

蒜-全球**唯一**一款 未知文件格式自动分析软件

IFFA实验室-光刃
www.asm64.com/new
公众号：IFFA

蒜是什么

- 蒜-未知文件格式自动分析软件
可用于自动化漏洞挖掘

- 参考资料:

第一篇：什么是大蒜：<http://www.asm64.com/1/>

第二篇：再谈大蒜：

<https://mp.weixin.qq.com/s/oqudl8FMTJl8BCPyBb40JQ>

参考资料汇总：<http://www.asm64.com/new/>

大蒜可用于哪类产品的漏洞挖掘？所有的文件格式或者协议类。对未知的效果最好。冰山一角：5000多种文件格式
<http://www.asm64.com/file.html>

Fuzzer发展	代表作	优点	缺点
第一代	EasyFuzzer等	速度快	效率低
第二代	Peachfuzzer等	速度慢	效率高
第三代	AFL 等	速度快	外界依赖性高， Windows 下需要逆向能力。
第四代	大蒜	速度快 效率高 依赖性低 无竞争对手	丑

挖洞是一枚硬币，不逆向，和不看源码只能对立。

你会选择哪一面？今天，大蒜选择两面。

或许在未来，“静态未知文件格式识别”方向，大蒜做不到最好的那个，但是大蒜已经做到了第一个。

蒜开发历程

蒜是光刃的个人产品，休息日在家没事的时候开发。起始于2016年，经历了长达6年的构思，开发，放弃的反复过程。最终于2022年成型。历史过程如下：

第一次：2016年 蒜的早期项目garlic开启，初期定位静态动态结合的方式，最终放弃。

第二次：2018年IFFA再次开启，最终再次放弃。

第三次：2019年8月项目再次开启，最终再次放弃。

第四次：

2020年4月5日：发布第一个公开的0.1版本。

2021年4月1日：发布1.2版本。该版本起有了最基本的方向。

2021年10月：发布2.0版本，开启白皮蒜，紫皮蒜，独头蒜的分化。代表蒜进入了快速发展阶段。此时独头蒜为内部版本，并不开放。

2021年12月21日：蒜3.0版本，此时大蒜开始成熟，3.0开始独头蒜收费版也正式接受出租。

2022年5月2日：蒜4.0版本，此时，蒜已经是白帽安全研究领域的巅峰之作。

从构思到巅峰之作，蒜经历了6年。

蒜的租金

蒜(2022.5.22) 公众号: IFFA 售前人员微信号: Asm64help

软件属于
光刃个人
所有, 未
经光刃授
权使用软
件均属于
违法行
为!!!
本人保留
追究法律
责任的权
力!

最新租用协议:
[http://www.as
m64.com/IFFA/
VIP/IFFA_cont
ract2.2.pdf](http://www.as
m64.com/IFFA/
VIP/IFFA_cont
ract2.2.pdf)

版本	白皮蒜	紫皮蒜	独头蒜【个人】
目前版本	3.0	3.0	4.3
适用范围	超小规模软件	中小规模软件	大规模超大规模软件
引擎能力	弱	弱	强
更新状态	停止更新	停止更新	更新中
支持数据模型	少	少	多
文件格式	是	是	是
网络协议	是	是	是
自动分析	是	是	是
交互式分析	是	是	是
命令修改属性	是	是	是
测试模式	是	是	是
样本生成模式	是	是	是
基因地图	是	是	是
基因算盘	是	是	是
引擎参数修改	是	是	是
指令深度优化	是	是	是
核心引擎参数修改	否	否	是
指令数限制	200	800	65535
是否包更新	不涉及	否	是
文件大小限制	2KB	8KB	4MB
基因映射分析器	否	否	是
基因重组分析器	否	否	是
基因合成	否	否	是
基因密度	否	否	是
授权机器	不涉及	1个	1个
基因质量分析	否	否	是
基因建模(酶)	否	否	是
双擎分析(蒜+酶)	否	否	是
c-源码输出	否	否	是
基因修复	否	否	是
STR类型深度解析	否	否	是
授权方式	免费试用	免费试用【启动期内转发广告获得】	付费租用
首次租用价格			540元/首年
优惠续费价格(则期十天内)			240元/年
普通续费价格			540元/年
是否提供发票	不提供	不提供	不提供
是否可把生成的pH【大量】集成到自身产品内	不可以	不可以	不可以

