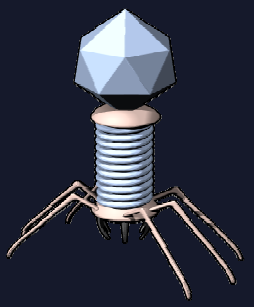
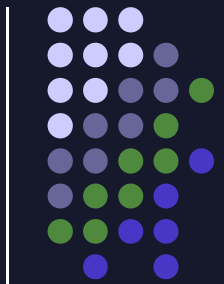
Desarrollo de aplicaciones seguras.
(Técnicas de ataque y defensa)



Jose Manuel Cejudo Gausi

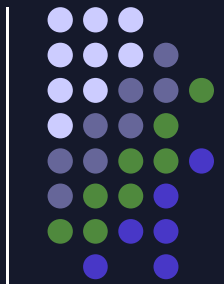
jmcejudo@multitrain.es

Contenido



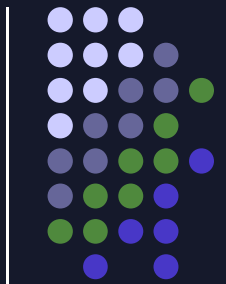
- La seguridad de aplicaciones.
- Atacando.
- Defendiendo.

Presentación.



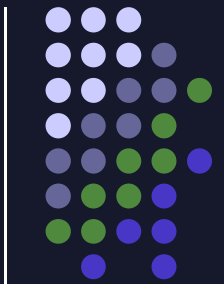
- MultiTrain
  - Empresa especializada en formación y consultoría.
  - Centro oficial de formación Microsoft y SUN.
- Jose Manuel Cejudo Gausi
  - Más de 15 años de experiencia en programación.
  - Certificaciones en desarrollo de Microsoft y SUN.
  - Formador y auditor en temas de seguridad.

La seguridad de aplicaciones.



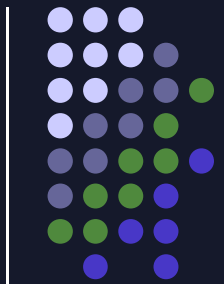
- La importancia de la seguridad.
- El auge de la seguridad.
- ¿Quién es quien?
- ¿Quién es seguro?
- Principios de la seguridad.
- La formación es seguridad.

La importancia de la seguridad.



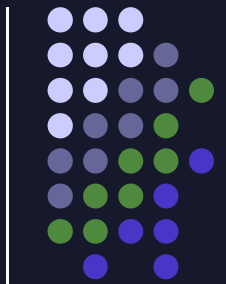
- La seguridad de las aplicaciones debe ser un pilar, no un añadido.
- Siempre hay alguien interesado en su información.
- Los problemas de seguridad:
  - Dañan la imagen de su empresa.
  - Cuestan tiempo y dinero.
  - Restan competitividad.
  - Reducen la confianza.
  - Implicaciones legales.

El auge de la seguridad.



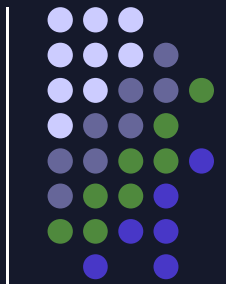
- Aumento del número de empresas y productos dedicados a la seguridad.
- Aumento de la preocupación.
- Extensa documentación e información sobre temas de seguridad.
- Buenas herramientas.
- + Facturación.

El auge de la seguridad (ejemplo)



- Una subasta reciente en eBay de una vulnerabilidad no conocida sobre Microsoft Excel alcanzó un precio de 1.200$ antes de ser retirada.
- Varias empresas pujan por información sobre vulnerabilidades:
  - www.idefense.com
  - www.zerodayinitiative.com

