



SECDEVOPS(DEVSECOPS) CON CONTENEDORES EN LOS DOCKERS

BY ANTONIO JUANILLA(SPECTER)

¿QUIEN SOY?

- Autodidacta
 - Proactivo
 - Amante de la tecnología
 - Defensor de la democratización de la tecnología para la mejora de la sociedad
-
- Twitter: @spectertj
 - Linkedin: <https://www.linkedin.com/in/spectertj>
 - Github: spectertj

Sólo el conocimiento nos hace libres



<https://hackmadrid.org>

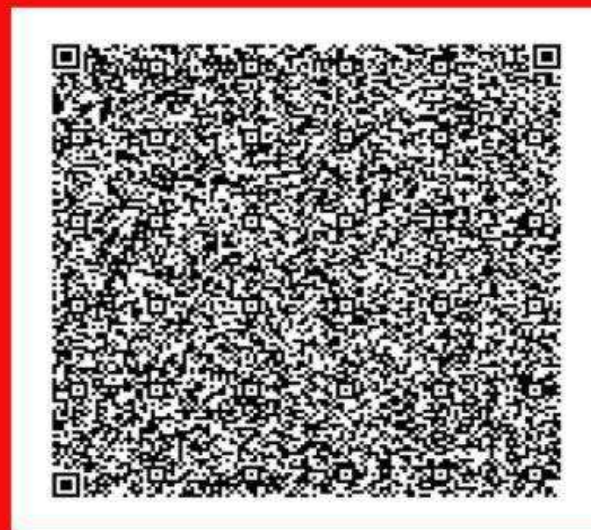
<https://twitter.com/hackmadrid>



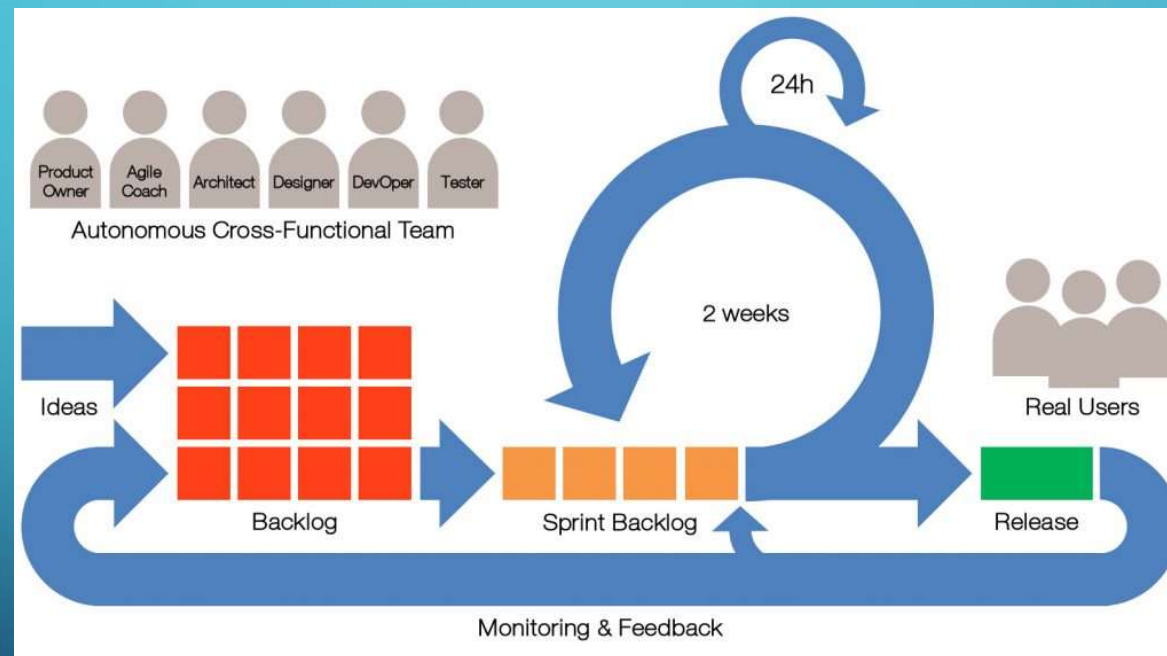
Telegram: t.me/hackmadrid

<https://meetup.com/HackMadrid-27>

