Seguridad web

www.flagsolutions.net

Índice

- Introducción
- Tipos de ataques

Introducción

- Los mismos problemas que aplicaciones de escritorio
- Particularidades
  - Miles de millones de potenciales agresores
- *"Lo que un hombre puede ocultar, otro lo puede descubrir"* (Sherlock Holmes)

Tipos de fallos

- Desbordamientos de buffer
- Almacenamiento inseguro
- Denegación de servicios
- Configuración insegura
- Errores en autenticación.

Tipos de fallos (2)

- Errores en sesión
- Entradas no validadas
- Errores del control de acceso
- Cross site scripting (XSS)
- Inyección de código
- Manejo incorrecto de errores

Descubrimiento de información

- Protocolo “legible” y plano
- Sniffers
- Referers
- Caché
  - Expires
  - Pragma: no-cache
  - Cache-Control (private, no-cache,no-store)
  - <meta http−equiv=”Expires” content=”Thu, 01 Dec 2007 12:00:00 GMT”/>
- Cookies

Autentificación

- Buena gestión de claves

```
sshd[21220]: Failed password for root from 80.93.99.229 port 33811 ssh2
sshd[21235]: Failed password for root from 80.93.99.229 port 33923 ssh2
sshd[21243]: Failed password for root from 80.93.99.229 port 34045 ssh2
sshd[21276]: Failed password for root from 80.93.99.229 port 34176 ssh2
sshd[21282]: Failed password for root from 80.93.99.229 port 34373 ssh2
sshd[21287]: Failed password for root from 80.93.99.229 port 34482 ssh2
sshd[21292]: Failed password for root from 80.93.99.229 port 34593 ssh2

sshd[21297]: Failed password for root from 80.93.99.229 port 34705 ssh2
sshd[21303]: Failed password for apache from 80.93.99.229 port 34824 ssh2
sshd[21309]: Failed password for root from 80.93.99.229 port 34942 ssh2
sshd[21314]: Failed password for root from 80.93.99.229 port 35060 ssh2
sshd[21319]: Invalid user lab from 80.93.99.229
sshd[21319]: Failed password for invalid user lab from 80.93.99.229 port 35185 ssh2
sshd[21325]: Failed password for root from 80.93.99.229 port 35460 ssh2
sshd[21330]: Invalid user oracle from 80.93.99.229
sshd[21330]: Failed password for invalid user oracle from 80.93.99.229 port 35582 ssh

sshd[21335]: Invalid user svn from 80.93.99.229
sshd[21335]: Failed password for invalid user svn from 80.93.99.229 port 35702 ssh2
sshd[21340]: Invalid user iraf from 80.93.99.229

sshd[21340]: Failed password for invalid user iraf from 80.93.99.229 port 35807 ssh2
sshd[21346]: Invalid user swsoft from 80.93.99.229
sshd[21346]: Failed password for invalid user swsoft from 80.93.99.229 port 35926 ssh
```

Gestión de sesiones

- Lado del servidor
- Asociarlas al cliente.
  - ¿Cookies?
  - ¿Campos ocultos?
  - ¿IP’s?
  - Parámetros

Robo de sesiones (2)

- Cómo
  - Adivinarla, calcularla, fuerza bruta, prueba y error,
  - XSS
  - Referers
  - Sniffers
- Contramedidas
  - Aleatorio
  - Id largo
  - Uso de datos accesorios
  - Cambio en cada petición
  - Expiración

Validar sesiones

- Misma política que los campos de entrada
  - Tipo
  - Tamaño
  - Contenido
  - Camino
  - Revocación y renovación ante la duda

Validación de entradas

- Base del resto de los problemas
- Semántica dependiente del contexto
  - Web
  - Lenguajes en el servidor
  - Bases de datos.
- Comprobar la validez
  - O'Neill
  - ; rm –RF /UTF-8
- Escapar caracteres válidos
- Expresiones regulares

Validación de entradas (2)

- Comprobar entradas en servidor
- Ante la duda, FALLAR
- Problemas añadidos
  - Codificación
  - Normalización y nominación
  - Palabras claves. Dominio.

Expresiones regulares

- En el servidor
- Presente en todos los leguajes
- Usarlas para determinar lo que es válido
- Proceso:
  - Sanear
  - Lo que no encaje, es invalido
  - Registrar

Normalización y nominación

- ¿DocumentoFinalDelProyecto004.pdf y Docume~1.pdf son iguales?
- Caracteres sobrantes
- Camino largo y camino corto
  - Directory Transversal: ../../../../
  - Caminos explícitos
- Dispositivos
  - CON, LPT1, /dev/hda1

Normalización (2)

- Nombres de servidores
  - IP’s
  - Nombres locales
- Múltiples representaciones
  - ASCII, UTF8, UCS-2
  - Hexadecimal
    - %20, %27
  - Entities
    - <script>

Proteger de normalización

- Obtener información de los ficheros:
  - GetLongPathName
  - Stats
- Longitud del fichero
- Expresiones regulares
  - ^[cd]:(?:\\\w+)+\\\w{1,32}\.(jpg|gif)$
- Decodificar y validar

Proteger de normalización (2)

