An Empirical Study of JVMs' Behaviors on Erroneous JNI Interoperations

Sungjae Hwang
College of Computing and Informatics
SKKU
Suwon, South Korea
sungjaeh@skku.edu

Sungho Lee
Dept. Computer Science and Engineering
CNU
Daejeon, South Korea
eshaj@cnu.ac.kr

Sukyoung Ryu
School of Computing
KAIST
Daejeon, South Korea
sryu.cs@kaist.ac.kr

February 3, 2023

1 Segmentation Faults

1.1 Type Check

Use reflection with ill-typed objects

Description	Call `FromReflectedMethod` or `FromReflectedField` with an object that is not `java.lang.reflect.Method` nor `java.lang.reflect.Constructor` as the second argument
Example	`FromReflectedMethod(JNIEnv*@!isNULLEnv, jobject@isGlobal0 && isLoader0 && !isDeleted0 && !isLocal0 && !isNULL0 && !isReflectConstructor0 && !isReflectField0 && !isReflectMethod0 && !isSubClass0)`

Store strings into invalid buffers

Description	Store translated UTF-8 encoded characters into an invalid buffer given as the last argument of `GetStringUTFRegion`
Example	`GetStringUTFRegion(JNIEnv*@!isNULLEnv, jstring@!isNULLS, jsize@!isNegativeE && !isPositiveE && !isValidIndexE && !isZeorE, jsize@isPositiveE && isValidIndexE, char*@!isNULLC)`

1.2 `NULL` Check

Call methods with NULL arguments

Description	Call Java methods via `Call<type>MethodA`, `CallNonvirtual<type>MethodA`, and `CallStatic<type>methodA` with `NULL` as the last argument
Example	`CallBooleanMethodA(JNIEnv*@!isNULLEnv, jobject@!isNULL0, jmethodID@isInThisClassM && isJBooleanM && isPrivateM && !isStaticM, jvalue*@isNULLJV && !isArrayPtrJV)`

Access fields using a `NULL` field ID

Description	Get/Set Java fields with a `NULL` field ID (`jfieldID`)
Example	`GetStaticBooleanField(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, jfieldID@isNULLF && !isStaticF)`

Get field/method IDs using a `NULL` signature

Description	Get field/method IDs using a `NULL` field signature given as the last argument for `GetFieldID`, `GetStaticFieldID`, `GetMethodID` and `GetStaticMethodID`
Example	`GetFieldID(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, char*@isFieldNameC && isUTF8C && !isNULLC, char*@isNULLC)`

Get field/method IDs and classes from a `NULL` object

Description	Get field/method IDs and classes from a `NULL` object by passing passing `NULL` as the second argument of `GetObjectClass`, for example
Example	`GetObjectClass(JNIEnv*@!isNULLEnv, jobject@isNULLO && !isDeletedO && !isGlobalO && !isLoaderO && !isLocalO && !isReflectConstructorO && !isReflectFieldO && !isReflectMethodO && !isSubClassO)`

Get strings into a `NULL` destination buffer

Description	Store strings into a `NULL` buffer by passing `NULL` as the last argument of `GetStringRegion`, for example
Example	`GetStringRegion(JNIEnv*@!isNULLEnv, jstring@!isNULLS, jsize@isValidIndexE, jsize@isNegativeE && isPositiveE && isValidIndexE && !isZeorE, jchar*@isNULLJC && !isGetCharArrayElementsJC && !isGetStringCharsJC && !isGetStringCriticalJC && !isThisCharArray && !isUnicodeJC)`

Get field/method IDs from a `NULL` name

Description	Get field/method IDs from a `NULL` name by passing `NULL` as the third argument of `GetFieldID`, for example
Example	`GetFieldID(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, char*@isNULLC && !isArrayClassSigC && !isClassSigC && !isEndWithBC && !isEndWithCC && !isEndWithDC && !isEndWithFC && !isEndWithIC && !isEndWithJC && !isEndWithLC && !isEndWithSC && !isEndWithVC && !isEndWithZC && !isFieldNameC && !isFieldSigC && !isGetStringUTFCharC && !isInitC && !isMethodNameC && !isMethodSigC && !isUTF8C, char*@isFieldSigC && isUTF8C && !isNULLC)`

