ALL YOUR DATABASE ARE BELONG TO US

```
UPDATE all_your_database
   SET are_belong_to="us";
```

Christian Martorella - Vicente Díaz
Edge-security
Fist Conference April 2007

Indice

- Introducción a la seguridad de DB
- Motores de Bases de Datos
- Ataques internos
- Ataques externos
- Conclusiones

Introducción

- ¿Qué es una base de datos?
- ¿Qué hay en una base de datos? ...
  - Tras pensar en ello diez segundos, se entiende la necesidad de protegerlas
  - Y de porqué hay tanta gente interesada en acceder a las mismas

Valor de los datos

Tipo de dato	Valor
Dirección	$0.50
Telefono	$0.25
Telefono no publicado	$17.50
Móvil	$10
Fecha de nacimiento	$2
Educación	$12
Historia crediticia	$9
Detalles de bancarrota	$26.50
Información judicial	$2.95
Historial laboral completo	$18
Archivo militar	$35
Tarjetas de credito	$1-6
Identidad completa	$16-18
Disco duro con transferencias del Banco Central de Rusia.	$1800
Historial de llamadas a través de moviles	$110 - 200
30.000 Emails	$5

Valor de los datos

- La cantidad TOTAL de registros personales sensibles que estuvieron relacionados con incidentes de seguridad es de: 150,520,490.

- Éstos son los declarados obligados por ley en USA ... pero HAY MÁS PAISES!

