

www.vip.com

API规范中的故事

宋浩

唯品会
vip.com
一家专门做特卖的网站

A collage of various programming language logos and symbols. The logos include: a green snake with blocks (Python), a cat face (JavaScript), a blue circle with 'Lua', Microsoft ASP.NET, a red gem (Ruby), a yellow triangle with a plus sign (C++), a blue square with 'CF', a blue and yellow Python logo, C#, a red lightning bolt (Scala), a blue oval with 'php', a blue and orange 3D shape (MATLAB), BASH in yellow, a black lambda symbol, Java with a coffee cup, a black lambda symbol, a blue square with a white 'X' (Xt), a blue circle with a flame (Erlang), a red 'E' (Erlang), a black rooster (Perl), and Self.

常见Web语言：

ASP

PHP

.NET → C#

J2EE → JAVA

.....

API规范理解或使用不当造成的安全问题：

SQL注入

OGNL注入（RCE）

对象反序列化安全

反射机制(权限绕过)

一、SQL注入:

外部参数污染执行的SQL语句

伪代码:

`select * from user where id = +外部参数`

JDBC API:

Statement、PreparedStatement...

SQL预编译方式:

安全、性能高效、代码可阅读性强

JDBC伪代码（错误理解）：

```
conn.prepareStatement("select * from  
user where id = "+外部参数)
```


JDBC伪代码(正确使用占位符方式):

PreparedStatement

```
ps=conn.prepareStatement("select *  
from user where id =?");
```

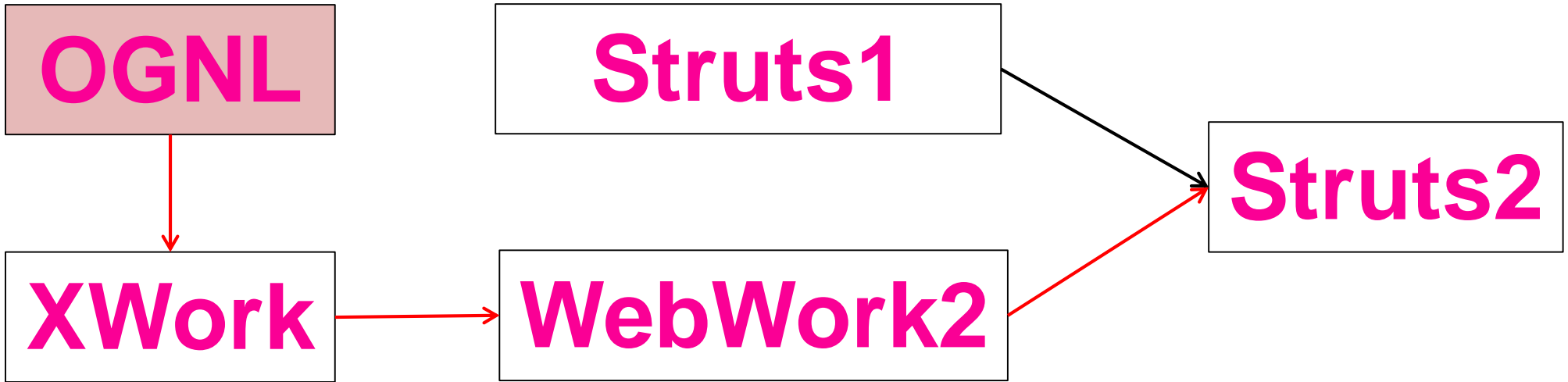
```
ps.setInt(1, 外部参数);
```

二、OGNL注入（RCE）：

OGNL是Object-Graph Navigation Language的缩写，对象图导航语言。

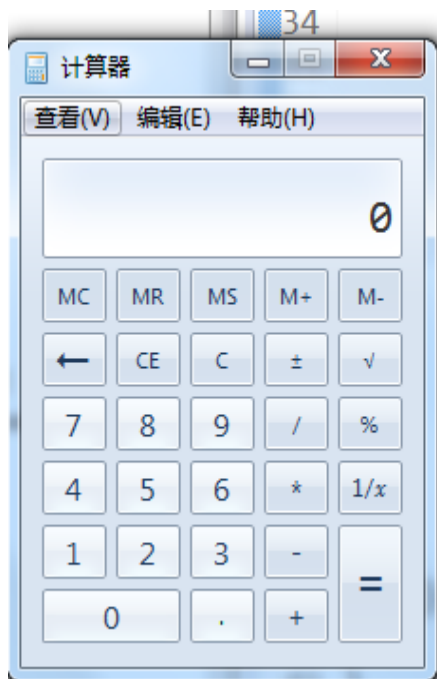
敏感设计：方法调用、**new**对象等

Struts2 OGNL RCE(CVE-2010-1870):



