UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Politécnica Superior de Gandia

Estudio de la ciberseguridad de la aplicación web O-City.org: análisis de vulnerabilidad y plan de mejora

Trabajo Fin de Grado

Grado en Ingeniería de Sistemas de Telecomunicación, Sonido e Imagen

AUTOR/A: Redondo Pereira, Sebastián

Tutor/a: Marín-Roig Ramón, José

CURSO ACADÉMICO: 2021/2022

Resumen

En la actualidad la seguridad de los sistemas de la información ha adquirido especial importancia debido al aumento exponencial que han tenido los ataques por parte de los cibercriminales. Es por ello que en este trabajo realiza una auditoria paso a paso de hacking ético a un portal/aplicación web, en este caso concreto se analiza el portal O-CITY.org. Durante el desarrollo de este trabajo se pueden ver algunos de los ataques más comunes a páginas web, con su explicación detallada y un propuesta de resolución. Además, se exponen algunas de las herramientas y estándares que se pueden usar en la elaboración de una auditoría.

Palabras clave: hacker, vulnerabilidad, ciberdelincuente, Sombrero blanco.

Summary

Currently, the security of information systems has acquired special importance due to the exponential increase in attacks by cybercriminals. That is why in this work a step-by-step ethical hacking audit of a web portal/application is carried out, in this specific case the O-CITY.org portal is analyzed. During the development of this work you can see some of the most common attacks on web pages, with their detailed explanation and a resolution proposal. In addition, some of the tools and standards that can be used in the preparation of an audit are exposed.

Keywords: hacker, vulnerability, cybercriminal, White Hat.

Tabla de contenidos

Tabla de figuras

1. Introducción

Este trabajo se embarca dentro de un proyecto europeo en el cual se ha desarrollado O-CITY.org. Esta aplicación geoposiciona los recursos naturales y culturales de las ciudades en un mapa y permite la interacción de usuarios a diferentes niveles. En este trabajo se ha realizado una auditoria detallada de seguridad de la información.

1.1 Motivación

Cabe decir que no me dedico profesionalmente al mundo de las auditorías de ciberseguridad, aunque sí que trabajo dentro del área de seguridad de la información de un organismo público como personal externo, el Hospital la Fe de Valencia. Mi papel dentro de esta entidad es más de mantener la red libre de ataques haciendo que se cumpla la política de seguridad del centro y manteniendo los sistemas actualizados y el firewall correctamente configurado.

Fue a través de la directora desarrollo de O-CITY, Marta Belén Ciudad, como conocí la plataforma y bajo su consentimiento dejé que mi curiosidad y mis conocimientos obtenidos de forma autodidacta hicieran el resto, no todos los días se tiene vía libre sobre una plataforma en producción aparentemente bien desarrollada.

Siempre he considerado que aquellos que decidimos estudiar una ingeniería tenemos algo en común, la curiosidad por saber cómo están construidas las cosas y su funcionamiento, no nos quedamos en la superficie, queremos ver las entrañas y solo así comprendemos la utilidad de cada una de las partes que forman la maquinaria, el software, la red, etc. Que tenemos delante. Esa visión nos hace encontrar puntos de fallo y poder replicar y mejorar todo aquello que hemos aprendido.

Desde siempre me he sentido atraído por el descubrimiento de puntos débiles y la explotación de ellos, pero como ya he dicho, no me he dedicado profesionalmente a ello y aunque sí que he leído mucho y he usado plataformas de retos como Atenea del CCN-CERT para poner a prueba mis conocimientos, no había tenido la oportunidad de desarrollar algo que siempre había querido realizar, mi propia auditoria web.

1.2 Objetivos

Los objetivos definidos en este trabajo son los siguientes:

- Realizar de una auditoria web.
- Ubicar el nivel de seguridad de la plataforma O-CITY, actualmente puesta en producción pero en continuo desarrollo y evolución.
- Evidenciar vulnerabilidades y categorizarlas según su criticidad (alta, media y baja).
- Concienciar tanto al equipo de desarrollo de O-CITY como al lector de este trabajo, sobre la importancia de la ciberseguridad en portales web y su implantación desde la fase inicial de desarrollo.

1.3 Impacto Esperado

Con la redacción de este documento se pretende aportar un nivel de seguridad alto para la plataforma O-CITY, evitando que un atacante pueda tener control total de la plataforma, pudiendo robar datos de gran valor para la plataforma, como contenido multimedia o información sobre el patrimonio cultural que en su base de datos se almacena, como información más sensible para el usuario como pueden ser su datos de perfil (usuario, correo y contraseña).

1.4 Estructura

Durante la lectura de este documento el lector conocerá a través del estado del arte los orígenes de la ciberseguridad y su evolución hasta día de hoy, aprenderá los diferentes tipos de hackers que existen según su código ético, entenderá la importancia de tener en cuenta la seguridad desde fases tempranas del desarrollo y la complejidad de cubrir ese área en una aplicación en producción. Con todo ello se podrá ver el valor de una auditoria de seguridad.

En los siguientes puntos veremos en que consiste el proyecto de O-CITY, analizaré la problemática del portal y la metodología a seguir, basándome en los 10 ataques más comunes categorizados por OWASP y sus recomendaciones.

Desarrollare lo propuesto mostrando las vulnerabilidades detectadas y desarrollando el proceso de investigación y detección. Además, se hará un análisis web a nivel de usabilidad, proponiendo cambios para mejorar la experiencia de usuario.

2. Estado del arte

En mundo digitalizado donde los servicios a través de internet están normalizados y la sociedad está hyperconectada, la seguridad de la información se convierte en una cualidad fundamental para todo aquel que quiere ofrecer sus servicios a través de la red.

En los años 70, la seguridad de los sistemas no se contemplaba como veremos a continuación. Es cierto que para esa década no había tanta accesibilidad a los equipos informáticos como se logró en los 80 y no se consideraba la posibilidad de un ciberataque.

Veamos cómo ha evolucionado la seguridad de la información en las últimas décadas, para comprender en el punto en el que nos encontramos hoy en día y el fin con el que se elabora este trabajo fin de carrera.

2.1. ¿Qué es la ciberseguridad?

Como ya se ha nombrado, la ciberseguridad hoy en día es fundamental para cualquier organización, formando parte de su estructura organizacional, siendo el área encargada de la protección de los sistemas informáticos y todo lo vinculado a estos, especialmente la información contenida en ordenadores, servidores, redes de datos, etc.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información.

Según ISACA (Information Systems Audit and Control Association), asociación internacional que apoya el desarrollo de metodologías y certificaciones para la realización de auditorías y control en sistemas de información, la ciberseguridad se define como "una capa de protección para los archivos de información"

2.2. ¿Cómo ha evolucionado la ciberseguridad?

Viendo la evolución de los sistemas de seguridad en el entorno de los datos, tenemos una visión mucho más clara de cómo ha evolucionado el mundo digital y los riesgos que han ido surgiendo a lo largo de los años.

En este punto es importante hacer una distinción entre hacker y ciberdelinuente, ya que habitualmente se confunden. El INCIBE (Instituto Nacional de Ciberseguridad) hace la siguiente definición de los dos términos:

> *"Un **hacker** es aquella persona que trata de solventar, paliar o informar sobre los problemas de seguridad encontrados en programas, servicios, plataformas o herramientas.*
>
> *El **ciberdelincuente** es la persona que buscará sacar beneficio de estos problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware."*

Una vez hecha esta aclaración, se entenderá mucho mejor el rol que ha tenido cada una de las personas nombradas a continuación.

Nevil Maskelyne en 1903 interceptó la primera transmisión de telégrafo inalámbrico, dejó al descubierto las vulnerabilidades del sistema desarrollado por Marconi. Hoy en día es considerado el primer hacker de la historia.

En la década de los setenta cuando apareció el primer ciberdelincuente, John Draper, también conocido como "Captain Crunch". Draper, descubrió que el sonido emitido por un silbato que regalaban en las cajas de cereal de "Captain Crunch", podía engañar a la señal de la central telefónica y realizar llamadas gratuitas. Por este delito fue arrestado en 1972. A la manipulación de un teléfono o la línea telefónica se le llama phreaking y no hacking como podríamos imaginar en un primer momento.

En 1975 el club llamado Homebrew Computer Club, formado por un grupo de hackers experimentó con los primeros PCs, como el Altair 8800, al que consiguieron programar para que cantara la canción Daisy Bell. Su principal motivación era la de divertirse, encontrar nuevos retos y puntos de desarrollo que marcaron algunos de los avances de la informática. Un dato importantes es que de este grupo surgieron 23 empresas de tecnología y algunos de sus miembros forman parte de empresa como Apple o Microsoft.

Fue también en los años 70s cuando apareció lo que se considera el primer malware de la historia: Creeper. Este programa se copiaba así mismo mostrando el mensaje "I'm a creeper, catch me if you can!" - Soy Creeper atrapame si puedes. En respuesta a este malware, se creó el primer antivirus, Reaper, su función era la de eliminar las infecciones por Creeper.

Figura 1 Texto que mostraba Creeper

A finales de los 80 se conoció por primera vez la utilización de la ingeniería social para obtener información personal y confidencial. Este ciberataque fue perpetrado por Kevin Mitnick y comenzó a popularizarse entre los cibercriminales. Actualmente sigue siendo uno delos métodos más usados para vulnerar los activos de una empresa, ya que si objetivo principal es el eslabón más débil de una empresa, el usuario.

Mitnick desarrolló los cuatro principios de la ingeniería social:

- Todos queremos ayudar.
- El primer paso es siempre confiar en el otro.
- No nos gusta decir «no».
- A todos nos gusta que nos alaben.

Mitnick pasó 5 años en prisión, en los que estuvo 8 meses en una celda de aislamiento por el miedo del Estado a sus habilidades.

Con el paso de los años y en la década de los 90 los ciberataques a empresas y gobiernos habían aumentado de forma sustancial, convirtiéndose en una de las principales preocupaciones para los políticos de entonces, llegando a convertir el tema en discusión internacional. El desconocimiento de Internet era gerenal, además de la falta de regulación, no existía normativa global alguna que regulara su uso y la falta de este componente legal afectaba especialmente a los países desarrollados, aquellos que mayor uso de la red hacían.

En 1995, se formó en Europa un comité de expertos en delitos informáticos para trabajar en estrategias y contrarrestar los ataques a través de Internet. Convencidos de la necesidad de aplicar una política penal para proteger a la sociedad frente a la

ciberdelincuencia y la importancia de fortalecer la cooperación internacional, para 2001 se aprobó y firmó el Convenio de Budapest, que hoy en día es integrado por 56 países.

En España, el Centro Nacional de Inteligencia, creó su propia división para estudiar y combatir los ciberataques, el CCN-CERT. Del mismo modo, cada comunidad autónoma ha creado su grupo de respuesta frente a ataques en sus sistemas, en la Comunidad Valenciana tenemos el CSIRT-CV. En la actualidad, el CCN-CERT trabaja en lo que han llamado "Un escudo único", un proyecto con el que se pretende aunar tanto empresas como entidades públicas, aportando una visión global de todo lo que ocurre en territorio nacional. Con este "escudo único" la infección de una empresa en Galicia, aportaría información en tiempo real a un ayuntamiento en Valencia, consiguiendo que este actúe antes de recibir cualquier tipo de ataque.

A pesar de saber que se han de proteger la información, no ha sido hasta hace un par de años que el mundo empresarial ha sido realmente consciente de la importancia de invertir en ciberseguridad, pues no solo es la protección de los sistemas informáticos la que hay que mantener, sino que además, es la confidencialidad, integridad, disponibilidad y autenticidad del dato.

Las aplicaciones web y en la nube son uno de los vectores de ataque favoritos por una sencilla razón: tienen más probabilidades de éxito. En su informe «2020 Data Breach Investigations Report», Verizon indica que los ataques a aplicaciones web siguen siendo uno de los principales vectores de amenaza en cuanto a violaciones de la seguridad.

Es en este punto en el que entra en escena la importancia del hacking ético y las auditorías de ciberseguridad o también llamadas auditorias de hacking ético.

Figura 2 Las tres categorias de hackers

Pero antes y como de colores va el asunto, veamos las tres categorías de hackers que existen y sus motivaciones éticas:

- **Sombrero negro:** son aquellos a los que les motiva ganar dinero de manera ilegal. Por lo general, suelen pertenecer a un grupo u organización que se encarga de realizar acciones delictivas con el único fin de lucrarse. Campañas de phishing, desarrollo de malware, robo de información, etc. Son algunas de las acciones que este tipo de hackers llevan a cabo en su día a día.

- **Sombrero blanco:** también conocido como hacker ético o hacker bueno. Se encuentran en el lado opuesto a los hackers de sombrero negro, su uníca

motivación es encontrar vulnerabilidades en los sistemas a los que acceden, informar y proponer mejoras para subsanar los errores detectados.

