

Wicket-Velocity-Modul-Hack

Meetup 14.12.2016 - Sergej

Wicket (Wystri Warrick)





- Java Web-Framework
- Komponentenbasiert
- Open-Source
- Ajax ohne JavaScript möglich
- Apache-Lizenz

Wicket Projekte

- ❖ <https://banking.postbank.de>



- ❖ <https://kunden.commerzbank.de>



- ❖ <https://banking.ing-diba.de>



Apache Velocity

- Template Engine
- Template Sprache
- Open-Source

Apache Velocity

Velocity Template:

```
## Velocity Hello World
<html>
  <body>
    #set( $foo = "Velocity" )
    ## followed by
    Hello $foo World!
  </body>
</html>
```

HTML Ausgabe:

```
<html>
  <body>
    Hello Velocity World!
  </body>
</html>
```

Apache Velocity Security

- <https://issues.apache.org/jira/browse/VELOCITY-179>
- VELOCITY-179 wurde am 30.05.2003 erstellt
- VELOCITY-179 wurde am 10.10.2006 behoben
- Minor Security Issue
- Der Zugriff auf den Java-Classloader ist möglich

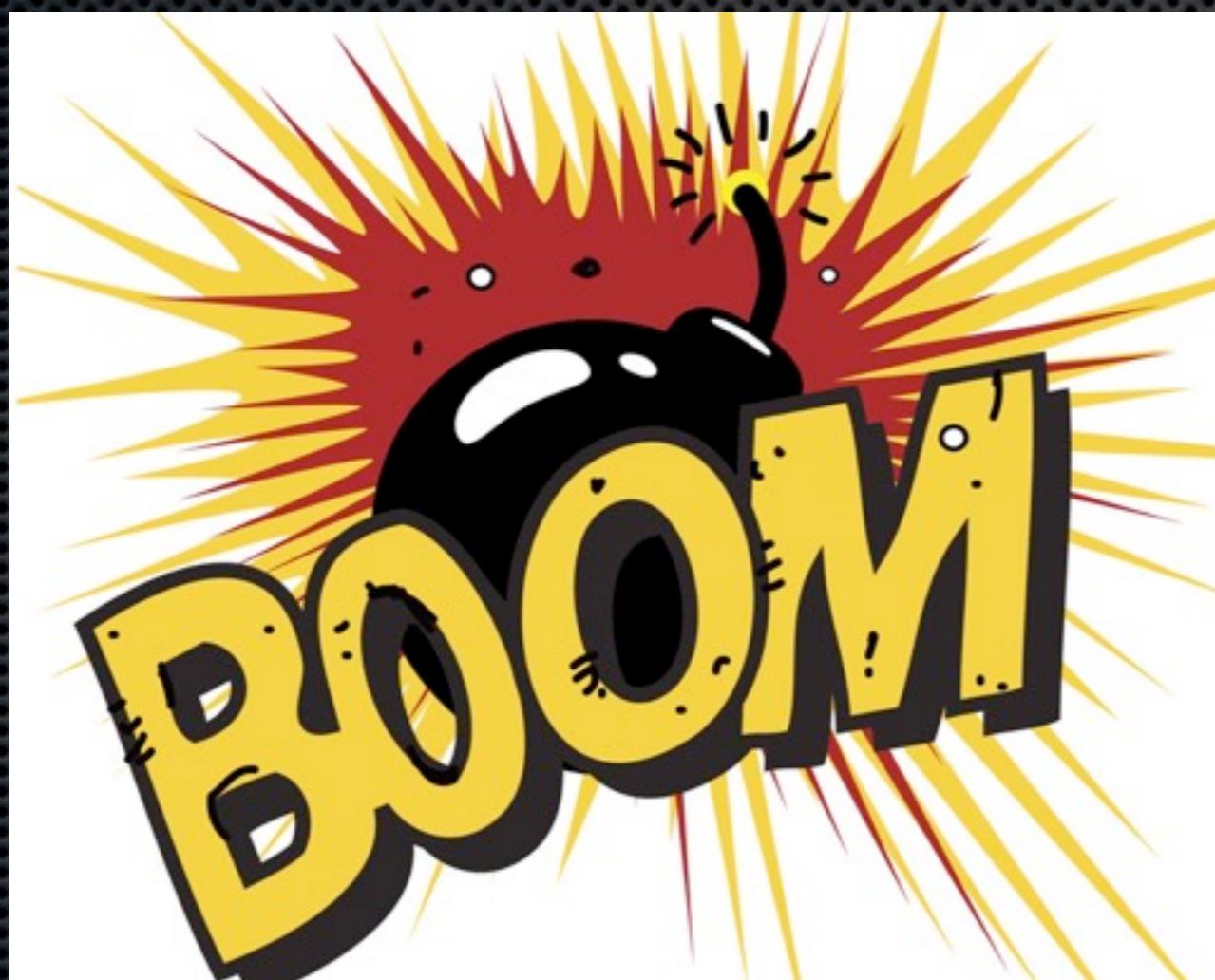
```
#set($myvar= "")  
$myvar.getClass().getClassLoader()
```

