

SEGURIDAD IOT EN SANIDAD

¿ESTAMOS PREPARADOS?

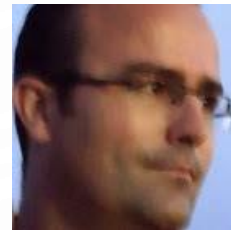
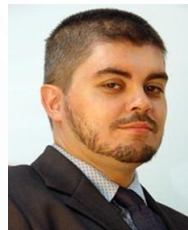


SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?



PUBLICACIÓN

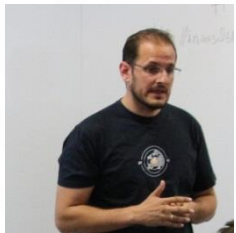
- APISA
- Autores: Miguel Ángel Arroyo Moreno, Josep Bardallo Gay, Juan José Domenech Sánchez, Francisco Jesús Gómez López, Ramón Salado Lucena
- Prólogo: Vicente Aguilera



PUBLICACIÓN



Arquitecto de soluciones e ingeniero de software, dedicado desde 2012 a proponer, asesorar y desarrollar arquitecturas (de aplicación, de infraestructura, de integración y de operaciones), tecnologías y productos enfocadas a Smart Cities, IoT, seguridad y soluciones empresariales. CoLeader de OWASP Sevilla, y CiberCooperante de INCIBE.



Analista de Seguridad, CoLeader de OWASP Sevilla, y CiberCooperante de INCIBE. He trabajado durante más 10 años en el sector de la CiberSeguridad, 5 de ellos en la Administración Pública. Actualmente CTO-Founder de BeeHackers.

VAMOS A VER...

- Situación Actual
- Normativa en entornos Sanitarios
- GDPR
- Seguridad IoT
- Seguridad Redes
- Seguridad Web

Seguridad aplicaciones móviles iOS y Android

- BLE
- ZigBee
- Firmware

SITUACIÓN ACTUAL

Momento catalizador para impulsar la tecnología en eSalud

- Seguimiento remoto: teleasistencia, localización, alarmas, seguimiento
- Gestión asistencial: listas de espera, acceso a historial e informes clínicos, etc.
- Programas de salud: atención cardiovascular, diabetes, etc.

UNIÓN EUROPEA

MODELO CENTRO DE INNOVACIÓN DEL SECTOR PÚBLICO DE PWC E IE BUSINESS SCHOOL



Smart environment

Medio ambiente



Smart mobility

Movilidad



Smart living

**Seguridad
Sanidad y salud**



Smart people

Educación



Smart economy

Economía



Smart governance

Gobierno

SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SITUACIÓN ACTUAL

eSalud

Se define, según la OMS, como el uso de las tecnologías de la información y la comunicación (TIC) para la salud.

mSalud

Término empleado para designar el ejercicio de la medicina y la salud pública con apoyo de los dispositivos móviles.

mSSPA

Es un proyecto orientado a la personalización e integración de servicios móviles de salud.

IoHT

Internet de las cosas en Sanidad digamos que sería la convergencia e integración de forma inteligente de los datos recopilados por los sensores de los dispositivos médicos y de las tecnologías móviles que se utilizan en la asistencia sanitaria.

PLANES DE SEGURIDAD IOT

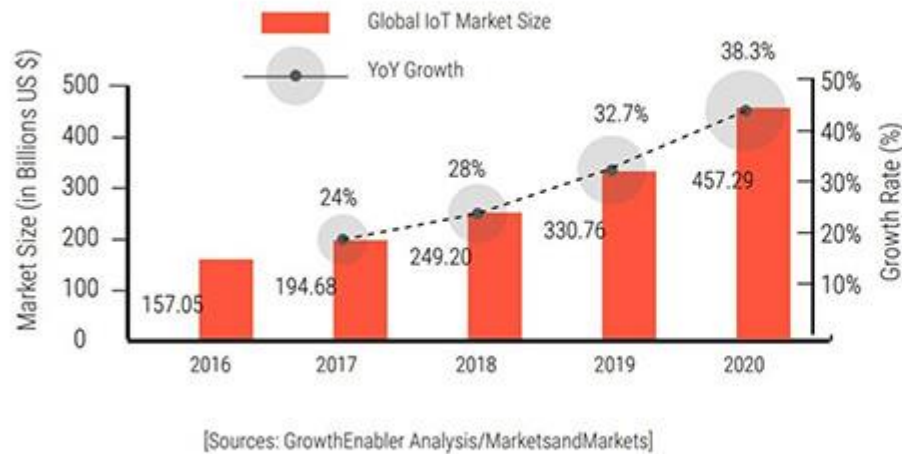
Europa

- Alianza para la innovación en Internet de las Cosas: ecosistema dinámico IoT europeo.
- ENISA (Agencia Europea de Seguridad de las Redes y de la Información) : informe anual con principales amenazas y tendencias
- Recomendaciones de NIST, IoT European Research Cluster, etc...

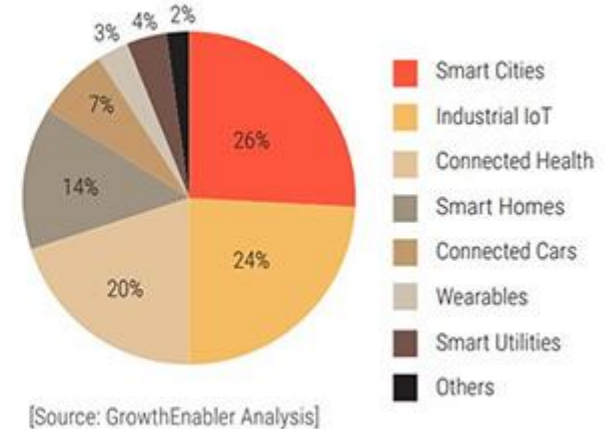
España

- INCIBE (Instituto Nacional de Ciberseguridad)
- El Equipo de Respuesta ante Emergencias Informáticas de Seguridad e Industria (CERTSI): publicación de guías orientadas para IoT
- Centro Criptológico Nacional (CCN): ha publicado un informe de buenas prácticas en IoT

SITUACIÓN ACTUAL



Global IoT Market Share by Sub-Sector



Gartner, Inc. Forecasts that 4.9 billion connected things will be in use in 2015, up 30 percent from 2014, and will reach 25 billion by 2020.

Gartner says 4.9 billion connected “things” will be in use in 2015, gartner.com/newsroom/id/2905717

SITUACIÓN ACTUAL



SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

GDPR



Las principales características de esta normativa aplicadas al entorno sanitario con dispositivos IoT son las siguientes:

- Obligatorio la creación de un DPO (“Data Privacy Officer”).
- Nuevo requisito de notificar incidentes de seguridad relativos a datos personales (“brechas”) en menos de 72 horas, a las autoridades competentes, y en algunos casos a los afectados.
- Nuevos requisitos sobre consentimiento del titular de los datos.
- Responsabilidad proactiva (“Accountability”)
- Seguridad por defecto
- Nuevos derechos: “derecho al olvido” y a la “portabilidad” de los datos
- Evaluación de impacto de las operaciones de tratamiento en la protección de datos personales (EIPD)

SEGURIDAD IOT

10/10 Permite '123456'

10/10 No Bloquea

10/10 Permite Enumeración de Usuarios

9/10 no tiene Doble Factor de Autenticación

8/10 Recoge Información Personal

7/10 no usa Cifrado

6/10 Interfaces Vulnerables a XSS/SQLi

SSH a la Escucha

Video Streaming sin Autenticación

Ausencia total de Actualizaciones



How safe are home security systems?
An HP study on IoT security

SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

Los problemas de seguridad del IoT son los problemas de las tecnologías que lo componen.

REDES

- Servicios, Encriptación, Firewall, ...

APLICACIONES

- authN, authZ, validación inputs, ...

MÓVIL

- APIs inseguras, capa cifrado, ...

CLOUD

- AuthSessionAccess, ...

