XII OWASP Spain Chapter | Barcelona, 13 de diciembre de 2018

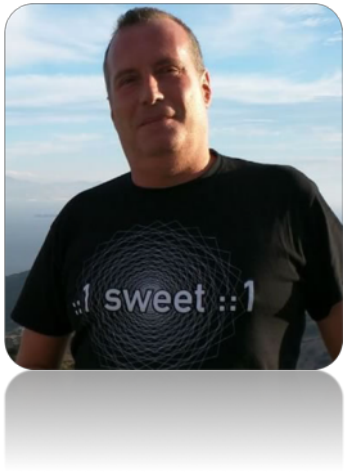
OWASP Top Ten 2017: "Rompiendo cosas"

Pedro C. aka "s4ur0n" (@NN2ed_s4ur0n)

Tipo de documento: Presentación
Autor del documento: CS³ Group by Pedro C.
Código del Documento:CS3-OWASP_SPAIN_XII.pdf
Versión: 1.1

Categoría: Público
Fecha de elaboración: 13/12/2018
Nº de Páginas: 60

Whoami




```
class PedroC:
    def __init__(self):
        self.name =      'Pedro Candel'
        self.email =     's4ur0n@s4ur0n.com'
        self.web =       'https://www.s4ur0n.com'
        self.nick =      '@NN2ed_s4ur0n'
        self.company =   'CS³ Group'
        self.role =      'Security Researcher'
        self.work =      [ 'Reversing', 'Malware', 'Offensive
                           Security', '…' ]
        self.groups =    [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```

mlw.re

OWASP Open Web Application Security Project

CS³ SECURITY SERVICES https://cs3group.com

SPAIN CHAPTER OWASP Open Web Application Security Project

CS³ Group

Formación en Seguridad
Cursos presenciales a medida impartidos en las instalaciones del cliente o las concertadas con prácticas reales desde el primer momento

Hacking Ético
Auditorías de caja negra, gris o blanca para aplicaciones web, sistemas y redes de comunicaciones

Análisis de Malware
Análisis de Malware automatizados y manuales con completos informes de comportamiento e indicadores de compromiso (IOC)

Ingeniería Inversa
Ingeniería Inversa para binarios de sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits, ARM y firmwares

Exploiting
Desarrollo y adaptación de exploits para sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits y Android

Desarrollo Seguro
Auditoría SAST, DAST, IAST y RASP para análisis de vulnerabilidades en el código de proyectos en Java, .Net, PHP, C/C++ y Cobol

Hardware Hacking
Análisis de vulnerabilidades en dispositivos hardware, sistemas embebidos y firmware con técnicas de ingeniería inversa

Seguridad en dispositivos móviles
Análisis estático, dinámico e instrumentación dinámica de aplicaciones Android (APK), iOS (IPA) y Windows Mobile (APPX)

Respuesta ante incidentes
Investigación remota de incidentes de seguridad, análisis de las situaciones y respuesta inmediata ante las amenazas

Forense
Adquisición y elaboración de informes periciales con garantía de imparcialidad y objetividad para todo tipo de sistemas de información

DevSecOps
Desarrollo, Seguridad y Operaciones en CSI (Continuous Security Integration) con pruebas automatizadas de seguridad para CI/CD

Intelligence
Recopilación, análisis y explotación de datos a gran escala con fuentes OSINT, SIGINT, HUMINT, Deep Web, redes P2P, etc.

SIGINT
Inteligencia de comunicaciones, análisis y auditoría de seguridad en señales y protocolos de radiofrecuencia (RF)

T.S.C.M.
Technical Surveillance Counter-Measures: Contramedidas electrónicas para detección y localización de dispositivos de escucha

Telecom
Análisis y auditoría GSM/3G/4G, implementación de servicios de operadores móviles virtuales (HLR, VLR, GGSN, Roaming voz y datos)

ATM
Análisis de vulnerabilidades, auditoría, forense, skimming, shimming y pruebas de blackbox para NCR, Hyosung, WRG, Diebold Nixdorf e Hitachi

PoS/TPV
Auditoría y cumplimiento de controles en terminales Verifone e Ingenico. Monitorización y transaccionabilidad completa según ISO 8583

LOPD/GPDR/Cumplimiento
LOPD, adaptación GPDR, ISO 27000, SGSI, análisis y gestión de riesgos, Políticas de seguridad, continuidad de negocio, ITIL, PCI DSS

CS³ SECURITY SERVICES https://cs3group.com

SPAIN CHAPTER OWASP Open Web Application Security Project

Agenda

OWASP Top Ten 2017: “Rompiendo cosas”

1. Introducción
2. Proyecto “Top Ten”
3. OWASP Top Ten 2017: Los 10 principales riesgos en Aplicaciones Web

Introducción

OWASP: Introducción

OWASP (Open Web Application Security Project)

https://www.owasp.org

- Es una **comunidad abierta** dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones Web y APIs en las que se pueda confiar.
- OWASP **no está afiliada** con ninguna compañía de tecnología.
- Comenzó en el año 2001 pero fue **constituida legalmente en 2004**.

OWASP: Introducción

- La Fundación OWASP es una **entidad sin fines de lucro** para asegurar el éxito a largo plazo del proyecto.

- Casi todos los asociados con OWASP **son voluntarios**, incluyendo la junta directiva, comités globales, líderes de capítulos, los líderes y miembros de proyectos.

- Apoya la investigación innovadora sobre seguridad a través de **becas** e **infraestructura**.

- La comunidad OWASP está formada por **empresas**, **organizaciones educativas** y **particulares** de todo mundo.

OWASP: Introducción

- OWASP es un nuevo tipo de organización. Su **libertad de presiones comerciales** le permite proveer información sobre seguridad en aplicaciones sin sesgos, completamente imparcial, de forma práctica y rinde beneficios.

- Todas las herramientas de OWASP, documentos, videos, presentaciones y capítulos **son gratuitos** y **abiertos** a cualquier interesado en mejorar la seguridad en aplicaciones.

OWASP: Introducción

En OWASP se encuentran de **forma abierta** y **gratuita**:

- ✓ Herramientas y estándares de seguridad en aplicaciones.
- ✓ Libros completos de revisiones de seguridad en aplicaciones, desarrollo de código fuente seguro y revisiones de seguridad en código fuente.
- ✓ Presentaciones y videos.
- ✓ Hojas de trucos en varios temas comunes.
- ✓ Controles de seguridad estándar y bibliotecas.
- ✓ Capítulos locales en todo el mundo.
- ✓ Investigaciones de vanguardia.
- ✓ Numerosas conferencias alrededor del mundo.
- ✓ Listas de correo.

OWASP: Introducción

Los proyectos OWASP se dividen en dos categorías principales: **proyectos de desarrollo** y **proyectos de documentación**.

Los **proyectos de desarrollo** incluyen:

- **WebScarab**: Una aplicación de chequeo de vulnerabilidades de aplicaciones web incluyendo herramientas proxy.

- **Zed Attack Proxy (ZAP)**: Es una herramienta para la realización de pruebas de penetración para encontrar vulnerabilidades en aplicaciones web.

OWASP: Introducción

- **Filtros de validación**: Filtros genéricos de seguridad perimetral que los desarrolladores pueden usar en sus propias aplicaciones.

- **WebGoat**: Una herramienta interactiva de formación para que los usuarios aprendan sobre seguridad de aplicaciones web de forma segura y legal.

- **OWASP .Net**: Un conjunto de herramientas para securizar los entornos .NET.

- Etc...

OWASP: Introducción

Los proyectos de **documentación** incluyen:

- **Guía OWASP**: Un enorme documento que proporciona una guía detallada sobre la seguridad de las aplicaciones web.
- **OWASP Top 10**: Documento de alto nivel que se centra sobre las vulnerabilidades más críticas de las aplicaciones web.
- **OWASP Top 10 Mobile**: Documento con las diez vulnerabilidades más críticas de las aplicaciones móviles.

OWASP: Introducción

- **OWASP (ASVS):** Guía especialmente para desarrolladores con las mejores prácticas.
- **OWASP Testing Guide**: Guía de pruebas para pentesters.
- **OWASP Cheat Sheet Series**: Hojas de consejos y trucos para desarrolladores y administradores.
- **OWASP Proactive Controls**: Categorías con los controles más importantes que los arquitectos y desarrolladores deberían de implementar e incluir en sus proyectos.

OWASP: Introducción

- **OWASP SAMM**: Modelo de Madurez de Aseguramiento del Software (Software Assurance Maturity Model).
- **OWASP Risk Rating Methodology**: Metodología de Evaluación de Riegos (parte de OWASP Testing Guide).
- Etc...

Proyecto “Top Ten”

OWASP: Proyecto Top Ten

- Su objetivo es **crear conciencia** acerca de la **seguridad en aplicaciones web** mediante la identificación de algunos de los diez riesgos más críticos que enfrentan las organizaciones.

- También educar a desarrolladores, diseñadores, arquitectos, gerentes y organizaciones sobre las **consecuencias de las vulnerabilidades de seguridad más importantes** en aplicaciones web.

- El proyecto **es referenciado por muchos estándares**, libros, herramientas y organizaciones entre las que se encuentran MITRE, PCI-DSS, DISA, FCT...

OWASP: Proyecto Top Ten

En general sirve para:

- **Organización**: Para iniciarse en la temática sobre la seguridad de aplicaciones web.
- **Desarrolladores**: Para aprender de los errores de otras organizaciones.
- **Ejecutivos**: Deben comenzar a pensar cómo gestionar el riesgo que las aplicaciones de software crean en sus empresas.

OWASP: Proyecto Top Ten

Evolución del proyecto “Top Ten”.

- **Primera versión** lanzada en **2003**
- **Revisiones menores** en **2004**
- **Top Ten** en **2007**
- **Renovación en 2010** para dar prioridad al riesgo, no sólo a la prevalencia.

OWASP: Proyecto Top Ten

- **Top Ten** coincidiendo con el **aniversario en 2013**
- Lanzamiento de **Top Ten** en **2017**
- ¿Nueva versión en **2019, 2020, ...**?

OWASP: Proyecto Top Ten

- Las 10 principales categorías fueron seleccionadas y priorizadas de acuerdo con estos datos de **prevalencia**, en combinación con estimaciones consensuadas de **explotabilidad**, **detectabilidad** e **impacto**.