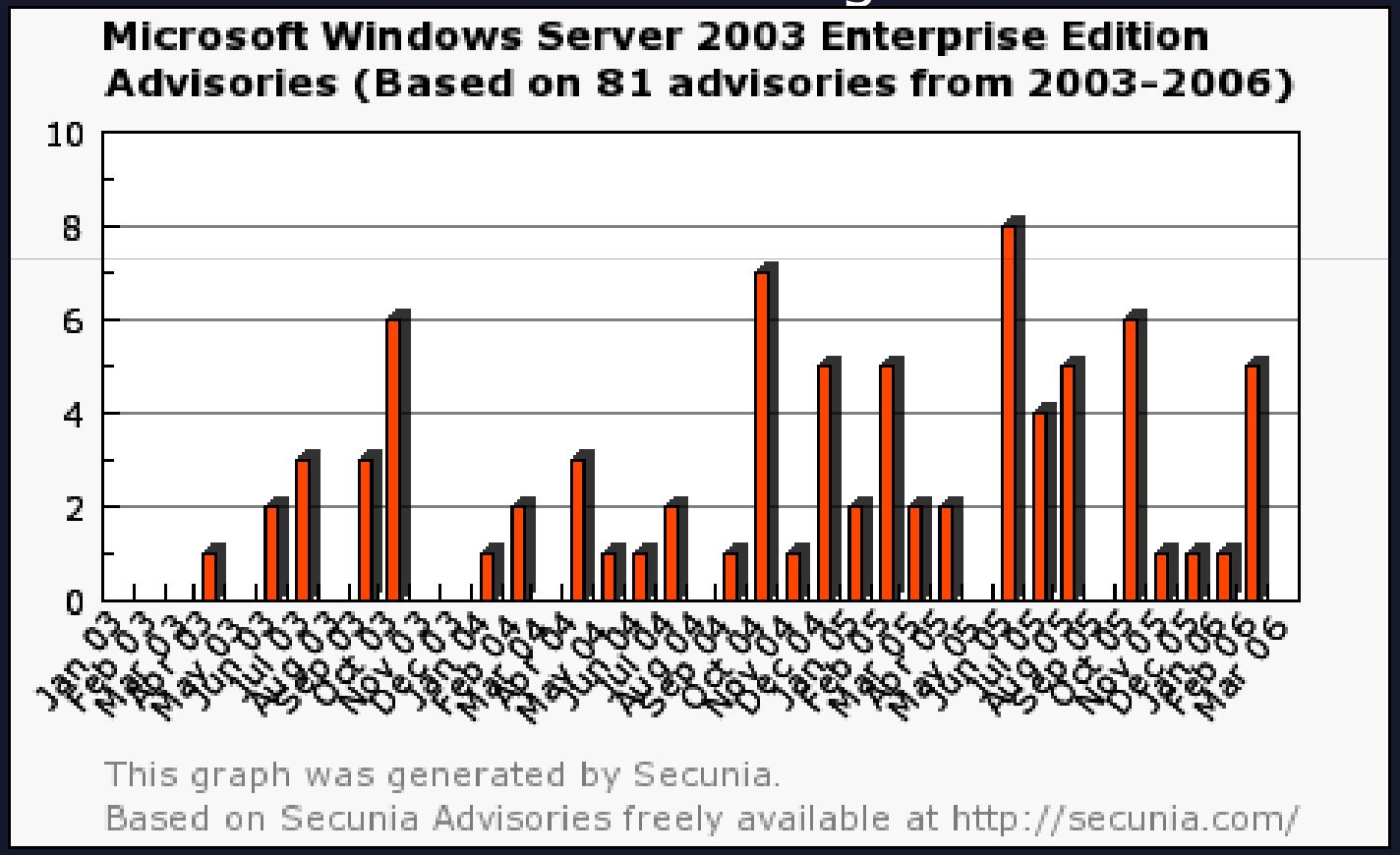
¿Quién es quien?



- Investigadores.
- Hackers.
- Tipos de atacantes:
  - Atacantes ocasionales.
  - Script kiddies.
  - Defacers.
  - Automatizados (virus, gusanos, etc)
  - Internos.
  - Competencia y espionaje industrial.
  - Crimen organizado.