IOT

- Red + App + Móvil + Cloud

IOT TOP TEN PROJECT

1

INTERFAZ WEB INSEGURA

AUTENTIC. / AUTORIZAC.
INSUFICIENTE

2

3

SERVICIOS DE RED
INSEGUROS

CIFRADO DE TRANSPORTE /
VERIFIC. DE INTEGRIDAD

4

5

PRIVACIDAD

6

INTERFAZ CLOUD INSEGURA

INTERFAZ MOVIL INSEGURO

7

8

CONFIGURACION DE SEGURIDAD
INSUFICIENTE

SOFTWARE / FIRMWARE
INSEGURO

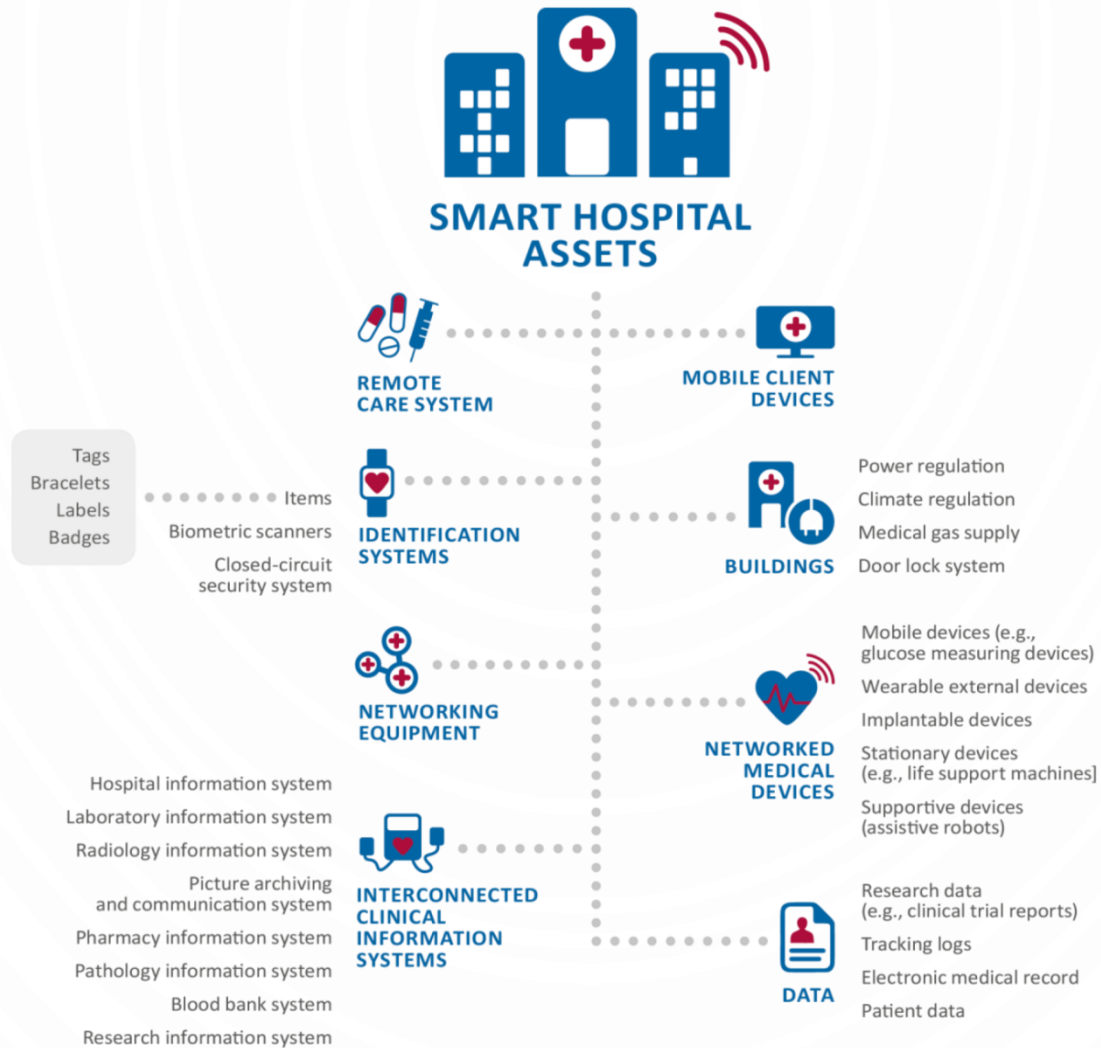
9

10

POBRE SEGURIDAD FISICA

SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD EN RED

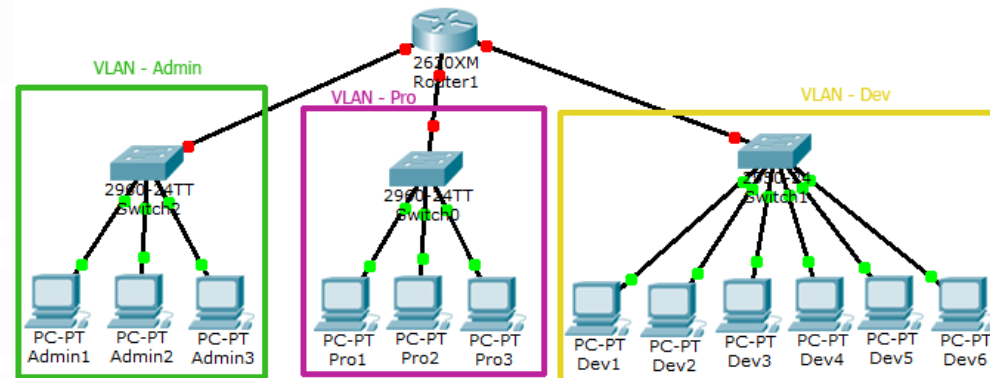


SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD EN RED

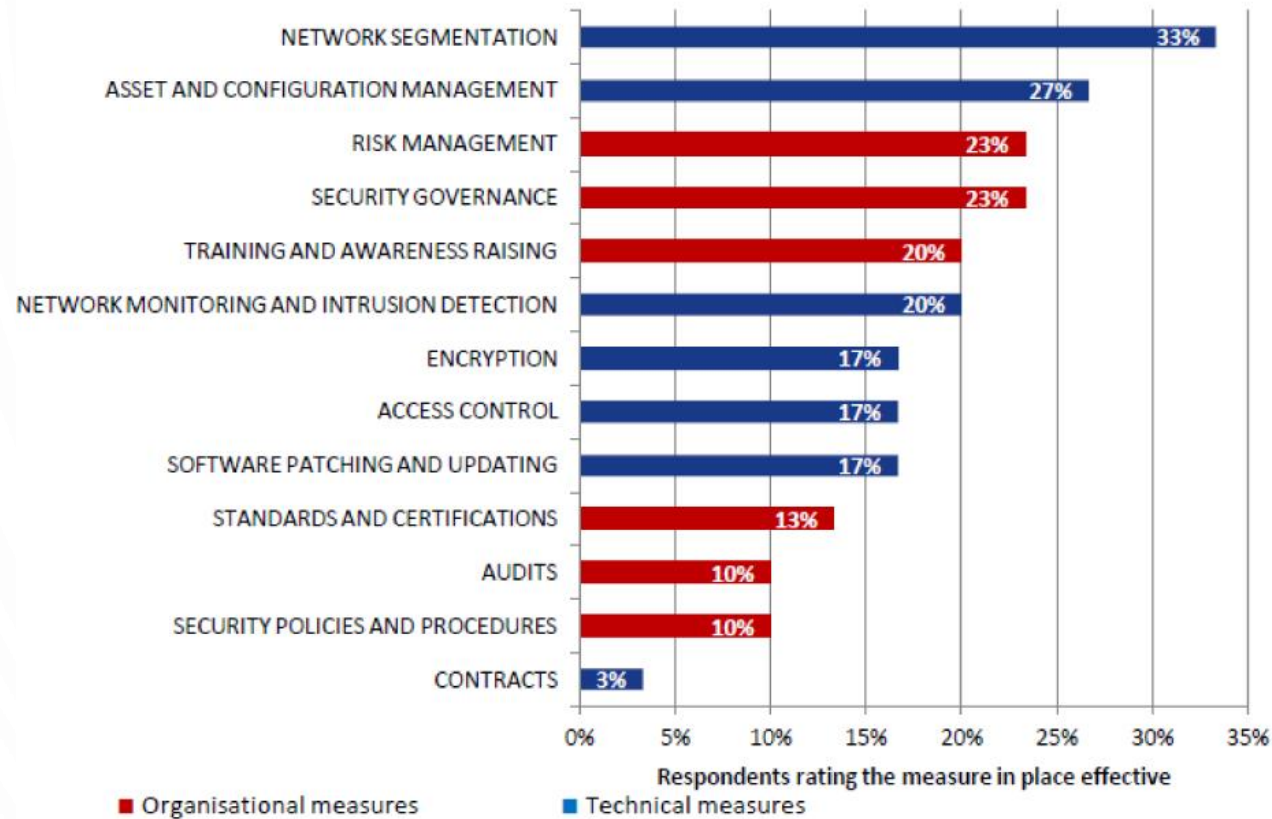
Aspectos a tener en cuenta en la arquitectura:

- Segmentación de la Red
- Cifrado máximo en conexiones inalámbricas (WPA2-PSK AES+TKIP, WPA3, RADIUS)
- Comunicación cifrada entre segmentos de red (SSL, SSH, SNMP v3)
- Uso de VPN's para dispositivos que transmitan en texto plano
- Sistemas IDS/IPS de detección de intrusos
- Conexiones con protocolos PACS y DICOM (apps vulnerables)
- Protocolo para dispositivos IMD
- Sistemas UTM, SIEM, ERD, etc.



SEGURIDAD EN RED

Cyber Security and resilience for Smart Hospitals



SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing

Information Gathering

Config. & Deploy Management

Identity Management Testing

Authentication Testing

Authorization Testing

Session Management Testing

Input Validation Testing

Error Handling

Cryptography

Business Logic Testing

Client Side Testing

ENJOY ;)

SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance for information leakage (0TG-INF0-001)

Hay elementos directos e indirectos para el descubrimiento con motores de búsqueda:

- ↘ Métodos directos se refieren a los índices de la búsqueda y el contenido asociado de cachés.
- ↘ Métodos indirectos se refieren a información sensible del diseño y configuración, buscando foros, grupos de noticias y otros sitios web.

Una vez que un robot del motor de búsqueda ha terminado de recórrela, comienza la indexación de la página web basada en etiquetas y atributos asociados, con el fin de devolver los resultados de búsqueda relevantes. Si el archivo robots.txt no se actualiza durante la vida útil del sitio web y es posible que los índices de contenido de la web, incluyan archivos no deseados.



DuckDuckGo



SHODAN



SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance
for information leakage (0TG-INF0-001)

GHDB

Google

inurl:"/wp-content/wpclone-temp/wpclone_backup/"

Todo Shopping Maps Noticias Imágenes Más Configuración Herramientas

Aproximadamente 72 resultados (0,27 segundos)

[Index of /pw3/wp-content/wpclone-temp/wpclone_backup - Sarah Yost](#)
▼ Traducir esta página
Index of /pw3/wp-content/wpclone-temp/wpclone_backup Parent Directory · database.sql · prefix.txt · wp-content/. Apache Server at Port 80.

[Index of /wp-content/wpclone-temp/wpclone_backup](#)
▼ Traducir esta página
Index of /wp-content/wpclone-temp/wpclone_backup Parent Directory · database.sql · wp-content/. Apache Server at Port 80.

[Index of /wp-content/wpclone-temp/wpclone_backup](#)
▼ Traducir esta página
Index of /wp-content/wpclone-temp/wpclone_backup Parent Directory · database.sql · wp-content/. Apache Server at Port 80.

[Index of /wp-content/wpclone-temp/wpclone_backup - Description](#)
▼ Traducir esta página
Index of /wp-content/wpclone-temp/wpclone_backup. Name · Last modified · Size · Description · Parent Directory, -. database.sql, 2015-10-24 10:13, 5.3M. prefix.txt, 2015-10-24 10:13, 3. wp-content/, 2015-10-24 10:13, -

SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance for information leakage (0TG-INF0-001)

SHODAN



SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance for information leakage (0TG-INF0-001)

SHODAN

HP Color LaserJet 3800 / [REDACTED]
HP Color LaserJet 3800 Printers

[Log In](#)

Information

- Device Status
- Configuration Page
- Supplies Status
- Event Log
- Usage Page
- Diagnostics Page
- Device Information
- Control Panel
- Color Usage Job Log
- Print

Other Links

- [hp instant support](#)
- [Order Supplies](#)
- [Product Support](#)

Device Status

Ready

☐ Pause/Resume ☒ Continue

Supplies

Toners: (% remaining)

Black Cartridge 58% Cyan Cartridge 59% Magenta Cartridge 47% Yellow Cartridge 78%

[Supplies Details](#)

Media

Input/Output	Status	Capacity	Size	Type
Tray 1	☐ Empty	100 Sheets	ANY SIZE	ANY TYPE
Tray 2	☒ OK	250 Sheets	LETTER	PLAIN
STANDARD TOP BIN	☒ OK	N/A	N/A	

[Change Settings](#)

Capabilities

Printer Serial Number: [REDACTED]
Firmware Datecode: [REDACTED]
Duplex: OFF
CARD SLOT Storage: 2 MB Capacity
RAM DISK Storage: 160 MB Capacity
DIMM Slot 1: Empty
Card Slot 1: SanDisk SDCFJ-64: 2 MB

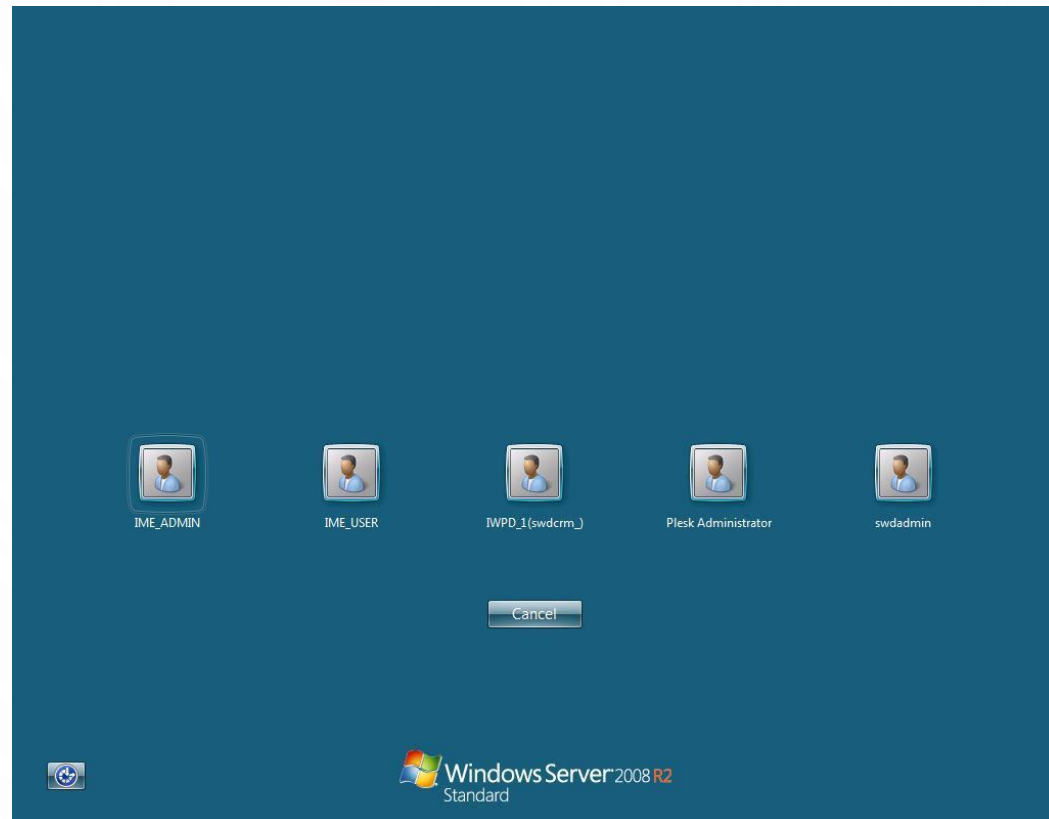
SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance
for information leakage (0TG-INF0-001)