- **No hay que detenerse en el Top 10**. Existen cientos de problemas que pueden afectar a una aplicación web.

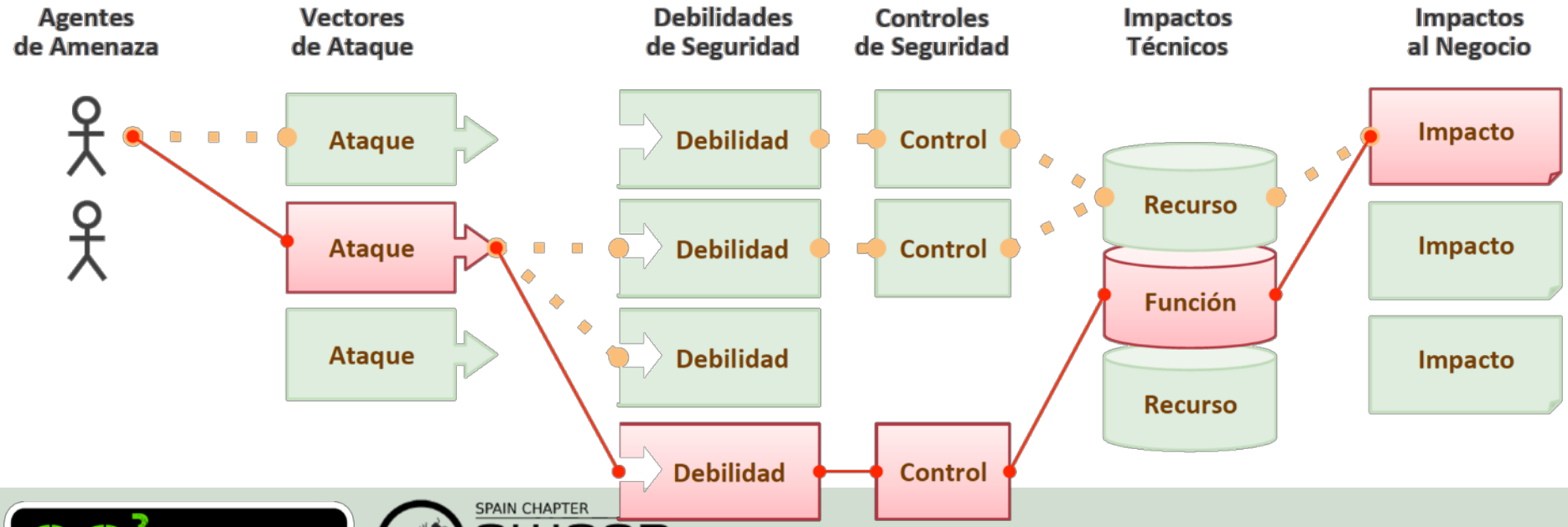
- **El cambio en el Top 10 es constante**. Incluso sin cambiar una sola línea de código en la aplicación, es posible llegar a ser vulnerable, ya que al descubrirse nuevos defectos, los ataques pueden ser más refinados.

Los 10 principales riesgos en Aplicaciones Web

Riesgos de Seguridad de las Aplicaciones Web

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**.



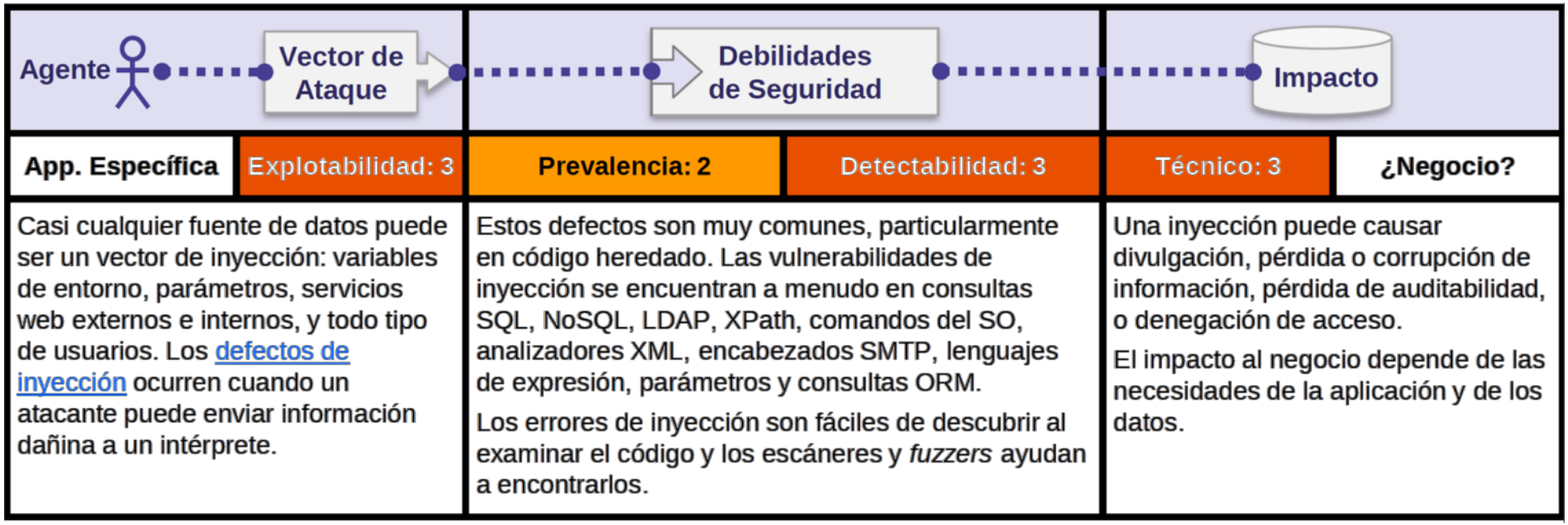
Riesgos de Seguridad de las Aplicaciones Web

OWASP Top Ten 2017

- **A1:2017** Inyección
- **A2:2017** Pérdida de Autenticación
- **A3:2017** Exposición de datos sensibles
- **A4:2017** Entidades Externas XML (XXE)
- **A5:2017** Pérdida de Control de Acceso
- **A6:2017** Configuración de Seguridad Incorrecta
- **A7:2017** Secuencia de Comandos en Sitios Cruzados (XSS)
- **A8:2017** Deserialización Insegura
- **A9:2017** Componentes con vulnerabilidades conocidas
- **A10:2017** Registro y Monitoreo Insuficientes

A1:2017 Inyección

A1:2017 Inyección	Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.



App. Específica	Explotabilidad: 3	Prevalencia: 2	Detectabilidad: 3	Técnico: 3	¿Negocio?
Casi cualquier fuente de datos puede ser un vector de inyección: variables de entorno, parámetros, servicios web externos e internos, y todo tipo de usuarios. Los defectos de inyección ocurren cuando un atacante puede enviar información dañina a un intérprete.		Estos defectos son muy comunes, particularmente en código heredado. Las vulnerabilidades de inyección se encuentran a menudo en consultas SQL, NoSQL, LDAP, XPath, comandos del SO, analizadores XML, encabezados SMTP, lenguajes de expresión, parámetros y consultas ORM. Los errores de inyección son fáciles de descubrir al examinar el código y los escáneres y *fuzzers* ayudan a encontrarlos.		Una inyección puede causar divulgación, pérdida o corrupción de información, pérdida de auditabilidad, o denegación de acceso. El impacto al negocio depende de las necesidades de la aplicación y de los datos.	

A1:2017 Inyección

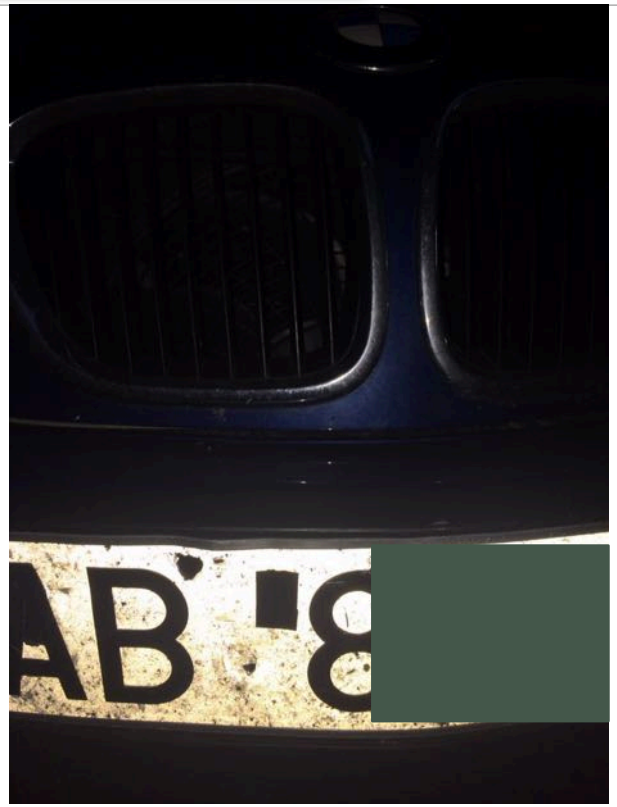
A1:2017
Inyección

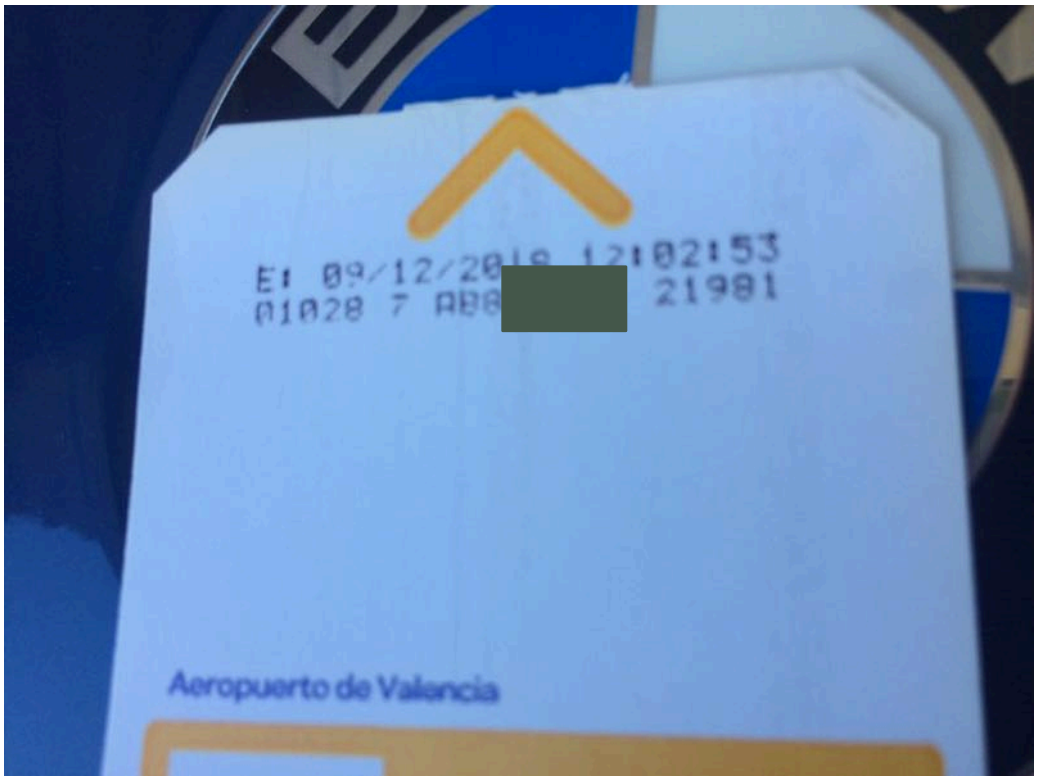
Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.

