查看: 2220 | 回复: 42

[Web逆向] 反调试-编译pass彻底解决调试web无限debugger问题 [复制链接]

6767

发表于 2023-12-13 22:29 | 只看该作者 楼主 电梯直达

13 主题 | 300 回帖 | 389 积分

前途无量

精华 1
威望 9 点
热心值 121 点
悬赏值 3 点
听众 28
贡献值 0 点
吾爱币 3503 CB
违规 0 次
注册时间 2017-5-31

收听TA

本帖最后由 6767 于 2023-12-13 22:18 编辑

本文尝试从编译过程彻底解决调试web无限debugger问题

背景

当我们调试JS的时候，时常会遇见无限debugger。
debugger 语句用于停止执行 JavaScript(以下简称JS)，并调用 (如果可用) 调试函数。

使用 debugger 语句类似于在代码中设置断点。

复制代码 隐藏代码

```
setInterval(()=>{debugger;}, 100);
setInterval(()=>{eval("debugg"+"er");}, 100);
```

复制上述语句到控制台执行就可以触发了。

实际中的反调试语句会更加复杂和嵌套各种调试技巧,例如常见的无限制debugger、配合settimeout延迟debugger、代码混淆+debugger等等.

解决思路

任何代码都必须编译原理几步-词法语法中间代码机器码，js既然要编译，直接在编译时把关键词屏蔽掉/或生成空语句。

实现

Chrome浏览器内置的是v8 engine，

1源代码

chromium代码搜索:
https://source.chromium.org/chromium

<!--more-->

注意到v8和nodejs项目基本一致，直接下载nodejs进行关键词检索：

复制代码 隐藏代码

```
node/node-v12.22.9/deps/v8/src$ grep -Rn '"[xd]ebugger"'
parsing/keywords-gen.h:99:     {"debugger", Token::DEBUGGER},
parsing/token.h:139:  K(DEBUGGER, "debugger", 0)
parsing/scanner-inl.h:31:  KEYWORD("debugger", Token::DEBUGGER)
heap/heap.cc:3793:      return "debugger";
```

替换掉 `parsing` 目录下的几个 `"debugger"` 就达到了目标.

只编译nodejs比较简单， `make -j16` 一把梭，使用修改后的node调试即可。

但对于Chrome浏览器内置v8就非常无敌超级麻烦要下载工具链，具体请参考网文
V8系统解读(一): V8 在 Chrome 中的位置&编译调试V8

那怎么办呢？挠头.jpg

2二进制修改

系统环境 Windows 10，Chrome 109

先看看DLL内置的字符串信息，bingo，第一行就是了。

复制代码 隐藏代码

```
λ strings chrome.dll | grep debugger
debugger
ICE debugger
ICD2 in-circuit debugger
wait-for-debugger-children
Error loading debugger
await can not be used when evaluating code while paused in the
Cannot access '%' from debugger
debuggerStatement
debuggerId
debuggerEnabled
DevTools debugger
debuggerId
devtools-frontend/front_end/panels/browser_debugger/browser_deb
devtools-frontend/front_end/panels/browser_debugger/browser_deb
devtools-frontend/front_end/panels/browser_debugger/browser_deb
```

```
permission:debugger
wait-for-debugger
silent-debugger-extension-api
Cannot navigate to a devtools:// page without either the devtoc
[...其他...]
```

编译字符串常量必直接表示在rdata区，可直接修改这些hard token。

- 📢修改前请备份文件chrome.dll;

1. 打开chrome安装目录⚙，使用{010 editor/IDA Pro/Win HEX }暴力搜索实际字节为 `\x00debugger\x00` 的地方,前后都是16进制的00;.

2. `debugger` 修改为别的等长字符比如 `xebugger` ；
3. 重新打开 chrome 控制台测试 debugger 是否生效；正常情况下应该已经不会触发debug状态了。
4. 完工，这样就绕过编译Chrome的工程问题。

副作用

- 代码中的debugger成为非法语句，调试器中人工鼠标设置的line breakpoint依然生效。
- 破坏标准语法完整性，导致被探测到debug被破坏输出了warning error，相比之下源码解除debugger\修改ast编译过程更加安全。
- 部分插件失效，如油猴插件

EOF

/革命尚未成功，同志任需努力；
欲知后事如何，请听下回分解😁/

免费评分

参与人数 20	吾爱币 +19	热心值 +18	理由	收起
zhczf	+ 1	+ 1	我很赞同!	
allspark	+ 1	+ 1	用心讨论，共获提升!	
5omggx	+ 1	+ 1	用心讨论，共获提升!	
gmx1222	+ 1	+ 1	谢谢@Thanks!	
fzhhn		+ 1	我很赞同!	
pnccm	+ 2	+ 1	谢谢@Thanks!	
光影魔术	+ 1	+ 1	用心讨论，共获提升!	