SHODAN



SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance for information leakage (0TG-INF0-001)

SHODAN

Tjuntjuntjara SWRO & Sterilisation Plant

Tuesday, June 12, 2018

1:36:12 AM



RO Plant Mode:	All Sequences in Auto	RO Process Modes	SHS Process Modes	Trends List	Menu
SHS Plant Mode:	All Sequences in Auto				
RO Recovery:	0.00 %	RO Rejection:	0.00 %		
Permeate Flow - Current Day Total:	0.00 kL	Post-Treatment Selection			
Donga Water Flow - Previous Day Total:	0.00 kL	Calcite			
Media Filter Status:	In Filtration	Power Station Controller Status:	Stopped		
Media Filter Runtime Since Last Backwash:	0.92 hr	Donga Water Supply:	Fill Feed Tank		
Desalination Runtime:	5023 hr				
Potable Recirculation Runtime:	11197 hr				
AIT-301 - POTABLE WATER CHLORINE	0.09 mg/l	AIT-302 - POTABLE WATER pH	7.90 pH		...
Alarm Reset	SWRO Status: All Sequences in Auto SHS Status: All Sequences in Auto	Login =	DEFAULT	Login	
	LS201 CIP TANK LOW LEVEL WARNING				
	AIT204 DONGA WATER pH TX. FAULT				

SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance
for information leakage (0TG-INF0-001)

SHODAN



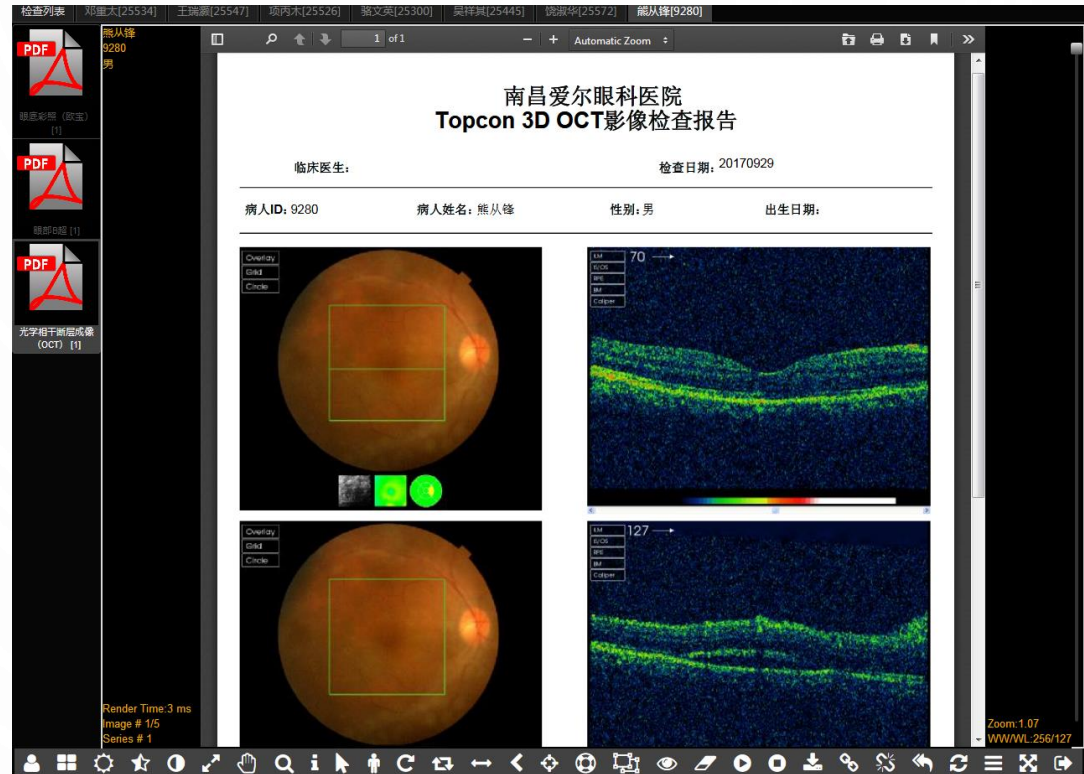
SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance for information leakage (0TG-INF0-001)

SHODAN



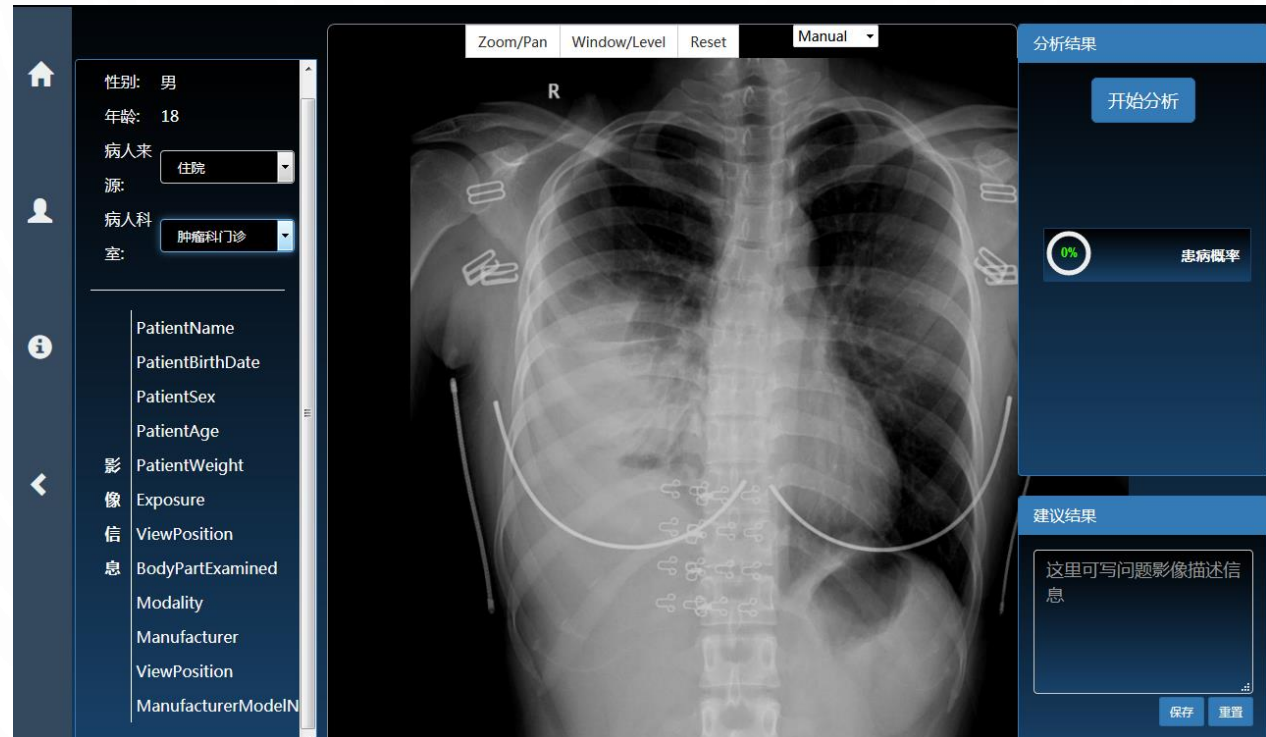
SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance for information leakage (0TG-INF0-001)