A1:2017 Inyección

A1:2017
Inyección

Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.





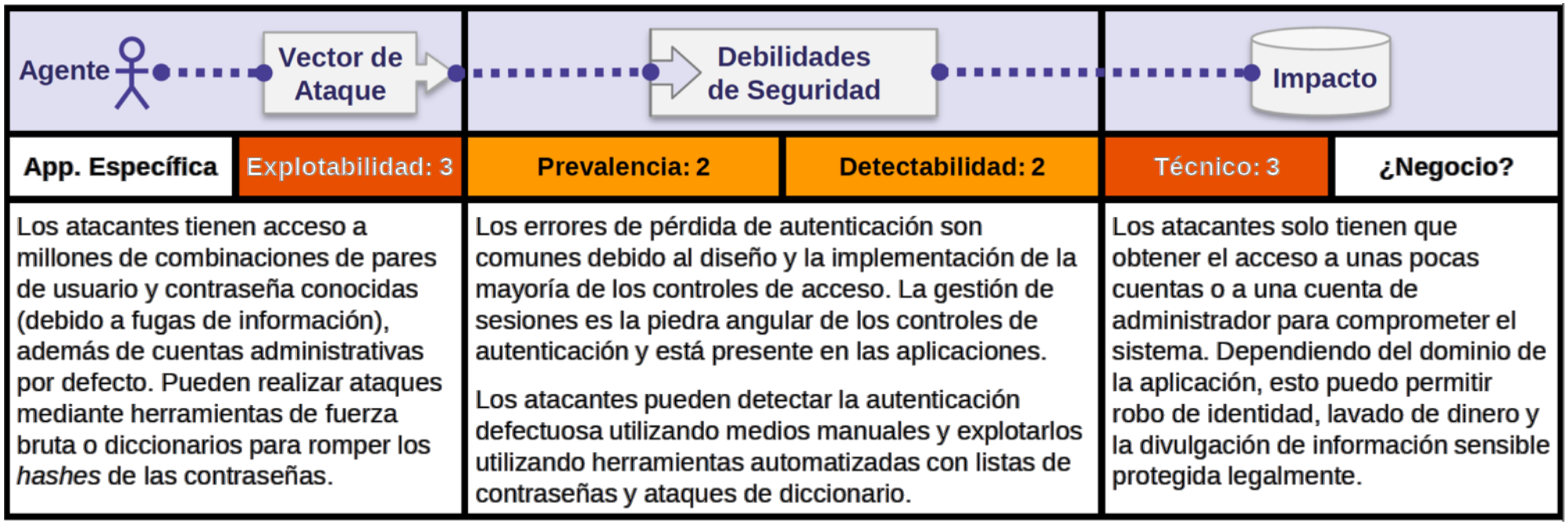
A1:2017 Inyección

A2:2017 Pérdida de Autenticación

A2:2017

Pérdida de Autenticación

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

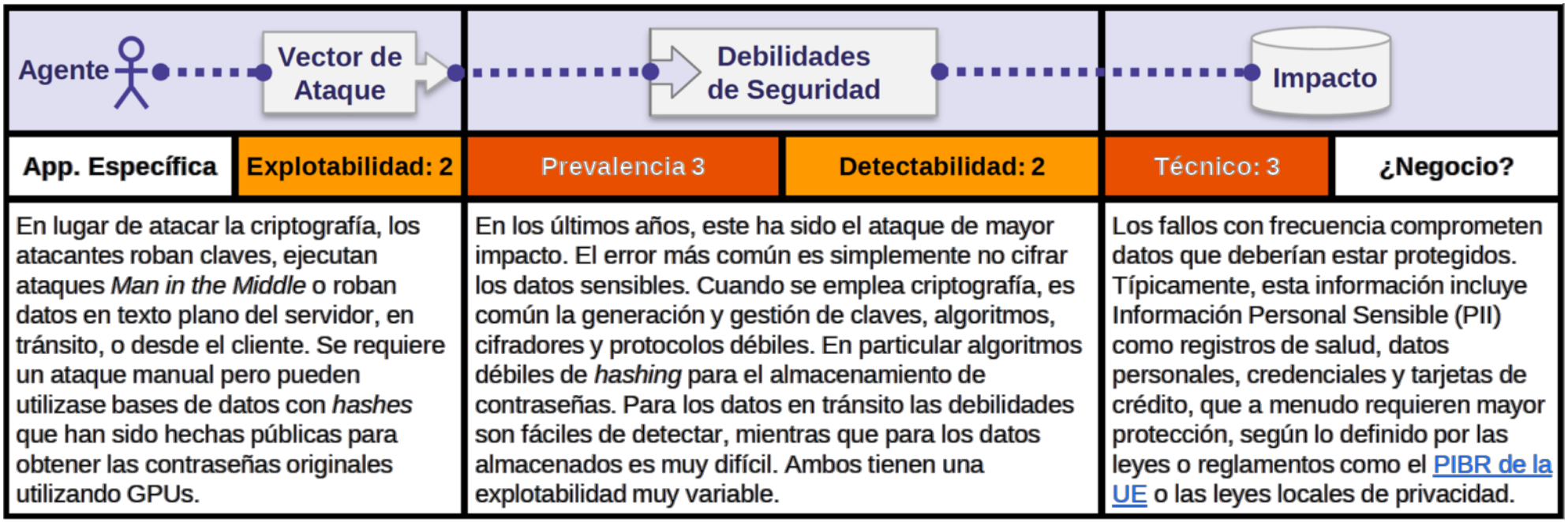


A3:2017 Exposición de datos sensibles

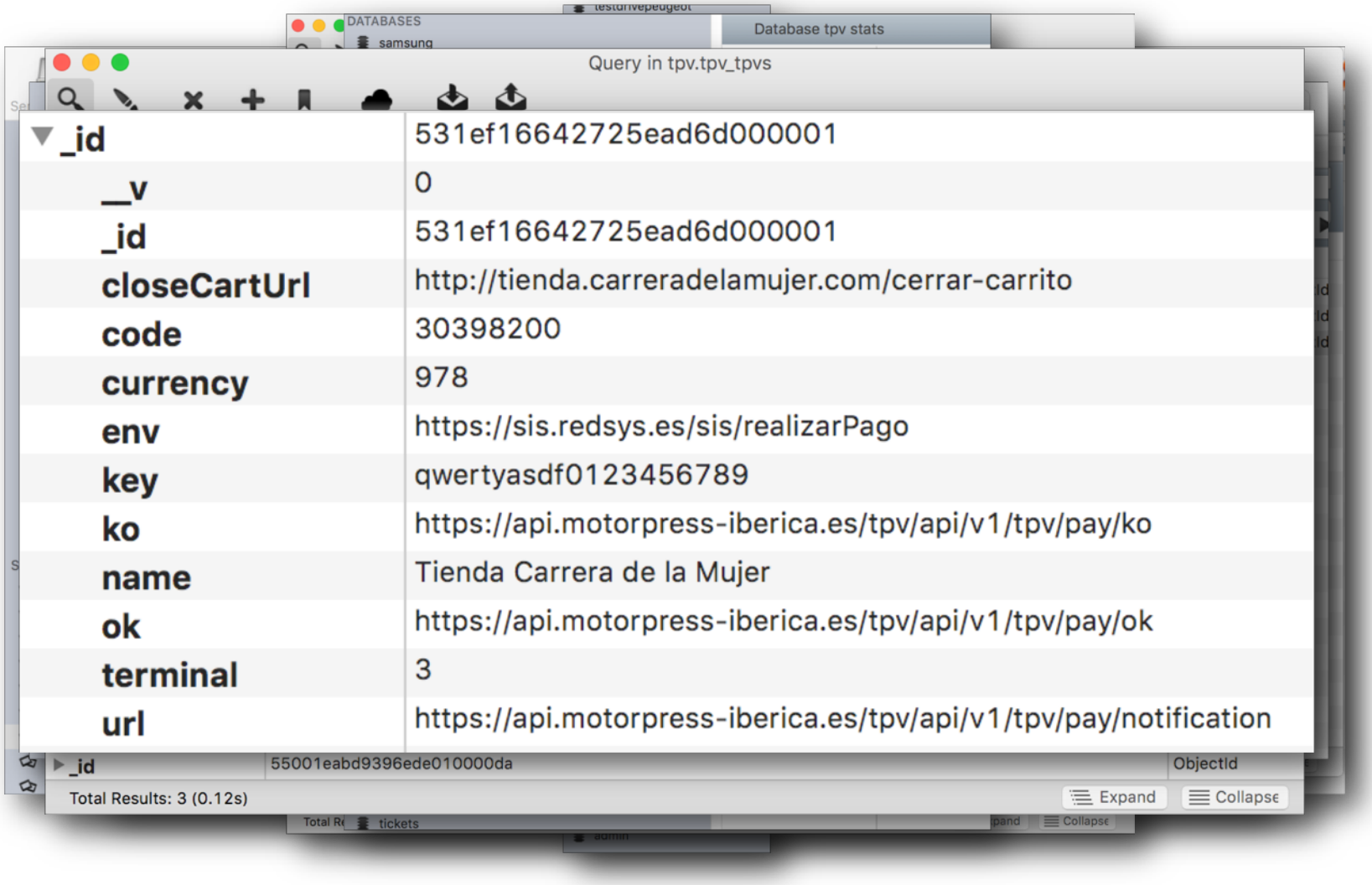
A3:201

Exposición de datos sensibles

Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.



