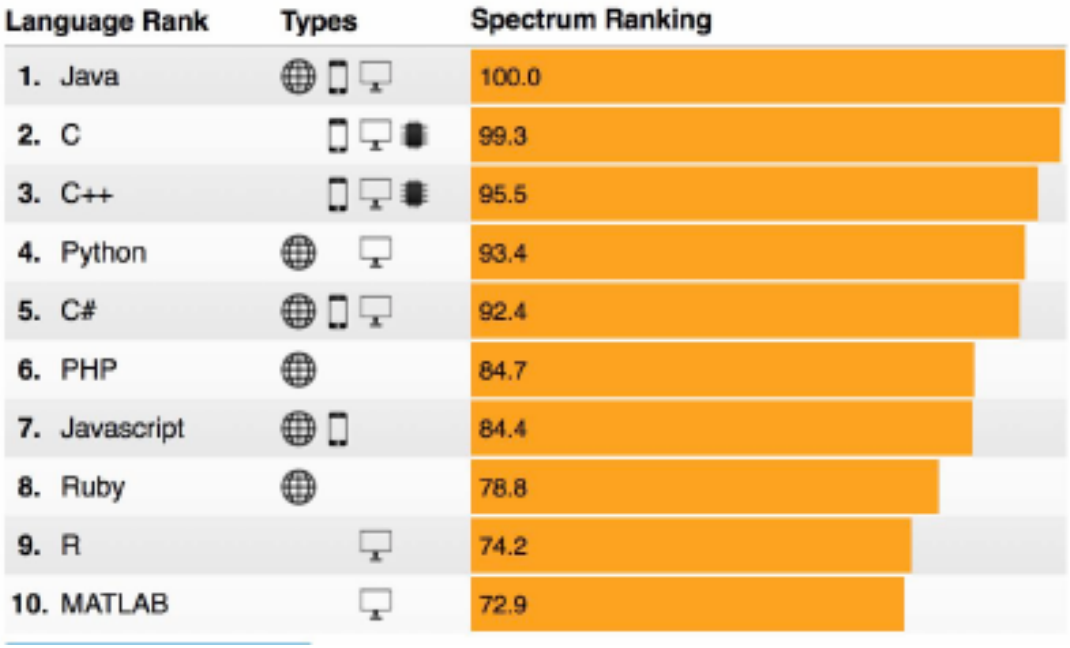
Ataques Buffer Overflow
e
Inyecciones SQL

Antonio Álvarez Caballero
Adrián Ranea Robles

Buffer overflow

Es un bug que afecta a código de bajo nivel, típicamente en C/C++, con implicaciones significativas en la seguridad.

Básicamente, consiste en insertar más datos en un buffer de los que puede almacenar, provocando en la mayoría de los casos que el programa aborte.