Motores de Base de datos

DB2

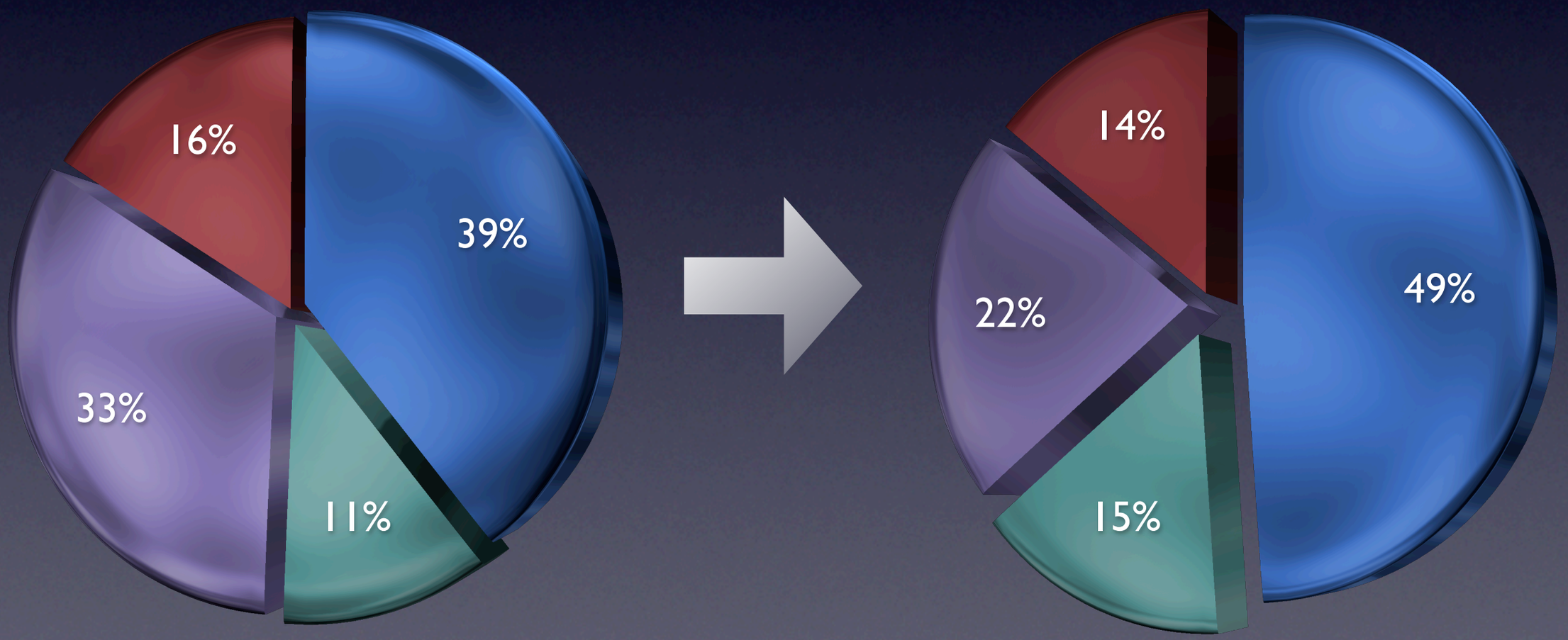
Mysql

Oracle

SQL Server

Postgresql

DB - Market Shares



IDC 2003

Gartner 2005

DB - Oracle

- Servidor de DB más popular
- Mayor cuota de mercado
- Uno de los primeros en entrar al mercado
- Multiples OS desde el principio
- Campaña Unbreakable 2001.
- Versiones más extendidas 9.2 y 10g.

DB Engines - SQL Server

- Uno de los últimos en entrar al mercado.
- Es una evolución de Sybase
- Solo funciona sobre plataformas Windows
- Problemas de seguridad en el pasado (Slammer Worm)
- Pocos problemas en la actualidad, salvo de configuración.

DB Engines - SQL Server

Ataques internos

- Atacando Oracle
  - DB-Links
- Atacando SQL Server

Atacando Oracle desde el interior

- Identificar:
  - Puertos
  - SID
  - Usuarios/Password, lista por defecto
  - Escalada de privilegios, Sql Injection

Atacando Oracle desde el interior II

- Detección de puertos, generalmente 1521
- Utilizar algún Scanner con identificador de servicios, nmap -sV

Atacando Oracle desde el interior III

- Identificar SID:
  - En caso de que el servicio LISTENER no esté protegido, con un simple comando “show services” obtendremos los SID de ese puerto. O con herramientas como Winsid, Integrigy Lsnrcheck.
  - Si el LISTENER esta protegido, habrá que adivinar el nombre del SID por ataque de diccionario (Sidguess, OAK)

Atacando Oracle desde el interior IV

- User/password:
  - Las cuentas con máximos privilegios: SYS y SYSTEM.
  - Hay otras cuentas con privilegios de DBA (ctxsys,wksys,mdsys,sysman)
  - Existen listas con más de 400 cuentas!!

Atacando Oracle desde el interior V

- Una vez dentro que hacemos?
  - Escalar privilegios si no los tenemos, SQL Injection, Buffer Overflows.
  - Explotar relaciones de confianza entre DB's. DB-Links.