A3:2017 Exposición de datos sensibles

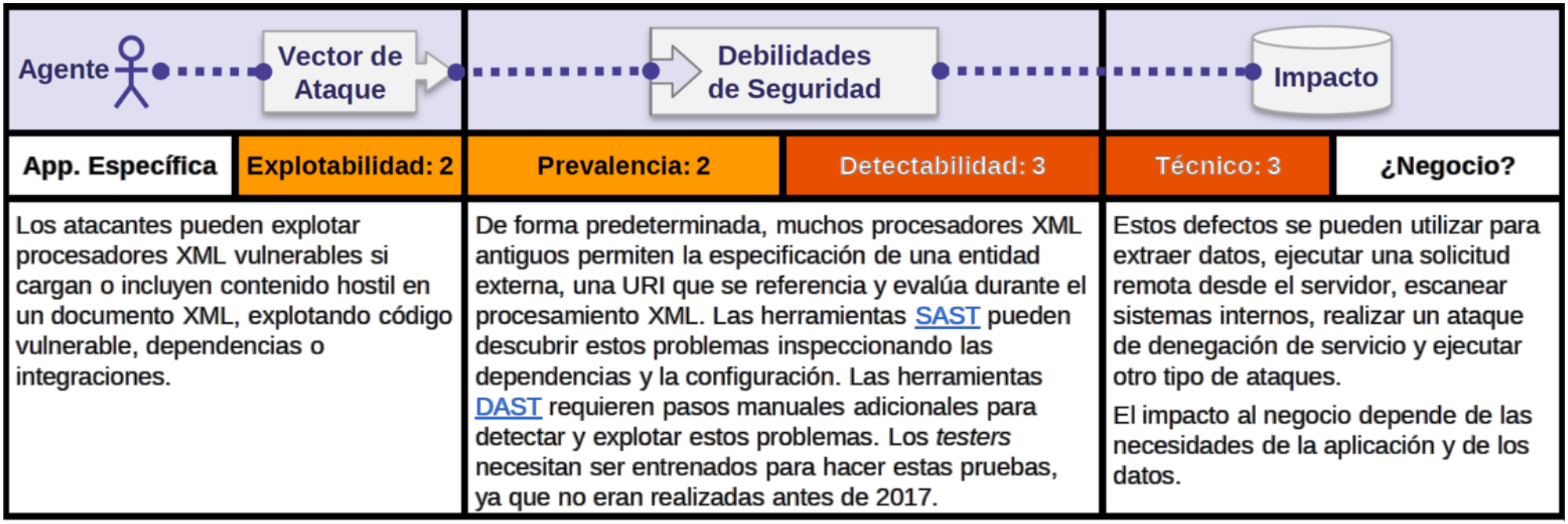


A4:2017 Entidades Externas XML (XXE)

A4:2017

Entidades Externas XML (XXE)

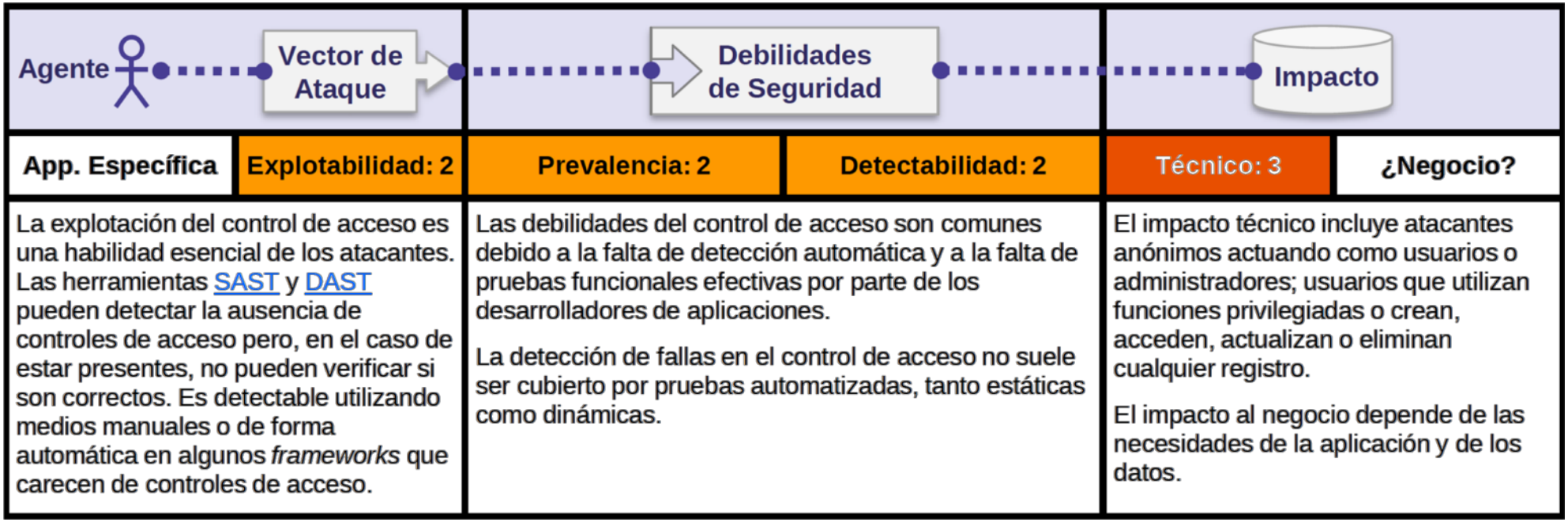
Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).



A5:2017 Pérdida de Control de Acceso

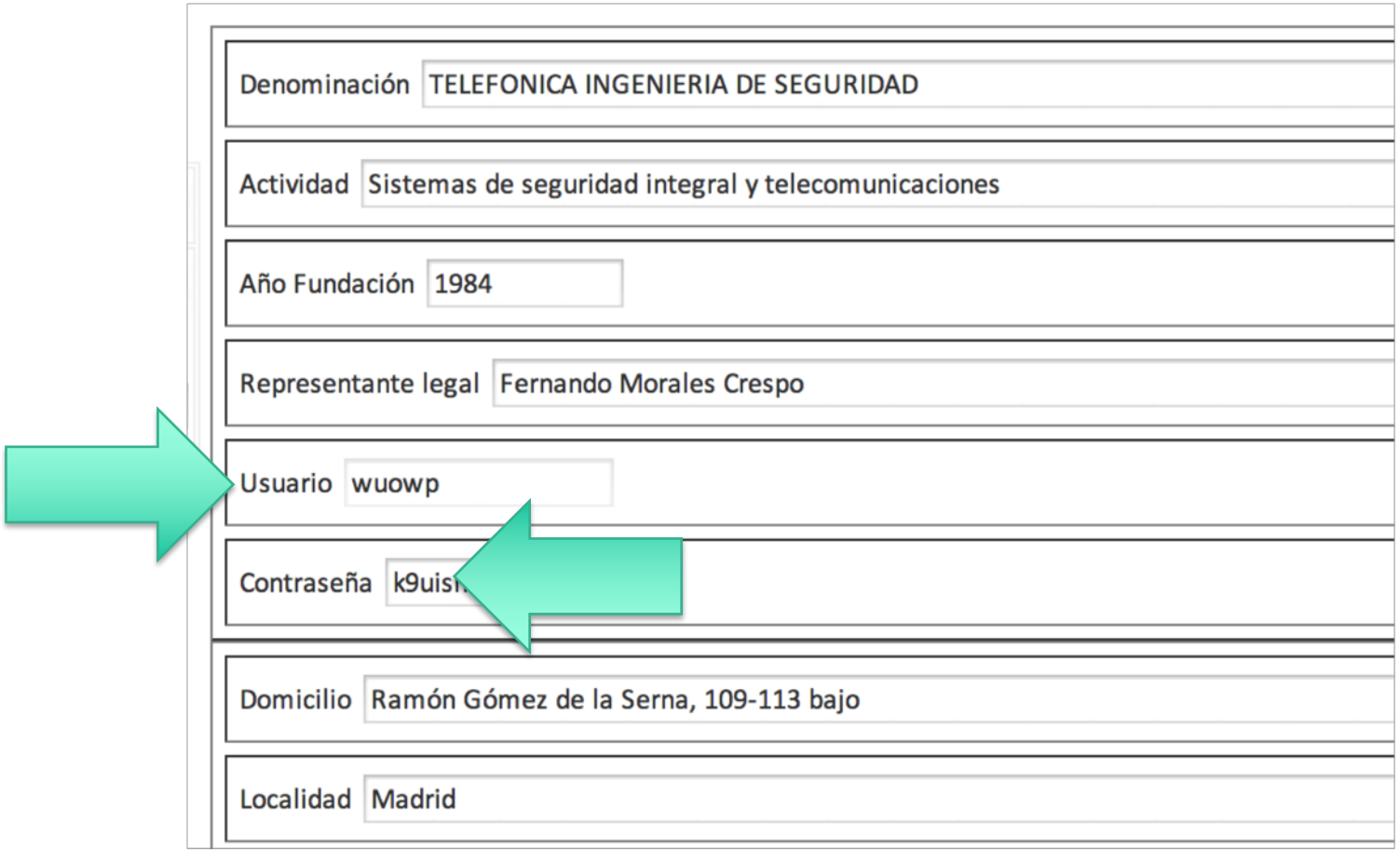
A5:2017
Pérdida de Control de Acceso

Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.