如何快速上手大蒜

- 1.了解peach fuzzer的原理和使用。从看雪 freebuf等知名网站搜索peach即可。
- 2.运行大蒜配合peach使用。

总结：peach的重点和难点就是编写对文件（或协议）建模的XML脚本（PIT文件），而大蒜是可以自动化对文件建模并生成PIT文件的软件。

参考资料：

早期：

<http://www.asm64.com/IFFA/help.pdf>

<http://www.asm64.com/IFFA/teach001.pdf>

GitLab收购Peach Tech和Fuzzit!以增强其DevOps安全测试工具

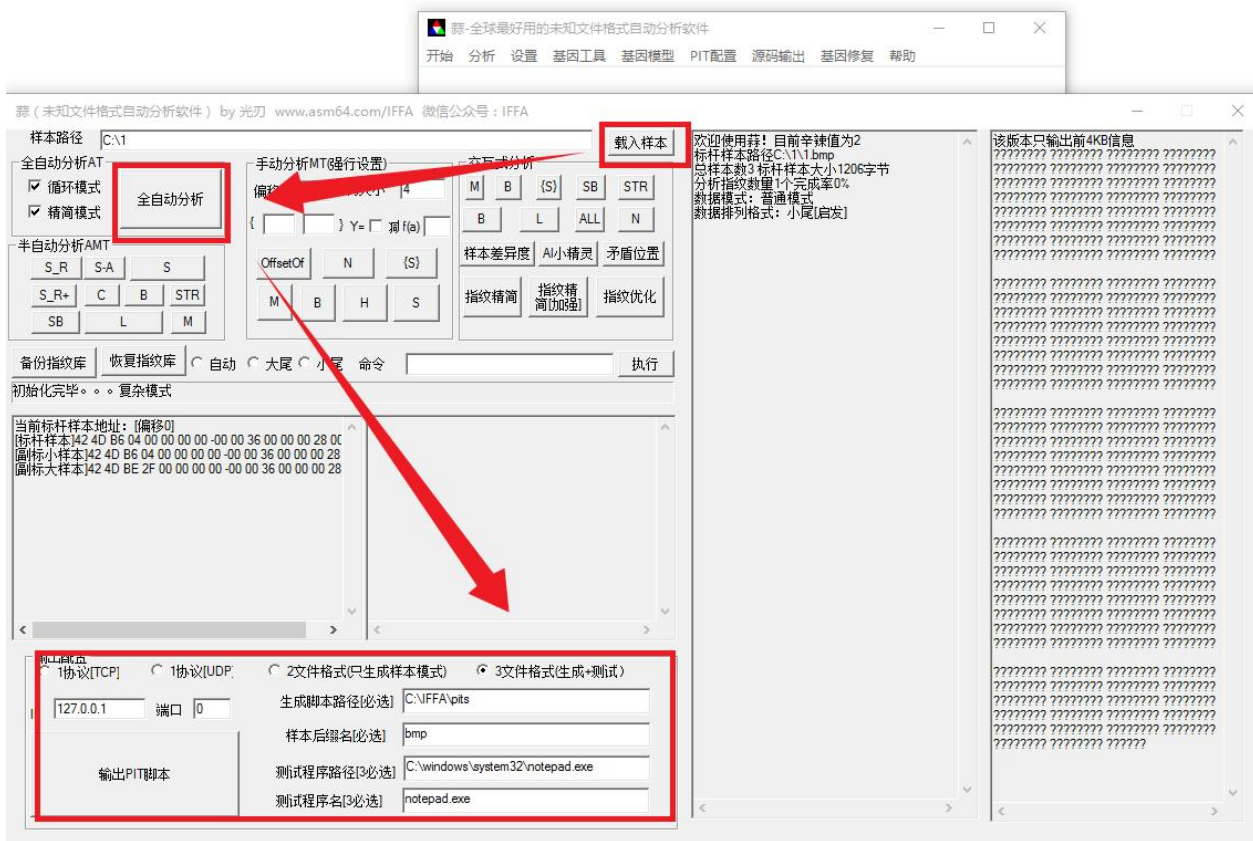
何斌 · 2020年6月25日 10:28 · 企业动态 · 阅读 280



如何快速上手大蒜

对于大部分普通用户，一般只需要三步：

1 载入样本。2全自动分析。3填写配置选项并输出,然后peach测试。
其他的一切交给我们。 没错，就这么简单。



蒜其他高级功能1

- 设置：
- 引擎开关设置。设置你关注的模型。
- 杂项： 大小尾以及辛辣值（变异的力度）

引擎开关设置

- | | |
|--|---|
| ☒ 位识别 | ☒ 固值识别 |
| ☒ 加密类型识别(不少于3样本) | ☒ HEX类型 |
| ☒ 循环类型识别 | ☐ 自然数类型识别 |
| ☒ 字符串类型识别 | ☒ SB复合结构识别200 |
| ☒ 文件大小识别 | ☒ SB复合结构识别204 |
| ☒ 数据段大小识别 | ☐ CRC识别(限4KB以内) |
| ☒ DWORD-LIST类型识别 | ☒ 小头识别 |
| ☒ WORD-LIST类型识别 | ☒ 大头识别 |
| ☒ BYTE-LIST类型识别 | ☒ 异常样本报警【载入时】 |
| ☒ DWORD-LIST*n类型识别 | ☒ DWORD-HEX*n类型识别 |
| ☒ 自定义基因模型【醋】识别且不变异 | |
| ☒ 500模块(至少需要3个样本) | |

确定

引擎开关设置

- | | |
|--|---|
| ☒ 位识别 | ☒ 固值识别 |
| ☒ 加密类型识别(不少于3样本) | ☒ HEX类型 |
| ☒ 循环类型识别 | ☐ 自然数类型识别 |
| ☒ 字符串类型识别 | ☒ SB复合结构识别200 |