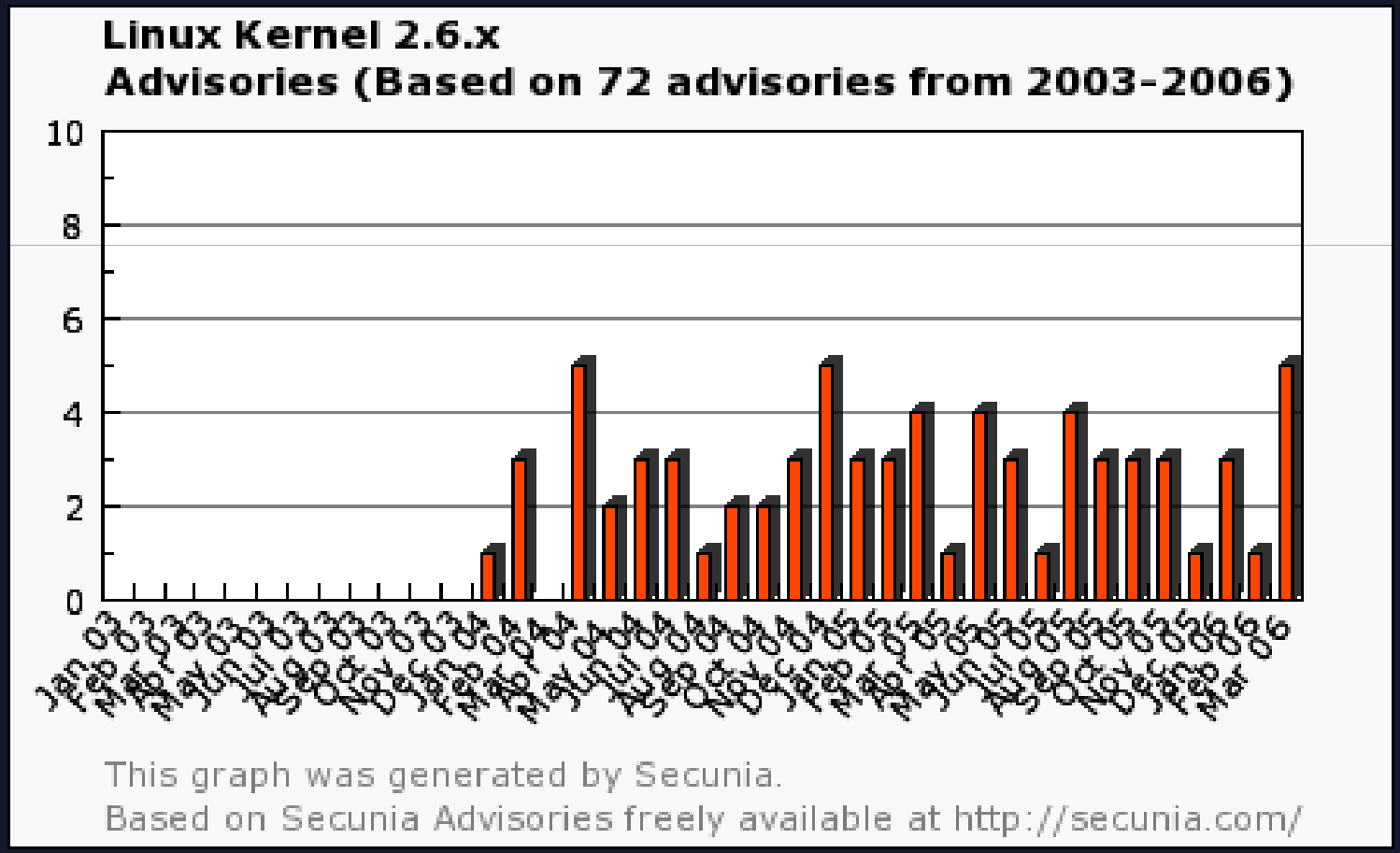
¿Quién es seguro?

- Microsoft tiene fallos de seguridad.



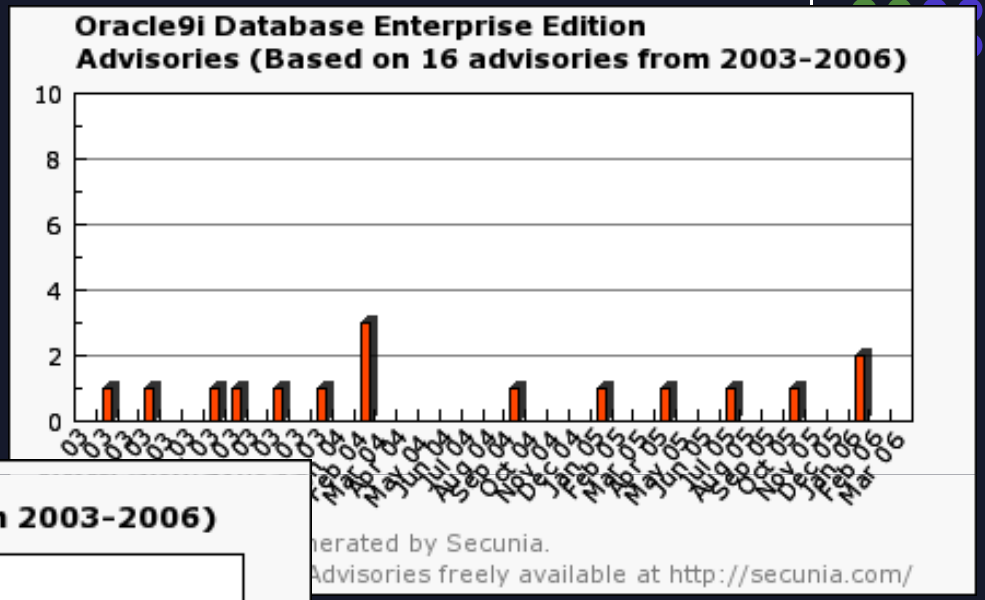
¿Quién es seguro?