A5:2017 Pérdida de Control de Acceso

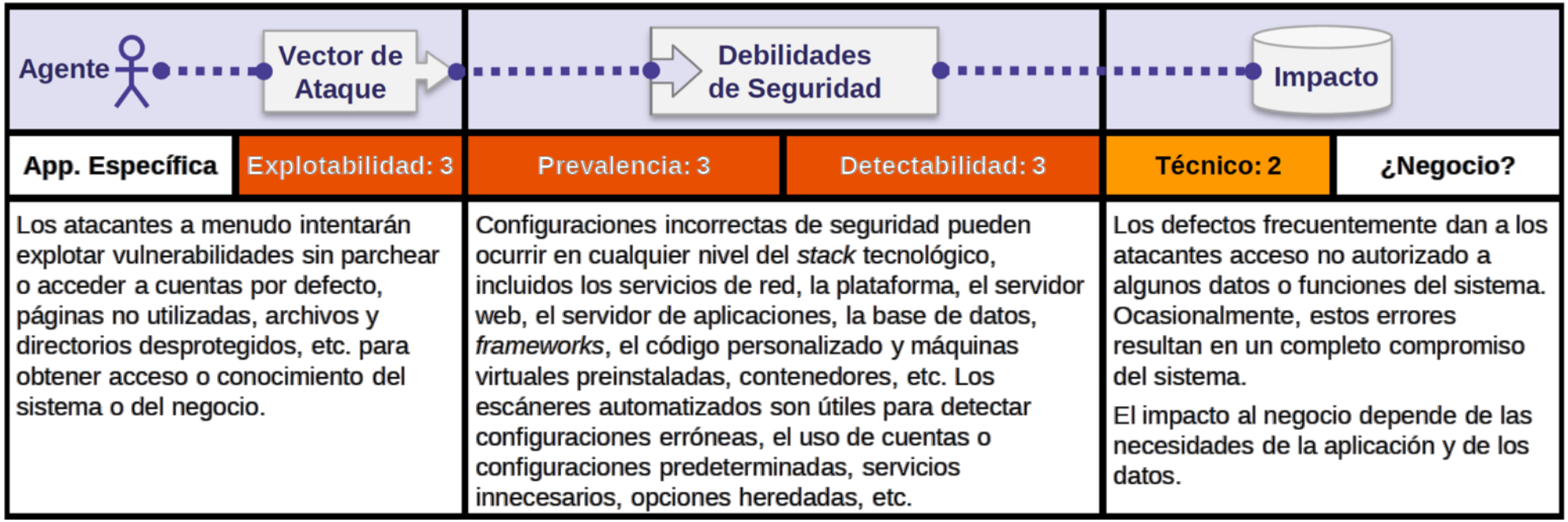
`http://www.aesseguridad.es/asociados/misdatos.asp?Cod_Asociado=81`



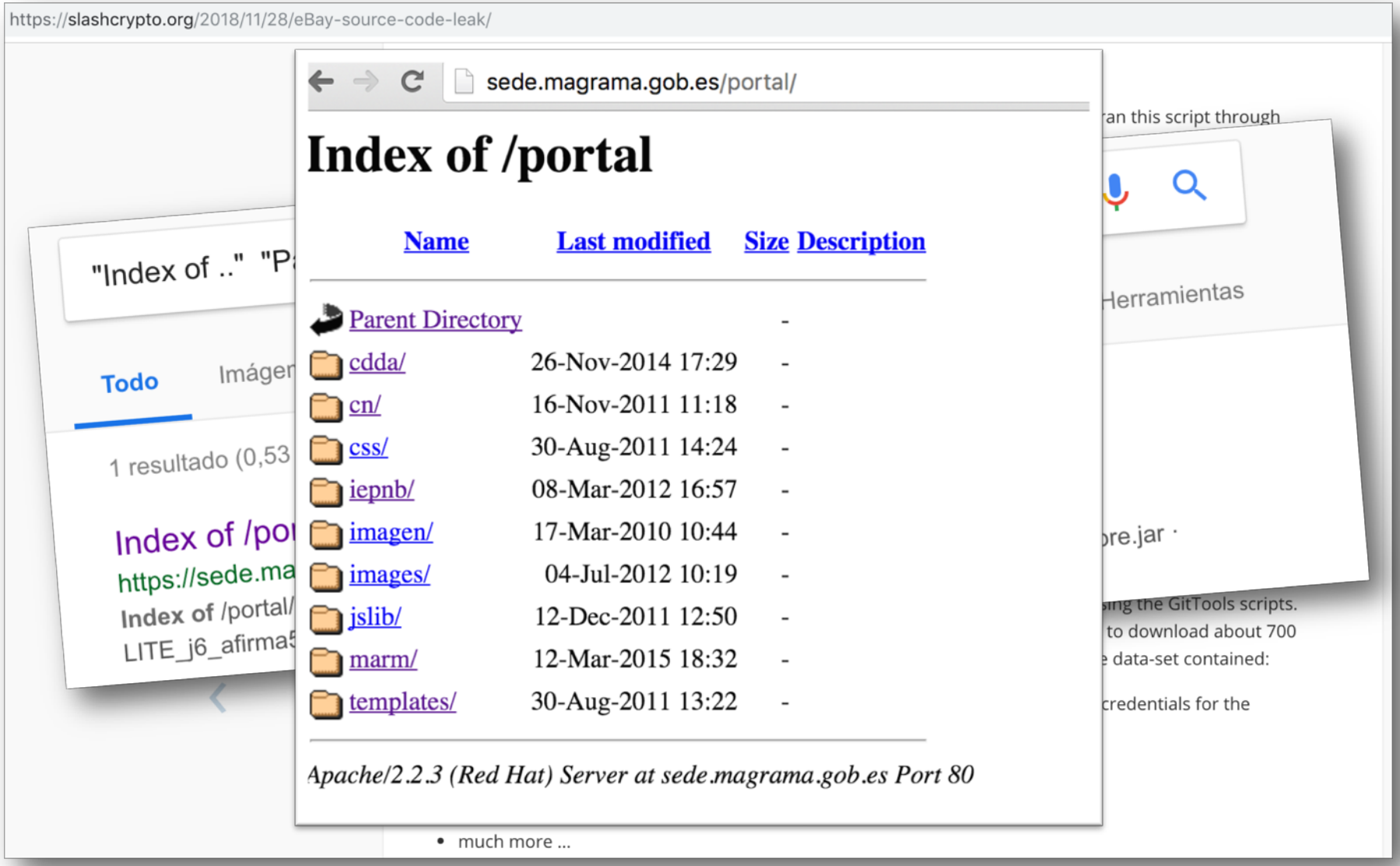
A6:2017 Configuración de Seguridad Incorrecta

A6:2017 Configuración de Seguridad Incorrecta

La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, *ad hoc* o por omisión *(*o directamente por la falta de configuración). Son ejemplos: *S3 buckets* abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, *frameworks,* dependencias y componentes desactualizados, etc.



A6:2017 Configuración de Seguridad Incorrecta

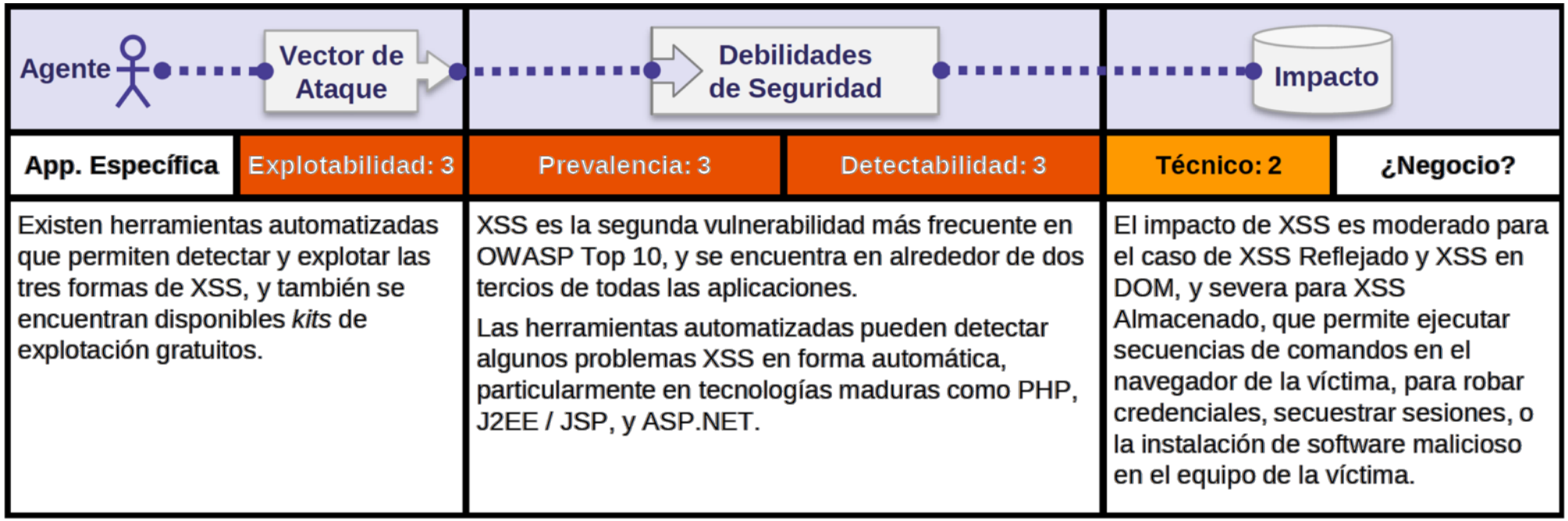


A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS)

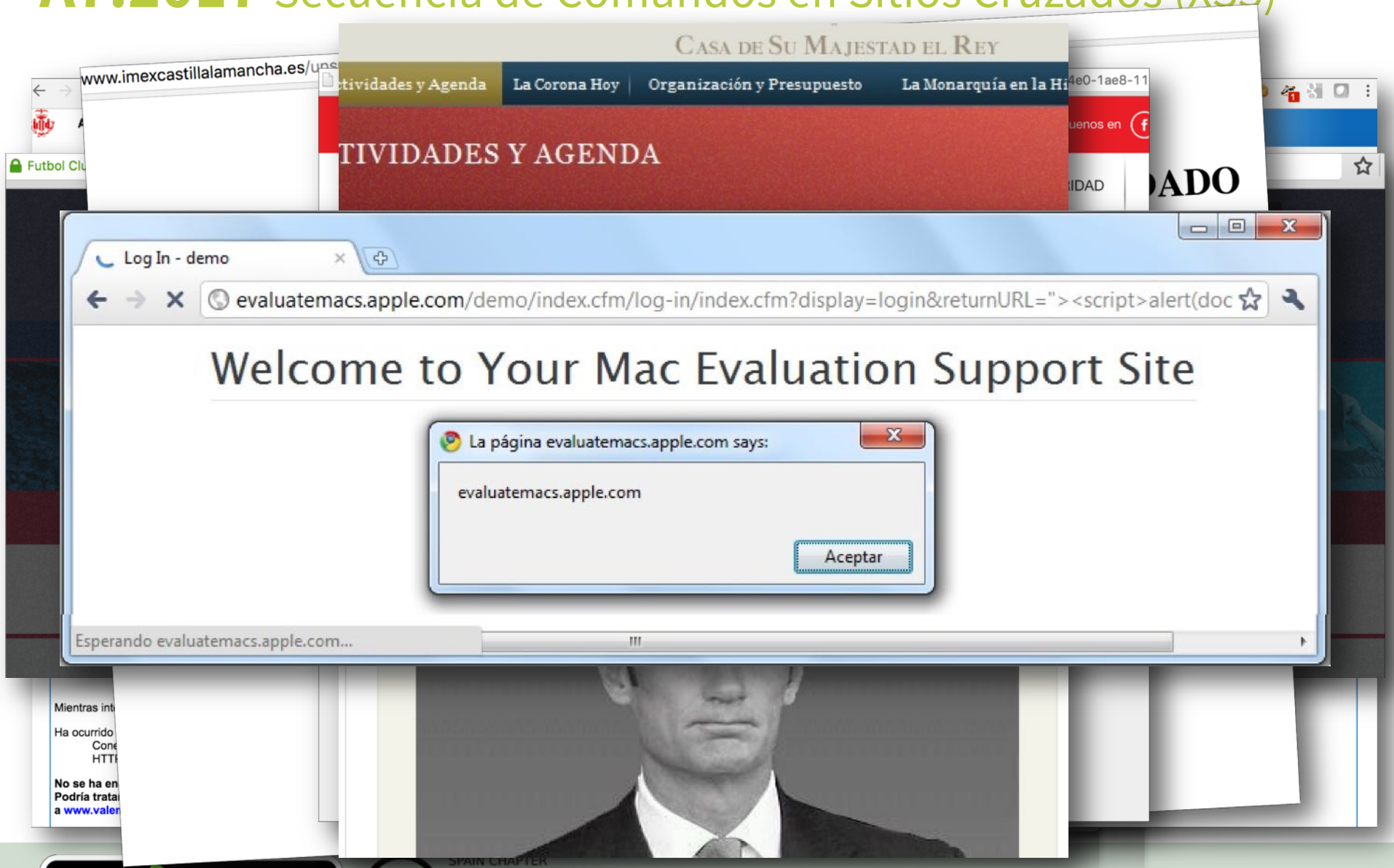
A7:2017

Secuencia de Comandos en Sitios Cruzados (XSS)

Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta *JavaScript* en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar (*defacement*) los sitios web, o redireccionar al usuario hacia un sitio malicioso.



