la caja de búsqueda, se sitúan varios botones entre los que el usuario deberá elegir según el tipo de búsqueda sobre la dirección IP que quiera realizar. Al seleccionar uno la página reaccionará, mostrándose el resultado. Desde la misma pantalla el usuario podrá seleccionar otra opción, en cuyo caso se reemplazará el resultado previo por el nuevo.

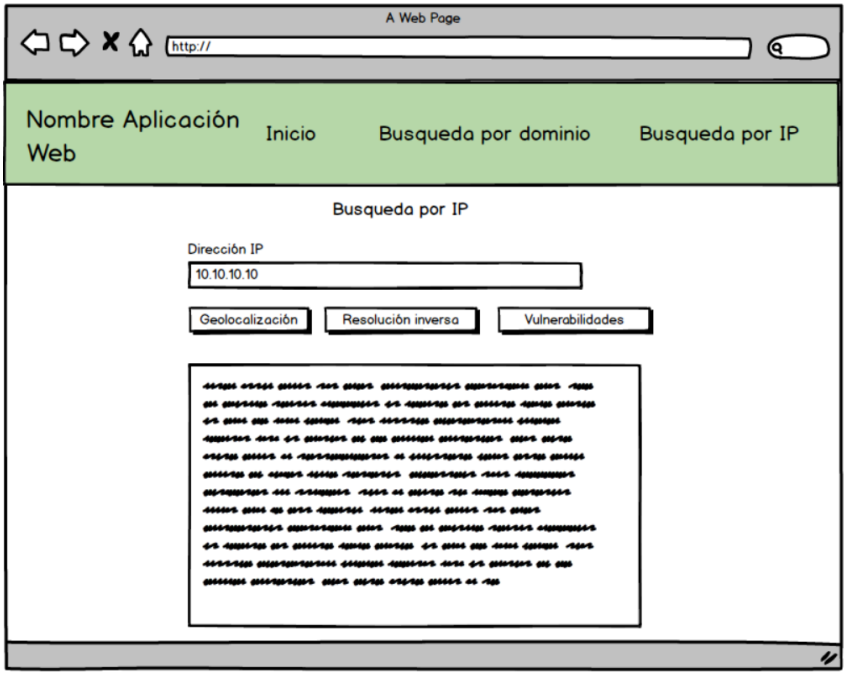

Figura 3: Pantalla de Búsqueda de IP

Flujo de datos de aplicación

- **Petición**: Ir a inicio. **Acción**: Recuperar información de la página. **Resultado**: Actualizar página.
- **Petición**: Ir a búsqueda por dominio. **Acción**: Recuperar información de la página. **Resultado**: Actualizar página.
- **Petición**: Ir a búsqueda por IP. **Acción**: Recuperar información de la página. **Resultado**: Actualizar página.
- **Petición**: Clicar en el botón subdominios. **Acción**: Mandar y recibir petición de la API Project Sonar. **Resultado**: Actualizar es espacio de resultados con una gráfica generada por Pandas y una tabla con información acerca de los subdominios relacionados con el dominio que se proporciona.
- **Petición**: Clicar en geolocalización (búsqueda por dominio). **Acción**: Mandar y recibir petición de la API IPStack. **Resultado**: Actualizar el espacio de resultados con una tabla cuyo contenido es información sobre la geolocalización del dominio introducido.
- **Petición**: Clicar en DNS. **Acción**: Mandar y recibir petición de la API Robtex. **Resultado**: Actualizar el espacio de resultados con una tabla que tiene por contenido los nombres de dominio de los servidores DNS relacionados con el dominio introducido.
- **Petición**: Clicar en servidores de correo. **Acción**: Mandar y recibir petición de la API Robtex. **Resultado**: Actualizar texto de la página.
- **Petición**: Clicar en direcciones de correo. **Acción**: Emplear script de búsqueda de correos. **Resultado**: Actualizar el espacio de resultados con una tabla que tiene por contenido los nombres de dominio de los servidores de correo relacionados con el dominio introducido.
- **Petición**: Clicar en rango de IPs. **Acción**: Mandar y recibir petición de la API Ripe. **Resultado**: Actualizar el espacio de resultados con un texto que indica el rango de direcciones IP a las que pertenece el dominio introducido.
- **Petición**: Clicar en vulnerabilidades (búsqueda por dominio). **Acción**: Mandar y recibir petición de la API Shodan. **Resultado**: Actualizar el espacio de resultados con dos cajas de resultados, una con los puertos que tiene abiertos el dominio introducido y otra caja cuyo contenido es una tabla con la lista de posibles vulnerabilidades de ese dominio.
- **Petición**: Clicar en vulnerabilidades (búsqueda por IPs). **Acción**: Mandar y recibir petición de la API Shodan. **Resultado**: Actualizar el espacio de resultados con dos cajas de resultados, una con los puertos que tiene abiertos la dirección IP introducida y otra caja cuyo contenido es una tabla con la lista de posibles vulnerabilidades de esa dirección IP.
- **Petición**: Clicar en geolocalización (búsqueda por IPs). **Acción**: Mandar y recibir petición de la API IPStack. **Resultado**: Actualizar el espacio de resultados con una tabla cuyo contenido es información sobre la geolocalización de la dirección IP introducida.
- **Petición**: Clicar en resolución inversa. **Acción**: Mandar y recibir petición de la API Project Sonar. **Resultado**: Actualizar el espacio de resultados con un texto que indica el dominio al que pertenece la dirección IP introducida.