<https://linkedin.com/company/hackmadrid>

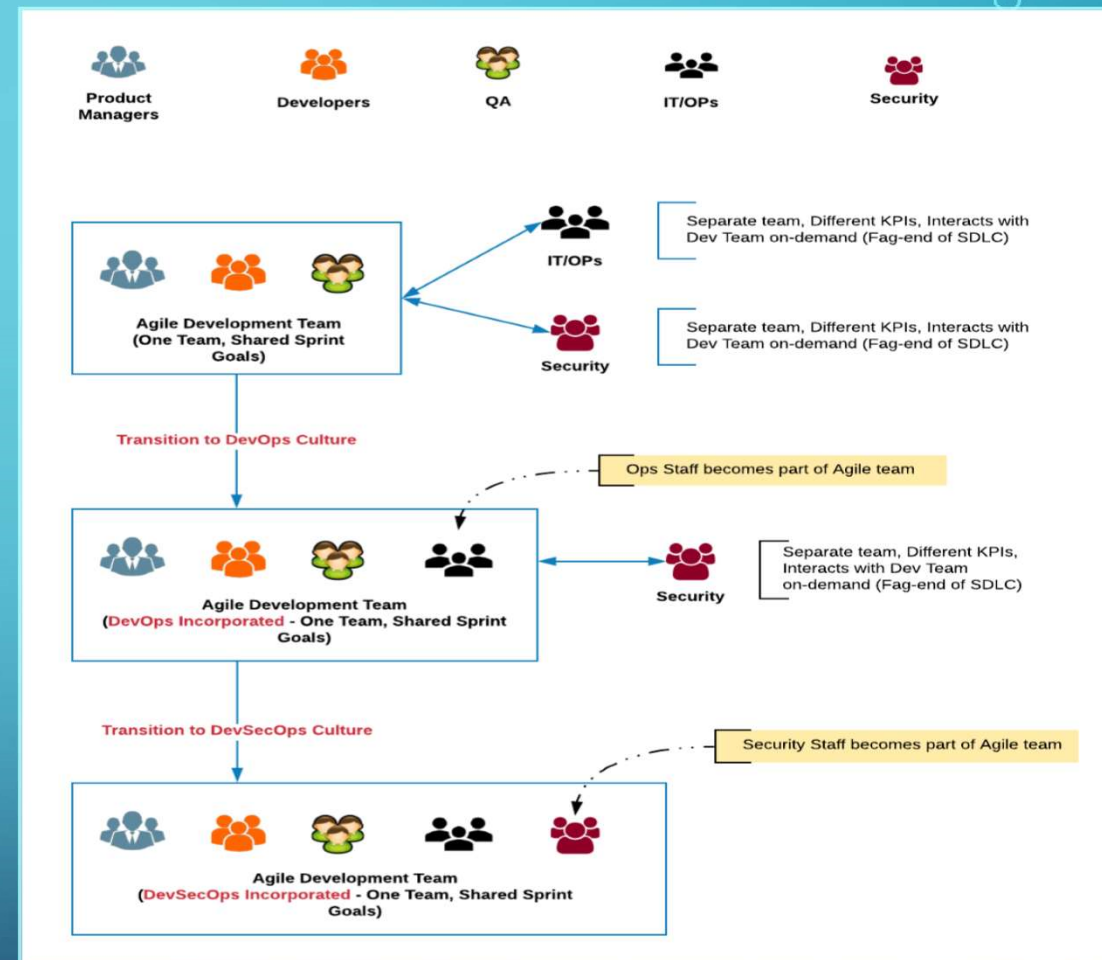


FLUJO DEL AGILISMO



TRANSICIÓN

1. Equipos de desarrollo
2. Equipos DevOps
3. Equipos SecDevOps



SEC – DEV – OPS

SECURITY

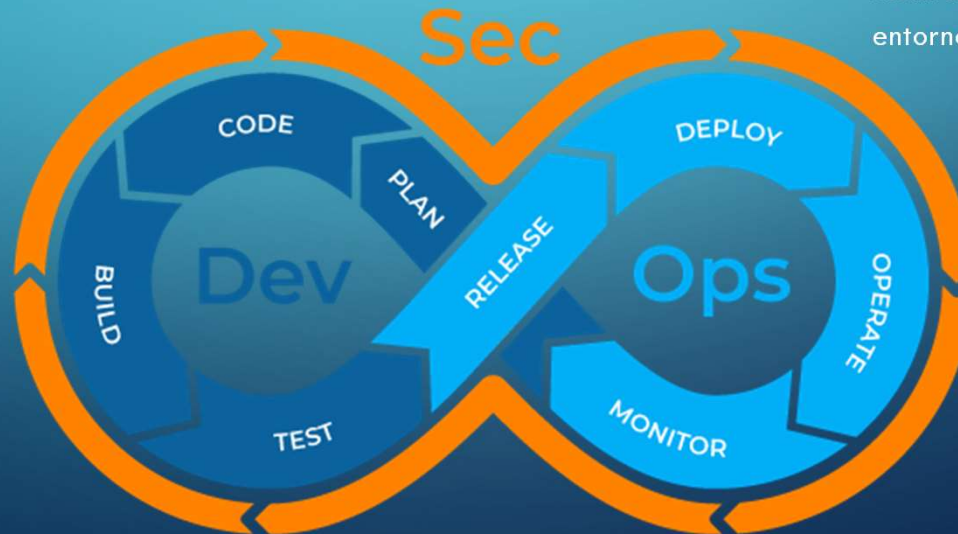
Seguridad en el desarrollo de aplicaciones y en los entornos de desarrollo y despliegue

DEVELOPMENT

Desarrollo de aplicaciones

OPERATIONS

Orquestación del despliegue de aplicaciones, configuración de entornos, monitorización de las aplicaciones y los entornos





DESARROLLO SEGURO