Call methods using a `NULL JNIEnv` object

Description	Call JNI functions using a `NULL JNIEnv` object
Example	`GetBooleanArrayElements(JNIEnv*@isNULLEnv, jbooleanArray@!isNULLJZA, jboolean*@isNULLJB)`

Construct a new array using a `NULL` class

Description	Construct a new array from a `NULL` class by passing `NULL` as the third argument of `NewObjectArray`, for example
Example	`NewObjectArray(JNIEnv*@!isNULLEnv, jsize@isPositiveE && isZeorE, jclass@isNULLCL && !isArrayCL && !isContainMethod && !isObjectCL && !isThrowableCL, jobject@isNULLO)`

Construct a new object using `NULL` arguments

Description	Construct a new object from `NULL` arguments by passing `NULL` as the fourth argument of `NewObjectA`, for example
Example	`NewObjectA(JNIEnv*@!isNULLEnv, jclass@!isArrayCL && !isNULLCL, jmethodID@isInitM, jvalue*@isNULLJV && !isArrayPtrJV)`

Get Java VM interfaces from a `NULL` pointer

Description	Get a Java VM interface (used in the `Invocation` API) from a `NULL` pointer by passing `NULL` as the second argument of `GetJavaVM`, for example
Example	`GetJavaVM(JNIEnv*@!isNULLEnv, JavaVM*@isNULLJVM)`

Get modules from a `NULL` class

Description	Get a `java.lang.Module` object from a `NULL` class by passing `NULL` as the second argument of `GetModule`, for example
Example	`GetModule(JNIEnv*@!isNULLEnv, jclass@isNULLCL && !isArrayCL && !isContainMethod && !isObjectCL && !isThrowableCL)`

Register a `NULL` native method

Description	Register native methods using a `NULL JNINativeMethod` by passing `NULL` as the third argument of `RegisterNatives`, for example
Example	`RegisterNatives(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, JNINativeMethod*@isNULLNMD, jint@isPositiveJI)`

Register native methods with a `NULL` class

Description	Register native methods using a `NULL` class by passing `NULL` as the second argument of `RegisterNatives`, for example
Example	`RegisterNatives(JNIEnv*@!isNULLEnv, jclass@isNULLCL && !isArrayCL && !isContainMethod && !isObjectCL && !isThrowableCL, JNINativeMethod*@!isNULLNMD, jint@isPositiveJI)`

Store strings into a `NULL` buffer

Description	Store strings into a `NULL` buffer by passing `NULL` as the last argument of `GetStringUTFRegion`, for example
Example	`GetStringUTFRegion(JNIEnv*@!isNULLEnv, jstring@!isNULLS, jsize@isValidIndexE, jsize@isValidIndexE && !isNegativeE && !isPositiveE && !isZeorE, char*@isNULLC )`

Unregister native methods from a NULL class

Description	Unregister native methods from a NULL class by passing NULL as the second argument of UnregisterNatives, for example
Example	`UnregisterNatives(JNIEnv*@!isNULLEnv, jclass@isNULLCL && !isArrayCL && !isContainMethod && !isObjectCL && !isThrowableCL)`

Use reflection with a NULL field ID

Description	Convert NULL to a java.lang.reflect.Field object
Example	`ToReflectedField(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, jfieldID@isNULLF && !isStaticF, jboolean@!isFalse && !isTrue)`

1.3 Releasability Check

Release unreleasable array elements

Description	Release array elements not derived from Get<PrimitiveType>ArrayElements()
Example	`ReleaseCharArrayElements(JNIEnv*@!isNULLEnv, jcharArray@!isNULLJCA, jchar*@isGetStringCharsJC && isThisCharArray && isUnicodeJC && !isGetCharArrayElementsJC && !isGetStringCriticalJC && !isNULLJC, jint@isJNI_ABORTJI)`