APIs utilizadas

- Project Sonar
- IPstack
- Robtex
- Ripe
- Shodan

Información a extraer de Project Sonar

Esta API se utilizará para extraer información relacionada con los subdominios relacionados con el dominio introducido por el usuario. Por cada subdominio se obtendrá:

- Su nombre (ej. ejemplo.des.udc.es).
- Su dirección IP.
- El tipo de registro (ej. cname, mx, ns, etc.).

También se utilizará para realizar una resolución inversa de IP a nombre de dominio.

Información a extraer de IPstack

La información a extraer de esta API estará relacionada con la geolocalización de la dirección IP o el dominio proporcionado. Los datos que se mostrarán son:

- La dirección IP.
- El país en el que está situada.
- La región en la que está situada.
- La ciudad.
- Las coordenadas de latitud y longitud.
- El emoticono de la bandera del país.

Información a extraer de Robtex

Esta API se utilizará para obtener los servidores DNS que pertenecen a un dominio y los servidores de correo. La información que se obtendrá tanto para los servidores DNS como los de correo será:

- El nombre de dominio.
- La dirección IP.

Información a extraer de Ripe

Esta API será utilizada para obtener el rango de direcciones al que pertenece un dominio, ya que es altamente probable que las direcciones de ese rango estén relacionadas con el dominio en cuestión. La información que se extraerá será:

- El rango de direcciones al que pertenece el dominio.

Información a extraer de Shodan

Esta API será utilizada para obtener un listado de los puertos abiertos de la dirección introducida, así como las posibles vulnerabilidades relacionadas con la versión de los servicios que están corriendo en la máquina a la que pertenece esa IP o dominio. La información que se extraerá de esta API será:

- Vulnerabilidades de la maquina a la que está asociado el dominio o IP.
- Lista de puertos abiertos en esa máquina.

Uso de Pandas dentro de la práctica

- **F1**: Se transformarán los datos obtenidos de la API *Project Sonar* en un *DataFrame*, se filtrarán los campos 'Nombre', 'IP' y 'Tipo de registro', y estos serán ordenados por el campo 'Nombre' alfabéticamente y contados (mediante *count()*). Además junto a matplotlib se proporcionará un gráfico de sectores que refleje los porcentajes de cada 'Tipo de registro'.
- **F3 y F4**: Se transformarán los datos obtenidos de la API *Robtex* en un *DataFrame* para ser mostrado.
- **F5**: Se transformarán los datos obtenidos con las librerías *google* y *beautifulsoup4* en una *Series* para ser mostrado.

Uso de librerías externas

Las librerías externas que utilizaremos serán:

- beautifulsoup4
- google
- mathplotlib
- shodan
- emoji-country-flag

Las librerías beautifulsoup4 y google se utilizarán para implementar la funcionalidad F5 (Descubrir direcciones de correo).

La librería mathplotlib la utilizaremos para hacer gráficos de los datos procesados por pandas en la funcionalidad F1 (descubrimiento de subdominios).

La librería shodan la utlilizaremos para interactuar de una manera más sencilla con el API REST de Shodan.

La librería emoji-country-flag se utilizará para obtener el emoticono de la bandera del país que se obtiene en la funcionalidad F2 (geolocalización de dominio o IP).

Integración con otros lenguajes de programación

Utilizaremos JavaScript (AJAX) en el *frontend* de la aplicación para manejar los eventos de pulsar los botones relacionados con las funcionalidades, además se utilizara para cambiar la zona de resultados de la página sin necesidad de recargar o cambiar de página.