1. VALIDACIONES DE DATOS DE ENTRADA
2. VALIDACIONES DE DATOS DE SALIDA
3. VALIDACIONES DE LLAMADAS A BBDD
4. ESCANEO DE CÓDIGO FUENTE PARA ENCONTRAR VULNERABILIDADES
5. ESCANEO DE CÓDIGO PARA CALIDAD
6. PRUEBAS Y MAS PRUEBAS



TIPOS DE TEST

1. PRUEBAS UNITARIAS
2. PRUEBAS DE INTEGRACIÓN
3. PRUEBAS DE REGRESIÓN



CULTURA DEVOPS Y CONTENERIZACION

CONTAINERIZATION SECURITY: WHAT ARE CONTAINERS & HOW TO SECURE THEM?



CONTAINERIZATION VS. VIRTUALIZATION

CONTAINERS

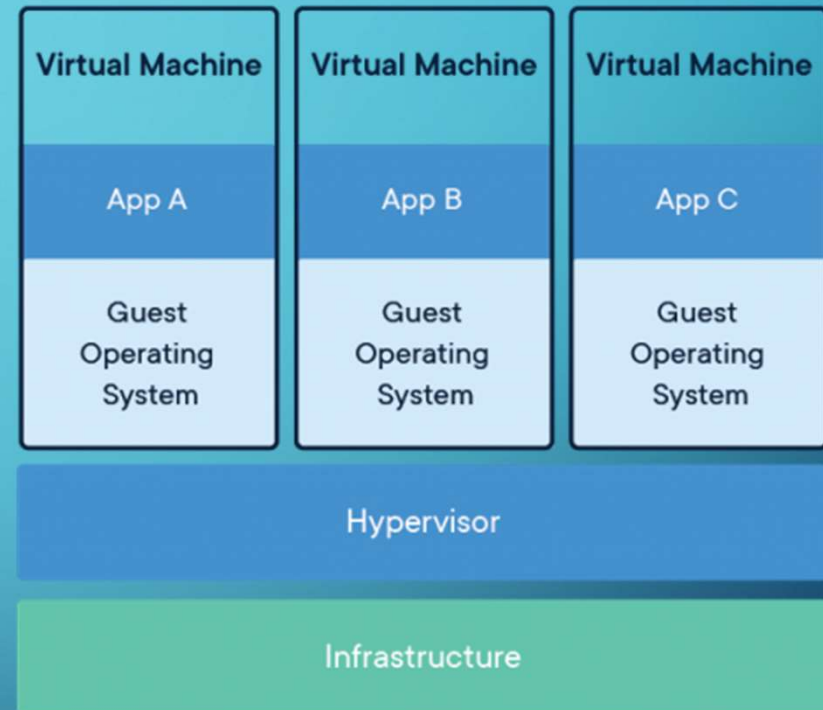
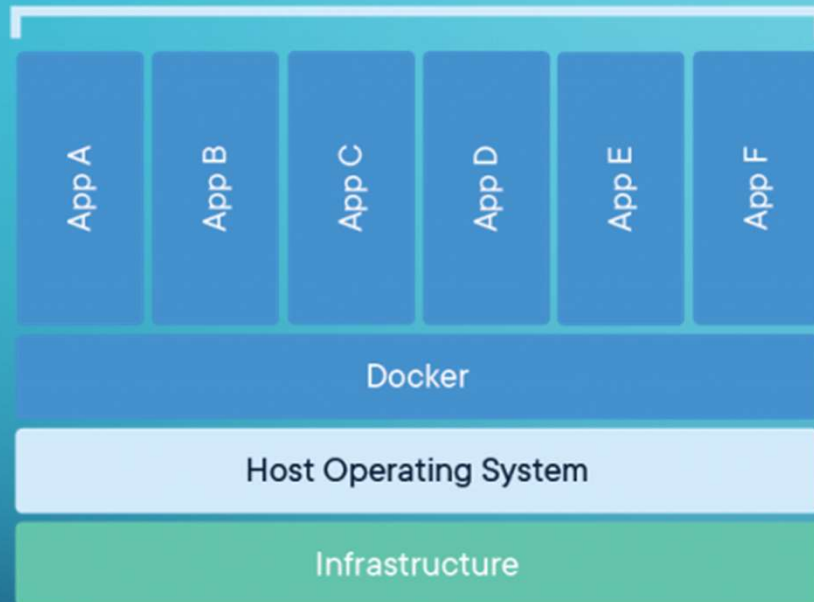
- Dockers
- LxC