OGNL表达式支持的代码规范:

十六进制Unicode: # \longrightarrow \u0023

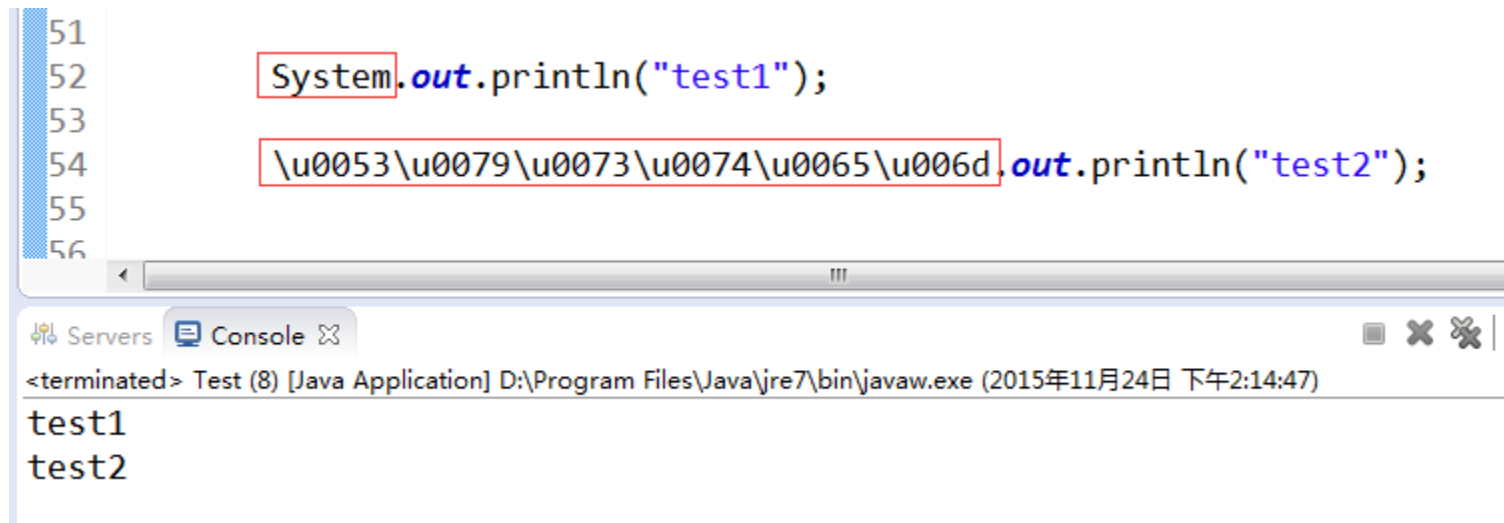


```
Ognl.setValue(new java.lang.ProcessBuilder((new java.lang.String[] {"calc"})).start(),
```

```
//Ognl.getValue("@java.lang.Runtime@getRuntime().exec('calc')", context, context.getRoot
```

```
Ognl.getValue("\u0040\u006a\u0061\u0076\u0061\u006e\u006c\u0061\u006e\u0074\u0020\u0061\u006e\u0063\u0061\u0020\u0028\u0029\u002e\u002e\u0065\u0078\u0065\u0063\u0028\u0027\u0063\u0061\u006c\u0063\u0027\u0029",
```

Java编译器支持的代码规范:



The screenshot shows an IDE window with a code editor and a console. The code editor contains two lines of Java code: `System.out.println("test1");` on line 52 and `\u0053\u0079\u0073\u0074\u0065\u006d.out.println("test2");` on line 54. The `System` and `out` identifiers are highlighted with red boxes. The console window, titled "Console", shows the output of the program: `<terminated> Test (8) [Java Application] D:\Program Files\Java\jre7\bin\javaw.exe (2015年11月24日 下午2:14:47)` followed by `test1` and `test2` on separate lines.

```
51
52     System.out.println("test1");
53
54     \u0053\u0079\u0073\u0074\u0065\u006d.out.println("test2");
55
56
```