hua_wu	+ 1		谢谢@Thanks！
ghd19940802	+ 1	+ 1	debugger攻防的革命性里程碑
月清晖	+ 1	+ 1	我很赞同！
无问且问	+ 1	+ 1	牛逼了
scz	+ 1	+ 1	用心讨论，共获提升！
hehehero	+ 1	+ 1	热心回复！
WFXL	+ 1	+ 1	用心讨论，共获提升！
MakiseSatsuki	+ 1		用心讨论，共获提升！
willbe001	+ 1	+ 1	我很赞同！
weiai987		+ 1	用心讨论，共获提升！
唐小样儿	+ 1	+ 1	我很赞同！
SKnight	+ 1	+ 1	我很赞同！
laos	+ 1	+ 1	这是要扬了无限debugger的骨灰呀

查看全部评分

收藏 50 免费评分 淘帖 有用 9 分享到朋友圈

In [1]: import antigravity
In [2]: print('hello world')

发帖前要善用【论坛搜索】功能，那里可能会有你要找的答案或者已经有人发布过相同内容了，请勿重复发帖。

回复 举报

alanfish

发表于 2023-12-14 08:06 | 只看该作者 推荐

感谢感谢，要加强学习

0 | 25 | 8

主题 | 回帖 | 积分

锋芒初露

吾爱币 71 CB

注册时间 2023-11-11

【吾爱破解论坛总版规】 - [让你充分了解吾爱破解论坛行为规则]

回复 支持 1 免费评分 举报

ghd19940802

发表于 2023-12-14 16:23 | 只看该作者 推荐

吾爱破解论坛没有任何官方QQ群，禁止留联系方式，禁止任何商业交易。

我早就想直接从浏览器上下手,可惜搞不懂chrome的源码, 到处问,问的也都是些不着边际的回答,这下简直通杀所有debugger了

2 主题 | 99 回帖 | 37 积分

锋芒初露

热心值 7 点

吾爱币 1978 CB

注册时间 2015-2-1

如何升级？如何获得积分？积分对应解释说明！

回复 支持 免费评分 举报

moruye

发表于 2023-12-13 23:09 | 只看该作者 **沙发**

《站点帮助文档》有什么问题来这里看看吧，这里有你想知道的内容！

感谢分享，学习了

0 主题 | 1151 回帖 | 326 积分

前途无量

热心值 1 点

吾爱币 1515 CB

违规 1 次

注册时间 2023-3-13

呼吁大家发布原创作品添加吾爱破解论坛标识！

回复 支持 免费评分 举报

wqstudyy

发表于 2023-12-13 23:24 | 只看该作者 3#

学习学习

如何快速判断一个文件是否为病毒！

回复 支持 免费评分 举报

iaoedsz2018

发表于 2023-12-13 23:45 | 只看该作者 4#

我还以为关键字实在v8相关的dll里面，原来就在chrome.dll里面啊

12 主题 | 75 回帖 | 30 积分

锋芒初露

热心值 4 点

吾爱币 144 CB

注册时间 2022-11-11

回复 支持 免费评分 举报

iaoedsz2018

发表于 2023-12-13 23:46 | 只看该作者 5#

你那个strings指令是哪儿来的

12 主题 | 75 回帖 | 30 积分

锋芒初露

热心值 4 点

吾爱币 144 CB

注册时间 2022-11-11

回复 支持 免费评分 举报

86618513

发表于 2023-12-14 06:38 | 只看该作者 6#

学习学习 感谢分享

1 主题 | 358 回帖 | 88 积分

锋芒初露

吾爱币 1745 CB

违规 1 次

注册时间 2021-11-11

回复 支持 免费评分 举报

CQGaxm

发表于 2023-12-14 06:45 | 只看该作者 7#

学习学习,感谢分享

1 主题 | 224 回帖 | 68 积分

锋芒初露

吾爱币 130 CB

注册时间 2019-3-13

回复 支持 免费评分 举报

yuleniwo

发表于 2023-12-14 08:54 | 只看该作者 9#

确实还不太成功，期待改改dll忽略掉debugger

0 主题 | 240 回帖 | 73 积分

锋芒初露

热心值 1 点

吾爱币 1512 CB

注册时间 2021-3-13

回复 支持 免费评分 举报

xzdatm

2 主题 | 27 回帖 | 9 积分

锋芒初露

吾爱币 348 CB

注册时间 2023-2-2

发表于 2023-12-14 08:56 | 只看该作者 10#

好看 爱看 下次还看点赞

回复 支持 免费评分 举报

下一页 »

发帖 回复

返回列表 1 2 3 4 5 1 / 5 页 下一页

| 拖入文件 或 浏览 高级模式

发表回复 警告：本版块禁止灌水或回复与主题无关内容，违者重罚！ 本版积分规则

回帖并转播 回帖后跳转到最后一页