



中间件&Jboss

讲师：空白





学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：<https://edu.hetianlab.com/>

合天网安实验室：<https://www.hetianlab.com/>

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关



目录

CONTENTS



01

中间件介绍



02

war包介绍



03

Jboos后台部署war包



/01 中间件介绍



1.1 概念

中间件（英语：Middleware），又译中间件、中介层，是一类提供系统软件和应用软件之间连接、便于软件各部件之间的沟通的软件，应用软件可以借助中间件在不同的技术架构之间共享信息与资源。中间件位于客户机服务器的操作系统之上，管理着计算资源和网络通信。



1.2 常见的中间件

weblogic、webshere、tomcat、apache、jetty、jboss、nginx等等



1.2.1 weblogic

Error 404--Not Found

From RFC 2068 *Hypertext Transfer Protocol -- HTTP/1.1*:

10.4.5 404 Not Found

The server has not found anything matching the Request-URI. No indication is given of whether the condition is temporary or permanent.

If the server does not wish to make this information available to the client, the status code 403 (Forbidden) can be used instead. The 410 (Gone) status code SHOULD be used if the server knows, through some internally configurable mechanism, that an old resource is permanently unavailable and has no forwarding address.



1.2.2 jboss



JBoss Online Resources

- [Getting started with JBoss 3.2 \[PDF\]](#)
- [JBoss Wiki](#)
- [JBoss forums](#)

JBoss Management

- [Tomcat status \(full\) \(XML\)](#)
- [JMX Console](#)
- [JBoss Web Console](#)



1.2.3 tomcat

HTTP Status 404 -

type Status report

message

description The requested resource is not available.

Apache Tomcat/6.0.36



/02 war包介绍



2.1 概念

war包是Sun提出的一种web应用程序格式，与jar类似，是很多文件的压缩包。war包中的文件按照一定目录结构来组织。根据其根目录下包含有html和jsp文件，或者包含有这两种文件的目录，另外还有WEB-INF目录。通常在WEB-INF目录下含有一个web.xml文件和一个classes目录，web.xml是这个应用的配置文件，而classes目录下则包含编译好的servlet类和jsp，或者servlet所依赖的其他类（如JavaBean）



/03 Jboos后台部署war包



3.1 jboss

一个基于J2EE的开放源代码的应用服务器。JBoss是一个管理EJB的容器和服务，但JBoss核心服务不包括支持servlet/JSP的WEB容器，一般与Tomcat或Jetty绑定使用。Jboss是Java EE应用服务器（就像Apache是web服务器一样），专门用来运行Java EE程序的。



3.2 jboss历史漏洞

JMX Console未授权访问Getshell

JMX Console HtmlAdaptor Getshell (CVE-2007-1036)

JMX控制台安全验证绕过漏洞 (CVE-2010-0738)

Administration Console 弱口令 Getshell

JBoss JMXInvokerServlet 反序列化漏洞 (CVE-2015-7501)

JBoss EJBInvokerServlet 反序列化漏洞

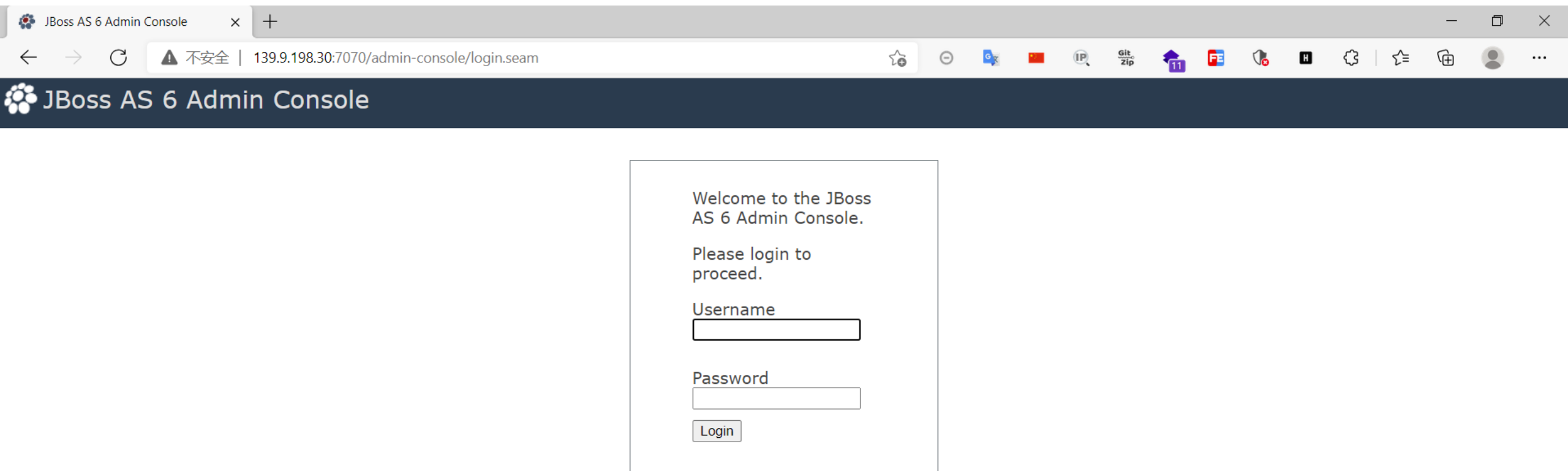
JBosS AS 6.X 反序列化漏洞 (CVE-2017-12149)