VM

- VmWare
- VirtualBox
- HyperV



Containerized Applications



BENEFICIOS DE LOS CONTENEDORES

- Multi plataforma en la nube
- Comparte el mismo OS
- Velocidad
- Costes de eficiencia
- Versionado
- Portabilidad
- Pruebas y **CI-CD**



Build, Ship, Run, Any App Anywhere

From Dev



To Ops



Any App



CONTAINERIZATION ENGINE

Any OS



Anywhere



Physical



Virtual



Cloud



DESVENTAJAS DE LOS CONTENEDORES

- Seguridad
- Falta de aislamiento
- Monitorización



SECURIZANDO DOCKERS

HOW TO SECURE AND MONITOR
CONTAINERS?





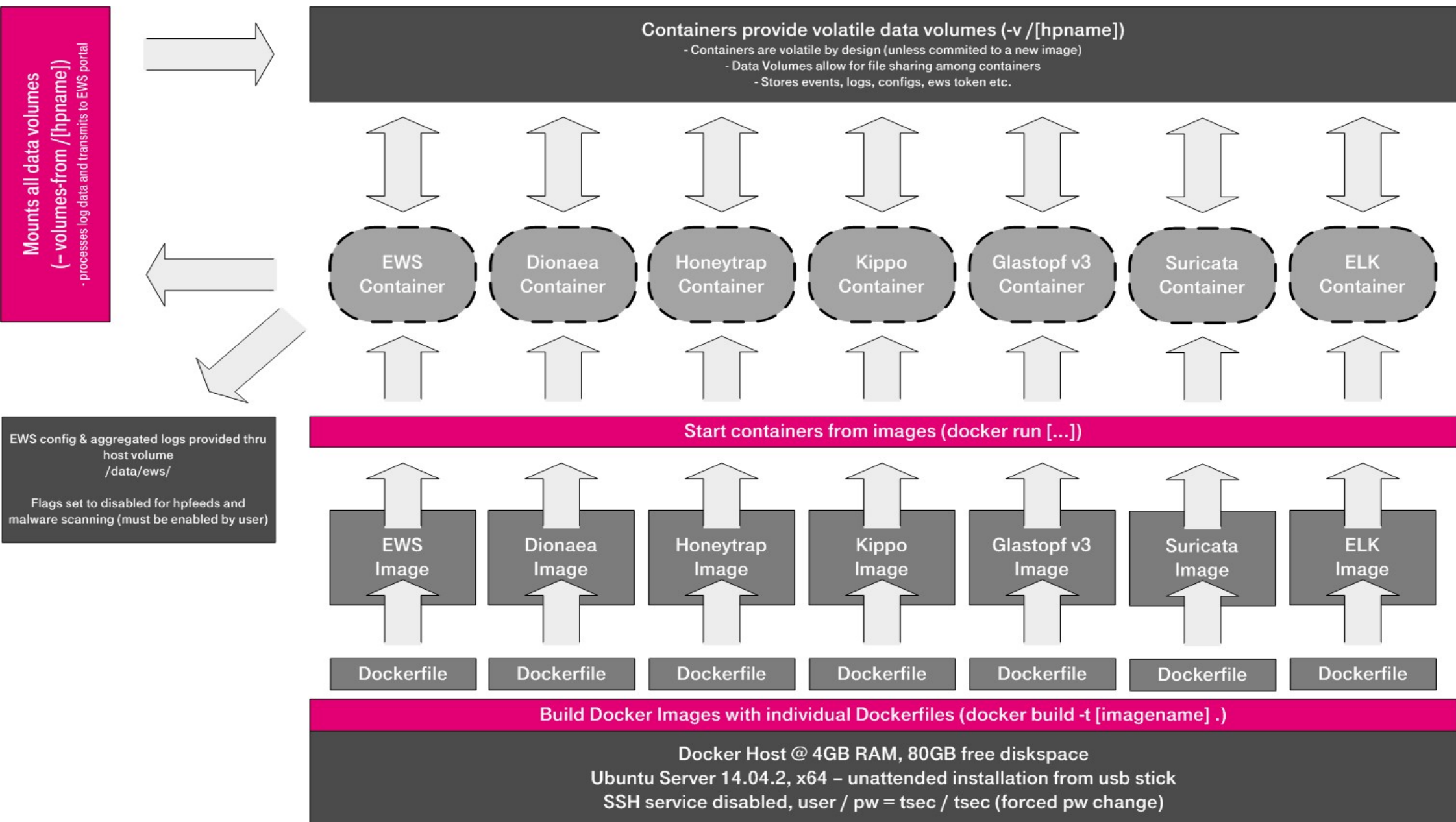
PLATAFORMAS DE CONTENEDORES

- Google Kubernetes Engine
- CoreOS'rkt (Rocket)
- Portainer
- AWS ECR
- Azure Kubernetes Service
- Swarm
- Marathon
- Hashicorp Nomad
- Open Stack Magnum



RECOMENDACIONES DE SEGURIDAD

- Securizar el host
- Incorporar proxy inversos
- Incorporar balanceadores de carga
- Uso de certificados ssl/tls
- Forzar https
- Herramientas contra ataques DoS
- Uso de WAF (Web Applications Firewall) si es aplicación web
- Pruebas de carga
- Usar Dockerfile y forjar imágenes propias
- Verificar el uso de imágenes Docker publicas





HERRAMIENTAS