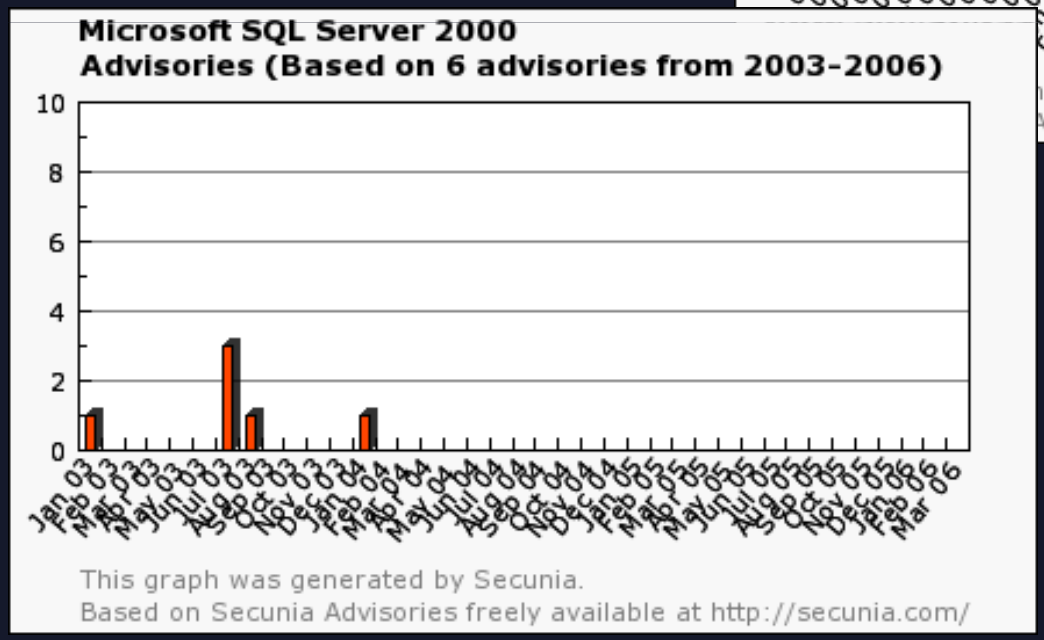
- Linux también…



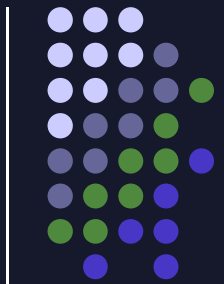
¿Quién es seguro?

- ¿Y Oracle?



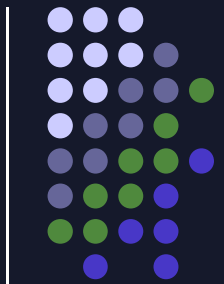


¿Quién es seguro?



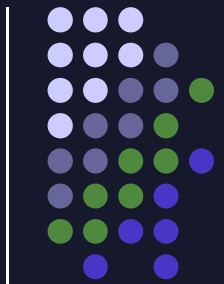
- ¡¡¡ NADIE !!!
- No confiar en los medios de comunicación generalistas. Buscar información especializada.
- No podemos estar seguros al 100%.
- La seguridad es un estado mental.

Principios de la seguridad.



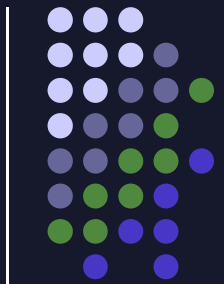
- La seguridad es un camino, no un destino.
- Preocuparse desde el principio.
- Ser paranoico (no demasiado :-).
- Contar con recursos especializados:
  - Información.
  - Herramientas.
  - Personal.
  - Formación.