| ☒ 文件大小识别 | ☒ SB复合结构识别204 |
| ☒ 数据段大小识别 | ☐ CRC识别(限4KB以内) |
| ☒ DWORD-LIST类型识别 | ☒ 小头识别 |
| ☒ WORD-LIST类型识别 | ☒ 大头识别 |
| ☒ BYTE-LIST类型识别 | ☒ 异常样本报警【载入时】 |
| ☒ DWORD-LIST*n类型识别 | ☒ DWORD-HEX*n类型识别 |
| ☒ 自定义基因模型【醋】识别且不变异 | |
| ☒ 500模块(至少需要3个样本) | |

确定

蒜其他高级功能2

- 设置：引擎参数设置：部分引擎的参数修改。

引擎参数设置

DwordList识别长度	8	FindLostDna识别最小长度	8
WordList识别长度	8	FindLostDna识别最大长度	512
ByteList识别长度	8	FindLostDnaToken长度	4
Str类型识别长度【混合】	8	☒ FindLostDnaToken辛辣状态(2字节后)	
Str类型识别长度【数字】	3		
Str类型识别长度【字母】	4		
Str类型识别长度【unicode】	6		
n*DwordList识别长度	4		
n*DwordHEXList识别长度	3		

确定

蒜其他高级功能3

- 基因算盘：数据关系的深度挖掘.(参考
<http://www.asm64.com/IFFA/IFFA260.html>)

算盘

配置

分析最大偏移 4096

范围：最大数值 97776

范围：最小数值 2

命中阈值【%】 90

☐ 分析WORD类型

数据探测

$Y=A*X1*X2*...*Xn$ 分析

要分析的DNA 5

单指纹 $Y=A*X+B$ 分析

Y数据池：文件内部筛选的不确定数据！【只读】

[ID=05:0X000A]	[54]	54	54
[ID=06:0X000E]	[40]	40	40
[ID=07:0X0012]	[16]	24	51
[ID=08:0X0016]	[24]	16	78
[ID=10:0X001C]	[24]	24	24

X数据池：蒜分析后筛选的重要数据！【只读】

[ID=02]直接数值型	[1206]1206	12222
--------------	------------	-------

藏宝图[质因数数，文件内因数数，最大质因数]