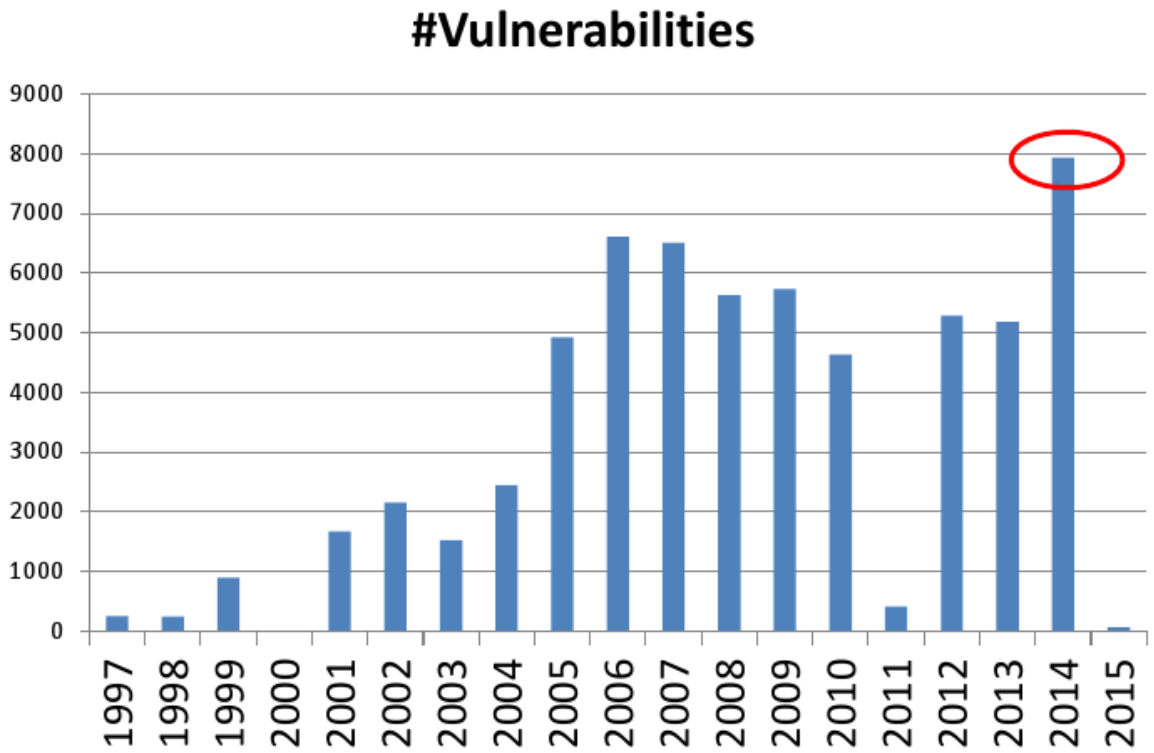


Historia

Gusano Morris - 1988

CodeRed - 2001

SQL Slammer - 2003



Repaso de conceptos I

Tamaño de los tipos de datos en C/C++

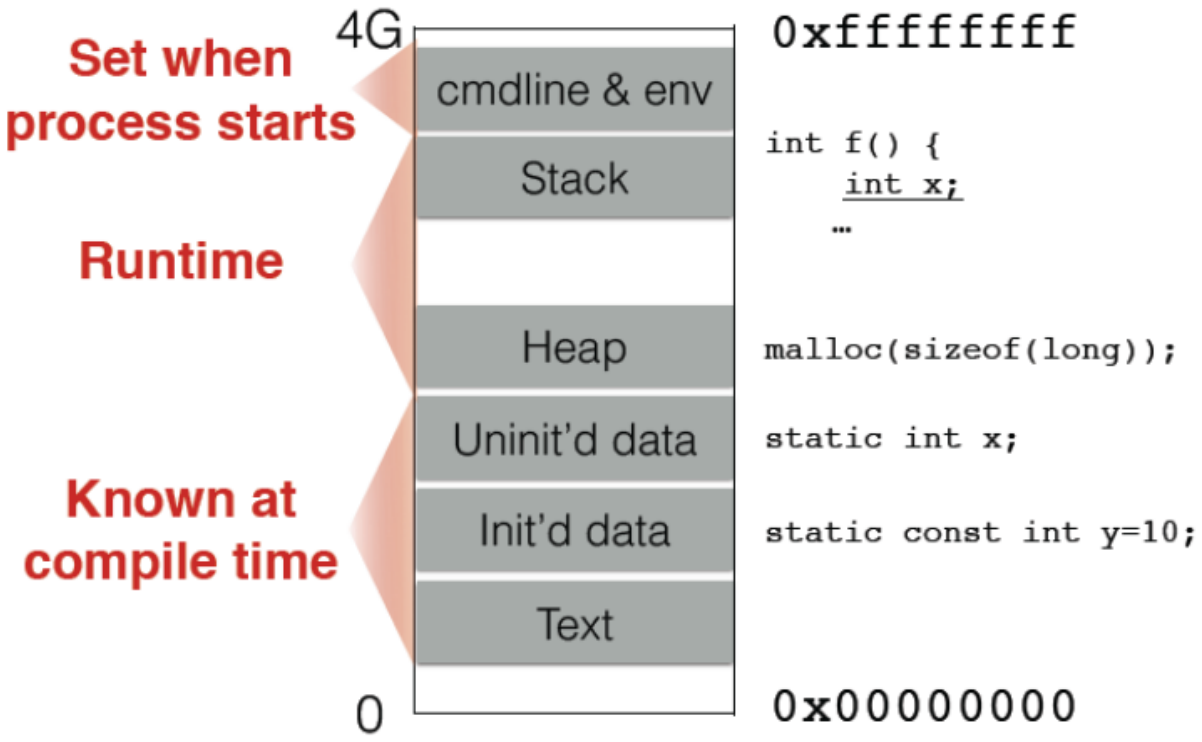
- Int: 32 bits
- Char: 8 bits
- Puntero: 32 bits

Registros en CPUs Intel 80x86

- Registros de propósito general: %eax, %ebx, %ecx, %edx
- Registro de instrucción: %eip
- Puntero de pila: %esp
- Puntero de marco de pila (frame pointer): %ebp

