

# OWASP

---

---

INTERNET OF THINGS

---

---

10  
TOP

**HACK**  
**& BEERS**

#HBsevilla

@OWASP\_Sevilla





@juanjodomech



@ramon\_salado

#HBsevilla

@OWASP\_Sevilla



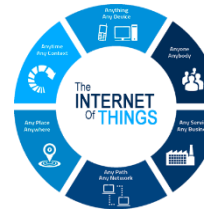
# OWASP

- Open Web Application Security Project
  - Sin fines de lucro, organización de voluntarios
    - Todos los miembros son voluntarios
    - Todo el trabajo es donado por los patrocinadores
  - Proporcionar recursos gratuitos para la comunidad
    - Publicaciones, artículos, normas
    - Software de Testeo y Capacitación
    - Capítulos locales & Listas de correo
  - Soportada a través de patrocinios
    - Apoyo financiero a través de empresas o patrocinadores
    - Patrocinios personales de los miembros

# OWASP

- Open Web Application Security Project
  - Promueve el desarrollo de software seguro
  - Orientada a la prestación de servicios orientados a la Web y Mobile
  - Se centra principalmente en el "back-end" más que en cuestiones de diseño
  - Un foro abierto para el debate
  - Un recurso gratuito para cualquier equipo de desarrollo de software

# OWASP, proyectos



#HBsevilla

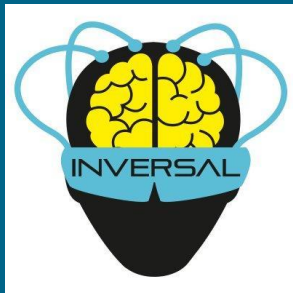
@OWASP\_Sevilla



# OWASP Sevilla



- 1 año, 8 eventos, 24 asistentes de media {8-68}
- Proyectos
  - Traducción Guía de Testing de OWASP
  - Bolsa de Trabajo
  - Punto de encuentro Universidades/IES y Centros de Trabajo
  - Incubadora
  - HackerSpace
  - Participación en Comunidades de Desarrollo de Sevilla



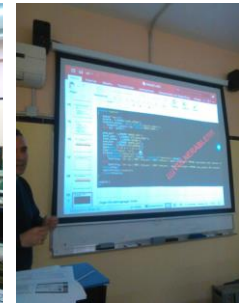
#HBsevilla

@OWASP\_Sevilla





# OWASP Sevilla



#HBsevilla

@OWASP\_Sevilla



# OWASP Sevilla



@OWASP\_Sevilla



Grupo OWASP Sevilla



Wiki OWASP Sevilla:

<https://www.owasp.org/index.php/Sevilla>

Canal OWASP Sevilla:

<https://inversal.slack.com>





# ¿Qué es IOT?

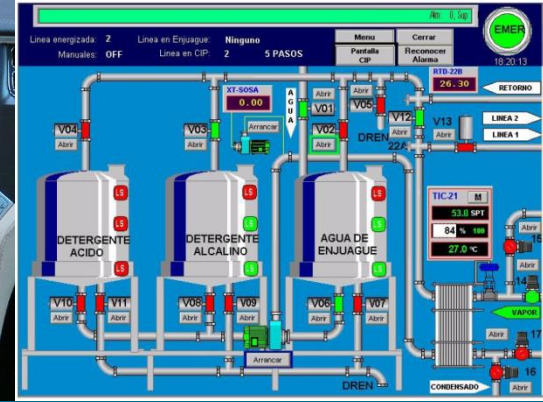


#HBsevilla

@OWASP\_Sevilla



# ¿Qué es IOT?



#HBsevilla

@OWASP\_Sevilla

# Problema actual de la Seguridad en IOT

## REDES

- Servicios, Encriptación, Firewall, ...

# Problema actual de la Seguridad en IOT

## REDES

- Servicios, Encriptación, Firewall, ...

## APLICACIONES

- authN, authZ, validación inputs, ...

# Problema actual de la Seguridad en IOT

## REDES

- Servicios, Encriptación, Firewall, ...

## APLICACIONES

- authN, authZ, validación inputs, ...

## MÓVIL

- APIs inseguras, capa cifrado, ...

# Problema actual de la Seguridad en IOT

## REDES

- Servicios, Encriptación, Firewall, ...