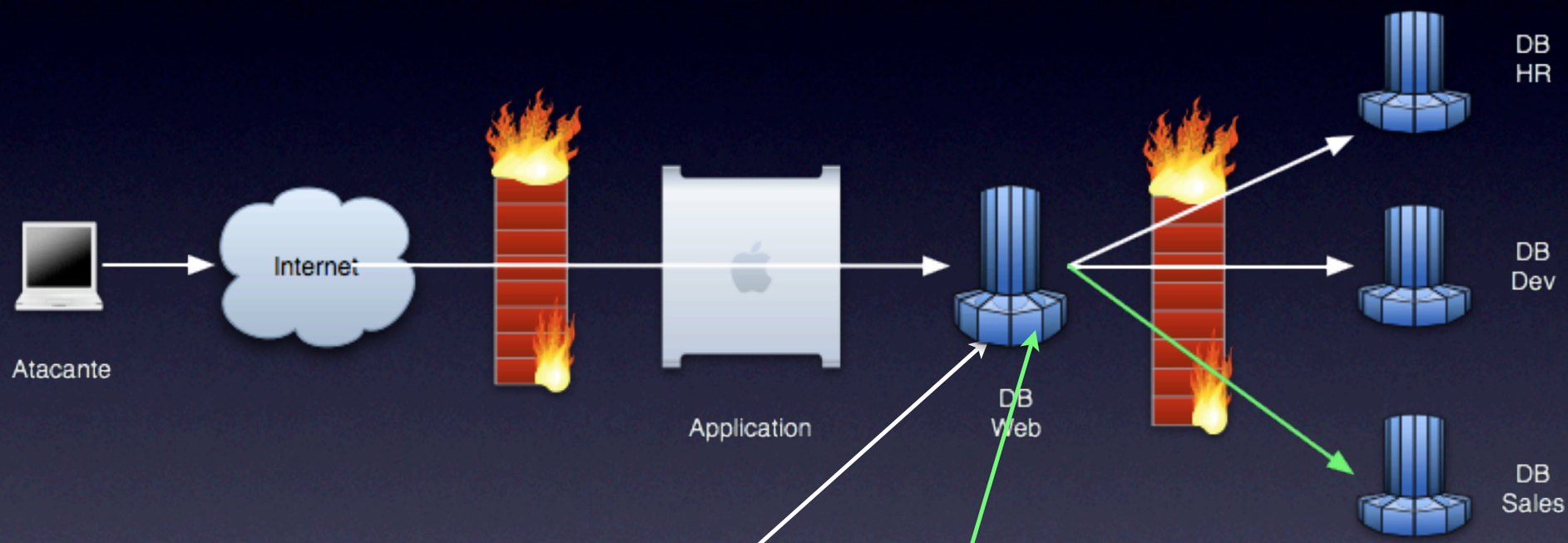
Atacando Oracle desde el interior

- Ejemplo práctico 4 pasos....

Atacando Oracle desde el interior - DB Links

- Es un objeto que permite realizar una conexión desde una base de datos a otra.
- Facilita el acceso a recursos en otras DB.
- A los atacantes les brinda facilidad de expansión...

Atacando Oracle - DB Links



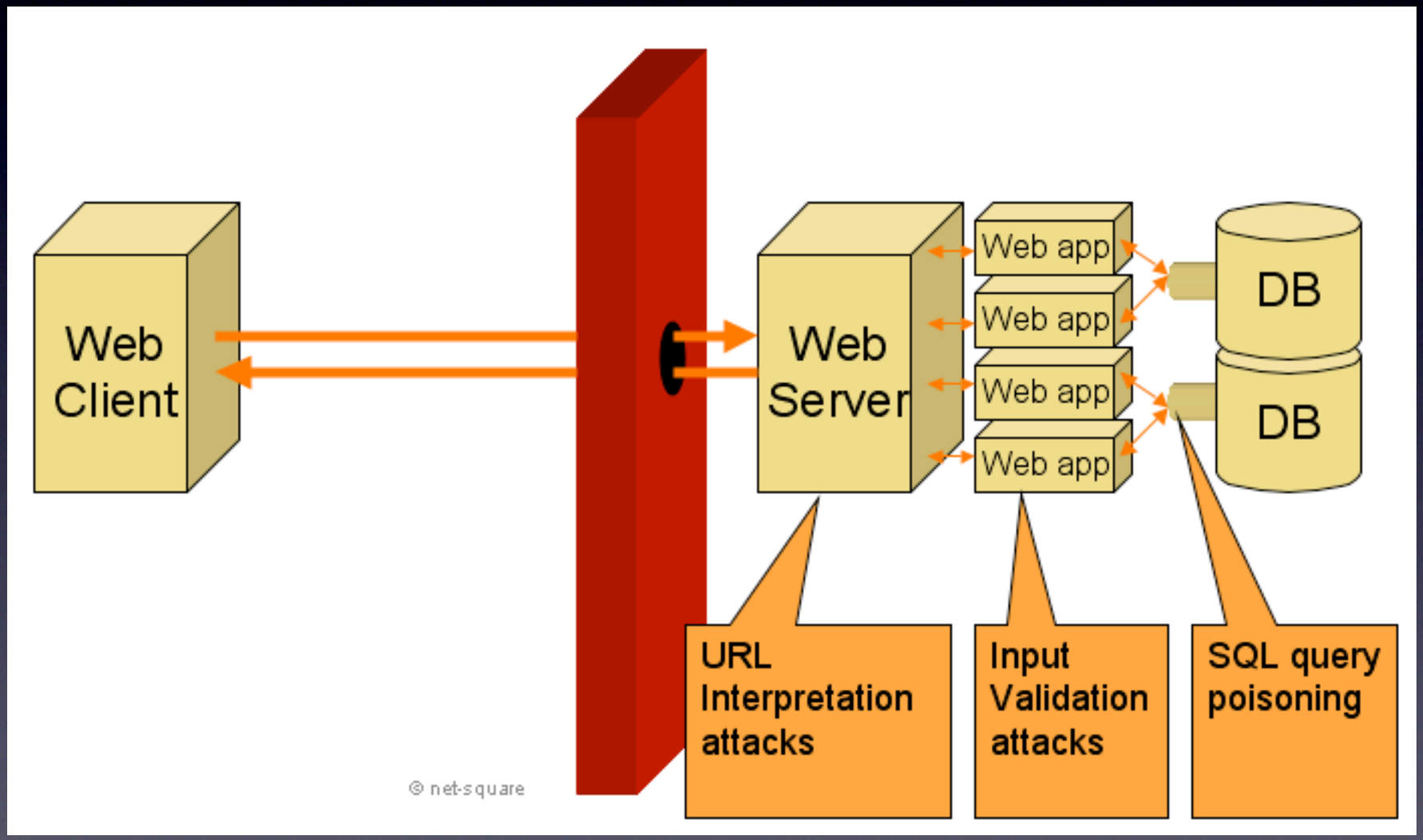
Select * from all_users;