1.4 Modifier Check

Use incorrect modifier flags

Description	Use JNI_TRUE when using a non-static field ID via ToReflectedField
Example	`ToReflectedField(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, jfieldID@!isNULLF && !isStaticF, jboolean@isTrue && !isFalse)`

1.5 Size Check

Access out-of-bound array elements

Description	Access array elements with out-of-bound indices
Example	`SetDoubleArrayRegion(JNIEnv*@!isNULLEnv, jdoubleArray@!isNULLJDA, jsize@isValidIndexE, jsize@isPositiveE && isZeorE && !isNegativeE && !isValidIndexE, jdouble*@!isNULLJD)`

Use strings of incorrect lengths

Description	Call NewString with NULL as the second argument and a positive integer as the third argument
Example	`NewString(JNIEnv*@!isNULLEnv, jchar*@isNULLJC && !isGetCharArrayElementsJC && !isGetStringCharsJC && !isGetStringCriticalJC && !isThisCharArray && !isUnicodeJC, jsize@isPositiveE && isValidIndexE && !isNegativeE && !isZeorE)`

1.6 Compatibility Check

Call unsupported JNI functions

Description	Call `DefineClass` on Android
Example	`DefineClass(JNIEnv*@isNULLEnv, char*@isNULLC && isUTF8C, jobject@isLoader0 && isNULL0, jbyte*@isBytePointerClassInfo && !isNULLB, jsize@isValidIndexE)`

Use Java bytecode or class files

Description	Call Java bytecode methods on Android
Example	`ReleaseByteArrayElements(JNIEnv*@!isNULLEnv, jbyteArray@!isNULLJBA, jbyte*@isBytePointerClassInfo && isThisByteArray && !isGetByteArrayElements && !isNULLB, jint@isJNI_ABORTJI)`

2 Differences of the Debug Option among JVMs

2.1 Type Check

Define classes with ill-typed classloaders

Description	Pass a non-classloader object as the third argument of `DefineClass`
Example	`DefineClass(JNIEnv*@!isNULLEnv, char*@isUTF8C && !isNULLC, jobject@isLocal0 && isSubClass0 && !isDeleted0 && !isGlobal0 && !isLoader0 && !isNULL0 && !isReflectConstructor0 && !isReflectField0 && !isReflectMethod0, jbyte*@isBytePointerClassInfo && !isNULLB, jsize@isValidIndexE)`

Call methods with unmatched return types

Description	Call Java methods returning `void` via `CallLongMethodV`
Example	`CallLongMethodV(JNIEnv*@!isNULLEnv, jobject@!isNULL0, jmethodID@isInThisClassM && isInitM && !isInThisOrSuperClasesM && !isJBooleanM && !isJByteM && !isJCharM && !isJDoubleM && !isJFloatM && !isJIntM && !isJLongM && !isJObjectM && !isJShortM && !isNULLM && !isPrivateM && !isStaticM && !isVoidM, va_list)`

Create objects with array classes

Description	Pass an array class as the second argument of `NewObject`
Example	`NewObject(JNIEnv*@!isNULLEnv, jclass@isArrayCL && isContainMethod && isObjectCL && !isNULLCL && !isThrowableCL, jmethodID@isInitM, ...)`

Use reflection for fields with ill-typed objects

Description	Call `FromReflectedField` with an object that is not `java.lang.reflect.Method` nor `java.lang.reflect.Constructor` as the second argument
Example	`FromReflectedField(JNIEnv*@!isNULLEnv, jobject@isGlobal0 && isLoader0 && isSubClass0 && !isDeleted0 && !isLocal0 && !isNULL0 && !isReflectConstructor0 && !isReflectField0 && !isReflectMethod0)`

Allocate objects using array classes

Description	Allocate a new Java object with an array class without invoking any constructors
Example	`AllocObject(JNIEnv*@!isNULLEnv, jclass@isArrayCL && isContainMethod && isObjectCL && !isNULLCL && !isThrowableCL)`