## APLICACIONES

- authN, authZ, validación inputs, ...

## MÓVIL

- APIs inseguras, capa cifrado, ...

## CLOUD

- AuthSessionAccess, ...

# Problema actual de la Seguridad en IOT

## REDES

- Servicios, Encriptación, Firewall, ...

## APLICACIONES

- authN, authZ, validación inputs, ...

## MÓVIL

- APIs inseguras, capa cifrado, ...

## CLOUD

- AuthSessionAccess, ...

## IOT

- Red + App + Móvil + Cloud



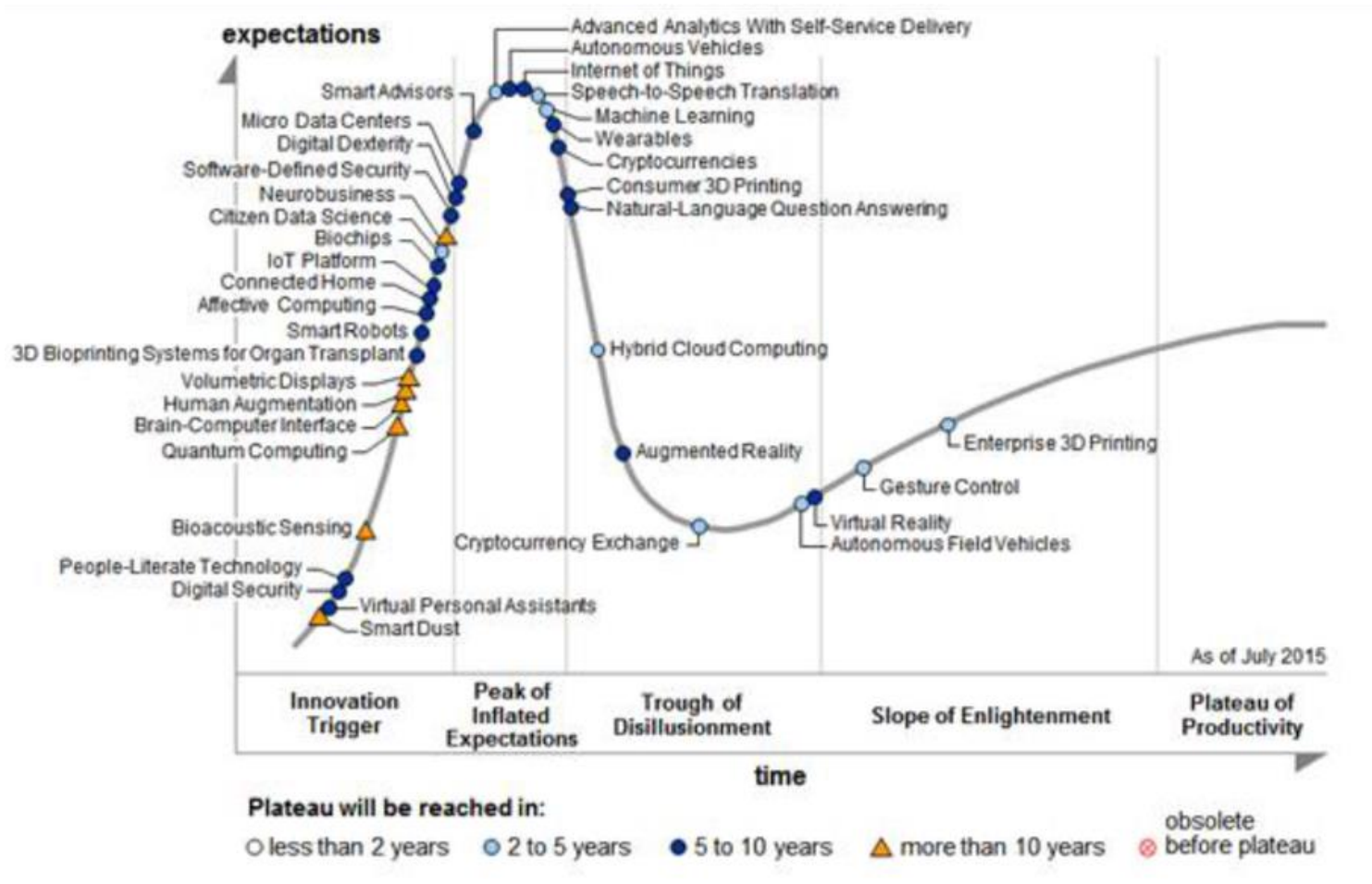
## Evolución IOT

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](http://gartner.com/newsroom/id/2905717)