SHODAN

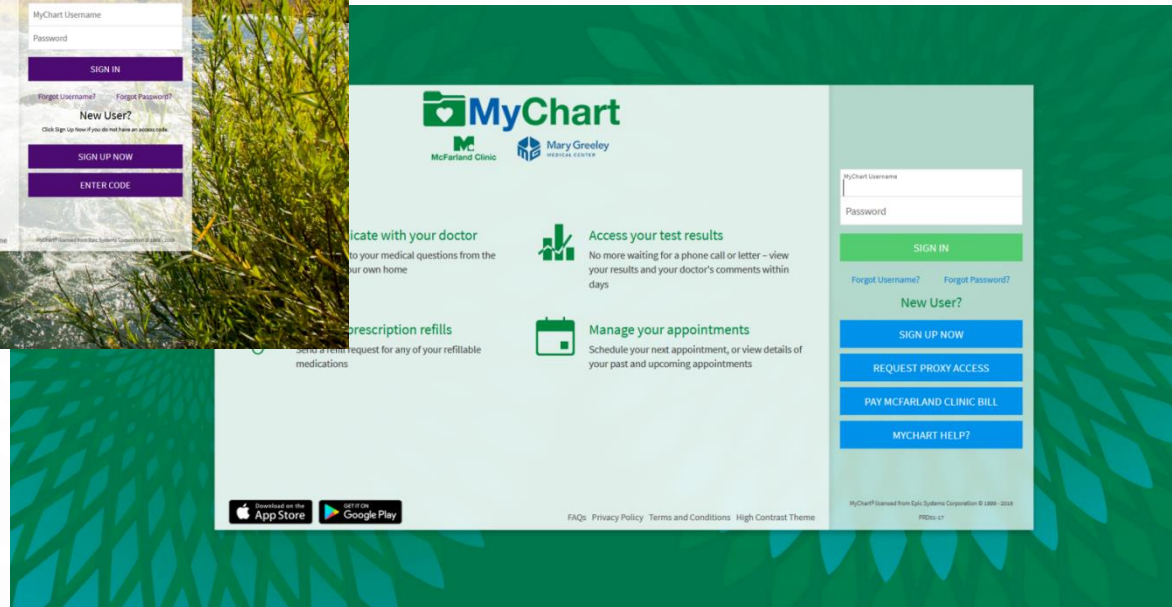
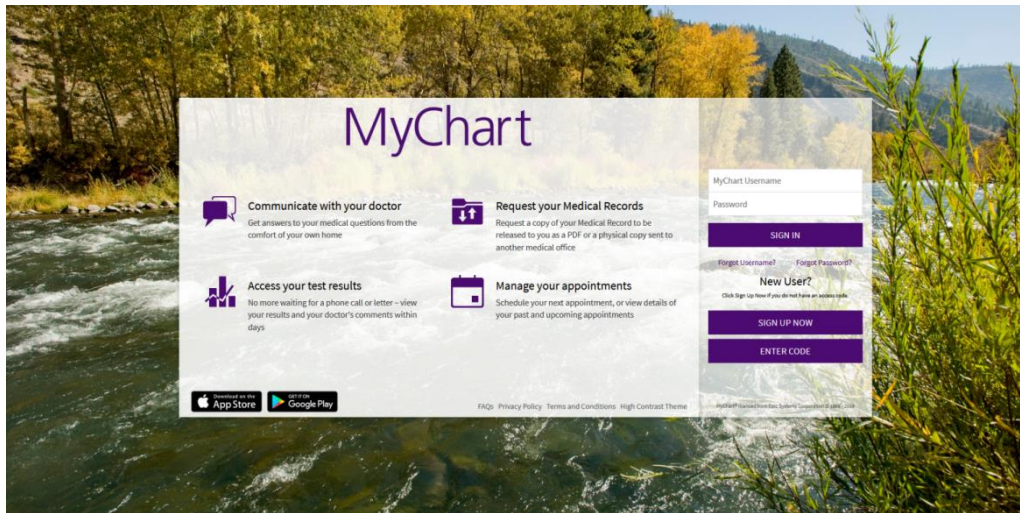


SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Conduct search engine discovery/reconnaissance for information leakage (0TG-INF0-001)



SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

Fingerprint Web Server (OTG-INF0-002)

Obtener las Huellas de un Servidor Web es una tarea fundamental para un test de penetración. Conocer la versión y el tipo de un servidor web en ejecución permite analistas determinar vulnerabilidades conocidas y las técnicas apropiadas para usar durante la prueba.

```
$ nc 202.41.76.251 80
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Mon, 16 Jun 2003 02:53:29 GMT
Server: Apache/1.3.3 (Unix) (Red Hat)
Last-Modified: Wed, 07 Oct 1998
11:18:14 GMT
ETag: "1813-49b-361b4df6"
Accept-Ranges: bytes
Content-Length: 1179
Connection: close
Content-Type: text/html
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Expires: Yours, 17 Jun 2003
01:41: 33 GMT
Date: Mon, 16 Jun 2003 01:41:
33 GMT
Content-Type: text/HTML
Accept-Ranges: bytes
Last-Modified: Wed, 28 May 2003
15:32: 21 GMT
ETag: b0aac0542e25c31: 89d
Content-Length: 7369
```

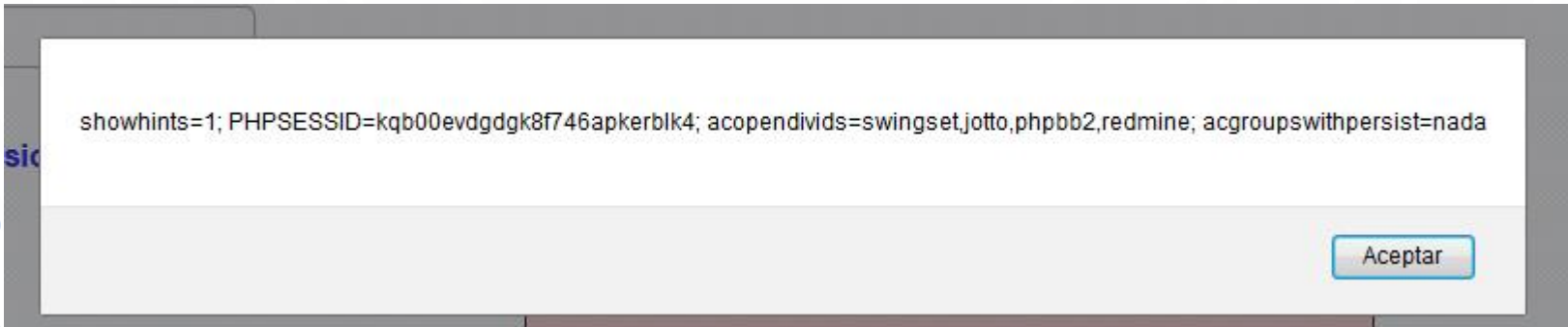
```
HTTP/1.1 200 OK
Server: Sun-ONE-Web-Server/6.1
Date: Tue, 16 Jan 2007 14:53:45
GMT
Content-length: 1186
Content-type: text/html
Date: Tue, 16 Jan 2007 14:50:31
GMT
Last-Modified: Wed, 10 Jan 2007
09:58:26 GMT
Accept-Ranges: bytes
Connection: close
```

SEGURIDAD WEB

Guía de Testing - Pruebas

TEST XSS REFLEJADO (OTG-INPVAL-001)

Cross Site Scripting una de las vulnerabilidades clásicas de las aplicaciones web. Son inyecciones de código malicioso, evitando las medidas de control. Existe diferentes tipos de inyecciones XSS, en este caso concreto, no quedan almacenadas las modificaciones, tan sólo se reflejan en el navegador durante la sesión.