Select * from all_users@sales;

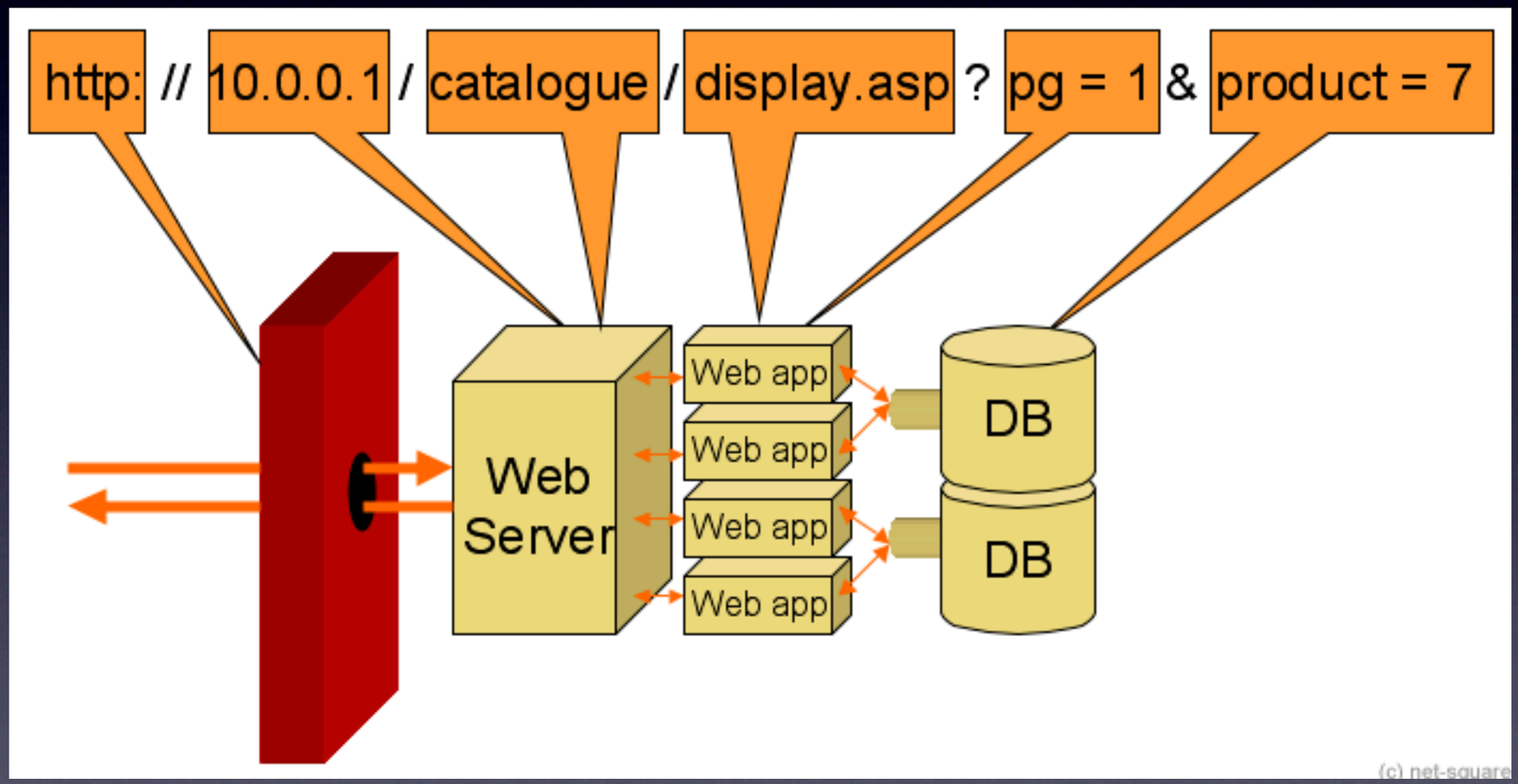
Ataques externos

- SQL Injection y Blind SQL Injection
- File upload and inclusion, Web frontend
- Obteniendo una DB completa (SQL Server)
- Database Rootkits

Escenario actual



Escenario actual II



SQL injection

sel id = X

union select user+’’+password user

Inicio » Catálogo » Barajas » APLU — Qué es NONBAIT | Mi cuenta | Ver cesta | Realizar pedido

Categorías

- *Catálogo COMPLETO*
- Alimentación
- Artesanía
- Banderas
- **Barajas**
- Camisetas
- CD-Rom / Multimedia
- Cerámica
- Complementos
- Cristal
- Deportes
- En la pared
- Figuras
- Hogar / Textil
- Infantil / Juegos
- Kukuxumusu
- Libros
- Llaveros
- Música
- Pañuelos de fiestas
- Postales, pegatinas y láminas
- Souvenir
- Sudaderas / Deportes
- Tazas - MUG
- Txapelas
- Vídeos / DVDs
- Vinilos y Posters

Búsqueda rápida

Búsqueda avanzada

Ofertas

Irakaslea I -

Baraja Lunnis - Lucho

[APLU]

7.20€

Baraja del conocido programa infantil de TVE "Los Lunnis", fabricada por la conocida marca de naipes de Vitoria-Gasteiz Heraclio Fournier.
Incluye mini-marioneta.

Haz clic para agrandar

Comentarios — Añadir a la Cesta

Recomendamos:

Baraja Lunnis - Lublú
7.20€
Compre Ahora

Algunos clientes que compraron este producto, también han comprado

Shin Chan Dance - Betizu (CD)

Goxua - Licor de crema

Compras

0 productos

Idiomas

Cuéntaselo a un amigo

Envía esta página a un amigo con un comentario.

Comentarios

