基于云的安全测试

Synopsys高级安全架构师 韩葆

UCLOUD

云服务下的安全挑战

分布式？

- 数据泄露或丢失

私有信息泄露

- 内控？
- 加密？

服务丢失

- 机房故障怎么办？安全其实也是可靠性要求（几个9？）

云服务下的安全挑战

- 恶意软件攻击
  - 上传个东东？
- 缺少有效的云安全行业标准

其实传统的安全攻击仍旧在云上存在

云服务下的安全挑战

- 另眼看世界 本地还是云服务？
  - 本地可访问的硬件更安全？
  - 数据中心更安全
  - 服务更安全？

其实传统的安全攻击仍旧在云上存在

一个真实的例子-Cloudbleed

- 谷歌研究人员披露了云服务商Cloudflare的Cloudbleed HTTPS流量泄漏漏洞，目前多家著名网站用户的一些会话令牌、密码、私人消息、API密钥和其他一些敏感数据被Cloudflare随机泄露给了访问者，甚至被搜索引擎缓存或已被黑客收集。该漏洞与心脏出血(Heartbleed)的原理类似，因此被称为“Cloudbleed”云出血。

解决方案之一：威胁建模

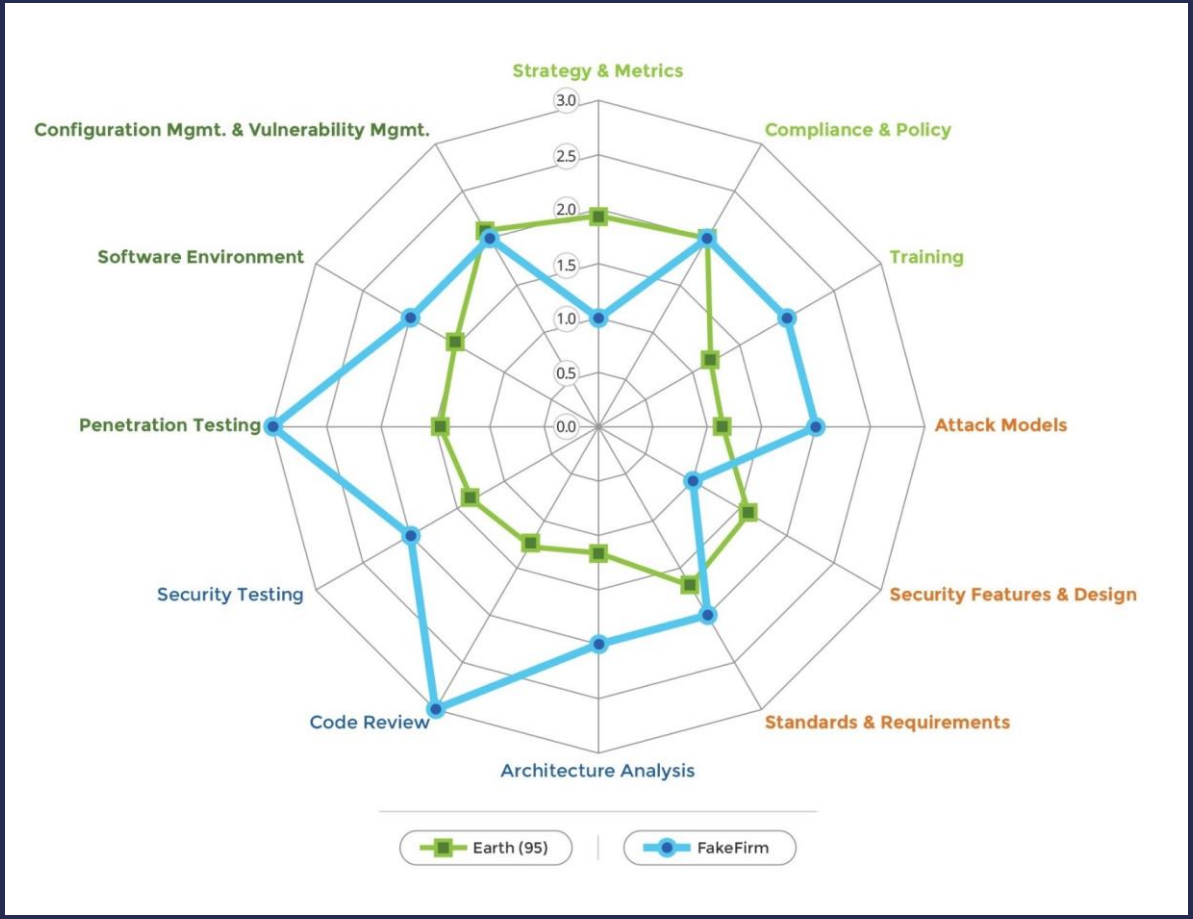
- 云架构上的安全风险 – 云平台的研发过程中引入的问题
- 安全攻击之外的风险 – 云端架构
- Top-N 列表，攻击漏洞，或者相关的场景
- 有可能带来问题的云组件
- 安全咨询建议

BSIMM

BSIMM
Building Security In Maturity Model

BSIMM - A Measuring Stick

- Validated model with data from 95 firms (BSIMM7) with 237 distinct measurements
- Use it to see where you stand.
- Use it to figure out what your peers do.



