蒜法导论

第一课：环境配置

- Windows 10
- Windbg
- Peach 3.x
- IFFA

第二课：更简单的方法

- 命令行测试
- **IFFA路径+被测试程序路径+样本路径**

第三课Hello Crash

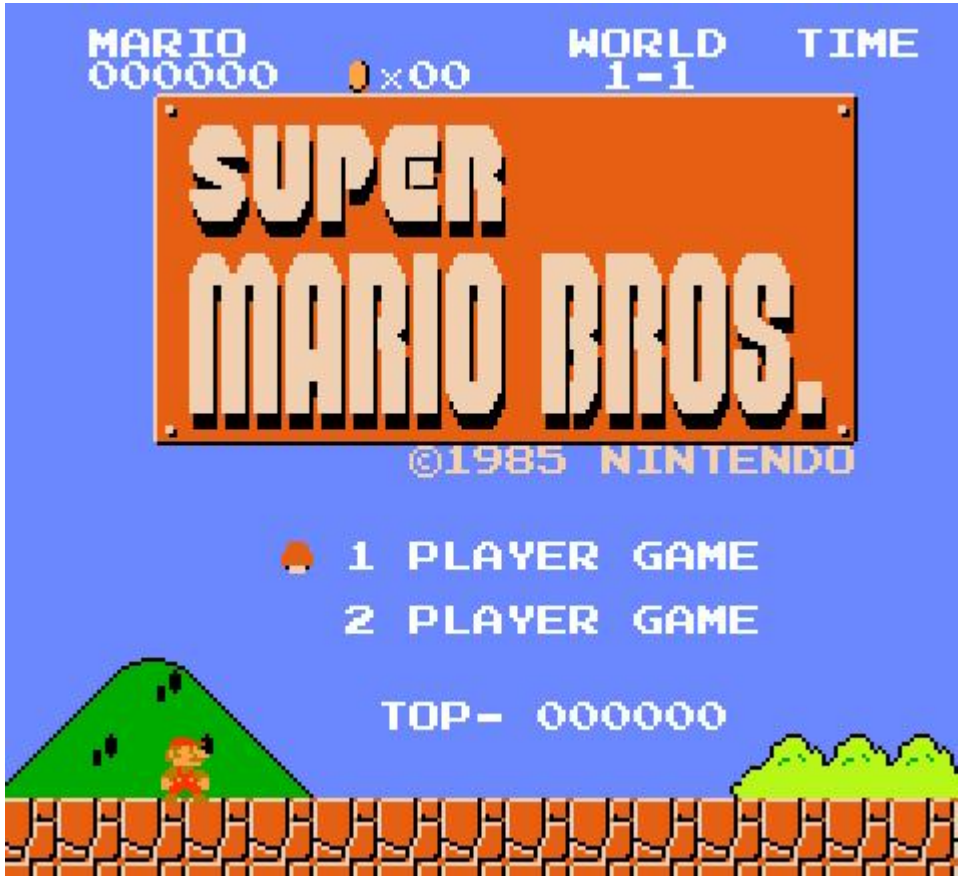
- 随便找个OFFICE软件 开启Fuzzing之旅。

第四课：挖掘点定位

- 1 打开功能
- 2 插入功能
- 3 潜在功能。INI文件。皮肤文件。各种资源文件。
- 4 其他程序功能。比如红色警戒，帝国时代这种游戏他有一些地图编辑器。
- 5 协议
- 加微信asm64help 进一步讨论