# Evolución IOT



# ¿Cómo son de seguros los sistemas 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**

4AA5-7342ENW, March 2015

# TOP10

#HBsevilla

@OWASP\_Sevilla



# Internet of Things Top Ten Project

- 1 INTERFAZ Web INSEGURA
- 2 AUTENTIC. / AUTORIZAC. INSUFICIENTE
- 3 SERVICIOS DE RED INSEGUROS
- 4 CIFRADO DE TRANSPORTE / VERIFIC. DE INTEGRIDAD
- 5 PRIVACIDAD
- 6 INTERFAZ CLOUD INSEGURA
- 7 INTERFAZ MOVIL INSEGURO
- 8 CONFIGURACION DE SEGURIDAD INSUFICIENTE
- 9 SOFTWARE / FIRMWARE INSEGURO
- 10 POBRE SEGURIDAD FISICA

1

## Interfaz Móvil Inseguro

covers IoT device administrative interfaces

### Obstáculos



Nombres de usuario  
contraseñas por defecto



Bloqueo de cuentas  
desactivado

Vulnerabilidades  
XSS, CSRF, SQLi

### Soluciones



Permitir el cambio de nombres de  
usuario y contraseña



Permitir el bloqueo de cuentas



Realizar auditorías a la  
interfaz web





## Autorización/Autenticación Insuficientes

covers all device interfaces and services

2



### Obstáculos

Contraseñas débiles



Sistemas de recuperación de contraseñas inseguros



No se dispone de autenticación de doble factor



### Soluciones

Obligar el uso de contraseñas fuertes y complejas



Verificar la seguridad del sistema de recuperación



Implementar la autenticación de doble factor siempre que se pueda



3

## Servicios de red inseguros

covers all network services including device, cloud, web and mobile



### Obstáculos

### Soluciones



Puertos abiertos es innecesarios

Dejar sólo los puertos necesarios abiertos



Puertos visibles en internet vía UPnP

No utilizar UPnP



Vulnerabilidad de los servicios de red para la denegación de servicios

Revisar los servicios de red en búsqueda de vulnerabilidades



## Obstáculos

Información sensible enviada en claro

No tener activado o configurado correctamente SSL/TLS

Uso de protocolos de encriptación privados/proprios

---

## Soluciones

Encriptar la comunicación entre los diferentes sistemas

Mantenimiento de las implementaciones SSL/TLS

No usar soluciones de encriptación privados/proprios

**Ausencia de encriptación**  
covers all network services including  
device, cloud, web and mobile

4



5

## Preocuparse por la privacidad covers all components of IoT solution



### Obstáculos

- ➔ Almacenamiento de mucha información personal
- ➔ La información almacenada no se protege correctamente
- ➔ No se ofrece elegir al usuario final recoger información

### Soluciones

- ➔ Minimizar el almacenamiento de datos
- ➔ Tratar los datos de forma anónima
- ➔ Ofrecer a los usuarios la opción de decidir que datos almacenar



## Interfaz Cloud Inseguro

covers cloud APIs or cloud-based web interfaces

6

### Obstáculos

Interfaces vulnerables  
XSS, SQLi, CSRF, ...

Contraseñas  
Básicas

Ausencia Doble  
Factor Autentic.

### Soluciones



Asegurar Interfaz y  
sus conexiones por API



Reforzar Control  
sobre el Usuario



Reforzar Autenticación  
en el sistema

7

## Interfaz Móvil Inseguro

covers mobile application interfaces



### Obstáculos



Permite Contras.  
Básicas



Ausencia Doble  
Factor Autentic.



No banea  
usuarios



Mecanismos de  
bloqueo de usuarios



Reforzar Sistemas  
Autenticación



Cambiar usuarios  
default

### Soluciones

## Config. de Seguridad Insuficiente

covers the IoT device

8

### Obstáculos

Pocas opciones avanzadas para Contraseñas

Cifrado no soportado en muchos casos


Sin log ni alertas de seguridad



### Soluciones

 AES 256

 Dotar de opciones para contraseñas seguras

 Incorporar sistemas de log y alarmas de seguridad

9

## Software/Firmware Inseguro covers the IoT Device



### Obstáculos



Actualizaciones de Servidores  
No Seguros



Actualizaciones transmitidas sin  
cifrado



Pocas/Ningunas Actualizaciones

### Soluciones



Actualizaciones Periódicas



Verificar antes de instalar



Actualizar desde Servidores  
Seguros



# Pobre Seguridad Física

covers the IoT device

10

## Obstáculos

Puertos Accesibles  
(USB, SD, RED, ...)