X-0:	[5 0 3]	[5 0 3]	[5 0 3]
X-1:	[2 0 53]	[2 0 53]	[2 0 53]
X-2:	[4 0 13]	[4 0 13]	[4 0 13]
X-3:	[3 0 17]	[3 0 17]	[3 1 17]
X-4:	[4 0 5]	[4 0 5]	[4 0 5]
X-5:	[3 0 7]	[3 0 7]	[3 0 7]
X-6:	[6 3 3]	[6 3 3]	[6 1 3]
X-7:	[2 0 47]	[2 0 47]	[2 0 47]
X-8:	[3 0 23]	[3 0 23]	[3 0 23]
X-9:	[4 0 5]	[4 0 5]	[4 0 5]
X-10:	[4 0 11]	[4 0 11]	[4 0 11]
X-11:	[2 0 43]	[2 0 43]	[2 0 43]

☆☆

发现1个特征，本版本最多输出16个特征
[匹配率33%][Y.id=10]该特征类型为 $Y=a*x$ 其中 $a=1$, $x.id=6$, $x=24$

蒜其他高级功能4

- 基因地图：快速了解基因的情况

地图

0x0000:	****B604	0000****	*****	*****	*****	*****	*****
0x0020:	*****	*****	*****	*****	*****	*****	*****
0x0040:	*****	*****	*****	*****	*****	*****	*****
0x0060:	*****	*****	*****	*****	*****	*****	*****
0x0080:	*****	*****	*****	*****	*****	*****	*****
0x00A0:	*****	*****	*****	*****	*****	*****	*****
0x00C0:	*****	*****	*****	*****	*****	*****	*****
0x00E0:	*****	*****	*****	*****	*****	*****	*****
0x0100:	*****	*****	*****	*****	*****	*****	*****
0x0120:	*****	*****	*****	*****	*****	*****	*****
0x0140:	*****	*****	*****	*****	*****	*****	*****
0x0160:	*****	*****	*****	*****	*****	*****	*****
0x0180:	*****	*****	*****	*****	*****	*****	*****
0x01A0:	*****	*****	*****	*****	*****	*****	*****
0x01C0:	*****	*****	*****	*****	*****	*****	*****
0x01E0:	*****	*****	*****	*****	*****	*****	*****
0x0200:	*****	*****	*****	*****	*****	*****	*****
0x0220:	*****	*****	*****	*****	*****	*****	*****
0x0240:	*****	*****	*****	*****	*****	*****	*****
0x0260:	*****	*****	*****	*****	*****	*****	*****
0x0280:	*****	*****	*****	*****	*****	*****	*****
0x02A0:	*****	*****	*****	*****	*****	*****	*****
0x02C0:	*****	*****	*****	*****	*****	*****	*****
0x02E0:	*****	*****	*****	*****	*****	*****	*****
0x0300:	*****	*****	*****	*****	*****	*****	*****
0x0320:	*****	*****	*****	*****	*****	*****	*****
0x0340:	*****	*****	*****	*****	*****	*****	*****
0x0360:	*****	*****	*****	*****	*****	*****	*****
0x0380:	*****	*****	*****	*****	*****	*****	*****
0x03A0:	*****	*****	*****	*****	*****	*****	*****