- MultiByteToWideChar y WideCharToMultiByte
- Utf8_decode
- String(<cadena>,’UTF8’)
- Probar

Inyección SQL. Introducción

- Vulnerabilidad pública y muy conocida
  - Facilidad de descubrimiento muy alta
  - Facilidad de explotación muy alta
- Cualquier atacante podría explotarla
  - Requiere un nivel de habilidad muy bajo
- Nivel de impacto crítico
  - Revelación de información privada o confidencial
  - Alteración o pérdida de información o disponibilidad
  - Daño económico y en la reputación de la empresa

Inyección SQL

- Dominio de las BBDD
  - Comillas, comentarios, fin de consulta…
- Las comillas es ampliamente conocida.
  - PHP escapa las comillas dobles
  - Es un valor correcto O’Connor
- Completar consultas
- Completar inserciones

Inyección SQL (2)

- Completar consultas:
  - **a' or 'a'='a || a" or "a"="**
  - Si el parámetro es numérico, no necesitamos comillas
- Comentarios: --, /*
- Terminadores: %00, \0, ;
- Objetos conocidos:
  - **Oracle**: base de datos dual
  - **MSSQL**: Sysobjects
  - **Access**: MSObjects

Inyección SQL (3)

- Codificación:
  - **Oracle**: chr(83)||chr(81)||chr(76)
  - **MS SQL Server**: char(83)+char(81)+char(76)
  - **PostgresSQL**: char(83)||char(81)||char(76)
  - **MySql**: char(83,81,76)
  - **MySql**: 0x53514C

SQL Basada en errores

- Errores por pantalla
- **Database error:** Invalid SQL: select * from noticias where idNoticia=7’
- Uso de funciones SQL
  - Agregadas: Group by, order by
  - Union

Blind SQL

- Cuando los errores no funcionan
- Dos comportamientos:
  - Un comportamiento conocido (error)
  - Otro comportamiento (éxito)
- EXISTS (SELECT … WHERE user LIKE ‘adm%')
- Herramientas automatizadas

Inyección basada en tiempos

- Si todo lo anterior no funciona
- Detecta la inyección por retardos
  - Comandos
  - Consultas pesadas
    - Select count(*) from tabla t1, tabla t1, tabla t1, tabla t1, tabla t1, tabla t1, tabla t1, tabla t1, tabla t1
    - Select sum(1) from tabla t1, tabla t1, tabla t1, tabla t1, tabla t1, tabla t1, tabla t1, tabla t1, tabla t1

Inyección basada en tiempos (2)

- Instrucciones de retardo del propio SGBD
  - Microsoft SQL Server
    - ; if (exists(select * from contrasena)) waitfor delay '0:0:5'
  - Oracle
    - ; begin if (*condicion*) then dbms_lock.sleep(5); end if; end;
  - MySQL (versión 5)
    - and exists(select * from contrasena) and sleep(5)
    - and exists(select * from contrasena) and benchmark(5000000,md5(rand()))=0

Inyección basada en tiempos (3)

- Tablas de los SGBD
  - Microsoft SQL Server
    - sysusers
  - Oracle
    - all_users
  - MySQL (versión 5)
    - information_schema.columns
  - Microsoft Access
    - MSysAccessObjects (versiones 97 y 2000)
    - MSysAccessStorage (versiones 2003 y 2007)

Contramedidas inyección

- Mecanismos de protección de la plataforma
  - Consultas SQL parametrizadas, filtros predefinidos,…
- Menor privilegio
  - Limita las consecuencias ante un ataque exitoso
- Deshabilitar errores

Protección .NET

- Para Access (System.Data.OleDb):

  *cmd = new OleDbCommand("SELECT * FROM usuarios WHERE nombre=? AND pass=?")*

  cmd.Parameters.AddWithValue("", usuario)

  cmd.Parameters.AddWithValue("", contraseña)

- Para SQL Server (System.Data.SqlClient):

  *cmd = new OleDbCommand("SELECT * FROM usuarios WHERE nombre=@usu AND pass=@pass")*

  cmd.Parameters.AddWithValue("usu", usuario)

  cmd.Parameters.AddWithValue("pass", contraseña)

- Web.config: *<customErrors mode="On">*

Proteccion PHP

- Sanear todo parámetro recibido:
  - mysql_real_escape_string( );
  - htmlspecialchars( )
  - is_numeric( )
  - $_POST / $_GET
- Desactivar errores en pantalla
  - error_reporting(0);
  - display_errors=false

Protección Java

- String selectStatement =
  "SELECT * FROM User WHERE userId = ? “;
  PreparedStatement prepStmt =
  con.prepareStatement(selectStatement);
  prepStmt.setString(1, userId);
  ResultSet rs = prepStmt.executeQuery();

- Evitar ex.printStackTrace() en producción

Otros problemas

- *RFI:*
  - *http://pagina/voy_a.php?page=**<PAGE>***
- *Code Injection:*
  - *http://servidor/pagina.asp?guarda=;cat /etc/password*
- *Bruteforce*
  - *Pipper*
- *Más inyecciones:*
  - *LDAP, Xpath, Web Services…*