Call methods with ill-typed method IDs

Description	Invoke a private method with a receiver object that does not contain the specified private method
Example	`CallLongMethodV(JNIEnv*@!isNULLEnv, jobject@!isNULLO, jmethodID@isJLongM && isPrivateM && !isInThisClassM && !isInThisOrSuperClasesM && !isInitM && !isJBooleanM && !isJByteM && !isJCharM && !isJDoubleM && !isJFloatM && !isJIntM && !isJObjectM && !isJShortM && !isNULLM && !isStaticM && !isVoidM, va_list)`

Get method IDs of non-existent methods

Description	Get a non-existent Java method
Example	`GetMethodID(JNIEnv*@!isNULLEnv, jclass@isContainMethod && !isNULLCL, char*@isClassSigC && isEndWithCC && isGetStringUTFCharC && isUTF8C && !isArrayClassSigC && !isEndWithBC && !isEndWithDC && !isEndWithFC && !isEndWithIC && !isEndWithJC && !isEndWithLC && !isEndWithSC && !isEndWithVC && !isEndWithZC && !isFieldNameC && !isFieldSigC && !isInitC && !isMethodNameC && !isMethodSigC && !isNULLC, char*@isUTF8C && !isArrayClassSigC && !isClassSigC && !isEndWithBC && !isEndWithCC && !isEndWithDC && !isEndWithFC && !isEndWithIC && !isEndWithJC && !isEndWithLC && !isEndWithSC && !isEndWithVC && !isEndWithZC && !isFieldNameC && !isFieldSigC && !isGetStringUTFCharC && !isInitC && !isMethodNameC && !isMethodSigC && !isNULLC)`

Use reflection for methods with ill-typed objects

Description	Call `FromReflectedMethod` with an object that is not `java.lang.reflect.Method` nor `java.lang.reflect.Constructor` as the second argument
Example	`FromReflectedMethod(JNIEnv*@!isNULLEnv, jobject@isGlobalO && isLoaderO && isSubClassO && !isDeletedO && !isLocalO && !isNULLO && !isReflectConstructorO && !isReflectFieldO && !isReflectMethodO)`

2.2 `NULL` Check

Call methods with `NULL` arguments

Description	Call Java methods via `Call<type>MethodA`, `CallNonvirtual<type>MethodA`, and `CallStatic<type>methodA` with `NULL` as the last argument
Example	`CallByteMethodA(JNIEnv*@!isNULLEnv, jobject@!isNULLO, jmethodID@isInThisClassM && isJByteM && isPrivateM && !isStaticM, jvalue*@isNULLJV && !isArrayPtrJV)`

Access fields using a `NULL` field ID

Description	Get/Set Java fields with a `NULL` field ID (`jfieldID`)
Example	`GetStaticByteField(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, jfieldID@isNULLF && !isStaticF)`

Get field/method IDs using a `NULL` signature

Description	Get field/method IDs using a `NULL` field signature given as the last argument for `GetFieldID`, `GetStaticFieldID`, `GetMethodID` and `GetStaticMethodID`
Example	`GetStaticMethodID(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, char*@isMethodNameC && isUTF8C && !isNULLC, char*@isNULLC && !isArrayClassSigC && !isClassSigC && !isEndWithBC && !isEndWithCC && !isEndWithDC && !isEndWithFC && !isEndWithIC && !isEndWithJC && !isEndWithLC && !isEndWithSC && !isEndWithVC && !isEndWithZC && !isFieldNameC && !isFieldSigC && !isGetStringUTFCharC && !isInitC && !isMethodNameC && !isMethodSigC && !isUTF8C)`

Get field/method IDs and classes from a `NULL` object

Description	Get field/method IDs and classes from a `NULL` object by passing passing `NULL` as the second argument of `GetObjectClass`, for example
Example	`GetObjectClass(JNIEnv*@!isNULLEnv, jobject@isNULLO && !isDeletedO && !isGlobalO && !isLoaderO && !isLocalO && !isReflectConstructorO && !isReflectFieldO && !isReflectMethodO && !isSubClassO)`