- **Sombrero gris:** el hacker de sombrero gris se encuentra en la frontera entre los actos de un hacker de sombrero blanco y uno de sombrero negro. Este tipo de hackers suele atacar sistemas sin el consentimiento de su propietario, cuando encuentra vulnerabilidades se pone en contacto con este para informarle, ofreciendo sus servicios para resolver los problemas detectados a cambio de una compensación económica.

De acuerdo con la historia del hacking, el mundo ha tardado en darse cuenta de que no todos los hackers son de sombrero negro. Es decir, practicar el hacking cibernético no es sinónimo de ser un ciberdelincuente. El hacking ético, actualmente dispone de gran valor en el mundo empresarial. Actualmente, los hackers de sombrero blanco pueden simular ataques a compañías, bajo su consentimiento, con el fin de reportar posibles fallos y vulnerabilidades. El hacking está perdiendo su estigma y la sociedad lo está aprovechando.

2.3. Crítica al estado del arte

Como hemos podido ver, los portales online son uno de los principales objetivos de los atacantes, ya que durante su desarrollo no se aplican los procedimientos de seguridad necesarios. Este es el caso de la plataforma O-CITY, desarrollada por la UPV, sin abordar en su primera fase el problema de la seguridad.

2.4. Propuesta

Con este trabajo fin de grado se realiza una auditoria web, explicando de forma didáctica el tipo de ataques que se van a llevar a cabo, de forma que todo aquel que lea el documento pueda entender sin necesidad de tener grandes conocimientos en seguridad lo que se está haciendo y en que afecta para el portal auditado. Además, se presentará una propuesta de mejora que ayudará a todo aquel que tenga un portal y quiera evitar tener las vulnerabilidades detectadas.

3. Descripción de la plataforma O-CITY.org

Los siguientes datos están obtenidos de la página web del portal O-CITY, cuento con el consentimiento de los jefes de proyecto para usar dicha información.

3.1. Datos Técnicos:

El proyecto O-CITY (Orange: Creativity, Innovation & TechnologY) ha sido desarrollado en el marco del programa europeo Erasmus+ (Knowledge Alliance). Ha recibido una financiación de 992.472€ y su periodo de implementación se extiende desde el 1 de enero de 2019, hasta el 31 de diciembre de 2021. 13 socios de 6 países diferentes (España, Italia, Grecia, Serbia, Eslovenia y Colombia) han Trabajó durante este período liderados por la UPV (Universitat Politècnica de València – España).

3.2. Retos del Proyecto:

El proyecto persigue tres objetivos.

1 La **transformación digital** de los sectores económicos tradicionales a través de la formación de profesionales y la promoción económica de las ciudades mediante el turismo cultural y natural.

2 La introducción de **herramientas educativas innovadoras** a través de planes de formación en competencias tanto profesionales como personales diseñadas para facilitar el trabajo de los profesores en sus aulas.

3 El **descubrimiento y la promoción de la cultura** , el patrimonio, las tradiciones y el entorno natural de las ciudades del mundo.

En resumen, **O-City es un proyecto de participación ciudadana** , donde los destinos turísticos a través de su sistema educativo, ofrecen a sus propios ciudadanos la posibilidad de **aportar** su punto de vista en formato multimedia, sobre el patrimonio natural y cultural de la ciudad, sin renunciar al rigor que exige la información pública (a disposición de los turistas) sobre el destino.

O-City permite **exportar sus datos de patrimonio a otras aplicaciones, a través de una API** . De esta manera, hay ciudades con App para turismo que usan los datos de O-City, junto con los de restaurantes, hoteles, eventos, diversión, etc., para ofrecer a sus turistas una experiencia integral en el destino.

3.3. Herramientas desarrolladas:

Se han desarrollado dos herramientras:

1. El mundo de las ciudades O-City.org , una aplicación web responsive para visualizar el patrimonio natural y cultural de las ciudades. En esta aplicación (de gestión

distribuida) participan diferentes actores como gestores públicos municipales, responsables universitarios, profesores, etc.

2. La plataforma educativa O-City , destinada a los profesores, que ofrece cursos (MOOC) distribuidos en 4 módulos de formación en materia de negocios, técnica (multimedia), cultural y habilidades blandas.
   El proyecto O-City no podría entenderse sin estas dos herramientas operando juntas:

- por una parte a través de los planes formativos, estudiantes de diferentes ciclos pueden desarrollar proyectos multimedia en sus aulas (**foto, video, podcast, animación, comic, infografía**), dirigidos por sus profesores, sobre elementos de patrimonio natural y/o cultural de sus propias ciudades;

- y por otra parte el premio por el trabajo bien hecho es poder exhibir estos trabajos en la plataforma del mundo de las ciudades, donde todo el mundo puede verlos y aprender con ellos.

3.4. Programa de Formación O-City :

O-CITY aborda la formación de los futuros profesionales de la economía naranja desde un punto de vista integral, es decir combinando enseñanzas y aprendizajes en diferentes áreas de conocimiento, a la vez que estimula el trabajo en equipo. Esto es así porque considera que un profesional de este sector del siglo XXI, para integrarse en el mercado laboral o para crear su propia empresa, va a necesitar tanto conocimientos técnicos como conocimientos en materia de negocios, culturales y por supuesto habilidades blandas.

3.5. Acreditación de competencias y certificación de conocimientos:

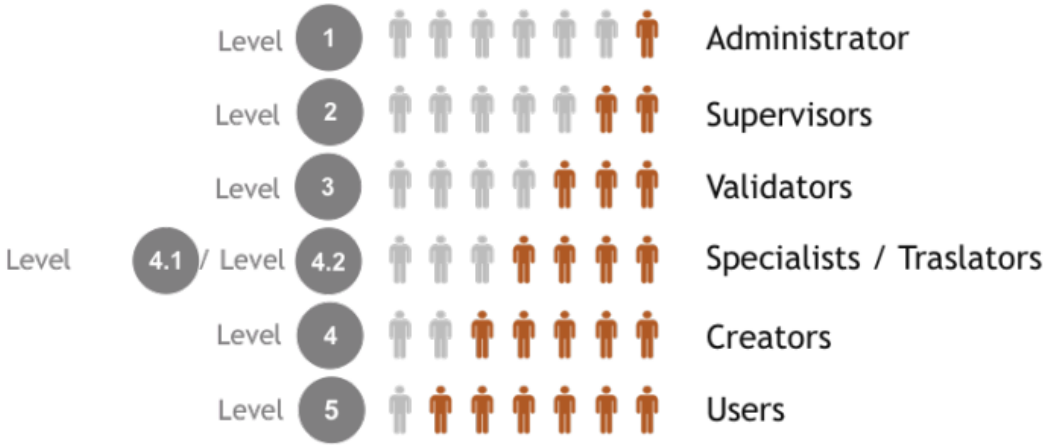
En el caso de los alumnos que participen en el proyecto, son los profesores los que validen las competencias, adquiridas a través de sencillos formularios que rellenarán cuando suban el multimedia a O-City.org. De esta manera **los estudiantes podrán ir completando su curriculum digital a medida que realicen diferentes proyectos,** y sumando insignias que acreditan las competencias adquiridas.

Los profesores que realicen cualquier curso de formación, podrán obtener en primer lugar, un **certificado de aprovechamiento del centro de formación permanente de la UPV** y en segundo lugar una **certificación EUROPASS** de la UE.

4. Estructura de usuarios en O-CITY

El proyecto O-City incluye una red de colaboradores que debe reflejarse en los usuarios de la plataforma. Cada uno de estos usuarios tendrá diferentes funcionalidades. La estructura de usuarios debe contemplar diferentes niveles, de forma que los usuarios de niveles inferiores dispongan de todas las funcionalidades de los niveles posteriores.

La siguiente figura muestra, a modo de estructura piramidal, la descripción de los diferentes usuarios y niveles:



5. Análisis del problema

Para comenzar a analizar el problema, lo primero que debemos es estudiar la página web que vamos a auditar. Por tanto, vamos a ver en que consiste O-CITY.

Figura 3 Página de inicio de O-CITY

Lo primero que vemos al acceder a https://O-CITY.org es un mapa, pero en esta primera imagen hay varias cosas que ya llaman la atención de alguien que esté buscando errores. En primer lugar, el favicon (icono de favoritos): Este icono ofrece una buena imagen del portal web en marcadores y barras de navegación. El favicon configurado actualmente para O-CITY no está bien dimensionado. Su visualización en la barra de navegación es la siguiente:

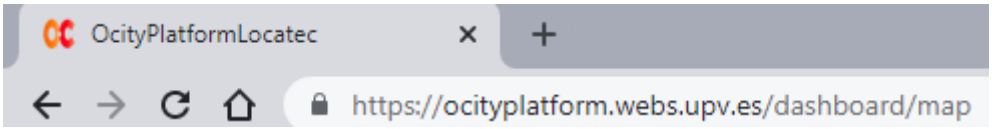


Figura 4 Barra de direcciones con favicon de O-CITY

Descargando la imagen utilizada obtenemos la siguiente:

Figura 5 Favicon bien dimensionado

Este icono tiene unas dimensiones de 16x9. Los tamaños más comunes para faviconos, según la calidad del icono, son 16x16, 32x32, 48x48, 64x64 y 128x128. Por tanto, el favicono utilizado no cumple con las medidas indicadas en las buenas prácticas de diseño web.

La imposibilidad de poder ver todos los filtros usando una resolución de pantalla de 1366x768.

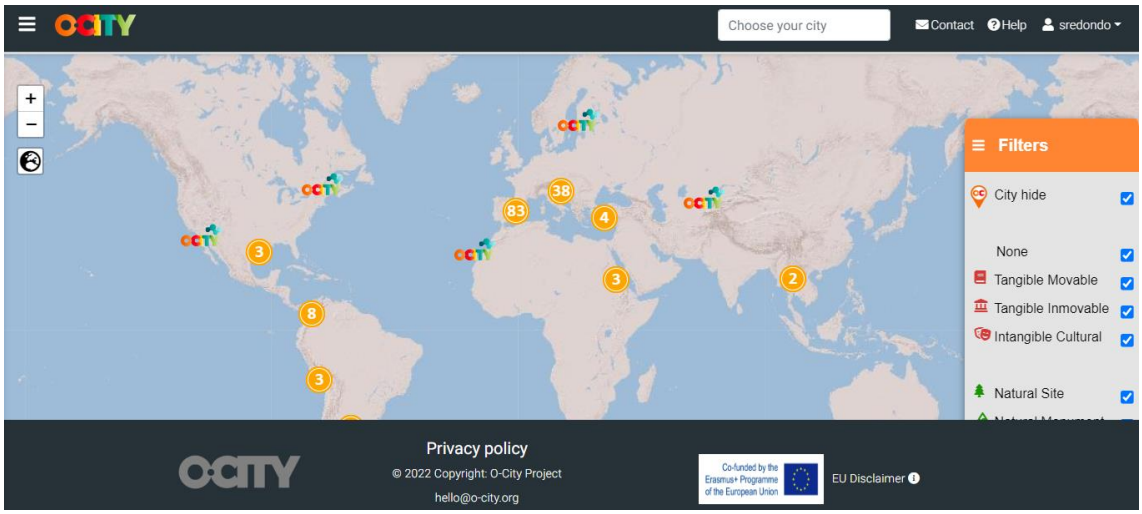


Figura 6 Filtros de O-CITY con problemas de visibilidad

La imagen del programa Erasmus vemos que está mal dimensionada.

Figura 7 Logo del programa Erasmus mal dimensionado

Y uno de los errores más importantes de esta página principal, la política de privacidad, no existe. Tenemos un hipervínculo pero no lleva a ningun sitio.

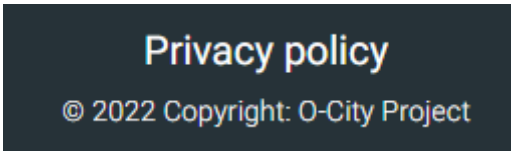


Figura 8 Política de privacidad

Encontrar todas estas deficiencias en la pagína principal no transmite confianza al usuario normal que acceda a la web y alerta a aquellos usuarios con conocimientos que no tengan buenas intenciones. Al fin y al cabo, si estos errores están a la vista de todo el mundo, que otros errores puede haber detrás. Es por ello que es necesario hacer un análisis en profundidad y comprobar si el portal es resistente a algunos de los ataques más comunes que sufren las aplicaciones web hoy en día.

Para analizar el estado en el que se encuentra la plataforma O-CITY se va a utilizar la categorización que OWASP (Open Web Application Security Project) de los 10 principales riesgos a los que se enfrentan las aplicaciones web/móviles.

La creación de este TFG viene motivada por la detección de fallos de seguridad en la plataforma O-CITY, portal en el que se almacenan información del patrimonio cultural y social a nivel mundial. Además es un portal en el que los usuarios pueden registrarse introduciendo sus datos personales y proponer lugares patrimoniales a los administradores del portal, pudiendo adjuntar archivos multimedia en sus propuestas. Este proyecto se encuentra en este momento en desarrollo, pero su portal web lleva unos meses en activo, lo que hace que sea de vital importancia realizar un análisis en profundidad de su estado de seguridad, ya que está comenzando a tener un flujo de usuarios pertenecientes a países de todo el mundo.