Escribe una opinión para este producto

Blind SQL injection

File Inclusion - File Upload
Web frontend

- Esta vulnerabilidad se encuentra en el Top 10 de OWASP como la número 3.
- Muchas aplicaciones permiten subir ficheros, fotos, documentos, etc...
- Si logramos subir un fichero de scripting...

File Upload -Web frontend

- Se puede crear un cliente SQL a través de http.
- Total interacción con la DB
- Veamos un ejemplo. . .

DB Backdoor

- Procedimientos de la base de datos, creados para establecer un canal de conexión con el atacante.
- Utiliza las funciones de HTTP disponibles en las bases de datos.

DB Rootkits

- Realizan algunas modificaciones a la base de datos SYS, lo que hace que Oracle NO muestre ciertos detalles, o modifique otros.

- Son bastantes sencillos pero efectivos

Conclusiones

- Securizar las instalaciones de las DB
- Eliminar usuarios por defecto y cambiar contraseñas
- Segmentar las redes (vlans)
- Segregar las funciones de los usuarios, roles, privilegios, etc
- Logs y alertas

Conclusiones II

- Reglas de firewall de salida (extrusión detection)
- Securizar los servidores web, y las aplicaciones.
- Realizar auditorías de seguridad para analizar la seguridad de nuestros sistemas, o evaluar la implementación de controles de protección.

Referencias

- Saumil Shah One way Hacking
- www.databasecurity.com
- www.argeniss.com
- www.petefinnigan.com

Muchas gracias por su atención.


LARRY: ALL YOUR DATA
ARE BELONG TO US