Get field/method IDs from a `NULL` name

Description	Get field/method IDs from a `NULL` name by passing `NULL` as the third argument of `GetFieldID`, for example
Example	`GetStaticMethodID(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, char*@isNULLC && !isArrayClassSigC && !isClassSigC && !isEndWithBC && !isEndWithCC && !isEndWithDC && !isEndWithFC && !isEndWithIC && !isEndWithJC && !isEndWithLC && !isEndWithSC && !isEndWithVC && !isEndWithZC && !isFieldNameC && !isFieldSigC && !isGetStringUTFCharC && !isInitC && !isMethodNameC && !isMethodSigC && !isUTF8C, char*@isEndWithZC && isMethodSigC && isUTF8C && !isNULLC)`

Call methods using a `NULL JNIEnv` object

Description	Call JNI functions using a `NULL JNIEnv` object
Example	`GetVersion(JNIEnv*@isNULLEnv)`

Get Java VM interfaces from a `NULL` pointer

Description	Get a Java VM interface (used in the `Invocation` API) from a `NULL` pointer by passing `NULL` as the second argument of `GetJavaVM`, for example
Example	`GetJavaVM(JNIEnv*@!isNULLEnv, JavaVM*@isNULLJVM)`

Register a `NULL` native method

Description	Register native methods using a `NULL JNINativeMethod` by passing `NULL` as the third argument of `RegisterNatives`, for example
Example	`RegisterNatives(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, JNINativeMethod*@isNULLNMD, jint@isPositiveJI)`

Register native methods with a `NULL` class

Description	Register native methods using a `NULL` class by passing `NULL` as the second argument of `RegisterNatives`, for example
Example	`RegisterNatives(JNIEnv*@!isNULLEnv, jclass@isNULLCL && !isArrayCL && !isContainMethod && !isObjectCL && !isThrowableCL, JNINativeMethod*@!isNULLNMD, jint@isPositiveJI)`

Store strings into a `NULL` buffer

Description	Store strings into a `NULL` buffer by passing `NULL` as the last argument of `GetStringUTFRegion`, for example
Example	`GetStringRegion(JNIEnv*@!isNULLEnv, jstring@!isNULLS, jsize@isValidIndexE, jsize@isPositiveE && isValidIndexE && !isNegativeE && !isZeorE, jchar*@isNULLJC && !isGetCharArrayElementsJC && !isGetStringCharsJC && !isGetStringCriticalJC && !isThisCharArray && !isUnicodeJC)`

Unregister native methods from a `NULL` class

Description	Unregister native methods from a `NULL` class by passing `NULL` as the second argument of `UnregisterNatives`, for example
Example	`UnregisterNatives(JNIEnv*@!isNULLEnv, jclass@isNULLCL && !isArrayCL && !isContainMethod && !isObjectCL && !isThrowableCL)`

Call methods of a `NULL` object

Description	Call Java methods with a `NULL` receiver object
Example	`CallByteMethodA(JNIEnv*@!isNULLEnv, jobject@isNULLO && !isDeletedO && !isGlobalO && !isLoaderO && !isLocalO && !isReflectConstructorO && !isReflectFieldO && !isReflectMethodO && !isSubClassO, jmethodID@isInThisClassM && isJByteM && isPrivateM && !isStaticM, jvalue*@isArrayPtrJV)`

Release a `NULL` string

Description	Release a `NULL` string
Example	`ReleaseStringChars(JNIEnv*@!isNULLEnv, jstring@!isNULLS, jchar*@isNULLJC && !isGetCharArrayElementsJC && !isGetStringCharsJC && !isGetStringCriticalJC && !isThisCharArray && !isUnicodeJC)`

Construct new string objects using a `NULL` string

Description	Construct a new `java.lang.String` object from `NULL`
Example	`NewString(JNIEnv*@!isNULLEnv, jchar*@isNULLJC && !isGetCharArrayElementsJC && !isGetStringCharsJC && !isGetStringCriticalJC && !isThisCharArray && !isUnicodeJC, jsize@isPositiveE && isValidIndexE && !isNegativeE && !isZeorE)`