Servers Console

<terminated> Test (8) [Java Application] D:\Program Files\Java\jre7\bin\javaw.exe (2015年11月24日 下午2:14:47)

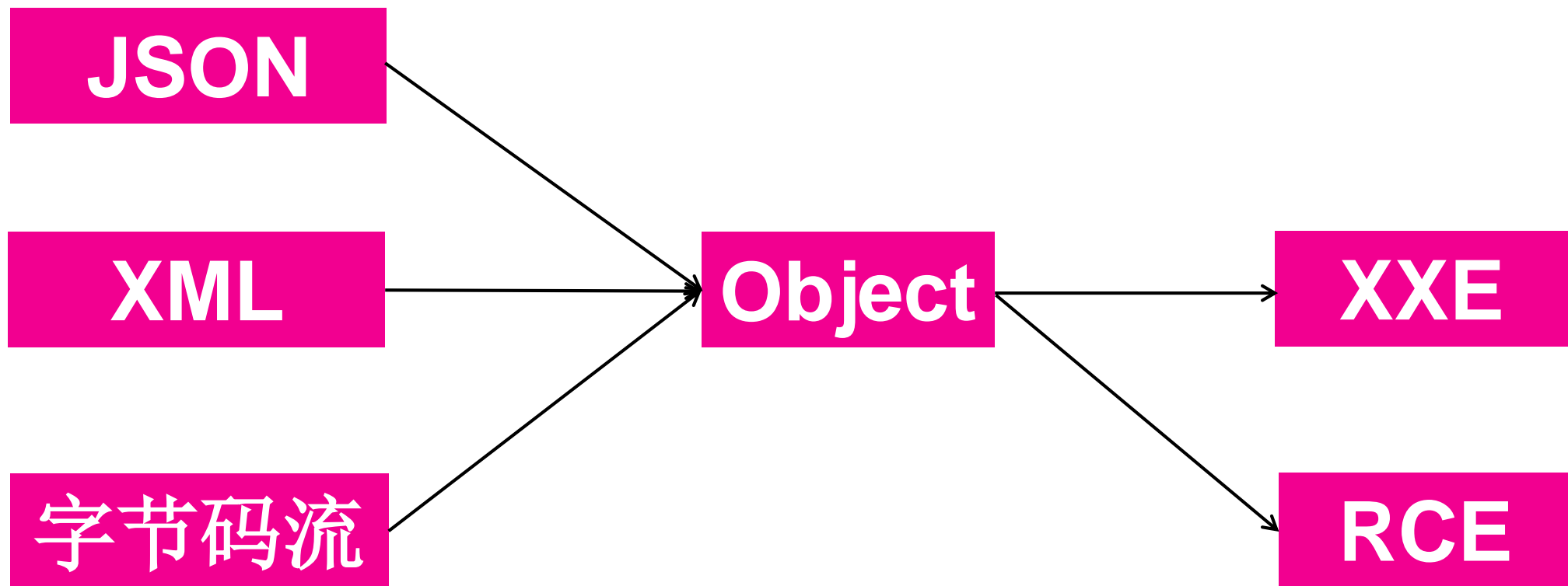
test1

test2

三、对象反序列化安全：

不同格式的对象存储状态转换成对象的过程中产生的安全问题。

对象反序列化常见场景（**JAVA**示例）：



四、反射机制(权限绕过)（**JAVA**示例）：

Java安全规范：Private修饰的属性（Field）、方法（Method），只有当前类能够访问。

但这是假象！

反射机制（Reflection）：

程序可以访问、检测和修改它本身状态或行为的一种能力。

反射API:

getField只能获取类的public属性

getDeclaredField获取一个类的所有属性

field.setAccessible(true);取消访问检查

getMethods获取所有**public**方法，包括其继承类的**public**方法。

getDeclaredMethods获取所有（**Private**）方法，但不包括继承的方法。

框架功能 缺陷



动态方法调用：
Struts2:s2-019
表单绑定功能：
Spring:cve-2010-1622
Struts2:s2-021

沙盒环境 缺陷



敏感类创建、方法调
用、属性值修改

唯品会
vip.com
一家专门做特卖的网站

Thanks !

www.vip.com