JBoss 4.x JBossMQ JMS 反序列化漏洞 (CVE-2017-7504)



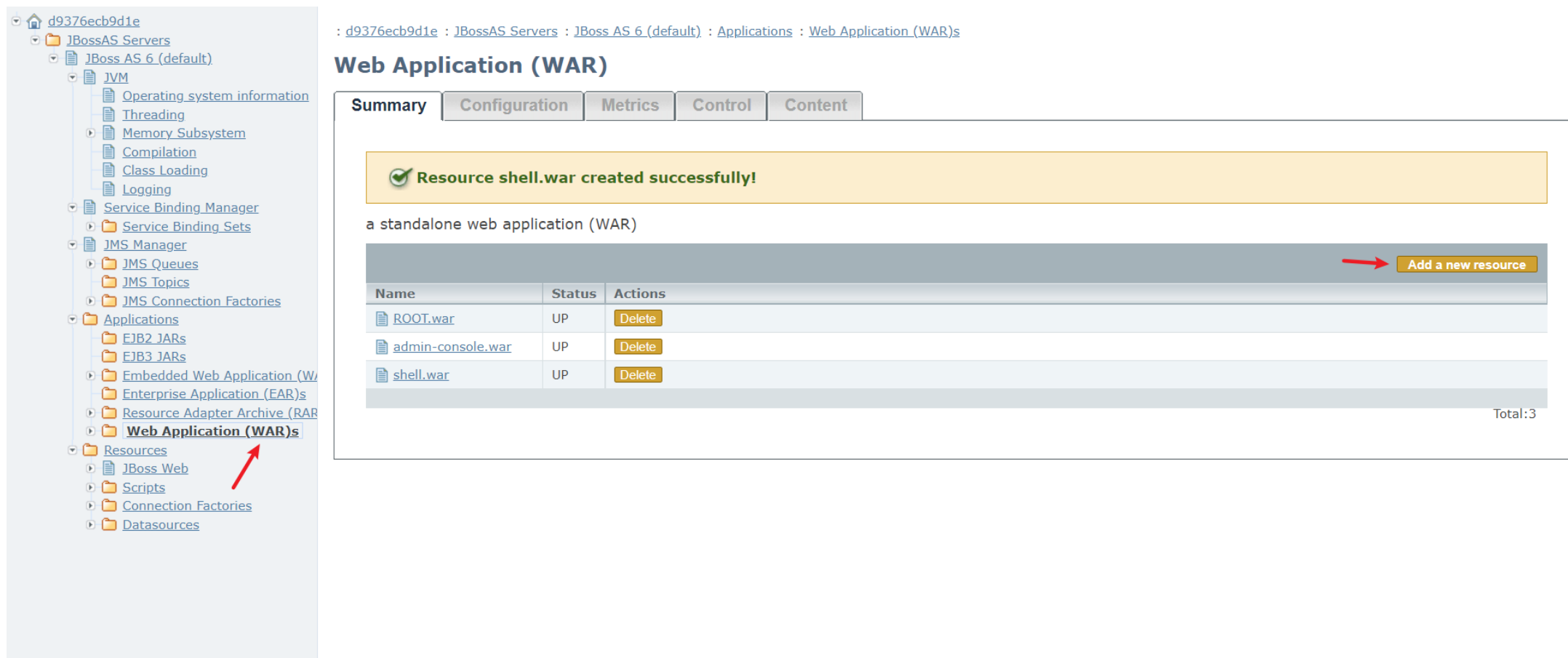
3.2.1 AdminConsole Getshell

admin/admin



3.2.1 AdminConsole Getshell

制作war包：将jsp马添加到压缩文件，然后将压缩文件的zip后缀修改为war



: d9376ecb9d1e : JBossAS Servers : JBoss AS 6 (default) : Applications : Web Application (WAR)s

Web Application (WAR)

Summary Configuration Metrics Control Content

✓ Resource shell.war created successfully!

a standalone web application (WAR)

[Add a new resource](#)

Name	Status	Actions
ROOT.war	UP	Delete
admin-console.war	UP	Delete
shell.war	UP	Delete

Total:3

3.2.1 AdminConsole Getshell

webshell路径: ip:port/war包名字/文件名





感谢您的聆听

▶ 学习工具、资料及课程回放



扫码免费领取