Create objects with a `NULL` argument

Description	Construct a new object from a `NULL` argument
Example	`NewObjectA(JNIEnv*@!isNULLEnv, jclass@!isArrayCL && !isNULLCL, jmethodID@isInitM, jvalue*@isNULLJV && !isArrayPtrJV)`

Define classes with a `NULL` classloader

Description	Pass `NULL` as the third argument of `DefineClass`
Example	`DefineClass(JNIEnv*@!isNULLEnv, char*@isUTF8C && !isNULLC, jobject@isLoaderO && isNULLO, jbyte*@isBytePointerClassInfo && !isNULLB, jsize@isNegativeE && isPositiveE && !isValidIndexE && !isZeorE)`

Define classes with a `NULL` class name

Description	Pass `NULL` as the second argument of `DefineClass`
Example	`DefineClass(JNIEnv*@!isNULLEnv, char*@isNULLC && isUTF8C, jobject@isLoaderO && !isNULLO, jbyte*@isBytePointerClassInfo && !isNULLB, jsize@isNegativeE && isPositiveE && !isValidIndexE && !isZeorE)`

Load classes with a `NULL` name

Description	Pass `NULL` as the second argument of `FindClass`
Example	`FindClass(JNIEnv*@!isNULLEnv, char*@isNULLC && !isArrayClassSigC && !isClassSigC && !isEndWithBC && !isEndWithCC && !isEndWithDC && !isEndWithFC && !isEndWithIC && !isEndWithJC && !isEndWithLC && !isEndWithSC && !isEndWithVC && !isEndWithZC && !isFieldNameC && !isFieldSigC && !isGetStringUTFCharC && !isInitC && !isMethodNameC && !isMethodSigC && !isUTF8C)`

Get reflection objects from a `NULL` field ID

Description	Convert `NULL` to a `java.lang.reflect.Field object`
Example	`ToReflectedField(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, jfieldID@isNULLF && !isStaticF, jboolean@isFalse && isTrue)`

2.3 Releasability Check

Release unreleasable array elements

Description	Release array elements not derived from `Get<PrimitiveType>ArrayElements`
Example	`ReleaseCharArrayElements(JNIEnv*@!isNULLEnv, jcharArray@!isNULLJCA, jchar*@isGetCharArrayElementsJC && isUnicodeJC && !isGetStringCharsJC && !isGetStringCriticalJC && !isNULLJC && !isThisCharArray, jint@isZeroJI)`

Release unreleasable strings

Description	Release strings not derived from `GetStringChars`
Example	`ReleaseStringChars(JNIEnv*@!isNULLEnv, jstring@!isNULLS, jchar*@isUnicodeJC && !isGetCharArrayElementsJC && !isGetStringCharsJC && !isGetStringCriticalJC && !isNULLJC && !isThisCharArray)`

2.4 Modifier Check

Access non-static fields with a static field ID

Description	Use a static field ID when accessing a non-static field
Example	`ToReflectedField(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, jfieldID@isStaticF && !isNULLF, jboolean@isFalse && !isTrue)`

Access static fields with a non-static field ID

Description	Use a non-static field ID when accessing a static field
Example	`ToReflectedField(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, jfieldID@!isNULLF && !isStaticF, jboolean@!isFalse && !isTrue)`

2.5 Size Check

Set capacities of local frames negative

Description	Pass a negative integer as the second argument of `EnsureLocalCapacity`
Example	`EnsureLocalCapacity(JNIEnv*@!isNULLEnv, jint@isNegativeJI && !isJNI_ABORTJI && !isJNI_COMMITJI && !isPositiveJI && !isThisArrayLenJI && !isZeroJI)`

Copy negative indices of strings

Description	Pass a negative integer as the third argument of `GetStringRegion`
Example	`GetStringRegion(JNIEnv*@!isNULLEnv, jstring@!isNULLS, jsize@isNegativeE && !isPositiveE && !isZeorE && !isValidIndexE, jsize@isPositiveE && isValidIndexE, jchar*@!isNULLJC)`