Limitaciones en las tareas  
de Administración

Controlar/Limitar la interacción  
del Usuario



## Soluciones

Reforzar Autenticación  
en el sistema

Control de Administración

Protección “física”

# ZONA DE DEMO



**KEEP  
CALM  
IT IS  
DEMO  
TIME**

#HBsevilla

@OWASP\_Sevilla



## Acerca de nombres de usuarios y contraseñas



Para enlaces con una llave roja (🔑), introduzca el nombre de usuario "admin" (respetando las minúsculas). La contraseña de administración predeterminada es "access".

Para enlaces con una llave verde (🌿), introduzca el nombre de usuario "user" (respetando las minúsculas). La contraseña de usuario predeterminada es "access".

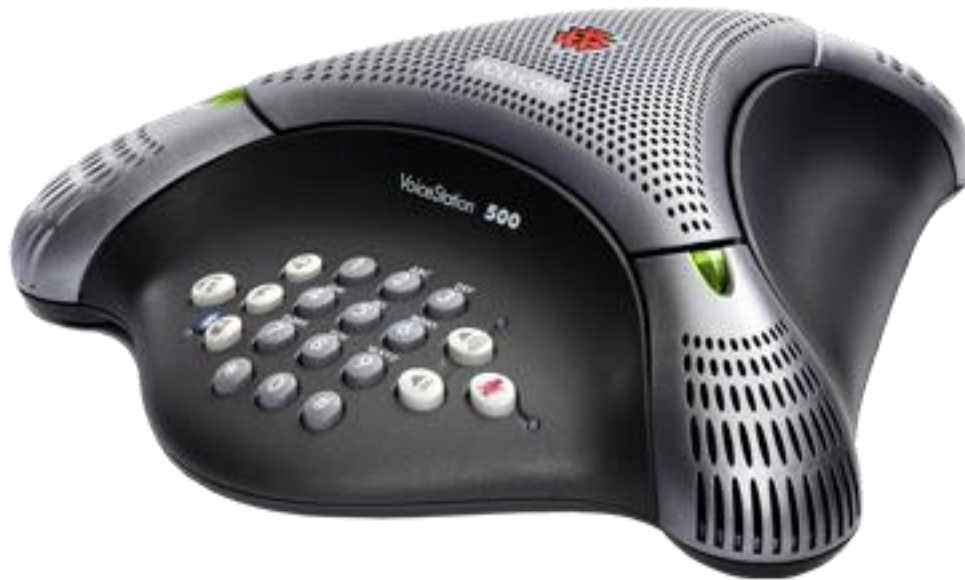
Tenga en cuenta que si utiliza el nombre de usuario "admin", podrá administrar todos los aspectos de este dispositivo; sin embargo, si utiliza el nombre de usuario "user", no podrá entrar en zonas que no pueda administrar.

Si desea cambiar la configuración de las contraseñas predeterminadas, haga clic en el enlace "Parámetros del administrador" en la página principal, introduzca "admin" como nombre de usuario y "admin" como contraseña.

[https://www.shodan.io/search?query=Server%3A+Virata-EmWeb%2FR6\\_2\\_1](https://www.shodan.io/search?query=Server%3A+Virata-EmWeb%2FR6_2_1)

<https://www.shodan.io/search?query=%22Sharp+MX%2>

<https://www.shodan.io/search?query=DATA+ARRIVE+%2FPOWER+SAVE>



<https://www.shodan.io/search?query=Polycom+Command+Shell>

<https://www.shodan.io/search?query=snom+embedded>

#HBsevilla

@OWASP\_Sevilla





## SNMP temperature & humidity sensors

Based on years of Industry Experience it's ready to run right out of the box, simply assign the IP address and connect to the embedded web server. sensorProbe2 has been field-proven with versatile measurement options. **It can be configured to prevent specific kinds of exposure to humidity, water leakage, gas, airflow and low / high temperature, etc.**