En la siguiente tabla hago uso de la categorización realizadas por OWASP del top 10 de amenazas que afectan a las aplicaciones web. En ella podemos ver de forma visual y rápida la amenazas que afectan de manera directa al *site* O-CITY.org

OWASP TOP 10 - 2017	Estado O-CITY
A1: Inyección	Vulnerable
A2: Fallos en authenticación	Sin evidencias
A3: Exposición de datos sensibles	Vulnerable
A4: Entidades externas XML	Sin evidencias
A5: Fallos en el control de acceso	Vulnerable
A6: Configuracion de seguridad incorrecta	Vulnerable
A7: Cross-Site Scripting (XSS)	Vulnerable

A8: Problemas en el software y en la integridad de los datos	Sin evidencias
A9: Componentes vulnerables y desactualizados	Vulnerable
A10: Logging y monitorización insuficiente	Vulnerable

Tabla 1 Estado de O-CITY en Top 10 amenazas OWASP

6. Análisis del marco legal y ético

Cuando hablamos del marco legal que debe cumplir las herramientas online como O-CITY, tenemos varias leyes y normas a seguir:

- El Reglamento General de Protección de Datos (RGPD) es el reglamento que afecta a la protección de personas físicas en lo que respecta al tratamiento de sus datos personales y la libre circulación de estos. Está fue publicada el 24 de mayo de 2016 y no fue hasta dos años después, 25 de mayo de 2018 cuando comenzó a aplicarse. Es de obligado cumplimiento para toda empresa que pertenezca la Unión Europea o trabaje en territorio de la Unión.

- La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD), adapta el derecho interno español al RGPD.

- ISO 27001. Aunque no es de obligado cumplimiento garantiza al desarrollador seguir las mejores prácticas en seguridad de la información, aportando al usuario confiabilidad en el sitio al cumplir con sus recomendaciones.

Dentro de las tareas de auditoria que se realizan dentro de este trabajo, al tratarse de acciones permitidas por los responsables del portal auditado, no entran dentro de ningún marco legal, este tipo de práctica se la conoce como Hacking ético.

El Hacking ético consiste en poner a prueba un sistema o red utilizando técnicas de ataque reales con el fin de evidenciar vulnerabilidades. A diferencia de lo que haría una ciberdelincuente, el hacker ético hace muestra al propietario del elemento analizado las vulnerabilidades detectadas, dándole además unas pautas de cómo proteger la empresa, los datos o la red.

Los ataques realizados de manera maliciosa como la introducción de un virus informático, el robo de cuentas y/o contraseñas, la suplantación de identidad o la publicación de contenido sin consentimiento del propietario del site, está regulado legalmente por las siguiente normativa:

A nivel europeo:

- SRI2
- Reglamento de Ciberseguridad de la UE

A nivel nacional**:**

- Normativas de seguridad nacional:

    - Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que regula los principios y organismos clave así como las funciones que deberán desempeñar para la defensa de la Seguridad Nacional.
    - Orden TIN/3016/2011, de 28 de Octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

- Normativas de seguridad:
    - Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
    - Ley 5/2014, de 4 de abril, de Seguridad Privada.
- Con relación a incidentes de seguridad, existe todo un entramado relacionado con las Fuerzas Armadas pero también se dispone de una inclusión parcial en la Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico.

- Relacionadas con las telecomunicaciones, existen las siguientes normas:
    - Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico (antes citada).
    - Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas.
    - La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
    - Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

- Relacionado con la ciberdelincuencia, encontramos inclusiones parciales en el Código Penal, la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores; o en el Real Decreto de aprobación de la Ley de Enjuiciamiento Criminal.

- También es de aplicación lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Todo esto se encuentra englobado en el Código de Derecho de la Ciberseguridad publicado en el BOE.

7. Plan de Trabajo

Aunque la realización de una auditoria de hacking ético no siempre se realiza siguiendo el mismo patrón de fases, esto depende de quien la realice y de cómo se adapte al producto (web o app) que se está auditando, si que hay algunos puntos que han de cumplirse en todo análisis. En la siguiente imagen, podemos ver los puntos que seguiremos para hacer frente al caso en el que nos encontramos:

Figura 9 Fases se una auditoria de hacking ético

Id	Tarea	Acciones realizadas	Tiempo
1	Recopilación de información	Búsqueda de información pública sobre el portal web mediante Open Sourcer Inteligent (OSINT).	6 horas
2	Escaneo de servicios	Revisión de los servicios utilizados por la herramienta O-CITY.	3 horas
3	Análisis de vulnerabilidades	Análisis del código fuente, detección y estudio de vulnerabilidades obtenidas de la recopilación de datos de las fases anteriores.	5 horas
4	Explotación de vulnerabilidades	Fase de explotación de las vulnerabilidades detectadas y realización de los ciberataques más comunes.	20 horas
5	Post explotación	Preparación de la documentación de los problemas detectados.	15 horas
6	Contramedidas y mejoras	Aportación de posibles soluciones para resolver las vulnerabilidades notificadas y propuesta de mejoras para aportar mayor confianza y fiabilidad al usuario.	16 horas
7	Redacción de TFG	Redacción y estudio de todo lo expuesto anteriormente en un solo documento para presentar como TFG.	40 horas

Tabla 2 Plan de trabajo

8. Desarrollo de la solución propuesta

8.1. FASE 1: RECOPILACION DE INFORMACIÓN PUBLICA

Con el fin de poder obtener un resultado lo más fiable posible, obtenemos de **NetMarketShare** los 7 motores de búsqueda más utilizados por los usuarios en el último año para realizar busquedas sobre O-CITY en cada uno de ellos.

Search Engine	Share
Google	69.80%
Bing	13.31%
Baidu	12.53%
Yahoo!	2.11%
Yandex	1.19%
DuckDuckGo	0.43%
Ask	0.18%

Figura 10 Los 7 motores de busqueda mas útilizados

Así se muestra el portal de O-CITY en los motores de búsqueda:

Google:

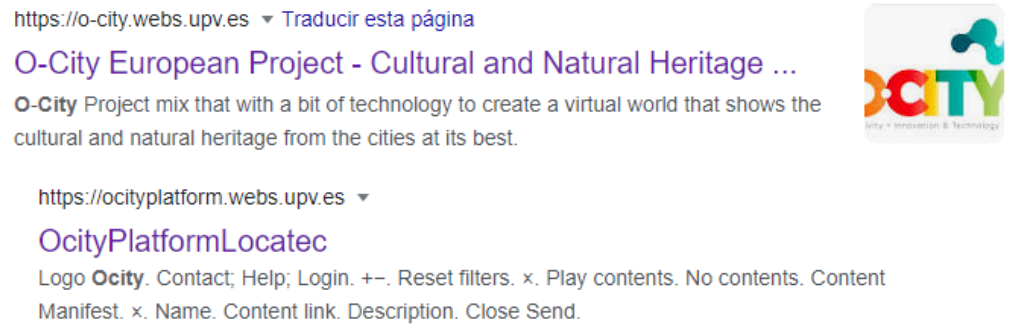


Figura 11 Resultados O-City en Google

Bing:

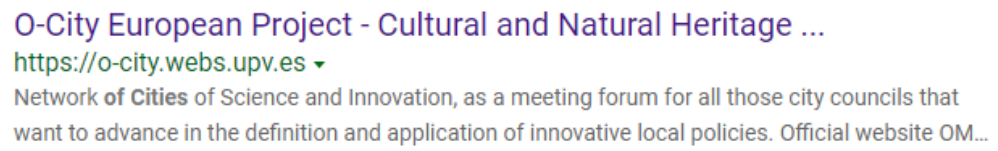


Figura 12 Resultados de O-CITY en Bing

Baidu (principal motor de búsqueda de China):

O-CITY no aparece en ninguna de las 10 primeras páginas de resultados.

Este buscador es considerado el Google chino.

Yahoo!:

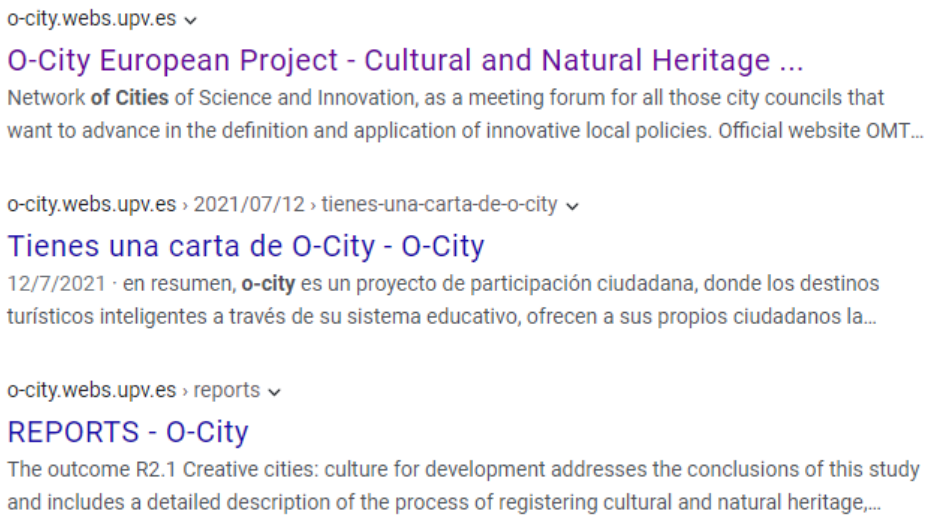


Figura 13 Resultado de O-CITY en Yahoo!

Yandex (principal buscador Ruso):

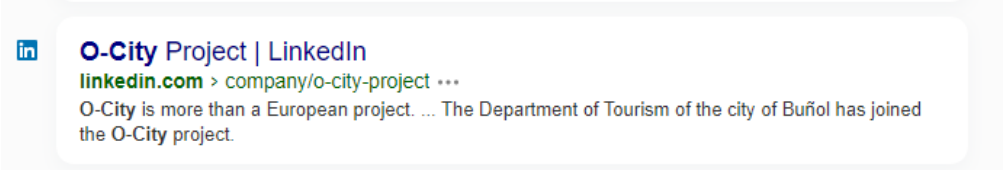


Figura 14 Resultdos de O-CITY en Yandex

Este buscador se encuentra ahora mismo en expansión, extendiéndose su uso por todo el mundo. Solo está indexado el perfil de LinkedIn, el portal no aparece en ninguna de las 10 primeras páginas de resultados. Tambien es importante tener en cuenta que este buscador es uno de los más usados por la comunidad hacker.

DuckDuckGo:

Figura 15 Resultados de O-CITY en DuckDuckGo

Ask:

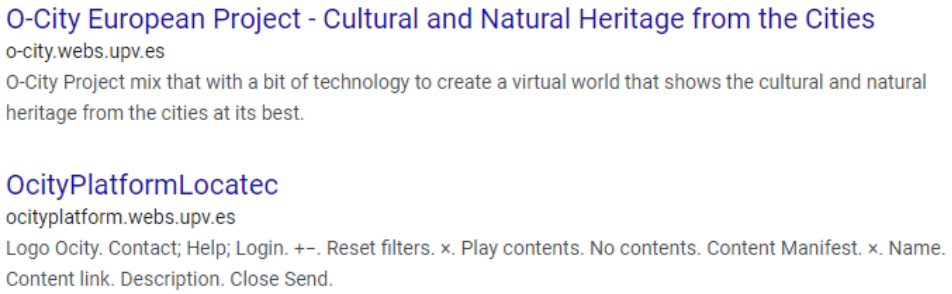


Figura 16 Resultados de O-CITY en Ask

Los resultados de búsquedas mostrados son los obtenidos de realizar la búsqueda de la palabra “O-CITY”. Si buscamos en concreto la URL del portal “ocityplatform.webs.upv.es” el resultado es el siguiente:

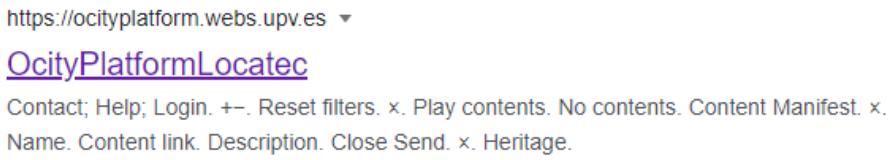


Figura 17 Resultado de buscar ocityplatform.webs.upv.es

En este caso se observa que el sitio carece de descripción, es recomendable añadir una descripción y crear un mapa del sitio, lo que ayudara a los motores de búsqueda a conocer la estructura del portal y rastrear mejor la información contenida en él. Se recomienda entonces:

- **Alargar el título de la página.**

  El título de la página seleccionado no tiene la longitud adecuada. Un título demasiado corto no tiene suficiente relevancia en los resultados de los motores de búsqueda.