A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS)



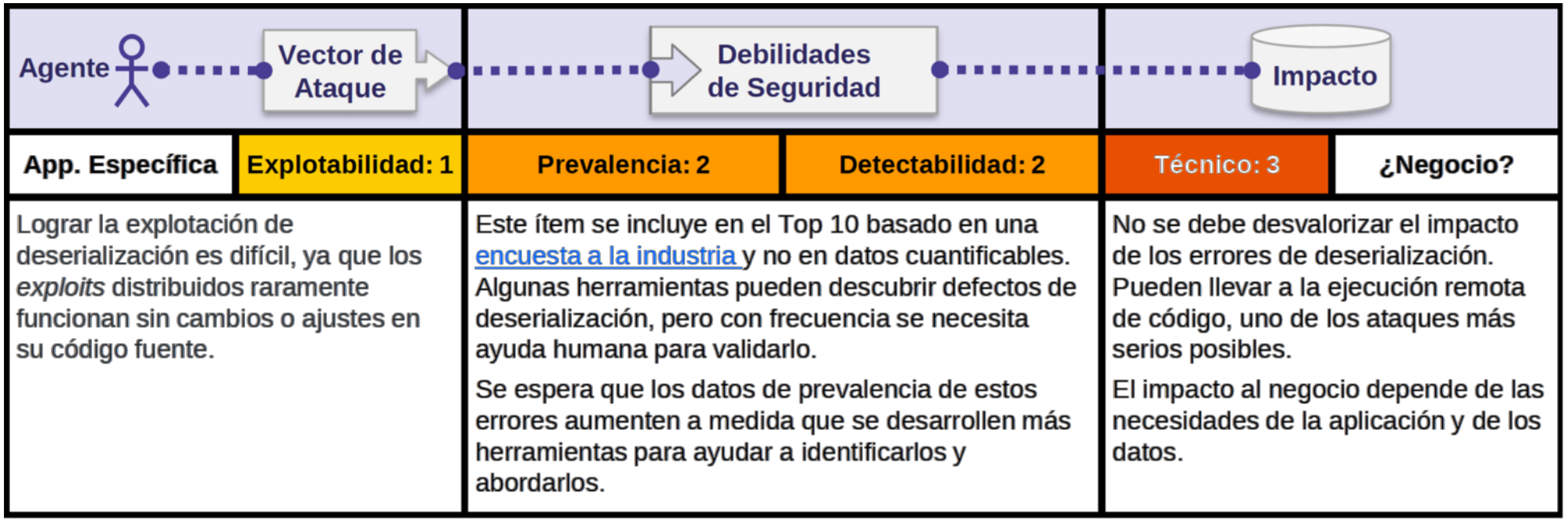
A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS)

https://www.gasmonkeygarage.com/wp-content/themes/gasmonkeygarage/image-processor.php?shopify=INJECT_IMAGE_HERE

A8:2017 Deserialización Insegura

A8:2017
Deserialización Insegura

Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

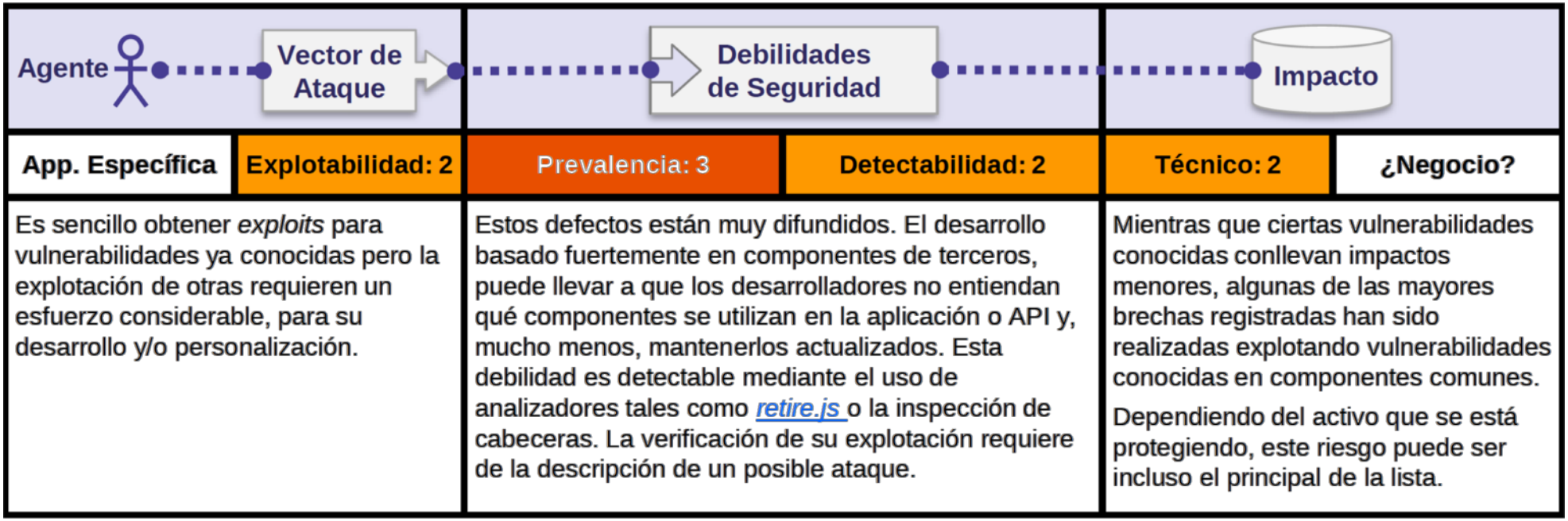


A9:2017 Componentes con vulnerabilidades conocidas

A9:2017

Componentes con vulnerabilidades conocidas

Los componentes como bibliotecas, *frameworks* y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.



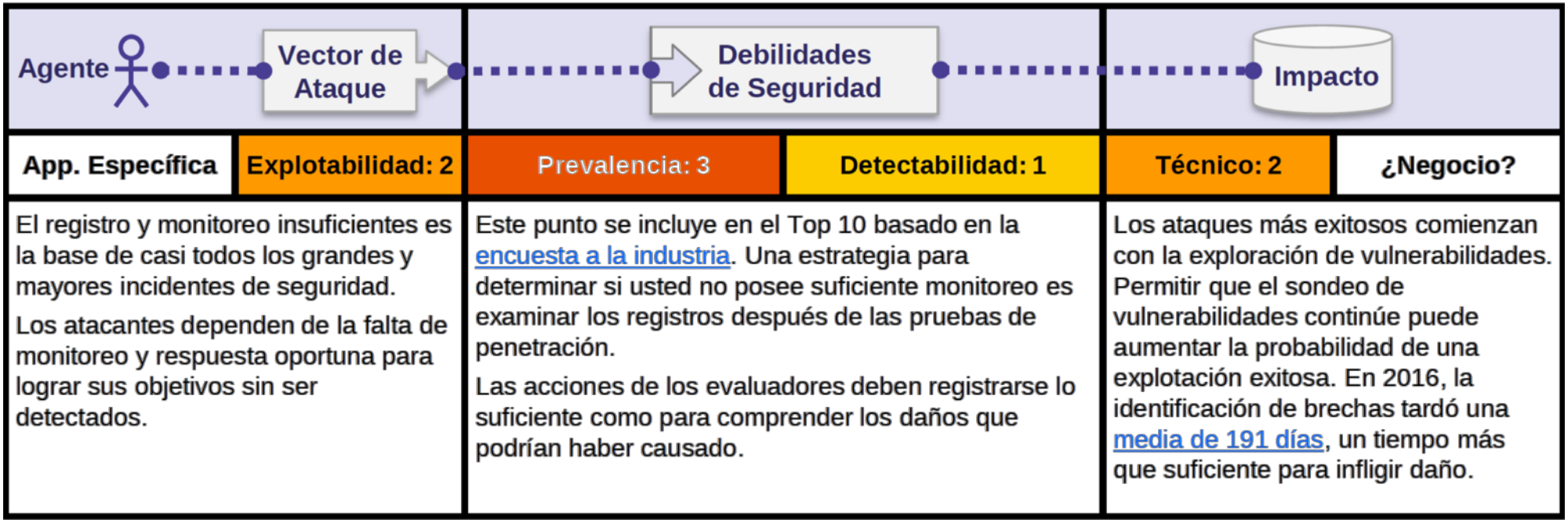
App. Específica	Explotabilidad: 2	Prevalencia: 3	Detectabilidad: 2	Técnico: 2	¿Negocio?