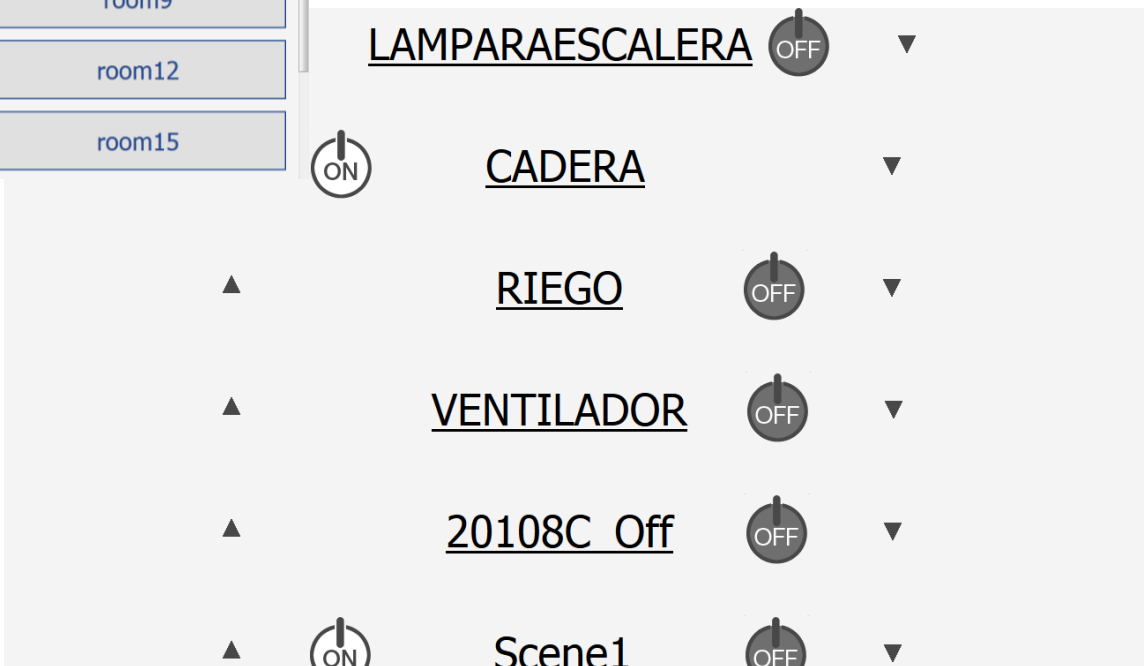
<https://www.shodan.io/search?query=AKCP>





```
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 2);
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x4D\x56", 2);
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);
add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x56", 1);
add_auth_entry("\x51\x47\x50\x54\x48\x41\x47", "\x51\x47\x50\x54\x48\x41\x47", 1);
add_auth_entry("\x51\x57\x52\x47\x50\x54\x48\x51\x4D\x50", "\x51\x57\x52\x47\x50\x54\x48\x51\x4D\x50", 1);
add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1);
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);
add_auth_entry("\x43\x46\x4F\x4B\x4C\x13", "\x52\x43\x51\x51\x55\x4D\x50\x46", 1);
add_auth_entry("\x43\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x13\x10\x11\x16", 1);
add_auth_entry("\x14\x14\x14\x14\x14\x14", "\x14\x14\x14\x14\x14\x14", 1);
add_auth_entry("\x1A\x1A\x1A\x1A\x1A\x1A", "\x1A\x1A\x1A\x1A\x1A\x1A", 1);
add_auth_entry("\x57\x40\x4C\x56", "\x57\x40\x4C\x56", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11\x16", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x78\x56\x47\x17\x10\x13", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x4A\x4B\x11\x17\x13\x1A", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x54\x40\x58\x46", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x4C\x49\x4D", 4);
add_auth_entry("\x50\x4D\x4D\x56", "\x58\x4E\x5A\x5A\x0C", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x54\x4B\x58\x5A\x54", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x51\x58\x51\x56\x47\x4F", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x4B\x49\x55\x40", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x50\x47\x43\x4F\x40\x4D\x5A", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x57\x51\x47\x50", 1);
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x47\x43\x4F\x56\x47\x49", 1);
```

```
// guest 12345
// admin1 password
// administrator 1234
// 666666 666666
// 888888 888888
// ubnt ubnt
// root klv1234
// root Zte521
// root hi3518
// root jvbzd
// root anko
// root zlx.
// root 7ujMko0vizxv
// root 7ujMko0admin
// root system
// root ikwb
// root dreambox
// root user
// root realtek
```