Create local frames with negative capacities

Description	Pass a negative integer as the second argument of `PushLocalFrame`
Example	`PushLocalFrame(JNIEnv*@!isNULLEnv, jint@isNegativeJI && !isJNI_ABORTJI && !isJNI_COMMITJI && !isPositiveJI && !isThisArrayLenJI && !isZeroJI)`

Create local frames with the zero capacity

Description	Pass zero as the second argument of `PushLocalFrame`
Example	`PushLocalFrame(JNIEnv*@!isNULLEnv, jint@isThisArrayLenJI && isZeroJI && !isJNI_ABORTJI && !isJNI_COMMITJI && !isNegativeJI && !isPositiveJI)`

Create arrays with negative sizes

Description	Pass a negative integer as the second argument of `NewCharArray`
Example	`NewCharArray(JNIEnv*@!isNULLEnv, jsize@isNegativeE && isPositiveE && isValidIndexE && !isZeorE)`

Get elements from negative-size arrays

Description	Pass a negative integer as the third argument of `GetObjectArrayElement`
Example	`GetObjectArrayElement(JNIEnv*@!isNULLEnv, jobjectArray@!isNULLJOA, jsize@isNegativeE && isPositiveE && isValidIndexE && !isZeorE)`

Register negative numbers of native functions

Description	Pass a negative integer as the fourth argument of `RegisterNatives`
Example	`RegisterNatives(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, JNINativeMethod*@!isNULLNMD, jint@isNegativeJI && !isJNI_ABORTJI && !isJNI_COMMITJI && !isPositiveJI && !isThisArrayLenJI && !isZeroJI)`

Register the zero number of native functions

Description	Pass zero as the fourth argument of `RegisterNatives`
Example	`RegisterNatives(JNIEnv*@!isNULLEnv, jclass@!isNULLCL, JNINativeMethod*@!isNULLNMD, jint@isThisArrayLenJI && isZeroJI && !isJNI_ABORTJI && !isJNI_COMMITJI && !isNegativeJI && !isPositiveJI)`

Set elements to negative-size arrays

Description	Pass a negative integer as the third argument of `SetIntArrayRegion`
Example	`SetIntArrayRegion(JNIEnv*@!isNULLEnv, jintArray@!isNULLJIA, jsize@isNegativeE && isPositiveE && isZeorE && !isValidIndexE, jsize@isValidIndexE, jint*@!isNULLJI)`

2.6 Liveness Check

Get types from deleted references

Description	Pass a deleted object as the second argument of `GetObjectRefType`
Example	`GetObjectRefType(JNIEnv*@!isNULLEnv, jobject@isDeletedO && isGlobalO && isReflectFieldO && isSubClassO && !isLoaderO && !isLocalO && !isNULLO && !isReflectConstructorO && !isReflectMethodO)`

Compare objects with deleted objects

Description	Pass a deleted object as the third argument of `IsSameObject`
Example	`IsSameObject(JNIEnv*@!isNULLEnv, jobject@isNULL0, jobject@isDeleted0 && isLoader0 && isLocal0 && isSubClass0 && !isGlobal0 && !isNULL0 && !isReflectConstructor0 && !isReflectField0 && !isReflectMethod0)`

Create references from deleted global reference objects

Description	Pass a deleted object as the second argument of `NewWeakGlobalRef`
Example	`NewWeakGlobalRef(JNIEnv*@!isNULLEnv, jobject@isDeleted0 && isLoader0 && isLocal0 && isSubClass0 && !isGlobal0 && !isNULL0 && !isReflectConstructor0 && !isReflectField0 && !isReflectMethod0)`

Create references from deleted local reference objects

Description	Pass a deleted object as the second argument of `NewLocalRef`
Example	`NewLocalRef(JNIEnv*@!isNULLEnv, jobject@isDeleted0 && isGlobal0 && isReflectMethod0 && isSubClass0 && !isLoader0 && !isLocal0 && !isNULL0 && !isReflectConstructor0 && !isReflectField0)`