1. <https://www.ssllabs.com/ssltest/>
2. <https://mozilla.github.io/server-side-tls/ssl-config-generator/>
3. <https://www.cisecurity.org/cis-benchmarks/>
4. <https://www.cisecurity.org/benchmark/docker/>
5. https://www.owasp.org/index.php/OWASP_WAP-Web_Application_Protection
6. <https://github.com/red-panda-ci/red-panda-ci-symfony>
7. <https://github.com/red-panda-ci/red-panda-ci-symfony/tree/master/ci-scripts/test/cucumber>
8. <https://www.cloudflare.com>
9. <https://hub.docker.com/r/chef/inspec/>



REFERENCIAS

<https://github.com/sergioortegagomez>

<https://github.com/pedroamador>

<https://medium.com/guayoyo>

<https://medium.com/guayoyo/hardening-fortaleciendo-ssh-ab3270e06661>

<https://medium.com/guayoyo/hardening-mejorando-configuraciones-ssl-tls-51d6a8bfb564>

<https://medium.com/guayoyo/asegurando-las-cabeceras-de-respuestas-http-en-servidores-web-apache-y-nginx-2f71e62ffda4>

<https://github.com/Spectertj>



Eventos Fijos

Jacqueando Kañas

Primer Martes de cada Mes

Beer Bang Madrid
Mercado de La Guindalera
Calle Eraso 14, 28028 Madrid

Hacking Hardware HackLab

Primer Sábado de cada mes

La Nave de Madrid
Aula 7



HACKMADRID

%27

Gracias.....