- **Ampliar contenido de la página.**

  La página de inicio no tiene contenido suficiente. Añadir más contenido a la página, dará la posibilidad de atraer más visitas. Actualmente se detectan solo 62 palabras, las recomendaciones indican que ha de tener un minimo de 500 palabras.

Por otro lado, llama la atención como Baidu, el buscador considerado como el Google chino, no hace ni una sola referencia a O-CITY, principalmente cuando se trata de un territorio con un gran valor cultural.

Del mismo modo ocurre con Yandex. Aunque gran parte de sus portales indexados son de origen ruso, en los últimos meses está teniendo una gran aceptación por usuarios de todo el mundo.

Este tipo de errores, en los que vemos que no se ha desarrollado la parte SEO para que el portal tenga una buena visibilidad pública, hace saltar las alarmas en cuanto a su programación y lo que puede llamar la atención de un hacker de sombrero negro en busca de sitios web vulnerables donde poder robar información que despues sera vendida en la red oscura.

8.2. FASE 2: ESCANEO DE SERVICIOS

En esta segunda fase haré uso del navegador Chrome con la extension Wappalyzer. Esta extension detecta las tecnologías utilizadas para el desarrollo de una aplicación web. Veamos que información se obtiene simplemente accediendo a la página principal:

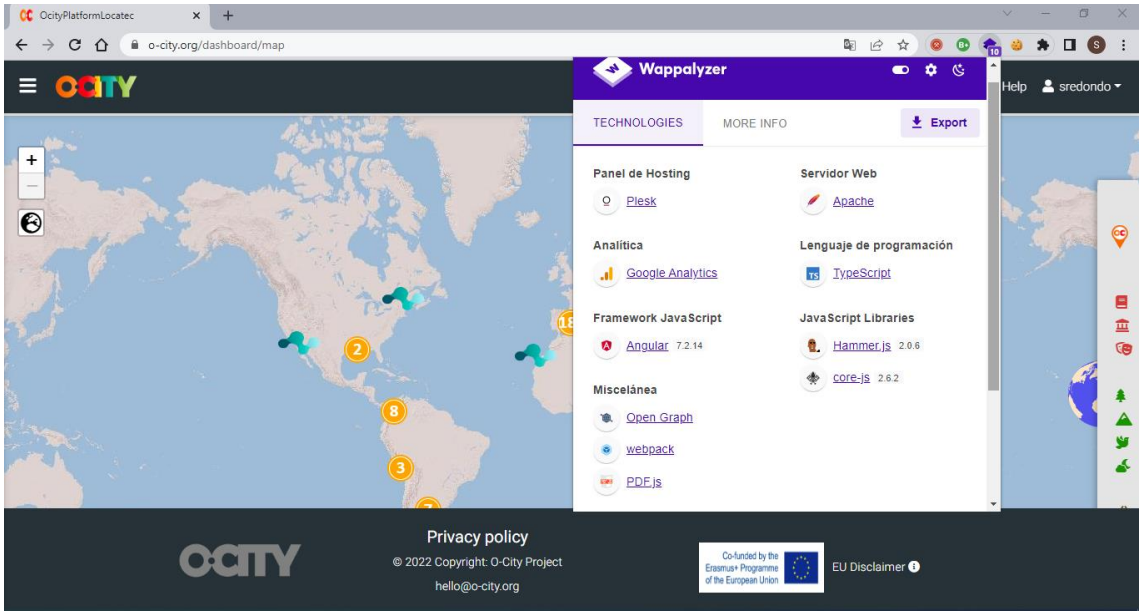


Figura 18 Servicios detectados por Wappalyzer

De esta información sacamos un dato importante, se está utilizando como hosting Plesk. Si revisamos que tipo de bases de datos admite Plesk, vemos que son tres:

- **phpMyAdmin** en el caso de bases de datos MySQL
- **pgMyAdmin** en el caso de bases de datos PostgreSQL
- **myLittleAdmin** en el caso de bases de datos SQL Server

Tambien obtenemos datos interesantes como las librerias JavaScript y su version:

- Hammer.js ver. 2.0.6
- Core.js ver. 2.6.2

Utiliza el framework Angular, version 7.2.14. En mi caso, no soy programador y no tengo conocimientos de que es realmente Angular, por lo que me veo obligado a buscar información al respecto para poder saber el motivo de estar usando este componente.

Figura 19 Logo de Angular

Por lo que he podido documentarme, Angular se trata de un Framework de JavaScript de código abierto escrito en **TypeScript** cuyo objetivo es desarrollar aplicaciones de una sola página, es decir, que toda inteccación del usuario con el portal no genere recargas en la página. Viendo el funcionamiento del portal de O-CITY, vemos que funciona en su mayoría sin necesidad de movernos de la página principal, mediante ventanas o menus superpuestos, lo que nos indica que tiene sentido que se esté usando ese framework.

8.3. FASE 3: ANALISIS DE VULNERABILIDADES

En esta fase comenzaré focalizandome en la última parte de la fase 2, las librerias javascript Hammer.js y Core.js.

Aunque esta información es importante, para nuestro objetivo no nos aporta gran valor. Consultando la página de Synk, vemos que las versiones que Hammer.js y Core.js están desactualizadas, Hammer se encuentra en la actulidad en la version 2.0.8 y Core en la version 3.25.0, pero no tienen ninguna vulnerabilidad conocida. Por tanto, damos por cerrada la posible explotación de vulnerabilidades de librerias javascript.

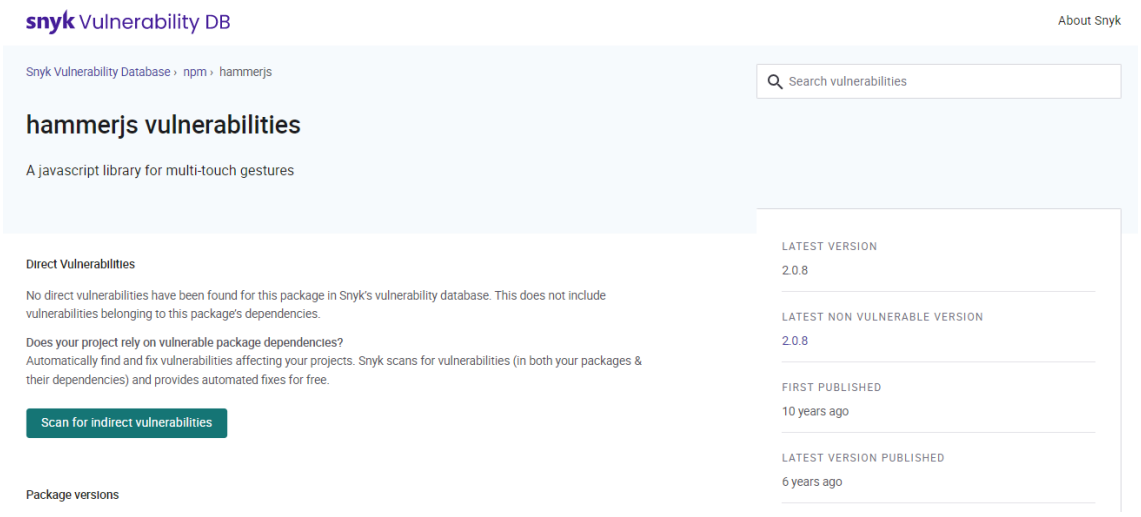


Figura 20 Vulnerabilidades de la librería hammer.js

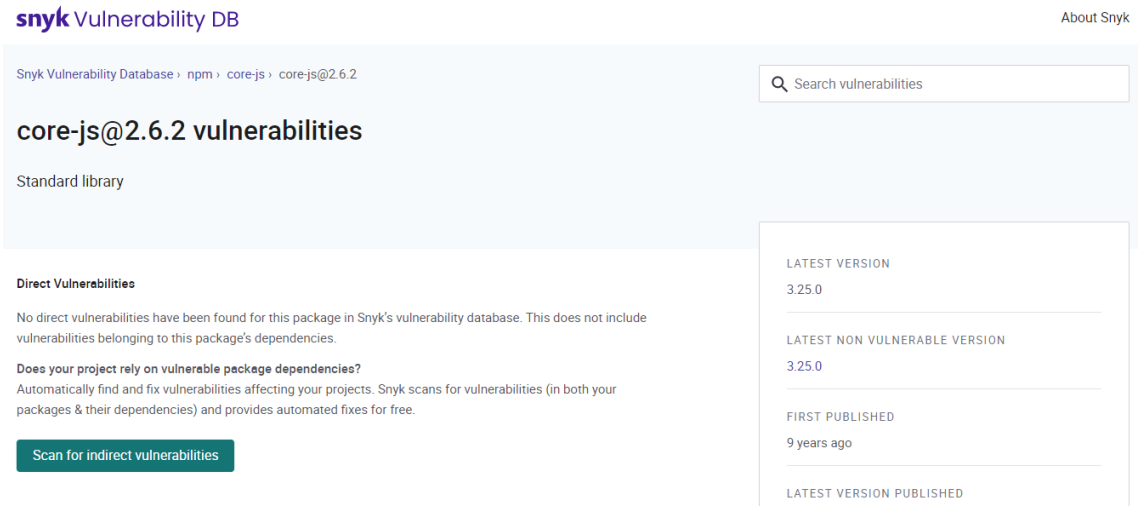


Figura 21 Vulnerabilidades de la librería core.js

Tambien vemos que utiliza el framework Angular, version 7.2.14. Del mismo modo con una simple busqueda en Google, vemos en el portal de snyk que la version de Angular utilizada si que tiene vulnerabilidades que podrian ser explotadas por un ciberdelincuente.

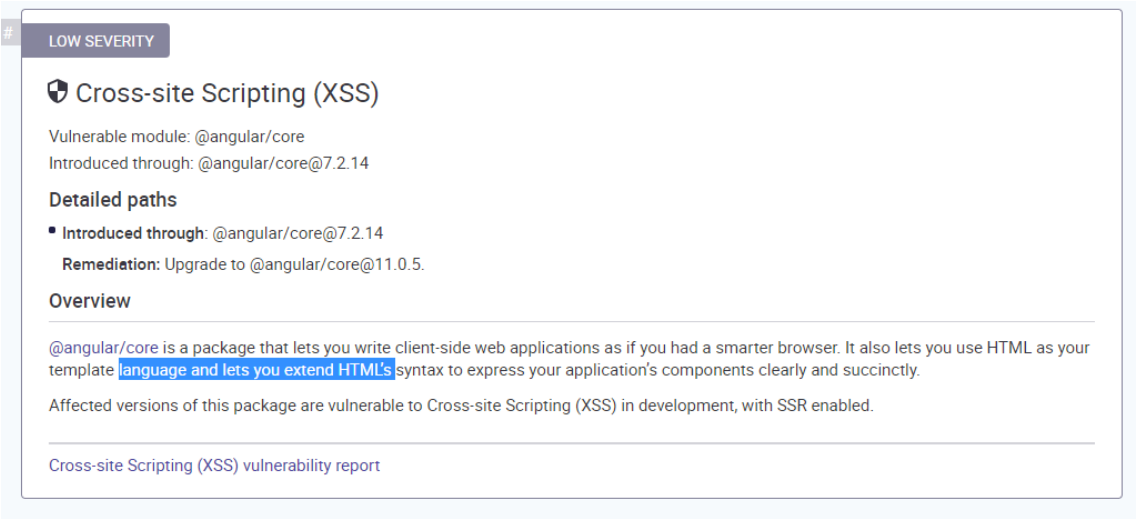


Figura 22 Vulnerabilidad de Angular

La version utilizada es vulnerable a un ataque de Cross-site Scripting (XSS). Un ataque XSS consiste en que ciberatacante introduzca codigo javascript en la página que se ejecutará en el cliente cuando este acceda. Haciendo uso de este tipo de ataques podemos encontrar:

- **Robo de sesiones**
- **Robo de información sensible**
- **Minado de criptomonedas**
- **Control del ordenador de la víctima**
- **Cambio de la apariencia visual de la web**

Por ultimo y antes de pasar a la explotación de vulnerabilidades, tenemos que la web almacena datos tanto de usuarios como de lugares patrimoniales, lo que nos indica que estará usando una de las bases de datos de que hemos nombrado en la fase anterior. Esto nos indica que puede ser vulnerable a ataques de inyección SQL.

8.4. FASE 4: EXPLOTACIÓN DE VULNERABILIDADES

Esta cuarta fase es posiblemente la mas importante de todas, es donde vamos a poner a prueba el nivel de seguridad del portal.

NOTA: En el momento de la realización de estas pruebas, se detectaron dos vulnerabilidades consideradas como críticas y de las que se notificó a las personas responsables para que fueran resueltas cuanto antes, ya que ponian en riesgo la integridad y confiabilidad de los datos de la plataforma.

A continuación paso a nombrar las pruebas realizadas y las vulnerabilideades detectadas.

