破解ZelixKla Master的字符串加密 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/287/2021_2022__E7_A0_B4_E8_A7_A3Zeli_c104_287860.htm 反编译 Java 小程序,并且转变为代码都很难,人们为了寻找隐藏的消息经常迷失在 java 代码中.一种方法就是打乱行号,替换所有的 classes 的名称, 方法和变量,我们 将会发现我们所需要的:字符串加密. 分析代码你所需要的工具: - Java 反编译器 (例如:JAD) - 编辑工具 (例如:vim) - 感觉能力 (例如:大脑) 最好能够有些 JVM 的知识, 不过不懂也不用担心，在这儿我会把一切都告诉你的. 但是想要制作你自己的破解程序，你就一定需要那些知识了. 要作弊 Java 游戏，你所需要的工具: - TCP 嗅探器 (例如:tcpdump) - 支持 Java 的浏览器 (例如:Mozilla) - C 编译器 (例如:gcc) - GNU 的工具 (例如:grep) - 支持 PHP 的服务器 .-) 第一步:是什么呢？ 当然是寻找破解的目标喽 :) 在 Coca~Cola ’ s 主页上的游戏看起来不错(nordic).打开 TCP 嗅探器(tcpdump -w file), 运行游戏.玩一会,然后记录你的分数.TCP 嗅探器可以停止了.打开记录文件(vi file).在文件中寻找你的分数,你应该看到这一行: GET /magazine/servlet/SetHighscoreServlet?score=6324amp.cookie=yourname&amp.md5=c404cd019e1a214487cd4c841 我们所要解决的就是 md5 的数值是怎么生成的，那么我们就可以作弊，自己加分数了. 第二步:反编译和分析 下载游戏的 .jar 文件夹(提示: 查看源文件, 标签中的 archive=...), 解开后，反编译每一个 class 文件.现在试着在代码中查找返回数据到服务器的地方 (fgrep -rn "URL" *). b/a/a.java 的第 122 行 (用 jad 反编译的结果) 看起来可以作为我们开始的地方: URL url = new URL(c, b("L9\001

qMdK|)\016rZ!\f\007cfg8\ndMa-\007DK|) \016rZ1,\001x\\kb") Integer.toString(i) b("DpOc:_") d b("DtA a4\013r\023") e b("DzJ.b") a.a.a.a.a.a(i, Integer.parseInt(d), e)). URL 看起来是这样的: "long text" i "text" d "text" e "text" result_of_calculation(i,d,e) 现在的问题是"这些是不是我们看到的字符串?"(不要紧张嘛~) 和 " a.a.a.a.a.a() 都干了些什么?". 打开文件 (vi b/a/a.java) 到 122 行.我们可以看到加密字符串的方法是 b() . 查看 b() (line 224). 是这样的: 224: private static String b(String s) 225: { 226: char ac[]. 227: int i. 228: int j. 229: ac = s.toCharArray(). 230: i = ac.length. 231: j = 0. 232: goto _L1 233: _L9: 234: ac. 235: j. 236: JVM INSTR dup2 . 237: JVM INSTR caload . 238: j % 5. 239: JVM INSTR tableswitch 0 3: default 76 240: // 0 52 241: // 1 58 242: // 2 64 243: // 3 70. 244: goto _L2 _L3 _L4 _L5 _L6 245: _L3: 246: 0x62. 247: goto _L7 248: _L4: 249: 23. 250: goto _L7 251: _L5: 252: 46. 253: goto _L7 254: _L6: 255: 14. 256: goto _L7 257: _L2: 258: 95. 259: _L7: 260: JVM INSTR ixor . 261: (char). 262: JVM INSTR castore . 263: j . 264: _L1: 265: if(j 266: _L8: 267: return new String(ac). 268: } 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com