第五课

- 超级玛丽


MARIO
000000
×00
WORLD
1-1
TIME
SUPER
MARIO BROS.
©1985 NINTENDO
1 PLAYER GAME
2 PLAYER GAME
TOP- 000000

第六课-基因建模

基因建模：适用于复合型文件格式解析，当大蒜成为越用越聪明的软件。

基因模型：C:\IFFA\DnaModelData

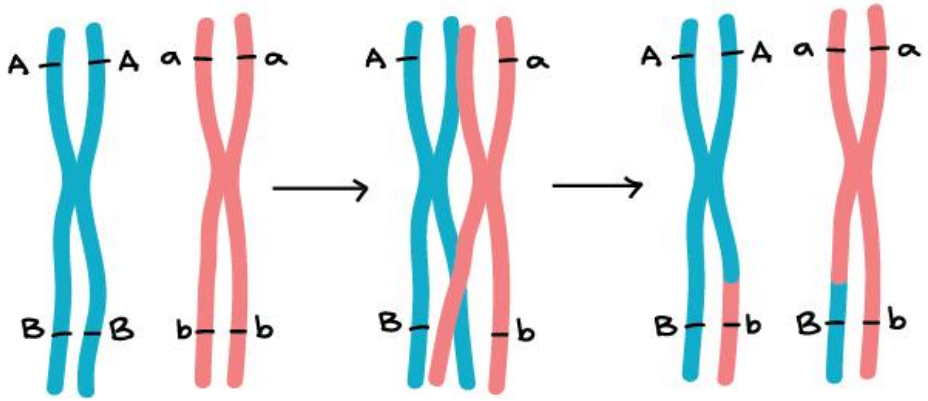
第七课-基因地图

基因地图：对当前的分析情况了如指掌

第八课-基因重组，基因修复，C源码输出

基因重组：生成的样本在标杆样本基础上变异，但是会在**适合的地方，以适合时机，适合的形式**添加其他样本的部分基因，（组到新的样本）。进而增强样本变异能力。

类似于 新冠的XBB病毒，正是因为基因重组，才有如此强的变



第八课-基因重组，基因修复，C源码输出

基因修复：

对生成的pit样本发现问题导致不能生成，点击基因修复自动解决问题。

C源码输出：

输出文件格式对应的C代码，方便二次开发。

第9课-靶向分析，设置，命令行

靶向分析：

对超大样本的重点定位，提高分析效率。

设置：

开启自定义设置，建议为默认格式。

命令行：

命令行改成部分指令。

第10课-样本DNA覆盖率分析&字典交互式分析

样本DNA覆盖率分析：

基因在各自样本的覆盖率，可以分析出样本基因相似度。

字典交互式分析：

点几下鼠标，自动分析出字典信息。

第11课-武器库

PIT样本库

武器库样本添加:自动加入

武器库使用1：通过格式选择（脱离大蒜，单个测试)

武器库使用2：通过样本选择（依赖大蒜，批量测试）

第12课-批量添加武器库

批量添加武器库：

同类样本武器库的批量添加测试。

1 大蒜根据样本，自动科学进行分组。

2 批量分析，添加武器库。

第13课-二蒜

1.二蒜 基于大蒜的漏洞挖掘工具

可取代对peach的依赖，于大蒜形成完美闭合。

也可以通过基因遗传等蒜法进行高效率漏洞挖掘（需要三蒜支持）（本节课不讲解）

2.大蒜二蒜联合使用测试

第14课-三蒜

三蒜1.0

最容易上手的动态分析工具

代码覆盖率&基因遗传&深度学习

通用&好用&易上手&简约不简单

大繁至简，极境至臻。

总结—大蒜的使用姿势

	软件1	软件2	软件3
方案1	大量时间	Peach	Windbg
方案2	大蒜	Peach	Windbg
方案3	大蒜	二蒜	
方案4	大蒜	Peach	三蒜
方案5	大蒜	二蒜	三蒜

IFFA Studio 核心三剑客

至此，IFFA Studio已经完成二进制漏洞挖掘领域产业链的全套产品布局！

产品	大蒜	二蒜	三蒜
英文名	IFFA	IFFA_Fuzzer	IFFA_Debugger
内部代号	蓝刃	红刃	绿刃
最新版本	6.1	1.4	1.1
口号	蓝色信仰，颠覆之作	红色狂热，高效之作	绿色清新，简约之作
介绍	颠覆性，唯一性。IFFA Studio灵魂产品。 这，就是大蒜。	二蒜：基于大蒜的漏洞挖掘产品，重新定义Fuzzer。致力于打造全球最容易上手最好用的智能Fuzzer。支持解析结果反馈的深度学习生成样本，以及生物遗传算法漏洞挖掘。	通用型的动态分析工具。将动态分析做到极致的简单。可用来分析代码覆盖率。可作为Fuzzer挖掘软件漏洞。也可用来或许的漏洞分析。
技术特点	过于强大，不宜展示。	反馈式模式，深度学习算法，生物遗传算法。独创科学变异引擎。速度快，效果好。传承大蒜，完美匹配大蒜FF文件。	代码覆盖率。生物遗传法。提高漏洞挖掘质量。提高漏洞分析效率。

IFFA.exe

IFFA_Fuzzer.exe

IFFA_Debugger.exe

第15课-二蒜+三蒜

基因遗传模式：

二蒜用于样本变异

三蒜用于对二蒜变异的样本进行动态分析，再将测试结果反馈给二蒜。

二蒜再此基础上，对进化后的样本继续进行分析，继续反馈给三蒜。

就像一只猴子，经过多代的变异，最终变成一个性感少女。

第16课-总结

1 看完前4课就可以挖掘漏洞，并且应该有很好的效果了。

2 新手强烈看我们公众号的《文件格式漏洞挖掘指南》这一篇文章。

3 关于价格，**个人版540元/首年 续费180元/年。**租用前仔细阅读《租用协议》。

严禁盗版，扩散软件。我们会严厉打击。

我们的联系方式：

微信：Asm64help 电话：18831330123

问题自查表

1 系统是否为win10系统？

2 系统可用内存是否达到2GB？

3cpu是否为双核心以上？

4 是否管理员权限运行？

5 是否有杀毒软件等程序因自身问题影响大蒜运行？

6 是否多开程序？

7 key路径，文件，是否正确？

8 是否因已知库信息影响?(删除目录下的各种库文件，包括字典库，建模库，基因库，删除前请备份)。

9 所填写的参数是否正确？

10 是否重启系统和软件后，问题依然不能解决。

结尾语

2023年2月26日大蒜商业化1周年，
做此视频，以感谢用户对我们的支持。

到此为止，大蒜的所有内容已经介绍完毕。
感谢多年以来大家对大蒜的支持，
我们不会辜负收费用户对我们的信任。
让我们一起努力。加油！！