8.4.1. Acceso sin contraseña

El 07/06/2022 se detecta que es posible acceder sin contraseña. Hasta la fecha indicada el acceso sin contraseña no estaba permitido. Este fallo podría estar provocado por un cambio en la configuración del portal. El desarrollador ha debido estar modificando partes del código o de los módulos que integran la aplicación, lo que ha eliminado la solicitud de autenticación.

Esta vulnerabilidad es considerada crítica y ha de ser resuelta lo antes posible, ya que en conjunción con algunas de las vulnerabilidades que veremos en los siguientes puntos de este documento, queda comprometida la totalidad de los datos de usuario.

La detección de este fallo da a entender dos cosas:

No existe entorno de pre-producción. Un entorno de PRE, como comunmente se suele llamar entre los programadores, consiste en tener una replica de la aplicación final, solo que no está expuesta al publico, en este caso sería tener una copia de O-CITY en un entorno privado sin visibilidad a Internet. En este entorno se realizan las pruebas cuando se han realizado modificaciones en el código. Si no se observan anomalías en su funcionamiento, pre-producción pasa a producción. De esta forma se evita que ocurran cosas como la que acabamos de ver en O-CITY.

El test de pruebas que realiza el desarrollador no es correcto. Si el desarrollador cuenta con un entorno de PRE, entonces el problema está en el test de pruebas que realiza y que no testea el acceso del usuario.

8.4.2. Formulario de login

Es necesario indicar que esta vulnerabilidad se encontró antes de que el acceso sin contraseña fuese detectado.

Un atacante puede acceder a la plataforma sin necesidad de saber la contraseña de acceso. A través de un ataque de **inyección SQL**, el atacante puede suplantar la identidad de cualquier usuario (admin o no) y acceder a sus datos y a todas las funciones que su perfil permita.

Al ser un proyecto con cierta relevancia publica, es facil poder obtener mediante **ingenieria social** que personas tienen perfiles con funciones especiales.

A continuación se detallan los pasos seguidos para la realización del ataque:

1. Accedemos a la plataforma

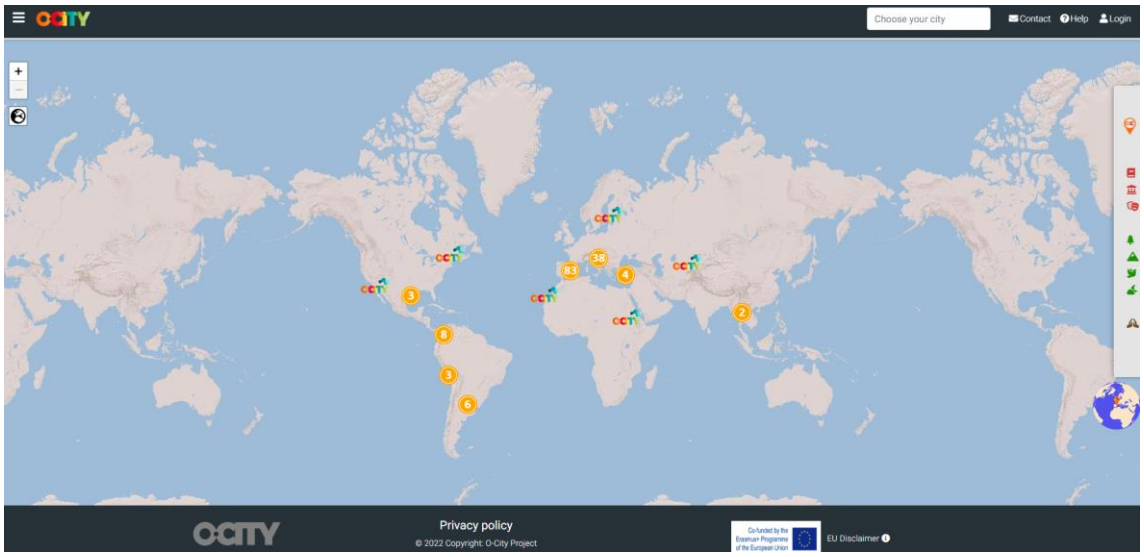


Figura 23 Página principal de O-CITY

2. Creamos un usuario, en este caso creamos el usuario Usuario_Prueba

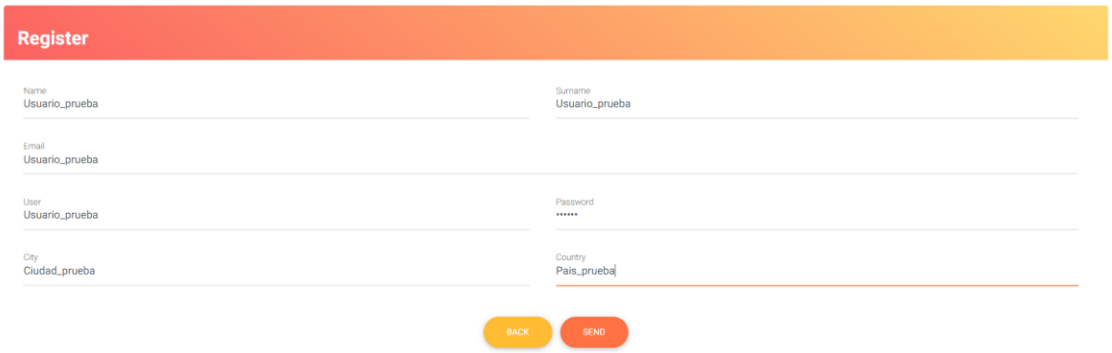


Figura 24 Perfil de usuario O-CITY

3. Una vez creado el usuario, procedemos a realizar el ataque

Realizamos una primera pruebas introducciendo el usuario “admin”.

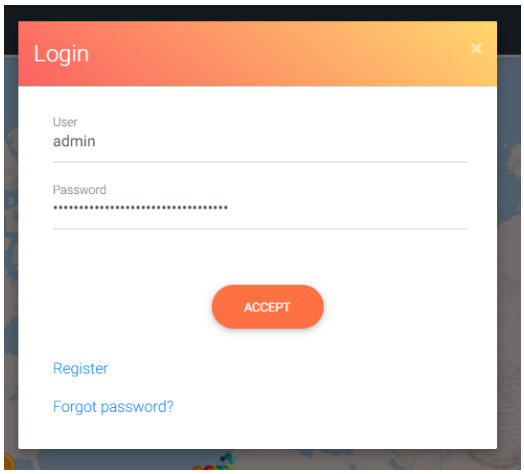


Figura 25 Vetana de login

En el campo contraseña introducimos el siguiente texto:

' OR username='Usuario_prueba' --

Se introduce una sentencia SQL, en la que desactivamos la consulta de la contraseña y la cambiamos por la busqueda el usuario que acabamos de crear. Como el usuario sí existe, nos permite el acceso.

Como en nuestro primer intento con el usuario ***admin*** no ha funcionado, realizamos una pequeña labor de investigación, buscando personas implicadas en el proyecto.

Probamos ahora con el usuario **pepe.**

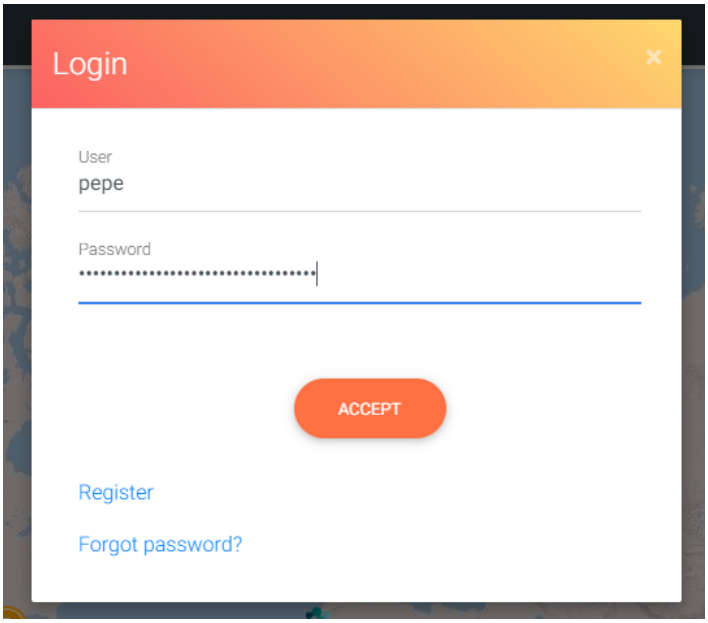


Figura 26 Ataque de inyección SQL

El usuario **pepe** existe.

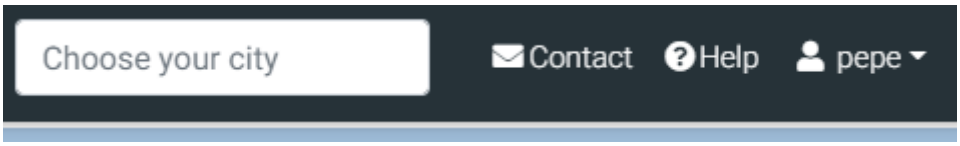


Figura 27 Barra superior con usuario logado

Si accedemos a su perfil, vemos que tiene permisos de Validador

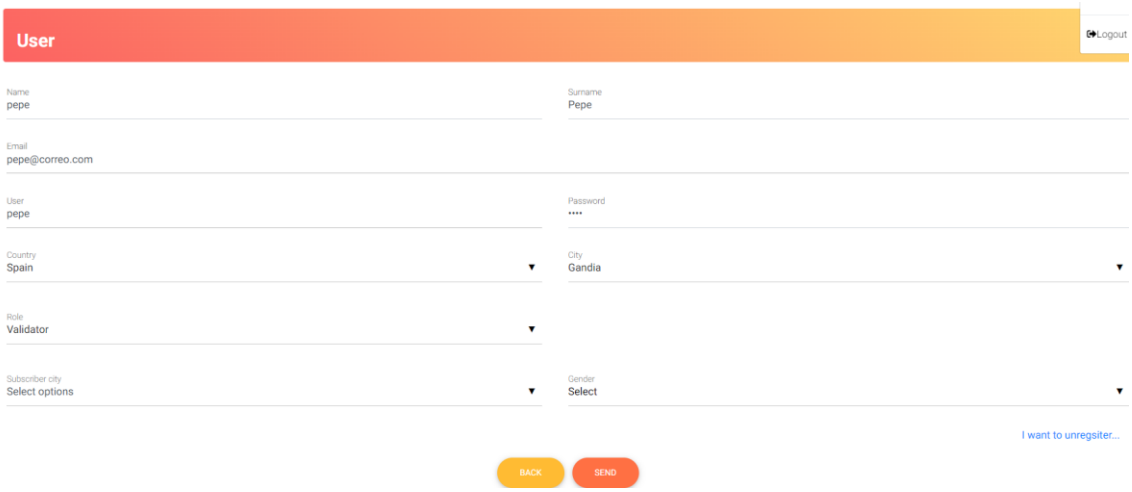


Figura 28 Perfil de usuario hackeado

Si continuamos buscado podemos obtener un usuario admin, como puede ser el de Marta.

Procedo a explicar mas detalladamente esta última parte para que quede bien claro en que consiste un ataque de inyección SQL y como se ha conseguido burlar el acceso sin necesidad de saber la contraseña de un usuario.

La consulta que se está utilizando para validar el usuario y contraseña en el portal es la siguiente:

*SELECT * from Usuario*
Where username = '${username}'
AND password = '${password}'

Lo que realizamos escribiendo el texto que el campo contraseña es lo siguiente:

*SELECT * from Usuario*

Where username = '${username}'
AND password = ''OR username='Usuario_prueba' --

Los dos guiones sirven para ignorar todo código SQL que vaya despues de esos guiones.

Como podemos ver lo que estamos consiguiendo en vez de buscar la contraseña del usuario, busque un usuario llamado "Usuario_prueba", como este usuario existe, nos validará y entraremos con el perfil del usuario que hemos introducido en el campo "Usuario".

8.4.3. Escalada de privilegios

Esta vulnerabilidad es más crítica que la citada en el punto anterior.

Como se han visto en la descripción de la aplicación O-CITY, se

Un atacante con un usuario genérico, puede realizar un cambio de rol sin necesidad de tener permisos especiales.

