Asegúrate de que estás "seguro"

- test de intrusiones en aplicaciones Web - Parte II

Alberto Moro aka "Mandingo"
Roman Medina aka "RoMaNSoFt"

Madrid, 4 de octubre de 2007

S21sec

¿cómo empezar?

"ponte cómodo y ten tus todas tus herramientas a mano"

pero antes...

¿qué hay detrás de la WWW ?

***personas* que controlan:**

- tecnologías (soft, hard)
- información (pública o no)
- negocios ($$$)
- ideas e ilusiones :)
- ...

T1: Todo ser humano es imperfecto

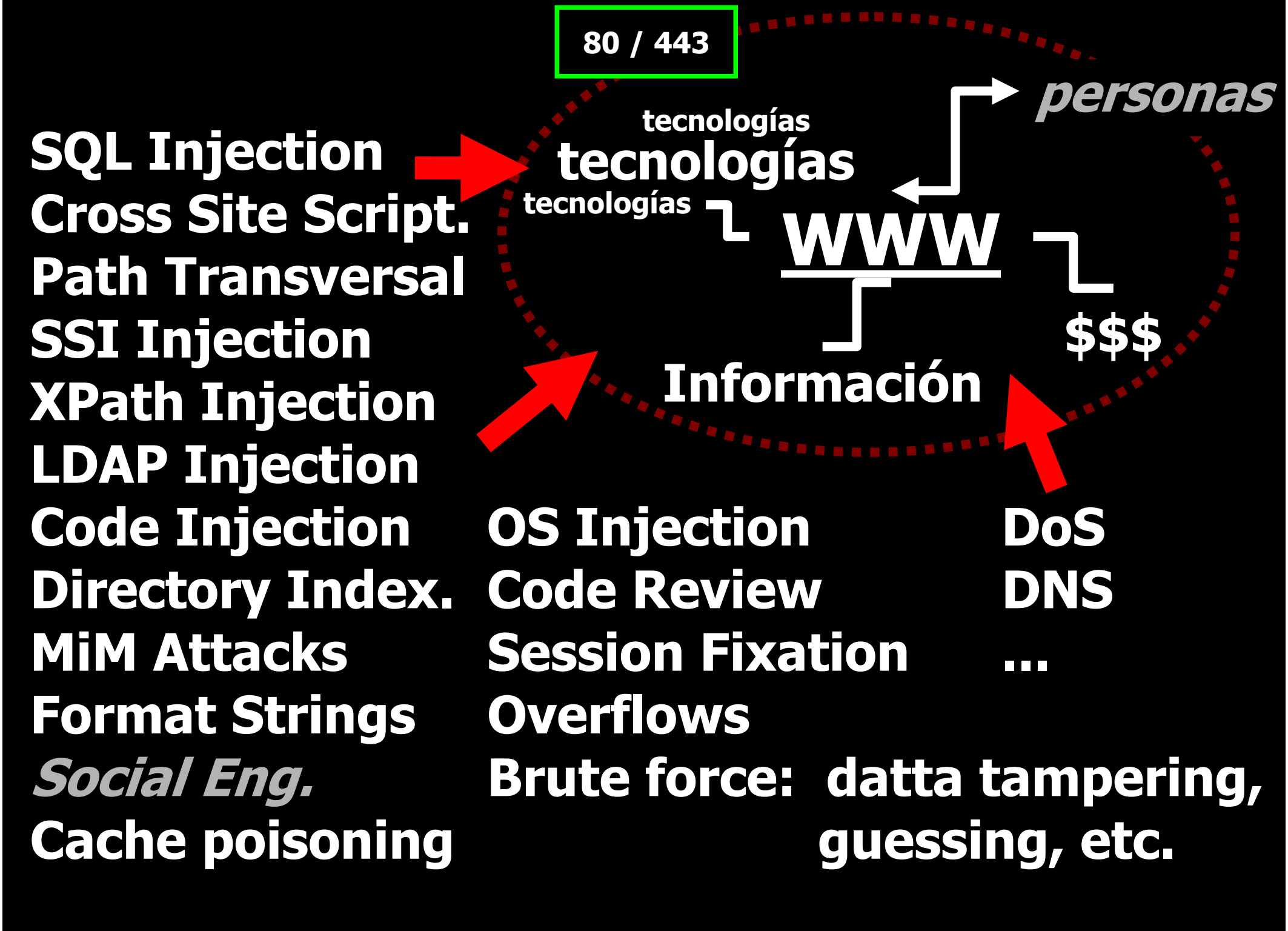
C1: Las creaciones humanas son imperfectas/inseguras

T2: formación+recursos+ dedicación: mayor perfección

C2: seguridad (WWW)≈ T2

Ahora que somos conscientes de la existencia de estas imperfecciones, naveguemos por este "mundo digital" imperfecto...

click here -> www :)


80 / 443
personas
tecnologías
tecnologías
tecnologías
WWW
$$$
Información
SQL Injection
Cross Site Script.
Path Transversal
SSI Injection
XPath Injection
LDAP Injection
Code Injection
Directory Index.
MiM Attacks
Format Strings
Social Eng.
Cache poisoning
OS Injection
Code Review
Session Fixation
Overflows
Brute force:
DoS
DNS
...
datta tampering,
guessing, etc.

“tools for the trade”

- Herramientas semi-automáticas:
  - burp suite (proxy+crawler+...)
  - sqlibf (sql injection)
  - pipper (bf)
  - *(private tools)*
- Herramientas automáticas gratuitas:
  - nikto
  - nessus
  - perl, python, php, gcc... ;)
- Herramientas de pago:
  - WebInspect
  - Qualys
  - AppScan
  - ...

“auto” vs “human”

+ Adaptable a situaciones poco homogéneas
  o nuevas; análisis experto -> nuevas vulns?

+ Permite trabajo en equipo - f(t,recursos)

  t=1/f(conocimientos, habilidades)

  + personas * -> + recursos físicos
                   + recursos humanos

  (*) los conocimientos y habilidades
  no crecen de forma lineal si se aumenta
  el número de personas...

metodología

veamos que hay detrás de este http://...

- Localizar páginas dinámicas
  * identificar parámetros: tipo, posible uso -> injecciones, bf, etc.
  * identificar paneles administrativos
  * “file uploads” -> cmdshell
- Localizar páginas no enlazadas
  * revisión código html
  * buscadores: google/msnsearch
  * webcaches
  * mensajes de error
  * fuerza bruta: diccionarios
    f (identificar tecnología usada, idioma, extensiones, etc.)
- Revisar código fuente (si disponible)

perseverancia

como proceder

consejos

qué hacer si nos quedamos atascados

1. Guardar todas las evidencias y pistas:
   cuaderno, freemind, txt, etc.
2. Si estamos bloqueados: hacer un paréntesis
   - olvidarse del ordenador
   - pasear o descansar ("siesta time")
   - volver manos a la obra...
3. Revisar: ¿qué tenemos? ¿qué necesitamos?
4. Proverbio: "No dejes que los árboles te
   impidan ver el bosque"
5. Organizar las ideas:
   hablar con alguien siempre ayuda
6. No descartar nada...
7. Documentarse más...
8. Meditar con la almohada (><)

hablemos de
“pipper”

”cómo vamos de tiempo Chema?”
^^

FiN

“ Gracias a tod@s ”

mandingo@yoire.com
roman@rs-labs.com