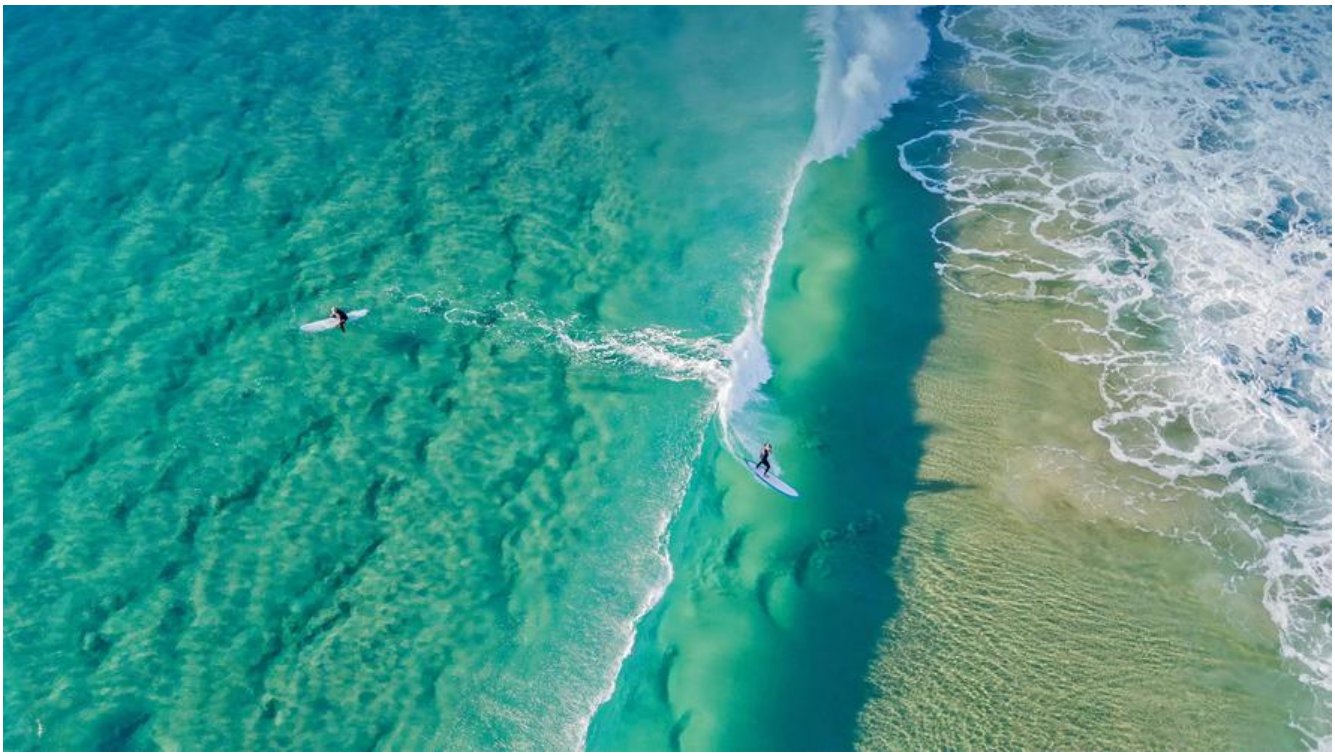
链滴

js 逆向的简单理解

作者：luofeng0603

原文链接：https://ld246.com/article/1677138172531

来源网站：链滴



学习了一点js逆向的知识

简单总结一下：

1.任何通过js进行加解密的方式都不是很安全的，可以防一下小白，但是对于懂一点逆向知识的人来，是防不住的，甭管你做了多少层混淆加密，只要对方肯花时间，足够细心，总是能找到你具体的加位置的，只要找到，就可以把你的加解密方法copy出来，实现破解！

2.反向思考一下，做接口安全的话，如果对安全性要求非常高的，除了常规的token方式，还可以对口调用的参数设计一套加密方式，然后对返回结果座做一套加密，然后对js做足够强度的混淆。这样话，就足够健壮了！因为要破解起来，难度已经变的巨大！

3.常规接口的破解步骤：

- 查找指定接口，分析参数和结果
- 定位加解密点
- 扣函数
- js调试

基本上就是这么几个步骤，难的地方在于，js基本都是混淆的，有的时候定位比较麻烦，需要极大的心，然后扣函数这里也是，有的时候函数里面能给你套上好几层函数，没办法只能一个一个分析。

调试的话可以使用chrome的overrids功能，把js弄到本地，这样查找变量和复制函数会方便很多！