<https://www.shodan.io/search?query=title%3A%22powered+by+insteon%22>

<https://www.shodan.io/search?query=webiopi>

<https://www.shodan.io/search?query=title%3A%22Status+%26amp%3B+Control%22&language=None>

#HBsevilla

@OWASP\_Sevilla







<https://www.shodan.io/search?query=KEE+NETIC+4G+admin%3A1234>

<https://www.shodan.io/search?query=Linksys+WAG120N>



#HBsevilla

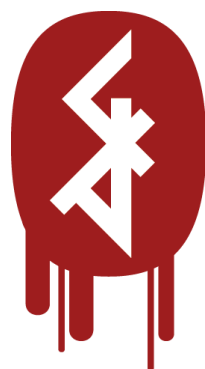
@OWASP\_Sevilla

```
package com.august.util;

+import android.content.SharedPreferences;

public class Settings
{
    private static final String ENC_KEY = "A[REDACTED]";
    private static final LogUtil LOG = LogUtil.getLogger(Settings.class);
    public static final String SIZE_SUFFIX = "*size*";
    public static final String STR_ACCESS_TOKEN = "API_ACCESS_TOKEN";
    public static final String STR_DEBUG_SETTINGS = "DEBUG_SETTINGS";
    public static final String STR_INSTALL_TOKEN = "API_INSTALL_TOKEN";
    public static final String STR_PUSH_ALERTS = "PUSH_ALERTS";
    public static final String VERSION_SUFFIX = "_v1";
    static Settings _instance = null;
    DebugSettings _debugSettings = new DebugSettings();
    Properties _encryptedProps = null;

    public static Settings init()
    {
```



# GATTacker

*OUTSMART THE THINGS*



Action	Service	Characteristic	Data
Connected			
notification	180f	2a19	.G
read	180f	2a19	.G
read	7b122568-6677-7f8c-f8e9-af0eedb36e3a	7b121991-6677-7f8c-f8e9-af0eedb36e3a	01 06
read	7b122568-6677-7f8c-f8e9-af0eedb36e3a	7b121993-6677-7f8c-f8e9-af0eedb36e3a	00 00 00 00
read	7b122568-6677-7f8c-f8e9-af0eedb36e3a	7b121998-6677-7f8c-f8e9-af0eedb36e3a	13
write	1803	2a06	02
write	b0ad1523-99b2-7e1d-fc0d-6d399e1edf02	b0ad1525-99b2-7e1d-fc0d-6d399e1edf02	00

## BtleJuice Framework

#HBsevilla

@OWASP\_Sevilla



Filter: `btl2cap.cid == 0x0004` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1402	45.7488450	Master	Slave	All	42	Rcvd write Command, Handle: 0x0028
1528	47.6707950	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
1530	47.6809380	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
1532	47.7004230	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
1533	47.7188490	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
2887	68.7319810	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
2891	68.7907370	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
3050	71.2209950	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
3056	71.2925470	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
3593	79.6234850	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028
3595	79.6521770	Master	Slave	ATT	42	Rcvd write Command, Handle: 0x0028

Frame 3595: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

- Nordic BLE sniffer meta
- Bluetooth Low Energy Link Layer
- Bluetooth L2CAP Protocol
  - Length: 12
  - CID: Attribute Protocol (0x0004)
- Bluetooth Attribute Protocol
  - Opcode: Write Command (0x52)
  - Handle: 0x0028
  - Value: 58010301ff00ce5f00

#e12d00
#ef0018
#47e756
#0f2373
#ce5f00

```

0000  03 06 23 01 4a c2 06 0a 03 0a 38 d7 06 79 73 00  ..#.J... ..8..ys.
0010  00 95 5c 65 50 0a 10 0c 00 04 00 52 28 00 58 01  ...\eP... ..R(.X.
0020  03 01 ff 00 ce 5f 00 11 5c 02                    ....._.. \.

```





**HACK  
& BEERS**

#HBsevilla

@OWASP\_Sevilla