Apache Velocity Security

- Remote-Code-Execution ist möglich!

Apache Velocity Security

Mit anderen Worten:



Apache Velocity der Fix

- Den SecureUberspector verwenden
- Die Konfiguration erfolgt in der Datei velocity.properties

Apache Velocity das Aber

- Die Datei velocity.jar wird **nicht** mit der sicheren Konfiguration ausgeliefert
- Die Konfigurationsdatei ist in der Datei velocity.jar versteckt

src/java/org/apache/velocity/runtime/defaults/
velocity.properties



9 Jahre später ...

Apache Wicket Online Editor

The screenshot shows the Apache Wicket Online Editor interface. At the top, there's an orange header bar with the "APACHE WICKET examples" logo. Below it, a grey navigation bar has the word "velocity" in white. The main area is divided into two sections: "velocity template input" on the left and "output" on the right.

velocity template input:

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

output:

```
persons
• Down, Joe
• Frizel, Fritz
• Vlieger, Flip
• Forrest, George
• Hazel, Sue
• Gump, Bush
```

At the bottom left of the input section is a small "update" button.

Apache Wicket der Fix

- <https://issues.apache.org/jira/browse/WICKET-5927>
- Das Problem wurde sehr schnell behoben
- WICKET-5927 wurde am 19.06.2015 erstellt
- WICKET-5927 wurde am 20.06.2015 behoben
- Der Patch stand sehr schnell zur Verfügung

Apache Wicket das Aber

- Wicket wird **nicht** mit der sicheren Konfiguration ausgeliefert
- Es wird an keiner Stelle in der Dokumentation auf die Gefahr hingewiesen
- Alle Wicket Version sind immer noch betroffen



Apache Wicket Apocalypse

- Das Minor-Issue (VELOCITY-179) wird kritisch
- Manipulation der Binaries
- Banken könnten betroffen sein

Demo

Fragen?

- ???

Quellen

- Links:
 - <https://cwiki.apache.org/confluence/display/WICKET/Websites+based+on+Wicket>
- Bilder:
 - http://vignette4.wikia.nocookie.net/starwars/images/4/4f/Wicket_RotJ.png/revision/latest?cb=20130622101905
 - https://de.wikipedia.org/wiki/Apache_Wicket#/media/File:Apache_Wicket_Logo.png
 - https://www.postbank.de/postbank/docs/PB_Zentrale_sRGB.jpg
 - https://www.ing-diba.de/site/www.ing-diba.de-site/get/params_E1108065520/415717/ing_diba_logo_pos_rgb.jpg
 - http://www.ci-portal.de/wp-content/uploads/commerzbank_logo3.jpg
 - http://s3.hulkshare.com/song_images/original/a/9/9/a99052a0b5d22b0f4b8e1f96c40d3f75.jpg
 - <http://images.uncyclomedia.co/encyclopedia/en/thumb/c/c4/Triple-facepalm.jpg/536px-Triple-facepalm.jpg>