Es sencillo obtener *exploits* para vulnerabilidades ya conocidas pero la explotación de otras requieren un esfuerzo considerable, para su desarrollo y/o personalización.		Estos defectos están muy difundidos. El desarrollo basado fuertemente en componentes de terceros, puede llevar a que los desarrolladores no entiendan qué componentes se utilizan en la aplicación o API y, mucho menos, mantenerlos actualizados. Esta debilidad es detectable mediante el uso de analizadores tales como *retire.js* o la inspección de cabeceras. La verificación de su explotación requiere de la descripción de un posible ataque.		Mientras que ciertas vulnerabilidades conocidas conllevan impactos menores, algunas de las mayores brechas registradas han sido realizadas explotando vulnerabilidades conocidas en componentes comunes. Dependiendo del activo que se está protegiendo, este riesgo puede ser incluso el principal de la lista.	

A10:2017 Registro y Monitoreo Insuficientes

A10:2017

Registro y Monitoreo Insuficientes

El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos



Resumen de Riesgos OWASP Top 10 2017

Riesgo	Agentes de Amenaza	Vectores de Ataque	Debilidades de Seguridad		Impacto		Puntuación
		Explotabilidad	Prevalencia	Detectabilidad	Técnico	Negocio	
A1: 2017- Inyección	Específico de la Aplicación	FACIL: 3	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	8,0
A2: 2017 - Pérdida de Autenticación	Específico de la Aplicación	FACIL: 3	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A3: 2017 - Exposición de Datos Sensibles	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A4: 2017 - Entidad Externa de XML (XXE)	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	7,0
A5: 2017 - Pérdida de Control de Acceso	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	6,0
A6: 2017 - Configuración de Seguridad Incorrecta	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A7: 2017 - Secuencia de Comandos en Sitios Cruzados (XSS)	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A8: 2017 - Deserialización Insegura	Específico de la Aplicación	DIFICIL: 1	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	5,0
A9: 2017 - Componentes con Vulnerabilidades Conocidas	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	MODERADO: 2	Específico de la Aplicación	4,7
A10: 2017 - Registro y Monitoreo Insuficientes	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	DIFICIL: 1	MODERADO: 2	Específico de la Aplicación	4,0


¿Jugamos a un juego?

Un pequeño juego

Un pequeño juego

Welcome to the FIBARO smart home

Imagine that you live in a house where everything happens by itself. FIBARO Smart Home takes care of your everyday comfort and safety of all family members and in the meantime, saves energy on every single occasion. All this is possible thanks to Home Center 2 smart home HUB.

Devices network communication

Launch of scenes

Power consumption

Safety and security

History and statistics

Un pequeño juego

Motion Sensor

Flood Sensor

Door/Window Sensor

CO Sensor

Smoke Sensor

Universal Binary Sensor

Wall Plug

The Heat Controller

Switches

Dimmer 2

Roller Shutter 3

RGBW Controller

Intercom

KeyFob

The Button

Swipe

Un pequeño juego

Un pequeño juego

The core of the smart home system

Home Center 2 is an indispensable part of the FIBARO System without which the rest devices of home automation would be only beautiful objects. The smart home HUB collects and analyzes information about devices, communicates them with each other and thus directs the operation of the entire system and takes care of its security.

CS³ SECURITY SERVICES https://cs3group.com

SPAIN CHAPTER OWASP Open Web Application Security Project

Un pequeño juego

Feel the potential of integration

By choosing Home Center 2, you can use the integration of FIBARO System with global brands such as Google Assistant and Amazon Alexa voice assistants. Joining forces and technology guarantees top notch features and potential of your smart home including all of the latest solutions available on the market.

Un pequeño juego

A system that constantly evolves

FIBARO technology with the biggest players in the industry results in a dynamically growing number of devices compatible with FIBARO system. This allows you to endlessly develop your home ecosystem over which Home Center 2 takes control.

Check the Compatibility >

Un pequeño juego

Monitoring, setup and management of the smart home system is possible thanks to a simple and functional app available for your PC, tablet, smartphone and even Apple Watch. Get notifications on selected devices, analyze your activity history, and see energy consumption statistics on a screen size that you prefer. Manage FIBARO System as you like whenever you want, wherever you want.

Download on the App Store

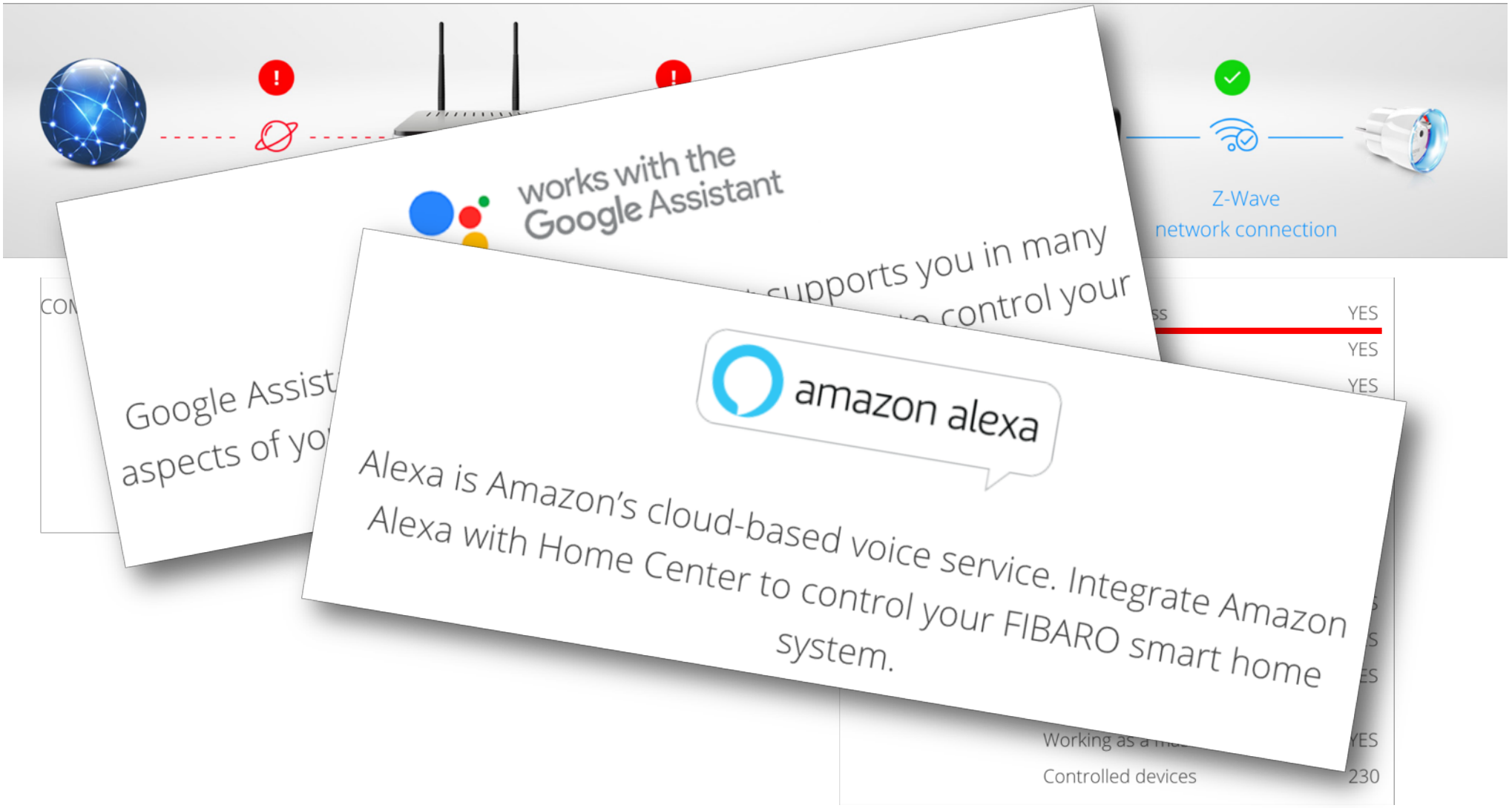
GET IT ON Google Play

DESKTOP Web App

CS³ SECURITY SERVICES https://cs3group.com

SPAIN CHAPTER OWASP Open Web Application Security Project

Un pequeño juego



Un pequeño juego

More possibilities with connected devices

PHILIPS

Control, automate, and monitor your lights from anywhere.

netatmo

The Weather Station Indoor Module measures your indoor comfort by providing vital information.

SONOS

Trigger your favorite playlist and automatically control your speakers.

D-Link

Stream live video on your phone or get video clip notifications when unexpected activity occurs in your home.

Yale®

The Yale Keyless Connected smart lock gives you freedom to secure your home without the need for a key.

DSC®

DSC is a world leader in electronic security. Since the company's genesis, the experts at DSC have been leading the way.

Un pequeño juego

Responsible disclosure

I've reported above described vulnerabilities to Fibaro. I tried to contact Fibaro multiple times and first came in contact with an employee that did not give the discovered vulnerability the priority it deserved. The employee communicated that the issue was being fixed by developers, however after 100+ days the vulnerability was still not fixed. This was frustrating, however I kept trying contacting employees of Fibaro. This is a timeline of the responsible disclosure report:

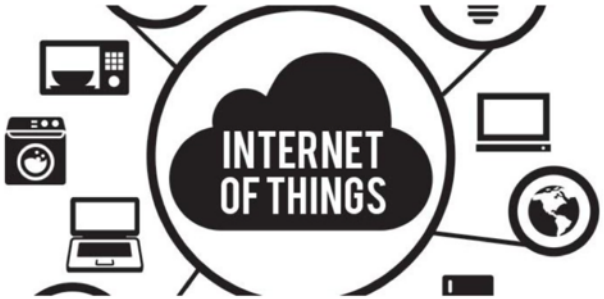
- 22/02/2017: Reported the vulnerability.