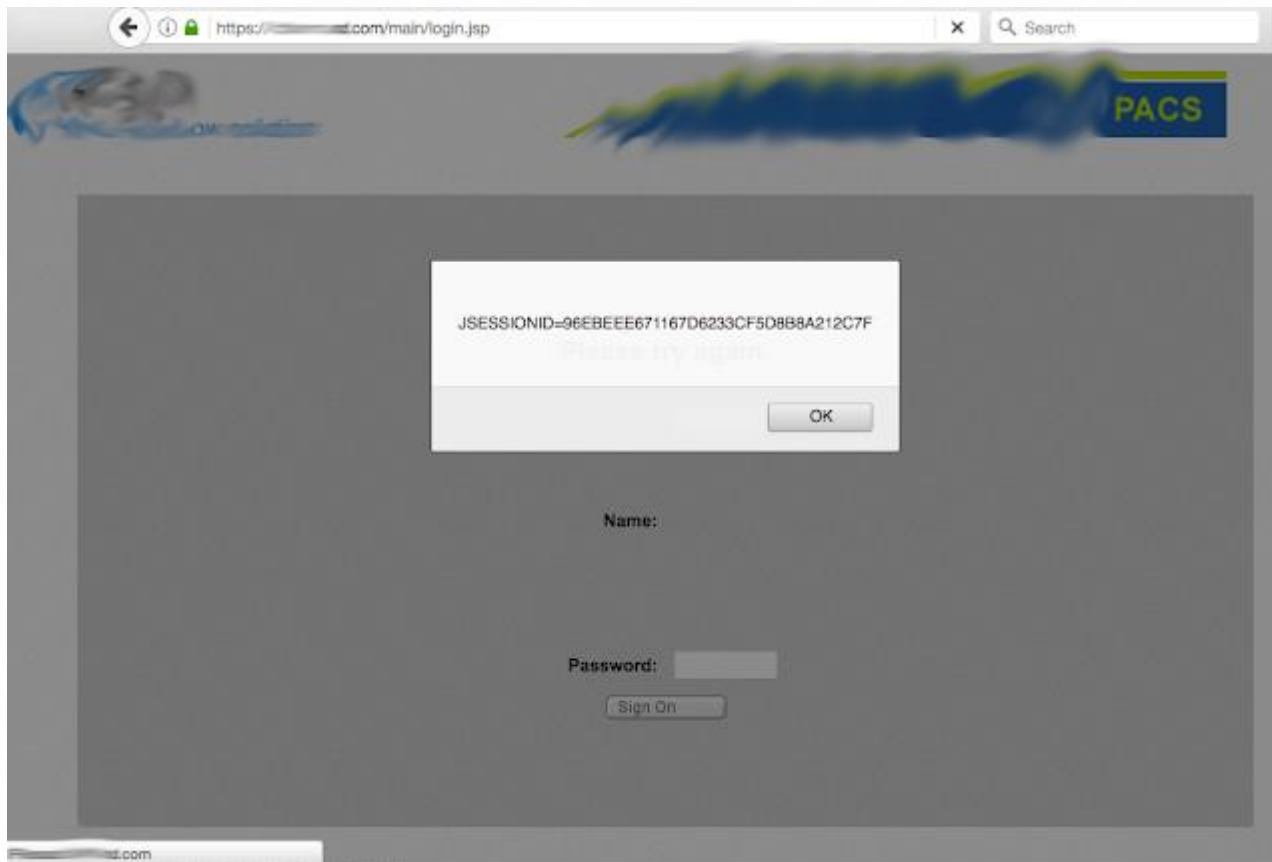
showhints=1; PHPSESSID=kqb00evdgdgk8f746apkerblk4; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada

Aceptar

SEGURIDAD WEB

Guía de Testing - Pruebas

TEST XSS REFLEJADO (OTG-INPVAL-001)



Eleven Paths

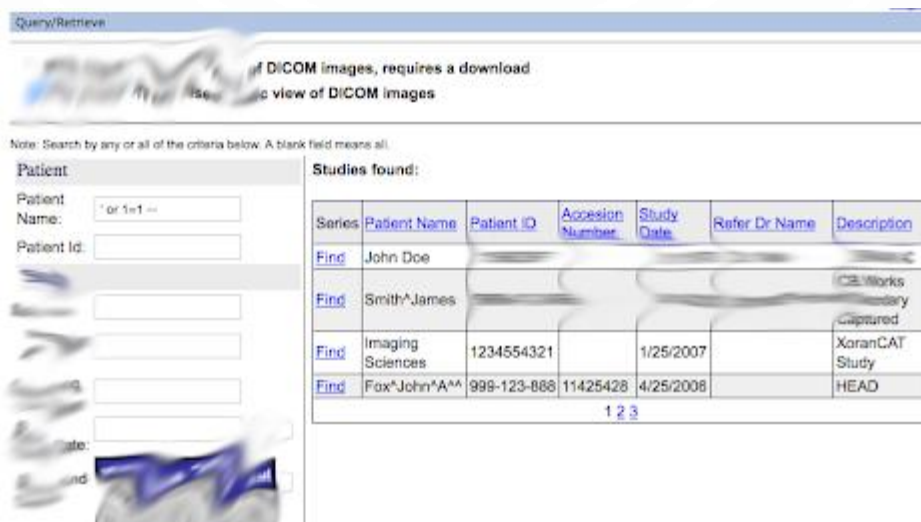
SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

SEGURIDAD WEB

Guía de Testing - Pruebas

TEST SQLi (OTG-INPVAL-005)

Otra de las vulnerabilidades más conocidas en las aplicaciones web. Se trata de una modificación de las consultas SQL de la aplicación web, para extraer, modificar o eliminar algunos datos. Hablamos de inyección ya que se trata de insertar código malicioso dentro de una consulta ya existente. Por ejemplo, introduciendo el código ' or 1=1 – obtendríamos un SELECT abierto para la consulta SQL, ya que la condición 1=1 se cumple siempre.



The screenshot shows a web application interface with a search bar and a table of results. The search bar has fields for Patient Name, Patient ID, and Date. The table has columns for Series, Patient Name, Patient ID, Accession Number, Study Date, Refer Dr Name, and Description. The table contains three rows of data.

Series	Patient Name	Patient ID	Accession Number	Study Date	Refer Dr Name	Description
Find	John Doe					
Find	Smith^James					CE Works Secondary Captured
Find	Imaging Sciences	1234554321		1/25/2007		XoranCAT Study
Find	Fox^John^A^^	999-123-888	11425428	4/25/2008		HEAD

Eleven Paths

SEGURIDAD WEB

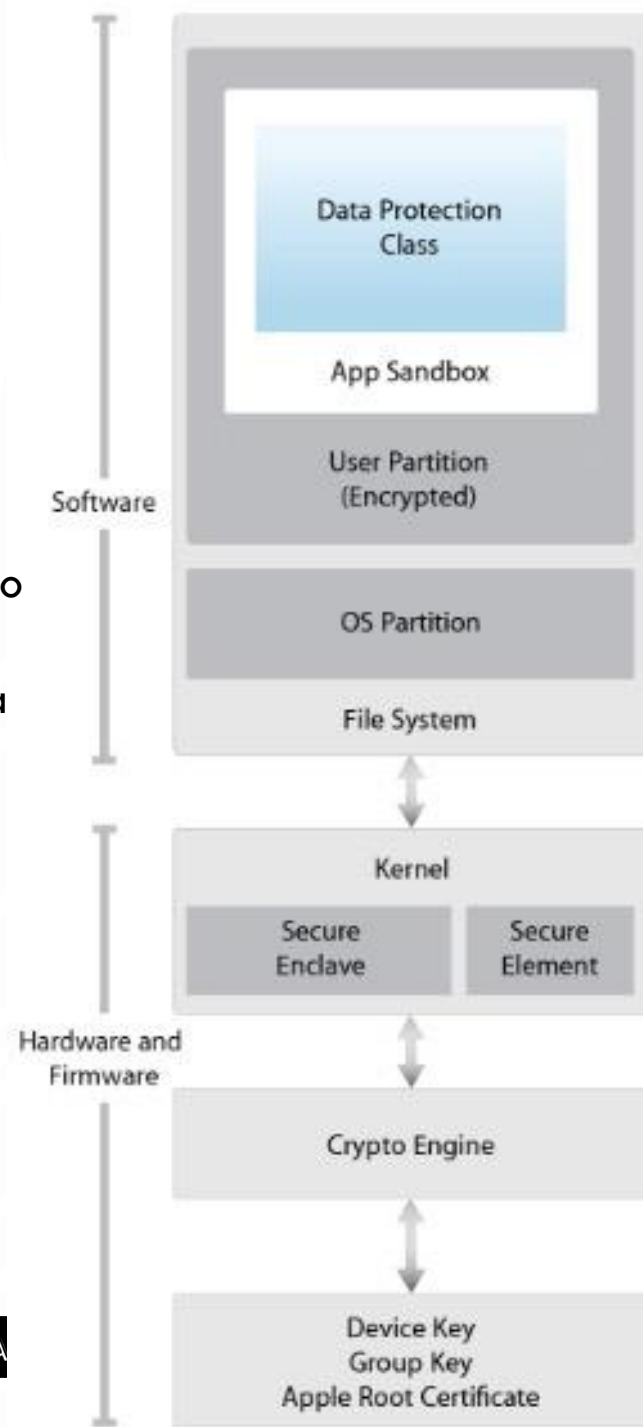
Guía de Testing - Pruebas

TEST SQLi (0TG-INPVAL-005)