A continuación se detallan los pasos seguidos para la realización del ataque:

1. Accedemos con el usuario creado "Usuario_prueba"

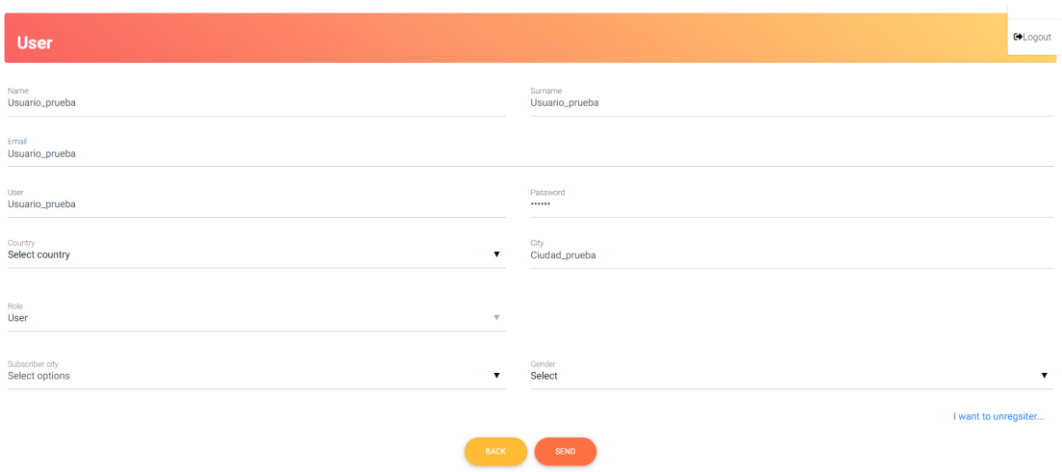


Figura 29 Perfil de usuario de prueba

Haciendo uso de las herramientas de desarrollador del navegador, en este caso Chrome, localizamos el desplegable de "Rol".

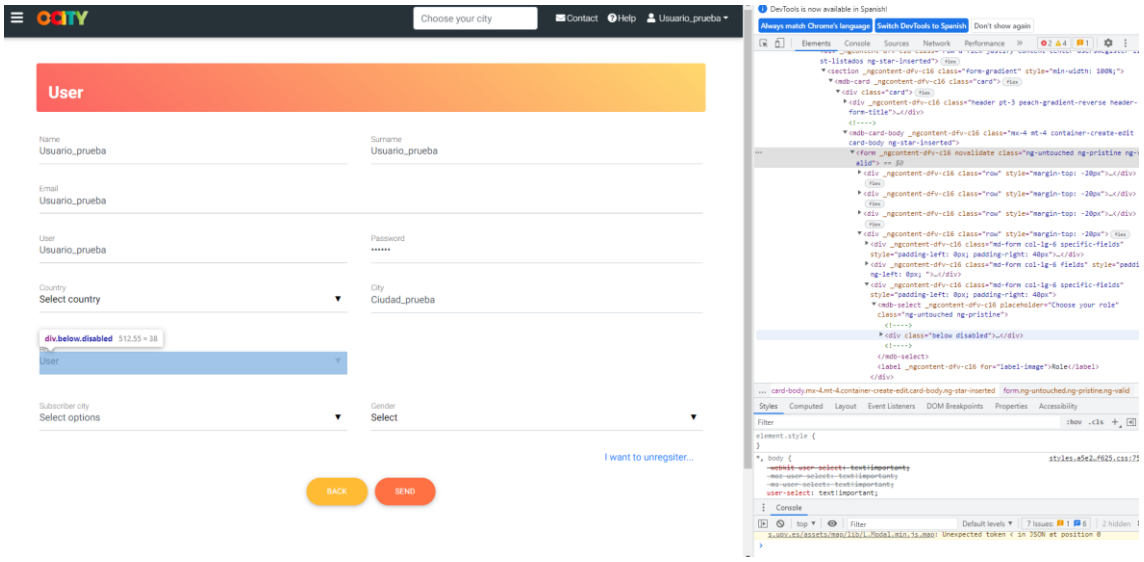


Figura 30 Modificación de campo bloqueado

Vemos que por código está deshabilitado, podemos cambiar su estado “en caliente” simplemente eliminando la palabra “disabled” y vemos como el desplegable pasa a estar activado.

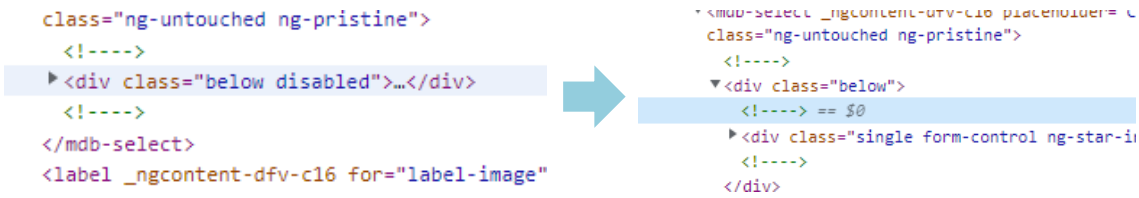


Figura 31 Resultado de modificar código

En este estado nos permite cambiar el rol del usuario.

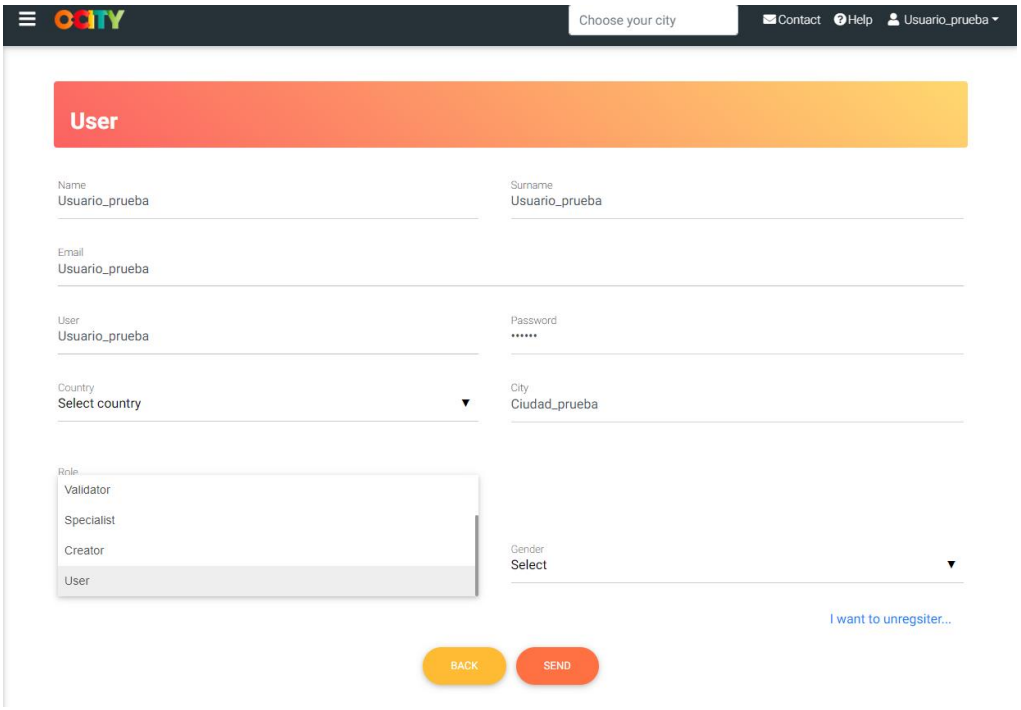


Figura 32 Modificación de rol de usuario

Pudiendo así darle permisos de “admin”.

8.4.4. Contraseña en texto plano

Otra vulnerabilidad crítica es la visualización de la contraseña de usuario almacenada en texto plano.

Un usuario registrado puede visualizar su contraseña de la siguiente forma:

1. Accediendo a su perfil

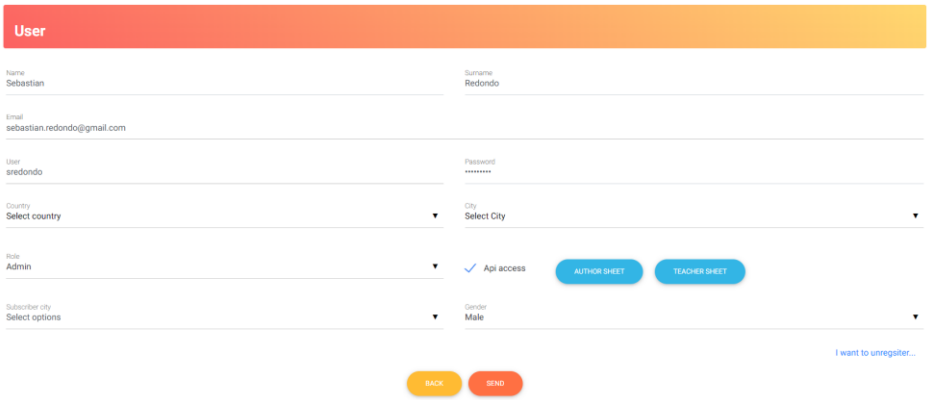


Figura 33 Perfil con nuevo rol

2. Abriendo la herramienta de desarrollador del navegador y modificando el tipo de "password" a "text"

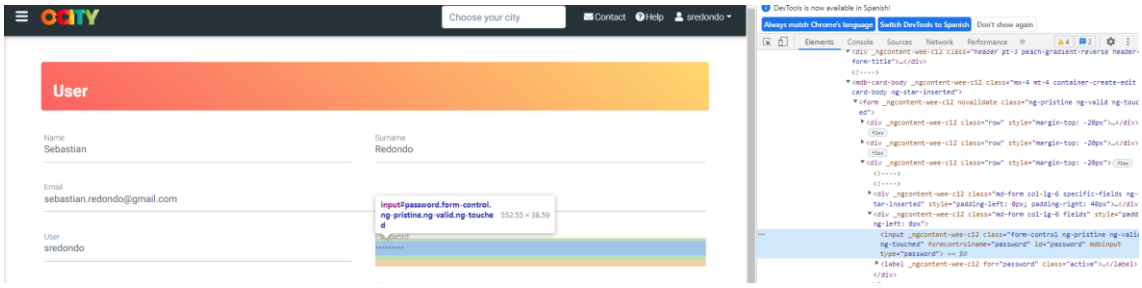


Figura 34 Modificación de campo contraseña 1

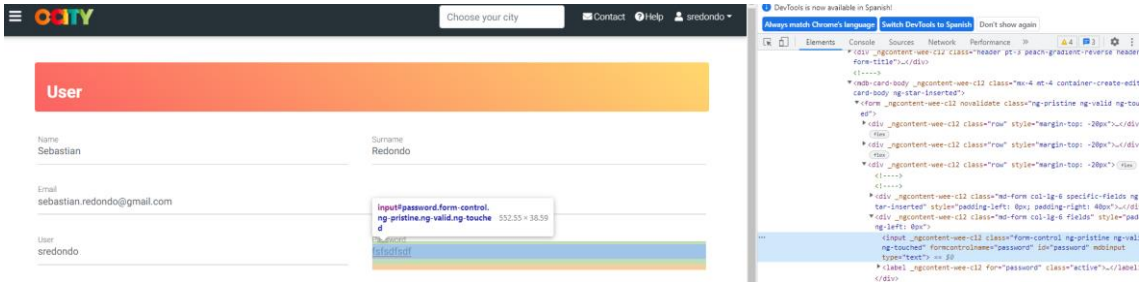


Figura 35 Modificación del campo contraseña 2

Esto puede indica que no se está almacenando la contraseña encriptado, lo que incumple el artículo 93.4 del Real Decreto 1720/2007, de 21 de diciembre, de la antigua LOPD. La actual ley RGPD, recomienda su encriptación desde los inicios del desarrollo del proyecto.

Este fallo podría categorizarse con criticidad media si no fuera por la siguiente vulnerabilidad, que trabajando junto con esta deja al descubierto toda la base de datos de usuarios.

8.4.5. Movimiento lateral

Este fallo de seguridad pone al descubierto los datos de cualquier usuario registrado en la plataforma.

¿En que consiste el movimiento lateral?

Un usuario logado accediendo a su perfil, puede saltar a cualquier otro perfil de usuario independiente del tipo de rol que tenga el usuario destino.

El perfil de usuario “sredondo” está en:

https://ocityplatform.webs.upv.es/dashboard/users/profile/286

Solo cambiando el numero 286 a por ejemplo 287 accedemos directamente al perfil de otro usuario.

https://ocityplatform.webs.upv.es/dashboard/users/profile/287

Este fallo hace que usando técnicas de web scrapping se puedan obtener todos los datos de usuario junto con sus contraseñas.

8.4.6. Encriptación de contraseñas de baja seguridad.

Esta vulnerabilidad ha sido detectada durante la redacción de este TFG y en principio surge en respuesta a la vulnerabilidad del guardado de contraseñas en texto plano. Tras detectarse dicha vulnerabilidad y debido a la criticidad que consideré en su momento, informé a los responsables del proyecto para que solventaran dicho problema, pero la solución no ha sido del todo correcta como ahora veremos.

Como podemos ver en la siguiente imagen, ahora en el perfil de usuario si modificamos el campo de tipo password a tipo texto, vemos que el resultado es un la rista de número y letras. Esto está muy bien, ya que nos indica que almenos algún tipo de encriptación se está realizando y no se está cargando el password en texto plano como estaba ocurriendo antes.