- 01/03/2017: Employee asked to verify whether the bug was fixed. Checked and it was not fixed.
- 02/03/2017: Employee communicated that the vulnerability is being fixed right now.
- 08/05/2017: Verified the newest firmware. Vulnerability still present, communicated this to the contact person. No reply.
- 15/06/2017: Verified the newest firmware. Vulnerability still present, communicated that I will post my findings in a blog. No reply.
- 20/06/2017: Contacted management employee of Fibaro through LinkedIn, replies directly.
- 21/06/2017: Technical employee contacting me that an fix is being implemented.
- 23/06/2017: Decided to sent my exploit and video to make sure everything is clear to the technical employee.
- 28/06/2017: Vulnerability fixed, technical employee asked to verify the patch.
- 03/07/2017: Patch received from Fibaro.
- 04/07/2017: Verified that the patch fixes the RCE vulnerability.
- 05/07/2017: Technical and management employees are happy with my findings and decide to send me a gift 🙂
- 14/09/2017: Patch released.

```
requests.post( http://' + args.rhost + '/services/liliSetDeviceCommand.p
```

bwssystems.com/#/habridge

BWS Systems | Home | Apps | News | About | Contact

Bridge Application for IoT



Description

Emulates Philips Hue api to other home automation gateways such as an Amazon Echo or the Google Home. The Bridge handles basic commands such as "On", "Off" and "brightness" commands of the hue protocol. This bridge can control most devices that have a distinct API.

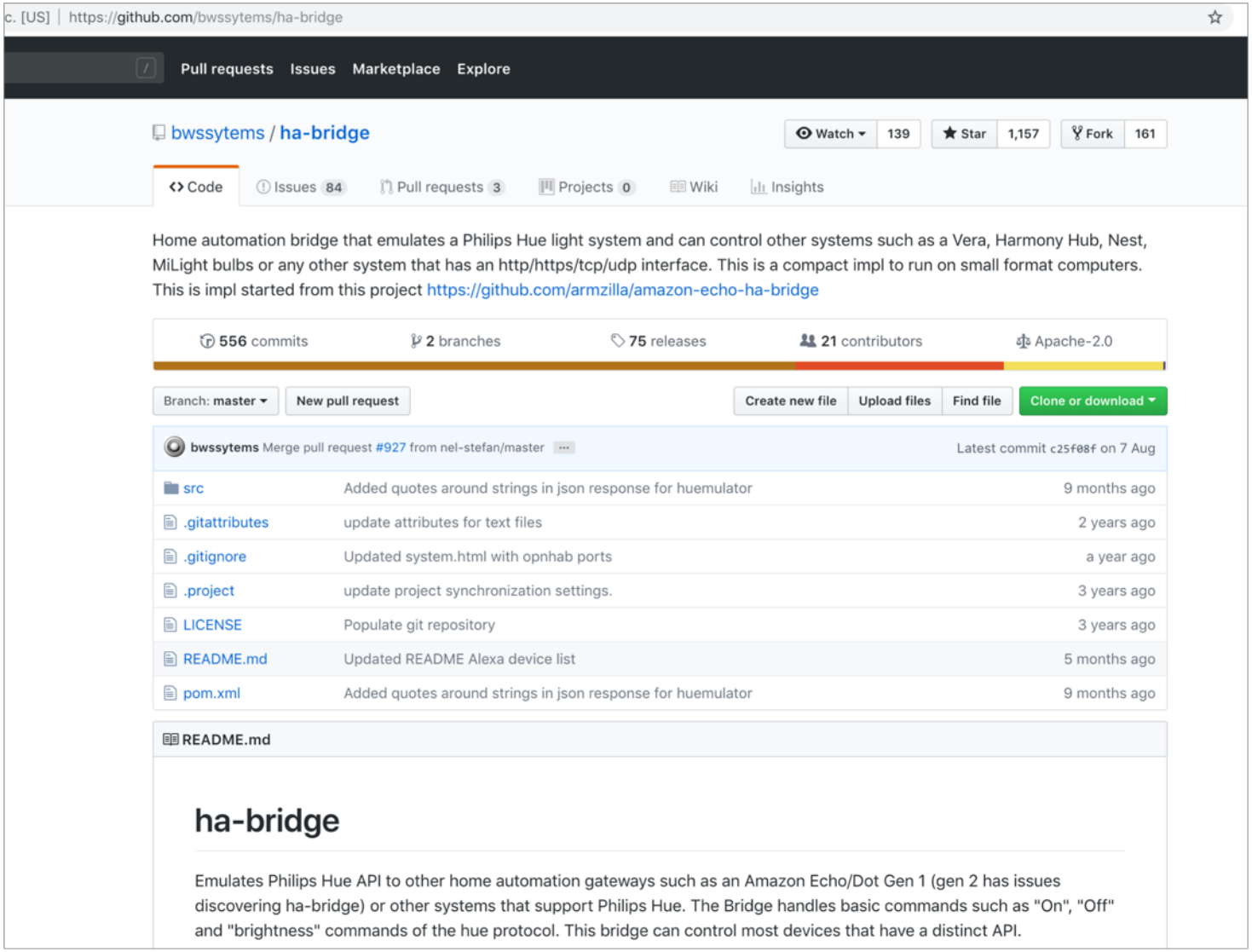
In the cases of systems that require authorization and/or have API's that cannot be handled in the current method, a module may need to be built. The Harmony Hub is such a module and so is the Nest module. The Bridge has helpers to build devices for the gateway for the Logitech Harmony Hub, Vera, Vera Lite or Vera Edge, Nest, HAL, MQTT, TCP, UDP, HTTP/HTTPS, Home Assistant, Domoticz, Somfy Tahoma Shades, Fibaro HomeWizard Smart Plugs and the ability to proxy all of your real Hue bridges behind this bridge.

Alternatively the Bridge supports custom calls as well systems such as the LimitlessLED/MiLight bulbs using the UDP protocol. Binary data is supported with UDP/TCP.

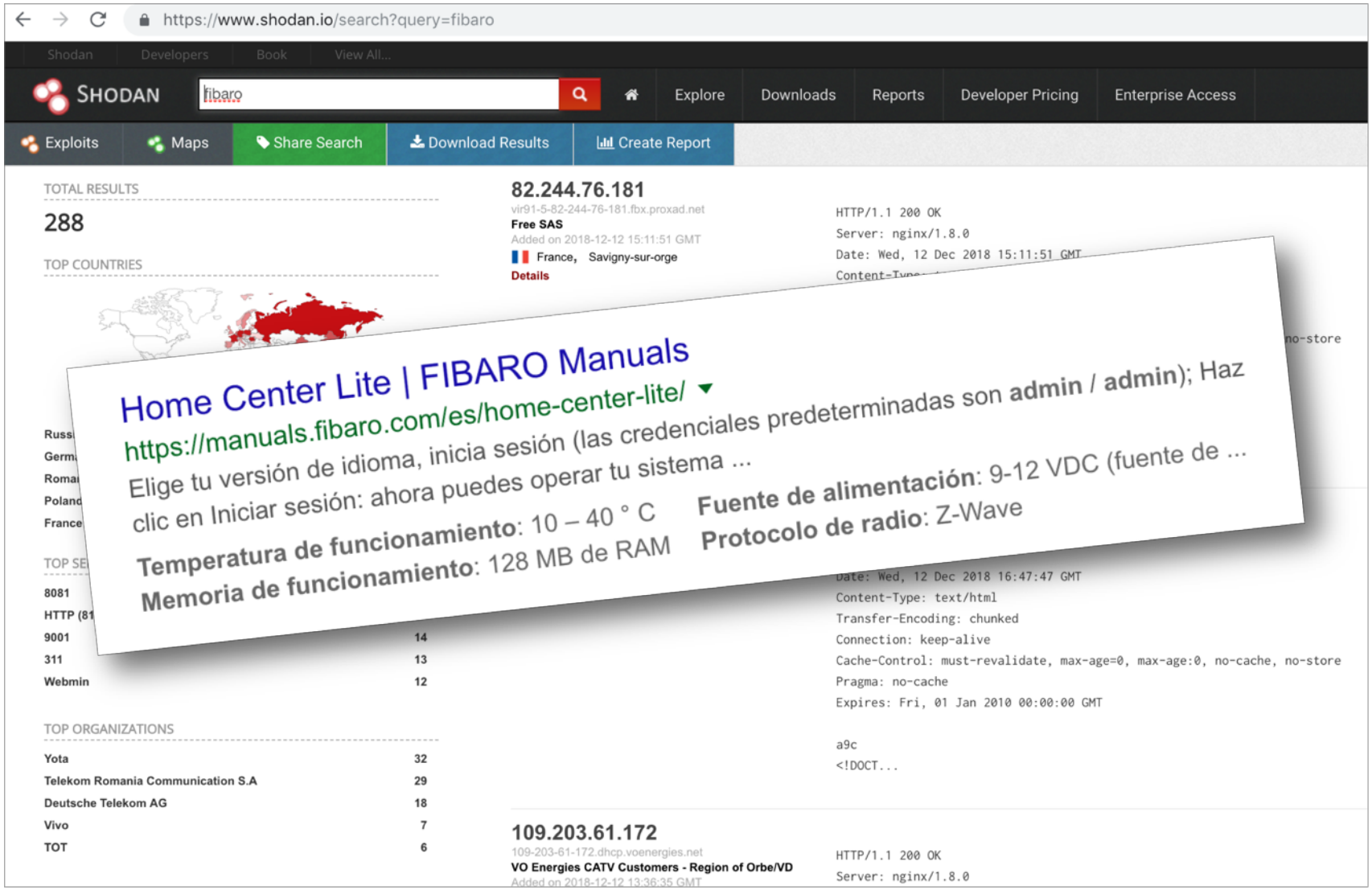
LIFX · somfy · FIBARO Home intelligence

FHEM · Home Automated Living™ · BroadLink · Domoticz control at your fingertips. · openHAB empowering the smart home

Un pequeño juego



Un pequeño juego



Un pequeño juego

Un pequeño juego

¡Muchas gracias!