指纹ID

上一条

当前指纹

下一条

显示全部数据

显示全部指纹

• 固定结构

• 16位结构

• 高熵结构

• 大型结构

• 类数组结构

显示指定类型指纹

【类型: 文件总大小, 非常

2

播放全部指纹

停止播放

显示全部数据

显示全部指纹

• 字符结构

• 32位结构

• 高值结构

• 部分其他

• 建模结构

蒜其他高级功能5

- 基因密度表：快速了解基因的情况

基因密度表

20分法第1个片段,大小2字节,包含1个基因,基因密度为512个/KB
20分法第2个片段,大小4字节,包含1个基因,基因密度为256个/KB
20分法第3个片段,大小2字节,包含1个基因,基因密度为512个/KB
20分法第4个片段,大小2字节,包含1个基因,基因密度为512个/KB
20分法第5个片段,大小4字节,包含1个基因,基因密度为256个/KB
20分法第6个片段,大小4字节,包含1个基因,基因密度为256个/KB
20分法第7个片段,大小4字节,包含1个基因,基因密度为256个/KB
20分法第8个片段,大小4字节,包含1个基因,基因密度为256个/KB
20分法第9个片段,大小2字节,包含1个基因,基因密度为512个/KB
20分法第10个片段,大小4字节,包含1个基因,基因密度为256个/KB
20分法第11个片段,大小2字节,包含1个基因,基因密度为512个/KB
20分法第12个片段,大小2字节,包含1个基因,基因密度为512个/KB
20分法第13个片段,大小18字节,包含1个基因,基因密度为56个/KB
20分法第14个片段,大小154字节,包含1个基因,基因密度为6个/KB
20分法第15个片段,大小1字节,包含1个基因,基因密度为1024个/KB
20分法第16个片段,大小155字节,包含1个基因,基因密度为6个/KB
20分法第17个片段,大小1字节,包含1个基因,基因密度为1024个/KB
20分法第18个片段,大小155字节,包含1个基因,基因密度为6个/KB
20分法第19个片段,大小1字节,包含1个基因,基因密度为1024个/KB
20分法第20个片段,大小155字节,包含1个基因,基因密度为6个/KB
20分法第21个片段,大小1字节,包含1个基因,基因密度为1024个/KB
20分法第22个片段,大小467字节,包含1个基因,基因密度为2个/KB
20分法第23个片段,大小1字节,包含1个基因,基因密度为1024个/KB
剩余片段,大小20字节,包含469个基因
总体基因密度为20个/KB

☐ 2分 ☐ 5分 ☐ 10分 ☒ 20分 ☐ 50分

确定

退出

蒜其他高级功能6

- 基因缺陷分析仪：分析可能缺失基因的结构。

基因缺陷分析仪

缺陷样本为C:\1\1.bmp[1206 B]
参考样本1为C:\1\2.bmp[1206 B]
参考样本2为C:\1\3.bmp[12222 B]

缺陷样本C:\1\1.bmp[1206 B]

提示

基因缺陷分析仪说明：

- 1 该功能用于分析标杆样本的缺陷结构，可以让基因标杆样本而生成的样本复杂度大于标杆样本。给的样本数量越多，效果越好。
- 2.该功能始于3.3 目前还不完善。目前只搭配在独头蒜上面。
- 3 主界面自动分析功能已经包含了该功能，但是分析时为了效果请不要勾选“自动分析”。
- 4 使用该功能要求至少提供3个样本。
- 5 相关参数设置在引擎参数 - 高级模式里面选择。