Repaso de conceptos II

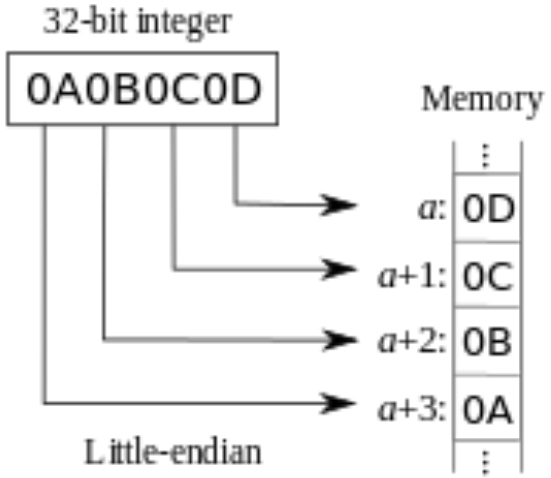
Estructura de la memoria



Repaso de conceptos III

La pila y el montón:

Little endian:



Repaso de conceptos III

Curso de acción cuando se llama a una función en C/C++:

Función llamante:

1. Pone los argumentos en la pila (en orden inverso).
2. Pone la dirección de retorno en la pila.
3. Salta a la dirección de la función.

Función llamada:

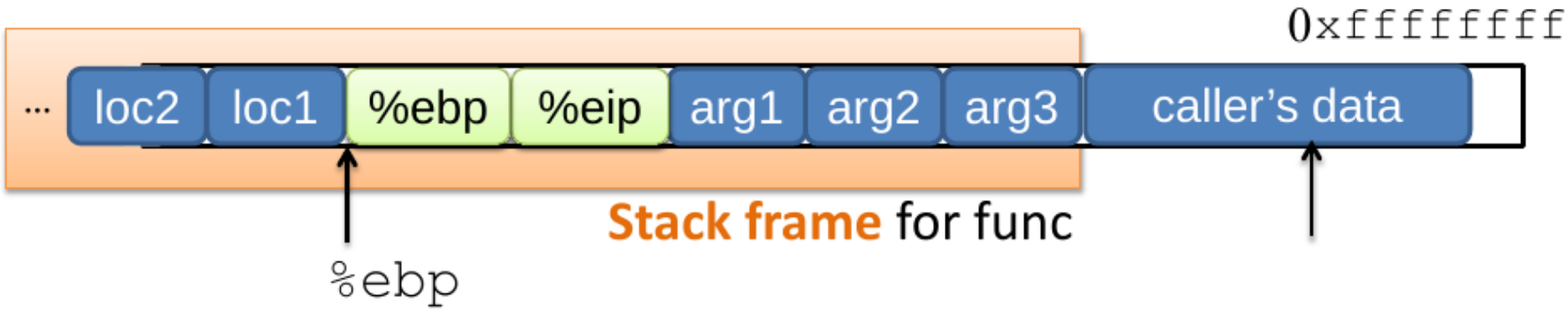
4. Pone el viejo puntero de marco en la pila (%ebp)
5. Fija el puntero de pila a donde al final de la pila actual
6. Pone las variables locales en la pila

Función que retorna:

7. Resetea el previo marco de pila: %esp = %ebp, %ebp = (%ebp)
8. Vuelve a la dirección de retorno, %eip = 4(%esp)

Repaso de conceptos IIII

Marco de pila



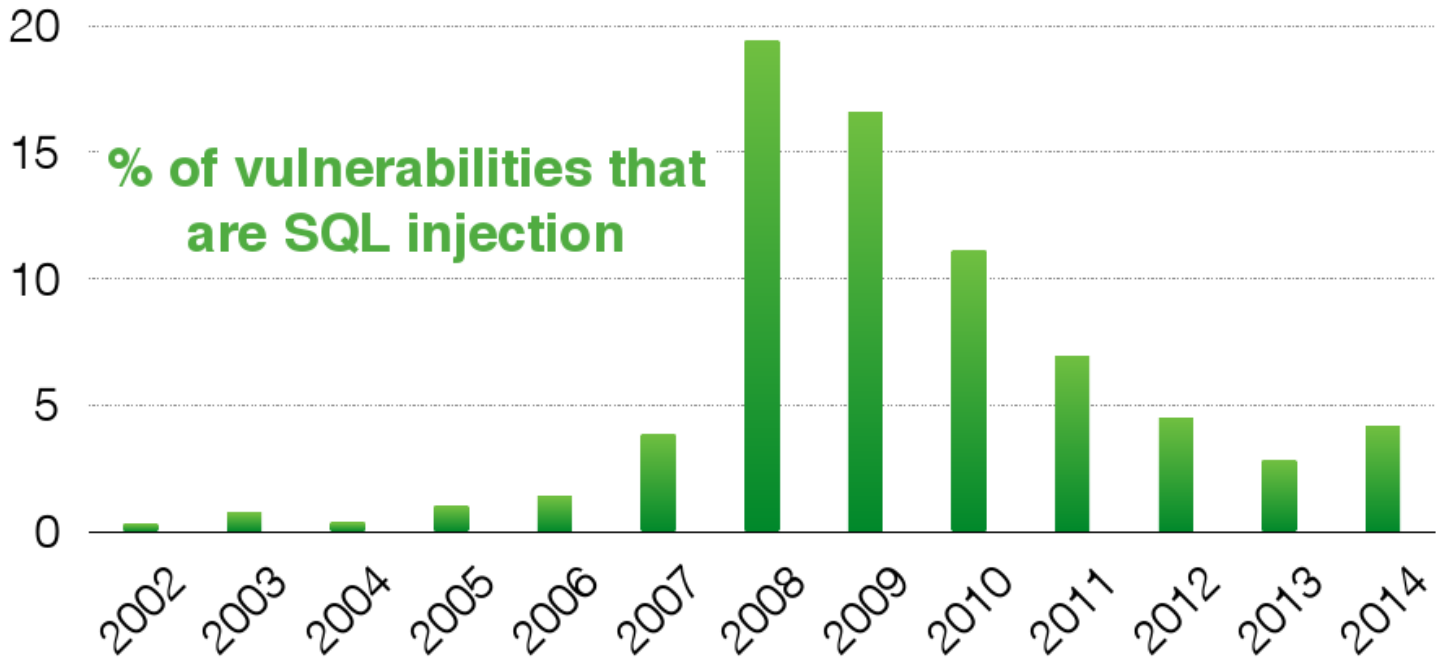

Hacker Attack!

SQL injection

Es una vulnerabilidad que se basa en aprovechar las características del propio lenguaje de consultas para inyectar código malicioso y obtener información o modificar una base de datos SQL.

Importancia

Casi cualquier sistema en producción tiene una base de dato accesible desde el exterior.



Repaso de conceptos I

En una petición de un recurso php, al final de la URL se añade ? y se modifican variables del script directamente.

Repaso de conceptos II

Nombre	Email	Password
Admin	admin@ugr.es	admin
Antonio	antonio@correo.ugr.es	123456
Adrián	adrian@correo.ugr.es	password

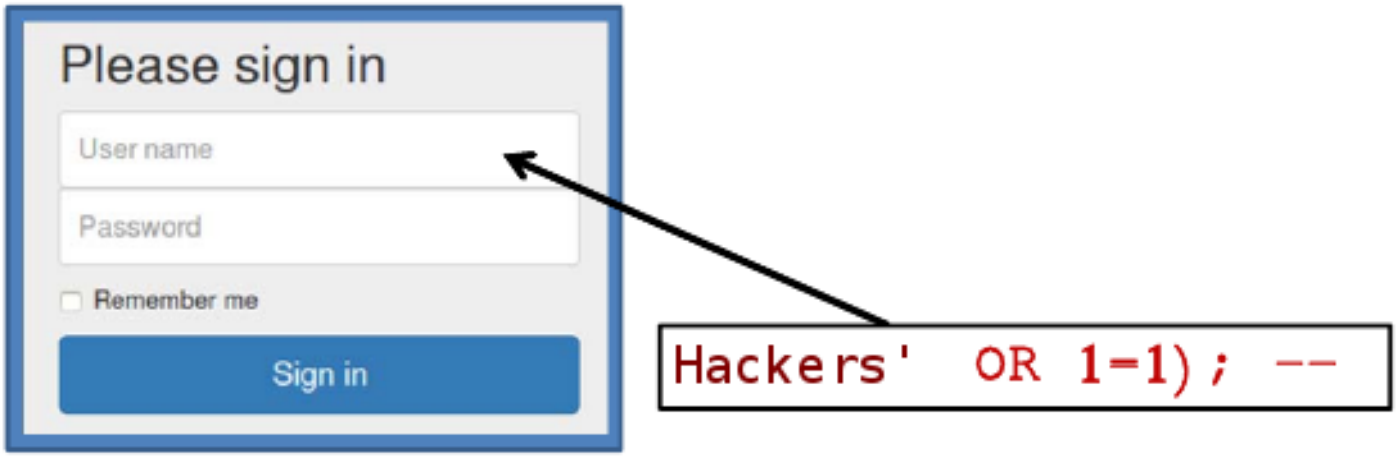
```
SELECT email FROM usuarios WHERE nombre='Antonio'; -- comentario

UPDATE usuarios SET email='adrian2@correo.ugr.es' WHERE nombre='Adrián';

INSERT INTO usuarios VALUES('Alejandro','alejandro@correo.ugr.es','alex');

DROP TABLE usuarios;
```

Repaso de conceptos III

Muchos login están implementados con PHP+MySQL, y en el código de la aplicación web nos encontramos sentencias PHP de la forma


```
$result = mysql_query("select * from users
          where(name='$user' and password='$pass');");
```

Repaso de conceptos IV




```
$result = mysql_query("select * from users
          where(name='Hackers' OR 1=1); -- and
          password='$pass');");
```


Hacker Attack!