La formación en seguridad.



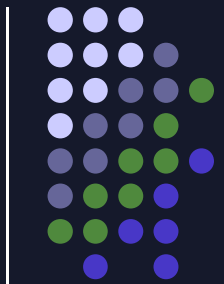
- La formación continua es muy importante para:
  - Arquitectos, analistas y jefes de proyecto.
  - Desarrolladores.
  - Técnicos de pruebas.
  - Administradores de sistemas.
  - Usuarios.
  - Directivos.

Enlaces.



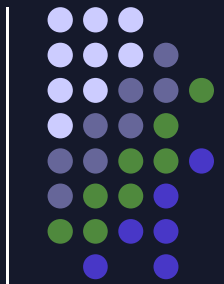
- www.securityfocus.com
- www.defcon.org
- www.kriptopolis.com
- www.owasp.org
- www.webappsec.org
- www.ntbugtraq.com
- msdn.microsoft.com/security
- java.sun.com/security

Atacando.



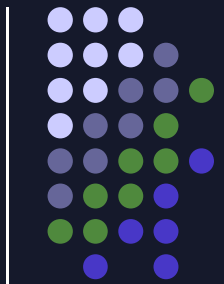
- OWASP Top Ten.
- El proceso de ataque.
- Obtención de información de la victima.
- Técnicas de ataque.

OWASP Top Ten



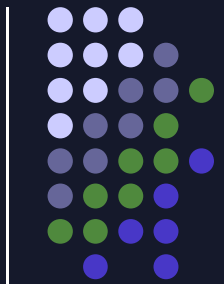
- Entradas incorrectamente validadas.
- Control de acceso vulnerado.
- Autenticación y/o administración de sesión vulnerados.
- Cross Site Scripting.
- Desbordamiento de buffer.
- Inyección de código.
- Control incorrecto de errores.
- Almacenamiento inseguro.
- Negación de servicio.
- Configuración insegura.

El proceso de ataque.



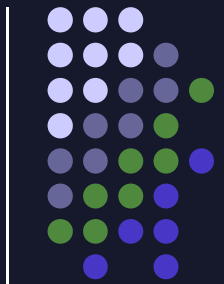
- Obtención de información.
- Explotación y penetración.
- Elevación de privilegios.
- Mantenimiento del acceso.
- Realización de la motivación.

Obtención de información.



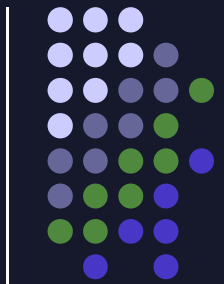
- Revisión visual.
- Footprinting.
- Mensajes de error.
- Comentarios.
- Buscadores.
- Analizadores y proxies de intercepción.
- Listas de vulnerabilidades.

Obtención de información. Footprinting.



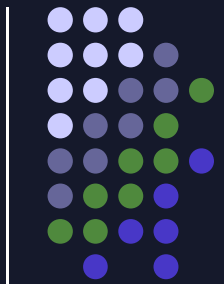
- Herramientas de red:
  - Telnet
  - Nslookup
  - Tracert
- Herramientas específicas:
  - Nmap (http://www.insecure.org/nmap)
- Registros de dominio:
  - https://www.nic.es
  - http://www.samspade.org
- Registros de IP:
  - http://www.arin.net
  - http://www.ripe.net
  - http://www.afrinic.net
  - http://www.apnic.net
  - http://www.lacnic.net

Obtención de información. Buscadores.



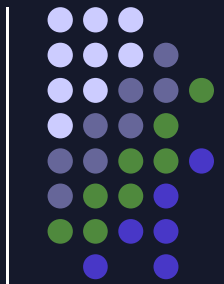
- Google
  - www.google.com
  - Google Hacking Database
    http://johnny.ihackstuff.com
- Wayback Machine
  - http://www.archive.org/web/web.php

Obtención de información. Google Hacking.



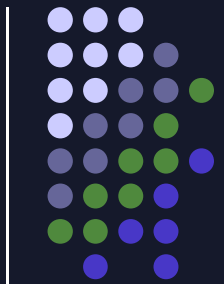
- site:dominio ext:doc
- site:dominio inurl:login
- site:dominio intitle:”Index of /”
- password site:dominio
- mdb site:dominio intitle:”Index of /”

Obtención de información. Proxy de intercepción.