确定

低变异

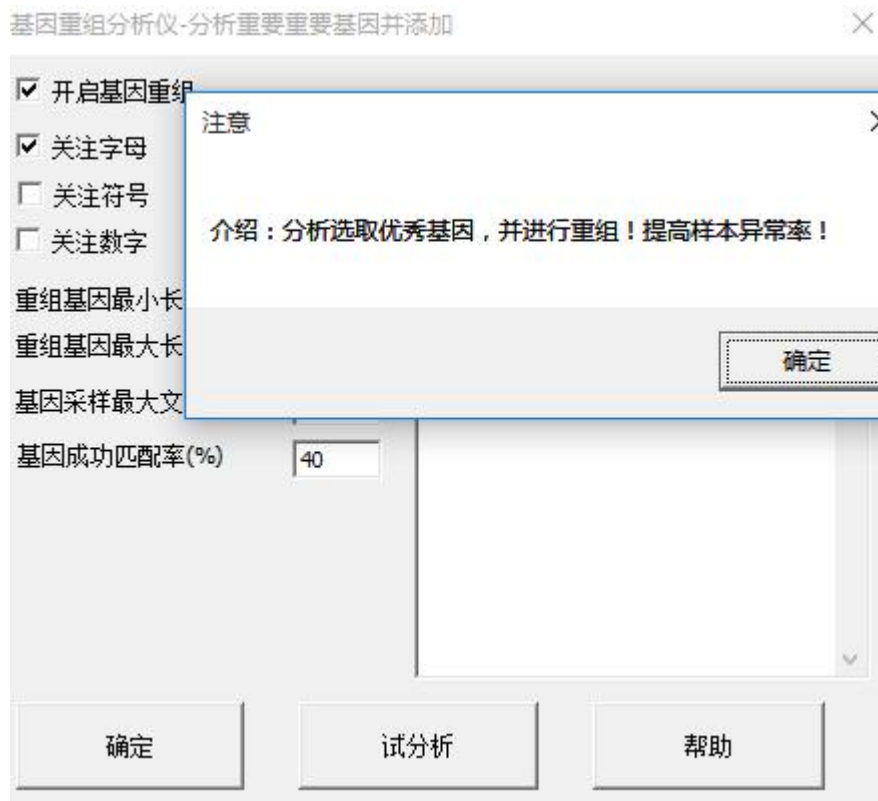
高变异

退出

帮助

蒜其他高级功能7

- 基因重组分析仪：重新组合重要基因，提高fuzz效率。



蒜其他高级功能8

- 基因建模【醋模块】：
- 对文件进行特征提取，并保存特征。适用于大规模的复杂格式的漏洞挖掘。
- 参考文档：<http://www.asm64.com/CH3COOH>
- https://mp.weixin.qq.com/s/cWR2v5iE_-FgtTpcOtFU-g

基因模型分析[醋8模块]

特征库位置: C:\IFFA\DnaModelData

2202.5.8 8度醋V1版本。搭配到独头蒜4.1软件上。
模型数量: 文件识别6条, 数据流识别4条

模型类型类别 文件大小token 文件头token 文件尾token

分析模型【建模】

文件夹(不包含子目录) 验证模型 用模型库分析样本

大型数据块文件 C:\BMP\1\5\5.rar 验证模型 用模型库分析样本

[0]次分析。特征类型:bmp找到匹配样本3个
[1]次分析。特征类型:pdf找到匹配样本2个
——共找到匹配样本5个,样本已经保存到C:\IFFA\SaveDumpFile\0508_085506文件夹内

说明: 该模块为醋模块, 非大蒜。目前只是孵化用。未来和大蒜无关的功能可能会删除。相关的功能或许会留下来。

输出至模型库

IFFA

蒜其他高级功能9

- 基因修复:

当某些原因导致生成的pit脚本有冲突不能生成的时候，基因修复功能可以自动查找并排除错误。(不能100%)



蒜其他高级功能10

源码输出：

用于文件格式到c源码的输出。高级用户可用此功能进行二次开发。

参考文档：

www.asm64.com/IFFA/VIP/IFFA430.pdf

源码输出-可用于不依赖peach的自编写的各种工具开发。

C代码已经保存到相应文件夹！

```
/*char Sample="C:\\BMP\\1\\1.bmp";*/
#include <stdio.h>
#include <windows.h>
struct DNA2C {
    struct S1{
        char D0[2];
        char D1[4];
        WORD D2;
        WORD D3;
        char A4[4];
        struct S2{
            char A5[4];
            char D6[1];
            BYTE D7;
            WORD D8;
            DWORD D9;
            WORD D10;
            DWORD D11;
            DWORD D12;
            char D13[18];
        };
    };
};

char D14[3][512];
};
void main()
{
    printf("本代码来自大蒜-基因转C代码模块v1,可用于工具开发.\r\n");
    printf("A是重要模块,D是相对于A不重要模块,S是结构体.\r\n");
    system("pause");
    return 0;
}
```

输出源码 退出

蒜更多其他高级功能

就当做没了吧（不想写了）

蒜的目录结构

C:\IFFA 总目录

C:\IFFA\project 工程目录

C:\IFFA\Log 日志目录

C:\IFFA\pits 输出的pit目录

C:\IFFA\samples 输入样本目录

C:\IFFA\SaveFile 保存文件目录

C:\IFFA\SavdDumpFile基因建模【醋】模块分析出文件的目录

C:\IFFA\DnaModelData 基因建模【醋】模块分析的特征目录

C:\IFFA\key 授权文件

.....

蒜的广告

从2022年2月26日，至今2022年5月22日。独头蒜一共有25个租户。

兼得之道

挖洞是枚硬币，
正反只能对立。
正方无需逆向，
反方无需审计。
你选择哪一面？
如今蒜选择两面。

爱

年迈的父母，
漂亮的妻子，
可爱的孩子，
你还有多少时间去爱？
你还忍心加班吗？
试试大蒜吧，
少一些加班，多回家看看。

联系我们

扫一下微信，
加我了解更多。
(该号不长期
加好友，扫码
拉群后即删除)
或者关注官方
微信号：IFFA



最后

大蒜并不便宜，但是没有一分钱是多余的。如今以步入中年，身体退化，走路不稳。颈椎病，高血糖，前列腺钙化。。。我不图发财，只图余生三餐有汤。

请不要再做无意义的攻击，
严禁盗版，违者必究。