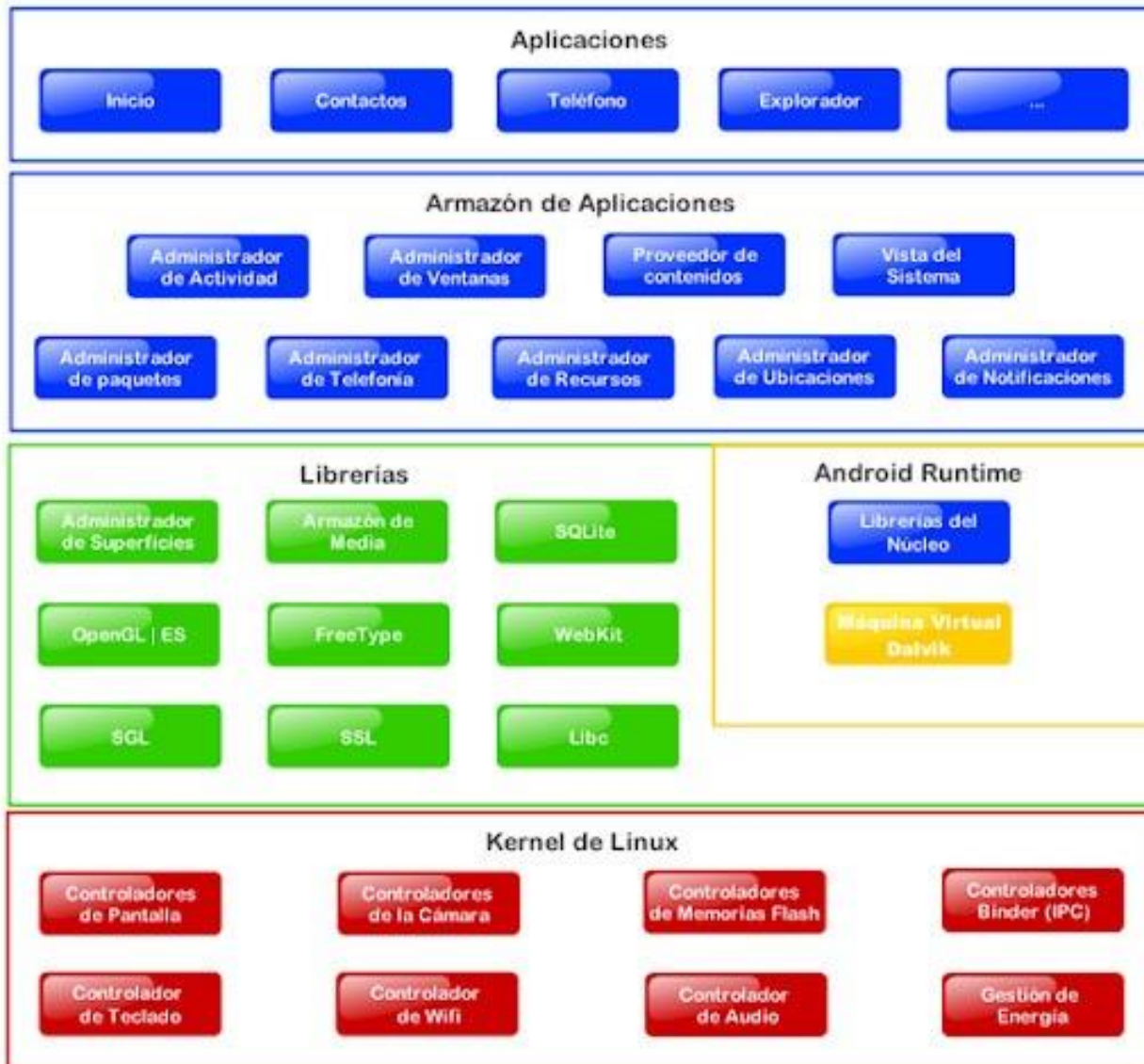
```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: username [REDACTED] UNION ALL SELECT NULL,CONCAT(0x717a7a7071,0x546c6f746c71645648467277494a494a661494f516e454366796f685452454f626e4f4c
),NULL,NULL,NULL,NULL,NULL-- [REDACTED] er-info-php-submit-button=View Account Details
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: password, type: Single quoted string
[q] Quit
> 0
[11:07:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL >= 5.0
[11:07:52] [INFO] fetching tables for database: [REDACTED]
[11:07:53] [WARNING] reflective value(s) found and filtering out
Database: [REDACTED]
[12 tables]
+-----+
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
| [REDACTED] |
+-----+
[11:07:53] [INFO] fetched data logged to text files under '/root/.sqlmap/[REDACTED]'
[*] shutting down at 11:07:53
root@kali:~# 3~
```

SEGURIDAD EN IOS

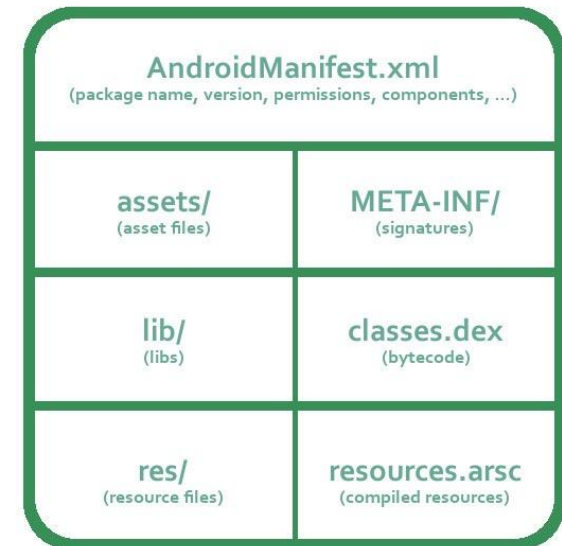
- Diferencia entre Software y Hardware/Firmware
- Sandbox
- Partición de usuario cifrada
- Firma para actualizaciones
- Sistema de arranque seguro donde se llevan a cabo diferentes procesos en distintas fases, donde se comprueba continuamente la integridad del sistema durante el encendido del dispositivo y carga del sistema operativo
- Firma de aplicaciones mediante clave asimétrica para su publicación
- Jailbreak



SEGURIDAD EN ANDROID I



APK



OS?

SEGURIDAD EN ANDROID II

- Los procesos en Android proporcionan un entorno seguro de ejecución
- Ninguna aplicación tiene autorización para ejecutar otras aplicaciones o las del propio sistema
- Las restricciones se saltan mediante **aprobación explícita** del usuario
- Modelo:
 - Ejecución en Sandbox
 - Permisos
 - Firma

“El eslabón más débil en la cadena sigue siendo el usuario final”.
Kevin Mitnick

OWASP MOBILE – TOP 10

Tanto como para desarrollador como para el auditor

- M1 – Uso inapropiado de la plataforma: permisos, touch ID, claves
- M2 – Almacenamiento inseguro de datos
- M3 – Comunicaciones inseguras
- M4 – Autenticación insegura
- M5 – Criptografía insuficiente: SSL/TLS usadas, Rot13, MD4,..., “tu mismo”
- M6 – Autorización insuficiente
- M7 – Calidad del código cliente: buffer overflow
- M8 – Manipulación de código
- M9 – Ingeniería inversa: ofuscación, accesos root, certificados
- M10 – Funcionalidad extraña: comentarios, contraseñas visibles,...