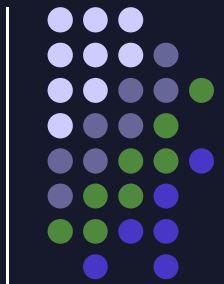
- Permiten interceptar todo el tráfico HTTP y HTTPS entre el navegador y el servidor.
- Permiten alterar los datos enviados y recibidos.
- Muy útil para analizar la aplicación y para realizar ataques.
- WebScarab
  - http://www.owasp.org/software/webscarab.html

Técnicas de ataque.



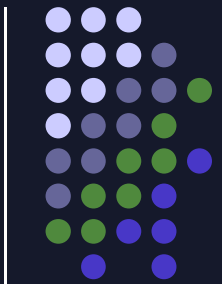
- Algunos de los principales ataques.
  - SQL Injection.
  - Cross Site Scripting (XSS).
  - Manipulación de parámetros.
  - Secuestro de sesión.
  - Fuerza bruta.
  - Path traversal.

SQL Injection.



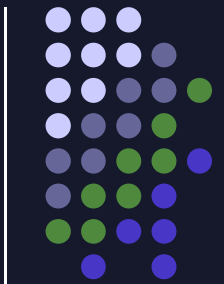
- Modificación de entradas de la aplicación para alterar las sentencias SQL que se envían a la BD.
- Suele permitir la consulta y modificación total de los datos.
- Es uno de los errores más dañinos y habituales.
- Usos habituales:
  - Robo de información.
  - Modificación de información.

Cross Site Scripting.



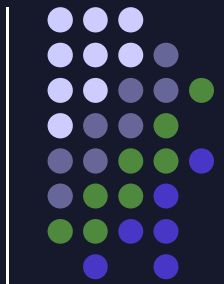
- Manipulación de parámetros para modificar el código HTML que se devuelve al navegador.
- Permite tomar control sobre el navegador del usuario.
- Usos habituales:
  - Secuestro de sesión.
  - Modificación de contenidos.
  - Engañar a usuarios.

Manipulación de parámetros.



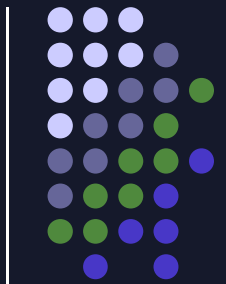
- Manipulación de parámetros de entrada a la aplicación para alterar el normal funcionamiento de la misma.
- Puede permitir realizar acciones no deseadas.
- Usos habituales:
  - Evasión de restricciones.
  - Obtención de permisos adicionales.
  - Robo de información.

Secuestro de sesión.



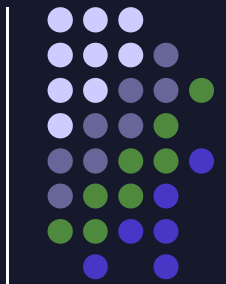
- Obtención de las credenciales de sesión del usuario victima para acceder a la aplicación en su nombre.
- Permite realizar cualquier acción que pudiera hacer el usuario propietario de la sesión.
- Usos habituales:
  - Robo de información.
  - Obtención de permisos adicionales.

Fuerza bruta y diccionarios.



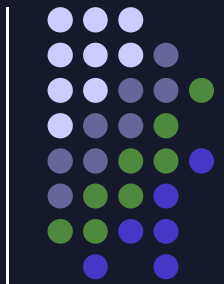
- Obtener las credenciales de un usuario mediante pruebas aleatorias y de palabras comunes.
- Permite autenticar en la aplicación con las credenciales obtenidas.
- Usos habituales:
  - Robo de información.
  - Obtención de permisos adicionales.

Path traversal.



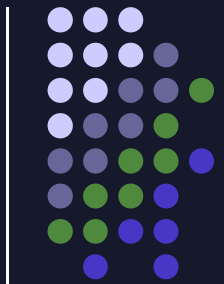
- Manipulación de parámetros de entrada a la aplicación para acceder a recursos protegidos.
- Permite acceder a información que no debería ser accesible.
- Usos habituales:
  - Robo de información.

Defendiendo.