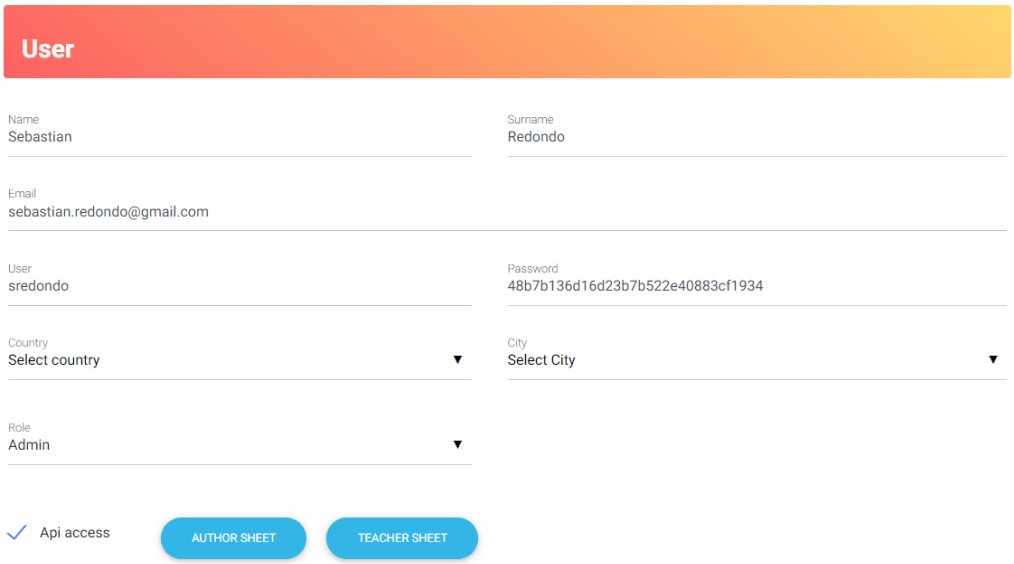


Figura 36 Encriptación de contraseña con MD5

Como muchas cosas en el mundo del hacking y la investigación, la intuición y trabajar a base de prueba y error es muy común, pero en este caso ha sido la intuición lo que me indicaba que la solución que le han dado al problema nombrado más arriba no era la más correcta. Así que he cogido el hash que aparece en el campo de contraseña de mi perfil y lo he colocado en una web que desencripta hashes en MD5, SHA1, MySQL, NTLM, SHA256, SHA512, etc., Hashes.com. Básicamente lo que hace es buscar en una base de datos/diccionario hashes ya conocidos.

El resultado es el siguiente:

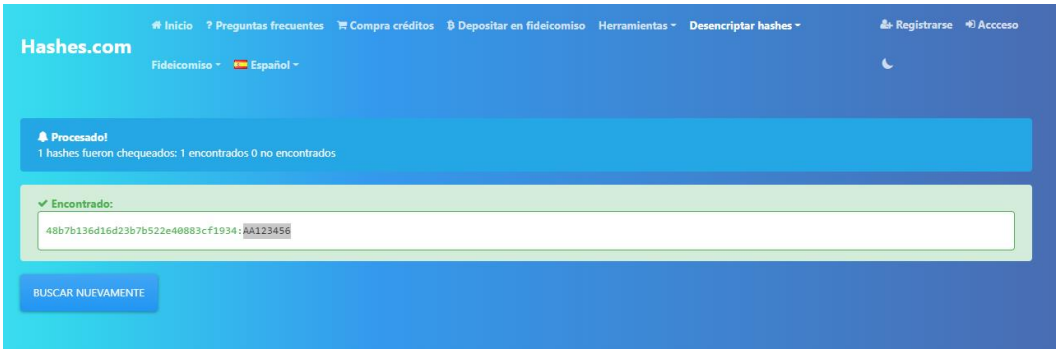


Figura 37 Portal hashes para desencriptar hash

Esto quiere decir que si el usuario tiene una contraseña que ya se encuentre en la base de datos de este portal, es descifrable en cuestión de segundos.

8.4.7. Eliminación de comentarios en código fuente.

Esto aunque parezca algo sin importancia, es otro punto clave para evitar dar información de más a los ciberdelincuentes y permitirles explotar funcionalidades de la página que no están en uso.

Algunas de las páginas de O-CITY tienen en su código fuente código comentado, es decir, codigo que está escrito por no está en uso. Lo recommendable es siempre eliminar de la version de producción todos los comentarios que puedan estar en el código fuente.

En los documentos adjunto incluyo el código fuente de una de las páginas en las que podemos ver como tanto al principio como al final hay partes del código comentadas, el código comentado empieza por "*<!—".*

9. Resumen de vulnerabilidades y criticidad

En la siguiente tabla se han recopilado las vulnerabilidades ya mencionadas. Ha estas se les ha asignado un mnemonico para hacer referencia a ellas y la categoria del top 10 de OWASP (vista en .Análisis del problema) en la que se encuentra.

Vulnerabilidad	Descripción	Criticidad	Cat. OWASP
OC-0101	Se detecta el 07/06/2022 que se puede acceder sin necesidad de rellenar el campo contraseña	Crítico	A5
OC-0102	Logín vulnerable a ataques de inyección SQL. Un atacante puede acceder sin contraseña.	Crítico	A1
OC-0103	En el perfil de usuario se puede hacer escalada de privilegios usando el desarrollador del navegador, cambiando el estado del desplegable Rol	Crítico	A6
OC-0104	En el perfil de usuario se puede visualizar la contraseña del usuario cambiando el tipo del campo contraseña.	Crítico	A3
OC-0105	Se puede acceder a cualquier perfil de usuario cambiando el ID en la URL (ej: https://O-CITY.org/dashboard/users/profile/284)	Crítico	A3
OC-0106	Encriptación de la contraseña de baja seguridad	Media	A6
OC-0107	Eliminación de comentarios en el código fuente	Baja	A6 y A7
OC-0108	Componentes vulnerables y desactualizados	Baja	A9

10. Soluciones propuestas

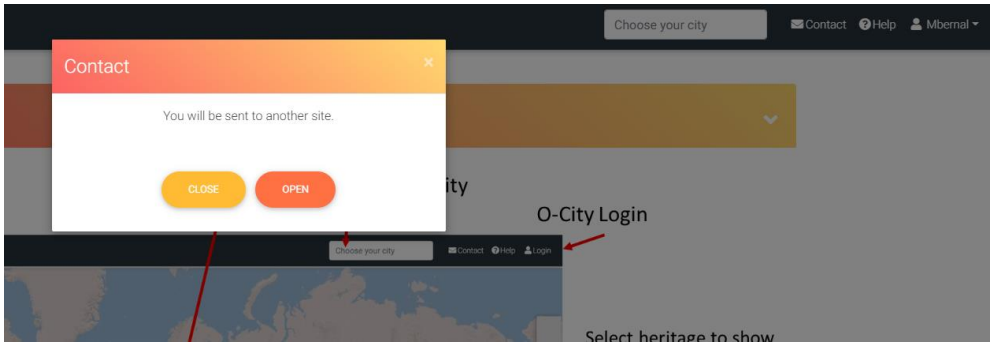
A modo de resumen y sin entrar en detalles, ya que se trata de una tarea que ha de realizar el desarrollador de la página y de trabajo de programación que no compete al objetivo de este trabajo fin de grado, procedo a enumerar en la siguiente tabla las soluciones propuestas para cada una de las vulnerabilidades.

Vulnerabilidad	Solución propuesta
OC-0101	Comprobar la funcionalidad del botón enviar del formulario de Login. No está realizando la petición correcta o la consulta a la que llama no está buscando en la base de datos.
OC-0102	Una solución es implementar el escapado de strings. Consiste en un librería que antepone barras invertidas a unos carateres especificos, de esta forma si se intentara hacer una inyección SQL como la que hemos mostrado no se podría ejecutar. Digamos que es una especie de encriptación básica para consultas a MySQL.
OC-0103	Eliminar el campo Rol del perfil del usuario. No es necesario que el usuario vea ese campo.
OC-0104	Eliminar el campo Contraseña. Como no se permite el cambio de contraseña en el perfil del usuario, lo correcto es eliminarlo.
OC-0105	Realizar una ocultación
OC-0106	La solución aportada para OC-0104 resolveria esta incidencia.
OC-0107	Eliminación de comentarios en el código fuente
OC-0108	Actualizar Angular a su última version.

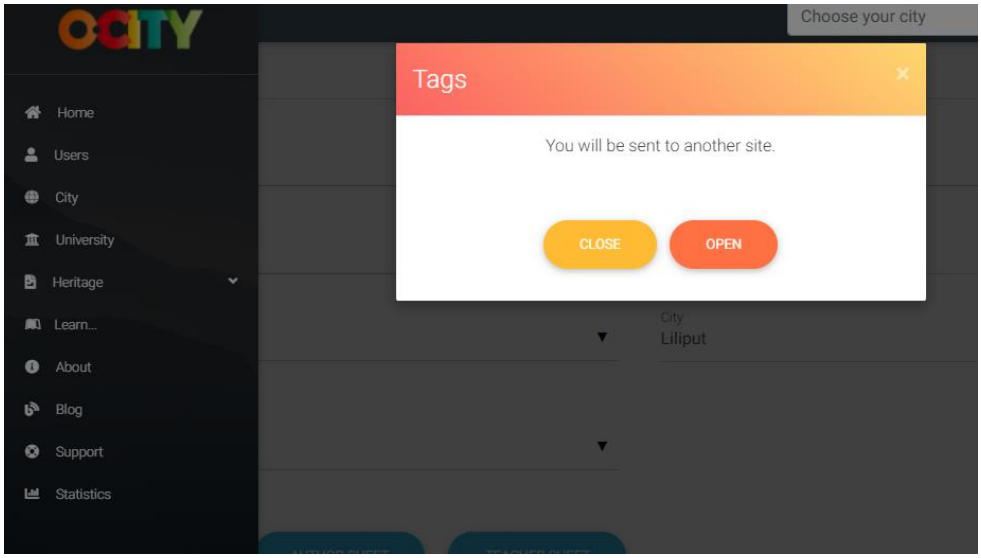
11. Extra: Propuesta de mejoras en el portal web

11.1. Experiencia de usuario: aspecto visual y usabilidad

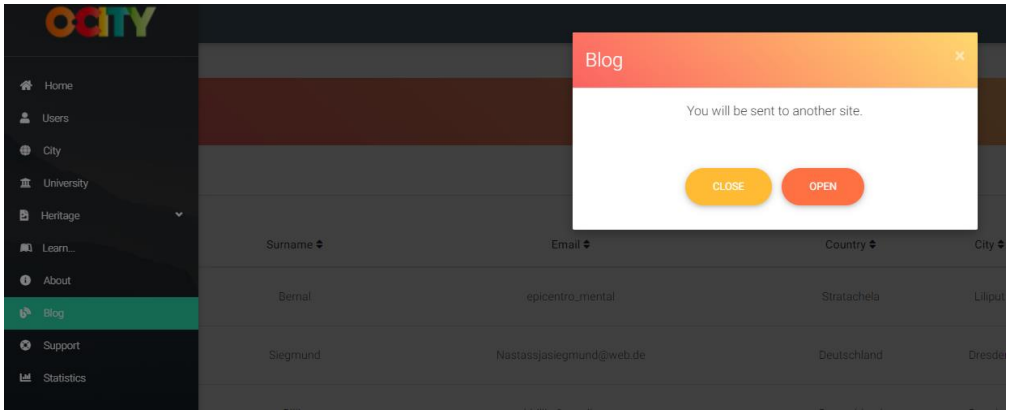
El menú de contacto muestra una ventana emergente que no hace nada, solo redirige al usuario “si quiere” al área de contacto de la web de O-CITY. Lo recomendable sería directamente abrir en una pestaña nueva la web indicada sin necesidad de mostrarle al usuario el pop-up.



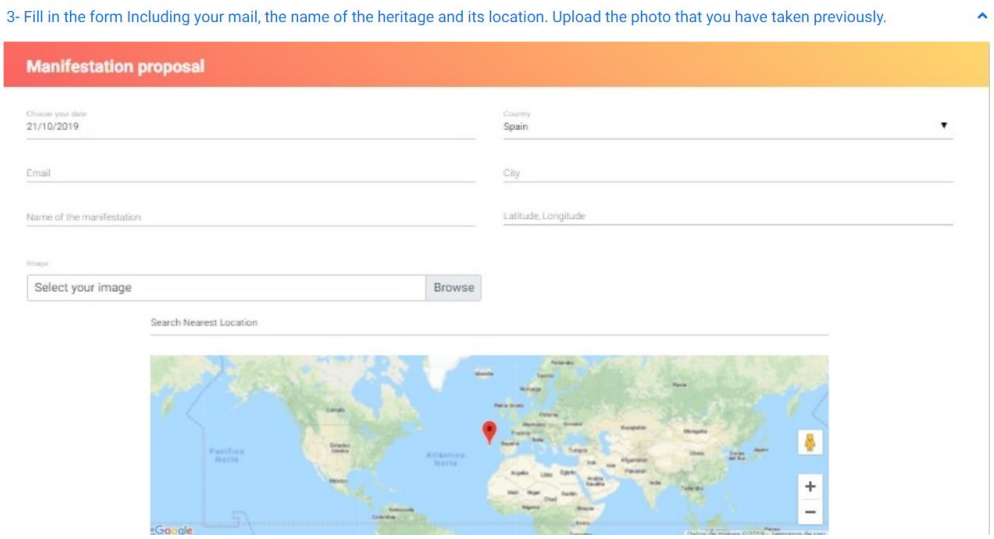
Del mismo modo ocurre al presionar en Learn, se abre un popup con título Tags y redirecciona a otra web.