解决方案之二：你自己的应用

- 云厂商们是非常关注安全的，比用户更关注– 比如UCloud….
- 绝大多数的问题仍旧来自用户自己的应用
  - ASP
  - JSP
  - JavaScript
  - 云服务
  - 游戏
  - …
- 传统的安全攻击手段仍旧有效 – 因此需要云端防护
- 数据分析是非常有效的手段 – AI层级防护- Ucloud方案

解决方案之三：云上安全测试

基于云进行安全测试

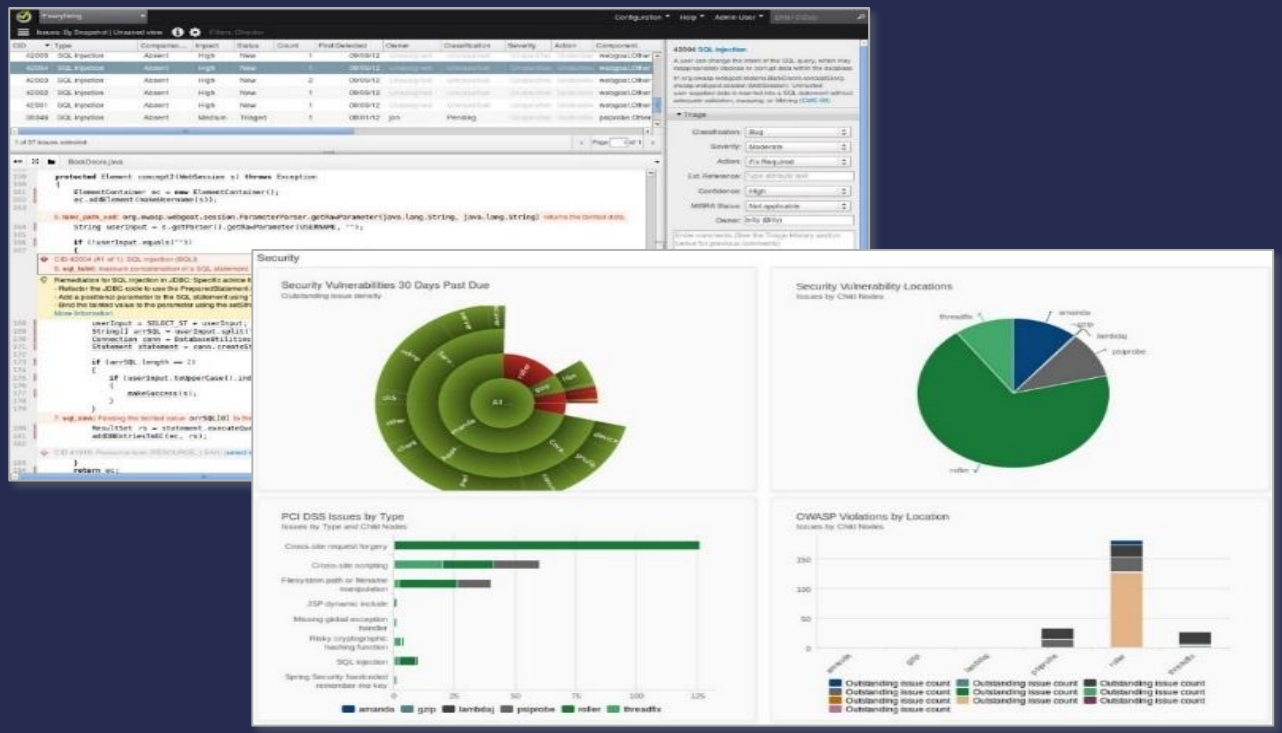
- 静态分析、黑盒测试、模糊测试、成分分析…
- 快速、大规模化的测试
- 成本低、可用性高、质量有保障