OWASP Y ENISA – TOP 10 CONTROLES

- C1: Identificar y proteger la información sensible de la aplicación
- C2: Proteger las credenciales de autenticación
- C3: Proteger los datos en tránsito
- C4: Correcta autenticación, autorización y gestión de sesiones
- C5: Asegurar servicios y servidores
- C6: Asegurar integración de terceros
- C7: Consentimiento para recolectar y usar datos del usuario
- C8: Proteger los servicios de pago electrónico
- C9: Mantener sistema y aplicación actualizada
- C10: Proteger la aplicación en tiempo de ejecución

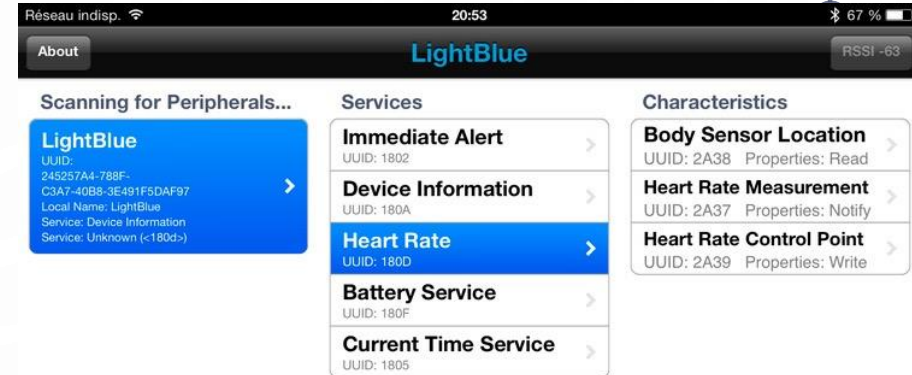
SEGURIDAD EN BLE - RECOMENDACIONES

El 80% de los dispositivos BLE no implementan encriptación en la capa de enlace y las aplicaciones móviles delegan el emparejamiento a nivel de sistema operativo.

- Recomendaciones:
 - Activar cifrado de comunicaciones
 - No aceptar conexiones de dispositivos desconocidos (listas blancas en master o slave) y emparejamiento con clave de 5 caracteres
 - Revisar lista de dispositivos de confianza
 - Asignar un nombre que no refleje información extra (marca, modelo, ubicación, servicio...)
 - Configuración en modo invisible

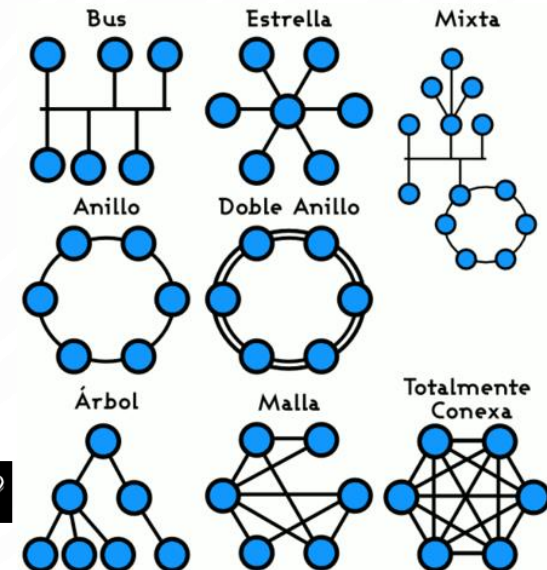
SEGURIDAD EN BLE - DEBUG

USB Dongle, Wireshark, Apps iOS
/ Android



SEGURIDAD EN ZIGBEE

- Opera por encima de la capa física y de enlace del modelo OSI
- Bajo consumo
- Topología de red en forma de malla/estrella/árbol (robustez comunicaciones y adecuado para entornos industriales) hasta 65535 nodos frente a las 8 de Bluetooth
- En auge en salud, transporte y Smart Cities
- Baja velocidad de transmisión comparado con BLE (250 kbps frente a 1 Mbps)
- Seguridad para las capas MAC, NWK y APS
- La seguridad de aplicaciones se genera en otro nivel superior
- Centro de Confianza (Trust Center): decide quien puede conectarse a la red y renueva la clave de red
- **Debilidades:** si existe acceso físico se pueden obtener las claves al guardarse en memoria



ANÁLISIS DE FIRMWARE

- El firmware es el software que está más integrado con el hardware del dispositivo
- Nos podemos encontrar:
 - Programas de arranque del dispositivo (Boot Loader)
 - Kernel (Núcleo del firmware)
 - Sistema de ficheros
 - Conjunto de programas que ejecuta el dispositivo
- Debemos realizar técnicas para:
 - Buscar contraseñas integradas en el código o almacenadas de forma insegura
 - Buscar certificados o claves de API (Interfaz de Programación de Aplicaciones) para conectar con aplicación del fabricante.
 - Buscar vulnerabilidades en el código de las aplicaciones web.
 - Buscar vulnerabilidades en los binarios presentes en el sistema de ficheros
 - Modificar el firmware, integrando una puerta trasera, para crear un firmware malicioso

ANÁLISIS DE FIRMWARE

- Acceso al firmware: web o ftp del fabricante, volcado a la memoria del dispositivo, interceptando el tráfico mediante una actualización.
- Sistema de ficheros: squashfs, cramf, JFFS2, YAFFS2, ext2
- Extracción: herramienta Binwalk

```
$ binwalk firmware.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	TRX firmware header, little endian
28	0x1C	LZMA compressed data, properties: 0x5D, dictionary size: 878029 bytes, Data Address: 0x80000000, Entry Point: 0x802B5000, data CRC: 0x00000000
2319004	0x23629C	Squashfs filesystem, little endian, non-standard inodes, blocksize: 65536 bytes, created: 2010-11-23 11:58:47

```
Hack&Beers #
Hack&Beers # binwalk -e Dlink_firmware.bin

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
48            0x30           Unix path: /dev/mtdblock/2
96            0x60           uImage header, header size: 64 bytes, header CRC: 0x00000000,
size: 878029 bytes, Data Address: 0x80000000, Entry Point: 0x802B5000, data CRC: 0x00000000
Kernel Image, compression type: lzma, image name: "Linux Kernel Image"
160           0xA0           LZMA compressed data, properties: 0x5D, dictionary
bytes
917600        0xE0060        PackImg section delimiter tag, little endian size: 0x00000000
917632        0xE0080        Squashfs filesystem, little endian, non-standard inodes, blocksize: 65536 bytes, created: 2010-11-23 11:58:47

Hack&Beers # ls -l
total 5312
-rw-rw-r-- 1 oit oit 2256896 Jan 25 10:39 dlink_filesystem
-rw-r--r-- 1 oit oit 3174528 Jan 25 10:04 Dlink_firmware.bin
drwxrwxr-x 3 oit oit 4096 Jan 25 10:46 _Dlink_firmware.bin.extracted
Hack&Beers #
```

Squashfs extraído aquí

ANÁLISIS DE FIRMWARE

- La arquitectura que habitualmente utilizan los dispositivos embebidos e IoT es diferente, por ejemplo, ARM o MIPS.
- QEMU

```
/home/oit/lab/pocs/_Dlink_firmware.bin.extracted/squashfs-root/bin [oit@ubuntu] [6:16]
> ls busybox
busybox

/home/oit/lab/pocs/_Dlink_firmware.bin.extracted/squashfs-root/bin [oit@ubuntu] [6:16]
> rabin2 -I busybox
file      /home/oit/lab/pocs/_Dlink_firmware.bin.extracted/squashfs-root/bin/busybox
type      EXEC (Executable file)
pic        false
has_va     true
root       elf
class      ELF32
lang        c
arch       mips
bits       32
machine     MIPS R3000 big-endian
os          linux
subsys      linux
endian      little
strip       true
static      true
linenum     false
lsyms       false
relocs      false
rpath       NONE
```

SEGURIDAD IOT EN SANIDAD

¿ESTAMOS PREPARADOS?



<https://bit.ly/2JLSjxe>



SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