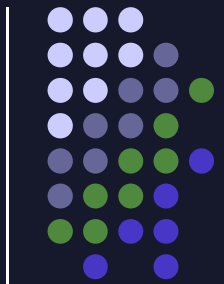
- Los pilares de la seguridad.
- Bases de la defensa.
- Desafíos en la implementación de la seguridad.

Los pilares de la seguridad.



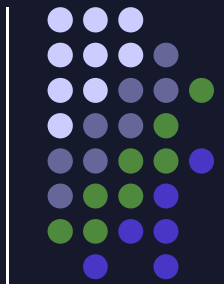
- Autenticación.
- Autorización.
- Auditoria.
- Confidencialidad.
- Integridad.
- Disponibilidad.

Autenticación.



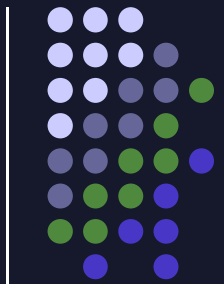
- Responde a la pregunta ¿Quién eres?.
- Identifica unívocamente a los clientes, procesos y servicios de la aplicación.

Autorización.



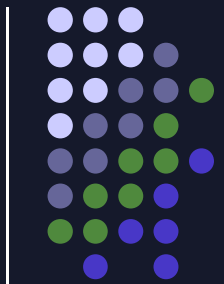
- Responde a la pregunta ¿Qué puedes hacer?.
- Controla los procesos, acciones y recursos que un usuario autenticado puede utilizar.

Auditoria.



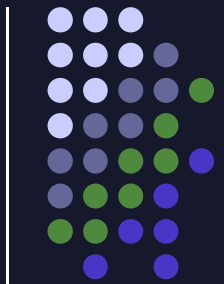
- Gestiona el registro de los sucesos y eventos que ocurren durante el funcionamiento de la aplicación.
- Es imprescindible para asegurar el “No Repudio”.
- Es muy útil para detectar errores y problemas de seguridad.
- En algunos casos es obligado por la regulaciones o leyes.

Confidencialidad.



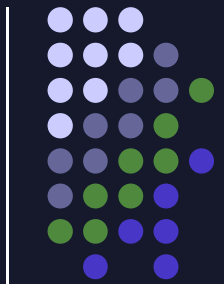
- También conocida como “Privacidad”.
- Asegura que los datos permanecen privados.
- Normalmente se logra mediante la encriptación y la autorización.

Integridad.



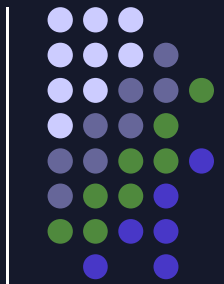
- Es la garantía de que los datos no son alterados accidental o deliberadamente.
- Normalmente se logra mediante encriptación, autorización y técnicas de sumas de control.

Disponibilidad.



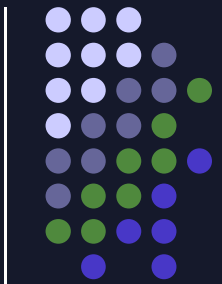
- Asegura que la aplicación siempre está disponible para los usuarios legítimos.

Bases de la defensa.



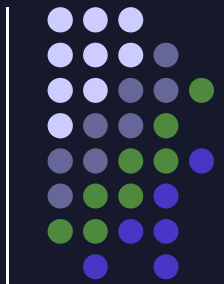
- Separación de funcionalidad.
- Mínimo privilegio.
- Defensa en profundidad.
- Desconfiar de las entradas de usuario.
- Fallos seguros.
- Asegurar el eslabón más débil.
- Modo seguro por defecto.
- Minimizar el área de ataque.
- No confiar en la seguridad por la oscuridad.
- Formación.

Desafíos en la implementación de la seguridad.



- Atacantes vs Defensores:
  - El atacante solo necesita conocer una vulnerabilidad.
  - Los defensores tienen que defender todos los puntos.
  - El atacante tiene tiempo ilimitado.
  - Los defensores tienen límites de tiempo y recursos.
- Seguridad vs Usabilidad:
  - Un sistema seguro es más difícil de usar.
- Seguridad vs Planificación:
  - La seguridad no se percibe como un fundamento.
  - Dejar la seguridad para el final.

Conclusión.



- Sean paranoicos.
- Presten atención a los nuevos tipos de vulnerabilidades y ataques.
- Obtengan formación y preparación.