适用场景：

- 大规模、高并发
- 非特高可靠性与安全性需求应用
- 控制成本且要求时间

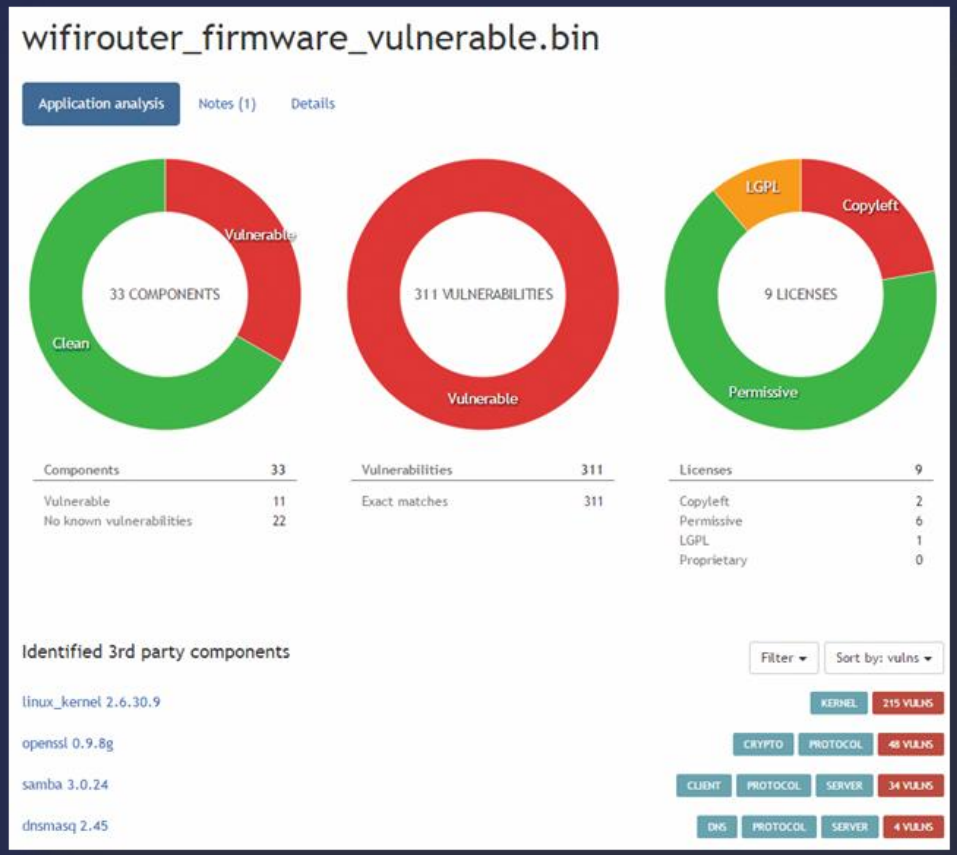
云上安全测试 – 研发过程安全

- 研发云
  - 开发过程安全检测
    - 代码分析



云上安全测试 – 外部组件安全

- 第三方组件的安全漏洞 – 统计数据



API Endpoints

PUT	/appcheck/api/upload/**filename**	Upload an application (note: no trailing /)
GET	/appcheck/api/app/**id**/	Get results of an appcheck
GET	/appcheck/api/app/**sha1sum**/	Get results of an appcheck
DELETE	/appcheck/api/app/**id**/	Delete results and the binary
DELETE	/appcheck/api/app/**sha1sum**/	Delete results and the binary
GET	/appcheck/api/groups/	List groups
GET	/appcheck/api/apps/	List applications
GET	/appcheck/api/apps/**group**/	List applications by group

Upload a new application:

request

```
$ curl -u test@example.com -T vlc-2.0.4.dmg https://appcheck.codenomicon.com/appcheck/api/upload/
```

response

```
{
    "meta": {
        "code": 200
    },
    "results": {
        "id": 122,
        "sha1sum": "3fcdbdb04baa29ce695ff36af81eaac496364e82",
        "status": "B"
    }
}
```

云上安全测试 – 模糊测试

- 未知漏洞查找利器
  - 向被测试方发送异常数据，试图引起系统错误或服务失败的过程。
- HeartBleed发现原理

典型云厂商们的安全防护？

- 典型方案：
  - 在本地研发过程中执行安全测试
  - 对外（用户）提供安全测试服务

典型云厂商们的安全防护？

The Synopsys Software Integrity Toolbelt

Everything you need to build security and quality into your SDLC

SYNOPSYS®

STAGE 1 PLAN

RECOMMENDED TOOLS:

BSIMM: What is the current state of your software security?

MAP: How can you improve your software security?

Test Optimization: Have tests been prioritized and created?

STAGE 2 DESIGN

RECOMMENDED TOOLS:

Architecture Risk Analysis: Have secure design best practices been implemented?

Threat Modeling: How can an attacker exploit your design?

Security Control Design Analysis: Are there any missing or weak security controls?

STAGE 3 IMPLEMENT

RECOMMENDED TOOLS:

SAST: Are you finding and fixing bugs while you code?

Software Composition Analysis (SCA): Are there any bugs in the OSS or third-party software?

IAST: Are you able to identify real business threats?

Fuzz Test: Can each code component properly handle malformed inputs and unexpected loads?

STAGE 4 VERIFY

RECOMMENDED TOOLS:

SAST / SCA: Are there any remaining bugs in custom code or OSS/third-party software?

IAST: Can you automate IAST testing into your CI/CD processes?

DAST: Are you able to dynamically test your app before release?

Fuzz Test: Is the integrated code able to properly handle malformed inputs?

Pen Test: Can you manually hack your app before it goes live?

STAGE 5 RELEASE

RECOMMENDED TOOLS:

DAST: Are new bugs uncovered when the app is running?

Network Pen Test: Is the network configuration secure?

Pen Test: What impact could an attacker have?

STAGE 6 RESPOND

RECOMMENDED TOOLS:

Insider Threat Detection: How easily can you be breached?

Red Teaming: Are you set to prevent and respond to incidents?

Threat Intelligence: Is your organization monitoring for known breaches?

UCLOUD

典型云厂商们的安全防护？

- 安全测试与安全防护服务：

题外话：
软件研发过程中的安全防护？