La pestaña de blog exactamente igual.

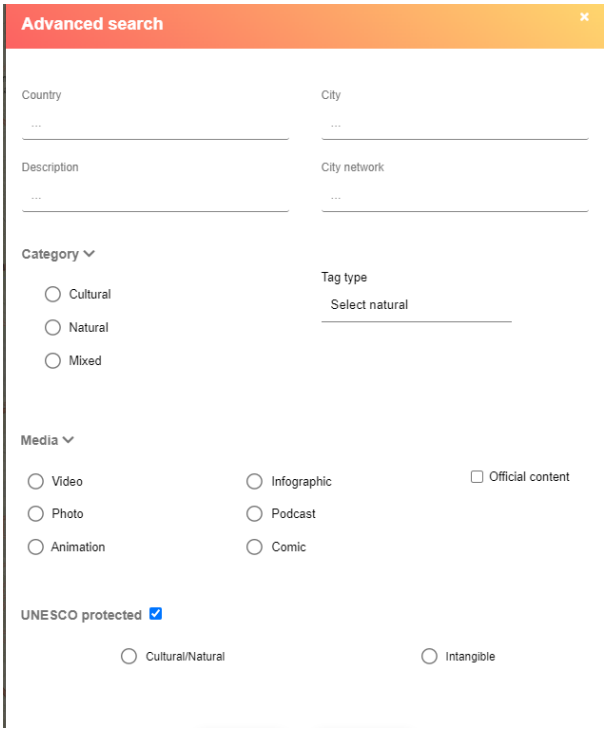


Se han añadido imágenes de mala calidad preguntas frecuentes, además de explicaciones básicas o inexistentes.



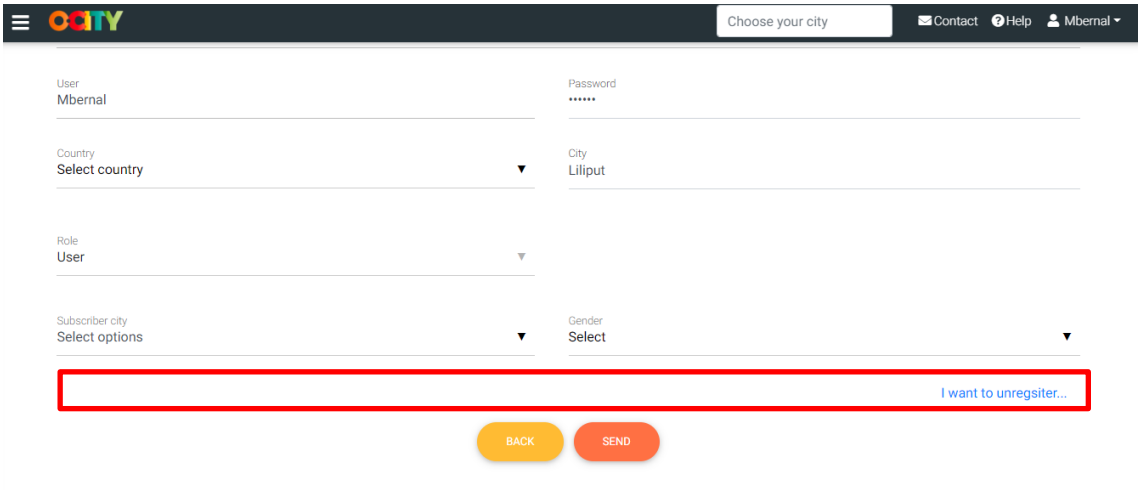
Área HELP poco desarrollada. Falta categorización de la ayuda.

Advanced search no sigue la estética del resto de formularios del portal:



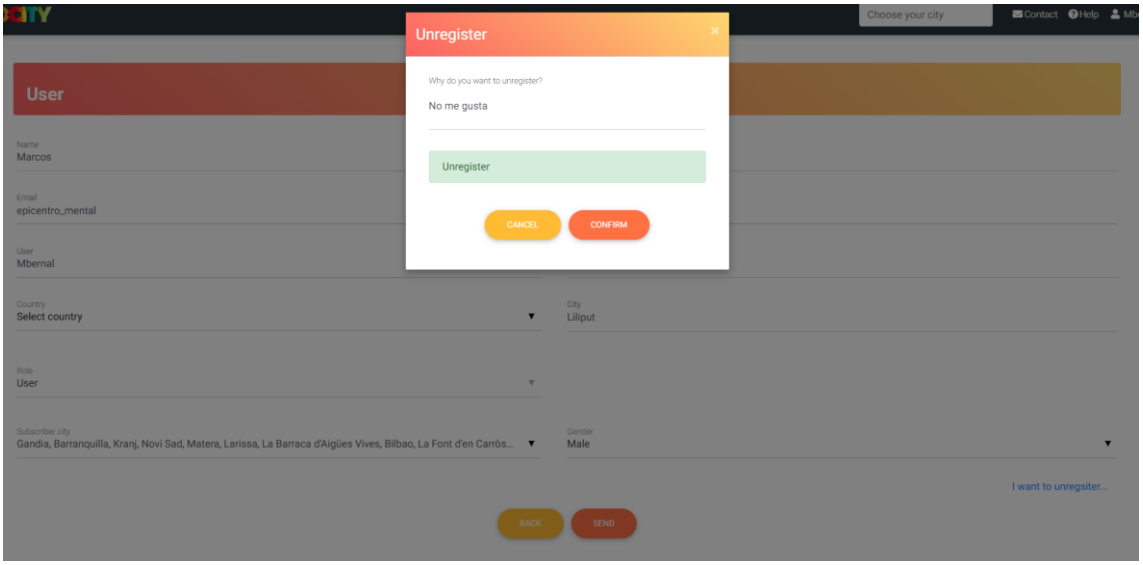
La tipología de letra, el color, no corresponde a lo encontrado en otros apartados del site.

En la página de perfil de usuario toda la línea de bajo es un botón “transparente” para desregistrarse.



Al desregistrar un usuario, no desloga y se queda en la página de perfil de usuario, lo que permite seguir modificando datos del usuario “eliminado”. Se realiza prueba “eliminando” el usuario, modificando el sexo y deslogando. El usuario no es eliminado.

Vuelvo a hacer una prueba, eliminando el usuario y deslogando, sin modificar nada. El usuario sigue sin eliminarse, puedo acceder de nuevo.



Correo de cambio de contraseña básico.

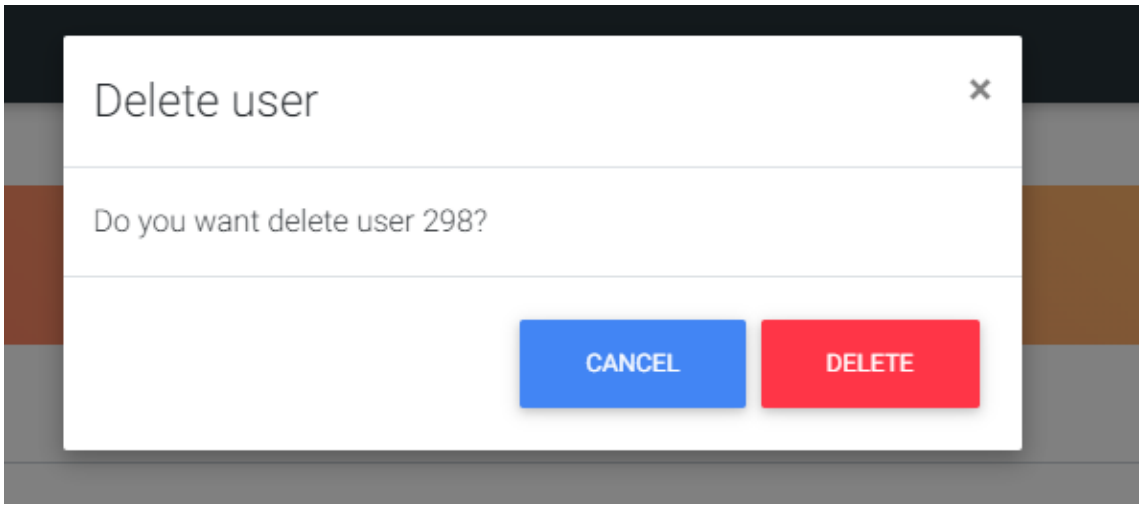
Cambia la contraseña

Nombre: Sebastián

Correo electrónico: sebastian.redondo@gmail.com

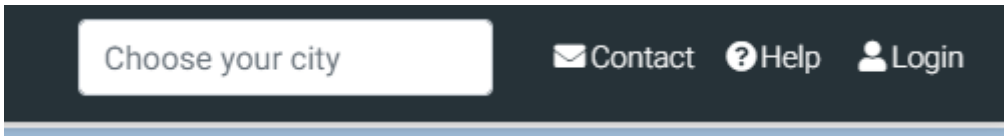
Sigue el enlace: Enlace

Al eliminar usuarios con un perfil de admin la ventana emergente es la siguiente



Debería salir el nombre de usuario, ese número no hace referencia a nada.

Se echa en falta un ***Sign In*** en el acceso principal, además del Register que ya existe en el pop up de login.



12. Conclusiones:

En este trabajo se ha realizado una auditoria de ciberseguridad de la aplicación web O-CITY.org. Se han detectado diferentes fallos de seguridad y se han dado las recomendaciones para solucionar estas vulnerabilidades que podrían causar problemas en protección de datos.

Cuando hablamos de seguridad de la información y concretamente de una auditoria de hacking ético como la que acabamos ver, se pueden obtener diferentes conclusiones en función del perfil de usuario que lo analice.

1. **Desde el punto de vista del auditor**. Como autor de este trabajo, obtengo como conclusión, que es necesario tener muy bien estructurado y planificado cada paso a realizar. Es muy fácil detectar una vulnerabilidad y automáticamente querer explotarla, cambiando así de fase sin haber finalizado el proceso de estudio anterior.

2. **Desde el punto de vista del desarrollador**. Es la mejor forma de poder ver que no hay que dejar de lado el plano de la seguridad en ningún momento del proceso de creación de una aplicación o portal web. Es una forma de ver que es vital contar con tres escenarios a la hora de programar (desarrollo, pre-producción y producción), para evitar errores que hemos podido ver a lo largo de este documento. También sirve para hacer ver que no hay que olvidar el marco legal en el que nos movemos y que está, todo aquel que desee publicar un sitio web, obligado a cumplirlo.

3. **Desde el punto de vista del usuario**. El usuario puede aprender de este documento que no todos los sitios web son fiables, que existen señales que indican que puede tener fallos de desarrollo que pueden llevar a fallos de seguridad, que no siempre meter nuestros datos en un portal, por muy bonito que parezca nos asegura que vayan a estar a buen recaudo y que si a pesar de todo vamos a ingresar nuestro usuario, no debemos utilizar la misma contraseña que en otras aplicaciones, ya que una vez obtenida nuestra contraseña en una web poco segura, el ciberdelincuente podría tener acceso a todas nuestras otras aplicaciones.

Finalmente, como futura línea de trabajo se recomienda realizar una monitorización periódica de la seguridad de O-CITY.org gestionada por un experto en ciberseguridad, ya que el proyecto O-CITY custodia información sensible para los distintos niveles de usuario que residen en ella.

13. Bibliografía y referencias:

El acceso a estos portales se realizó durante el mes de agosto y septiembre de 2022, meses en los que se ha redactado este TFG.

https://www.infosecuritymexico.com/es/ciberseguridad.html#introduccion

https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

https://es.wikipedia.org/wiki/ISACA

https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente

https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/

https://blog.signaturit.com/es/que-leyes-regulan-la-ciberseguridad-en-la-union-europea-y-en-espana#Que-podria-considerarse-como-ilegal-ilicito

https://keepcoding.io/blog/la-historia-del-hacking/#Los_inicios_de_la_historia_del_hacking

https://latam.kaspersky.com/resource-center/definitions/hacker-hat-types

https://www.incibe-cert.es/blog/desarrollo-seguro-de-aplicaciones-para-dispositivos-moviles

https://www.hiberus.com/crecemos-contigo/que-es-angular-y-para-que-sirve/

https://snyk.io/

https://docs.plesk.com/es-ES/onyx/customer-guide/bases-de-datos-de-sitios-web/acceso-a-bases-de-datos.71841/

https://owasp.org/Top10/es/A00_2021_Introduction/