1. 防止使用eval

如果你对用户输入的内容进行了eval运行，你就有可能受到注入攻击，并且这种运行方式很慢。

注：直接将字符串转化为代码执行，如： eval('alert("hi")')

1. 使用strict模式

'use strict';  
delete Object.prototype; // TypeError

1. 使用静态检测工具

JSLint, JSHint，ESLint

1. 在nodeJS前端架设代理

nodeJS进程中的任何一个错误/漏洞都将让整个系统宕机，需多台机器组成的集群+反向代理

1. 避免shell command注入

child\_process.exec('ls', function (err, data) {  
    console.log(data);  
});

在child\_process.exec引擎下，将调用执行"/bin/sh"。而不是目标程序。已发送的命令只是被传递给一个新的"/bin/ sh'进程来执行shell。攻击者可以使用一个分号";"来结束命令，并开始一个新的调用，他们可以使用反引号或$（）来运行子命令，如删除所有文件rm –rf。

解决方法：使用child\_process.execFile