FREEBUF

2017深圳站

FREETALK

深入CRS漏洞检测框架
——osprey(鱼鹰)

Cody

FREETALK
2017深圳站

TCC——斗象能力中心（Tophant Competence Center）

专注于以下安全领域：

- Web安全研究，0 Day挖掘，技术分享
- 突发事件，应急响应技术支持
- IoT智能硬件，包含固件安全、逆向分析、无线协议、智能APP等安全研究
- 机器学习，突破现有技术的不足，提升安全能力
- 企业级安全产品的安全研究和研发

— 提供前沿安全技术的研究与能力支撑

FREEBUF

FREETALK

2017深圳站

Osprey

斗象能力中心出品的开源漏洞检测框架

鱼鹰，寓意：快、精、准

FREEBUF

FREETALK

2017深圳站

osprey for what

- 快速漏洞检测
- 拒绝重复性工作，实现自动化
- 规范PoC编写，快速输出PoC
- 安全能力的积累与输出——开源

osprey for who

- 白帽子、渗透测试人员、运维人员、安全专家……
- 企业用户

how to use osprey

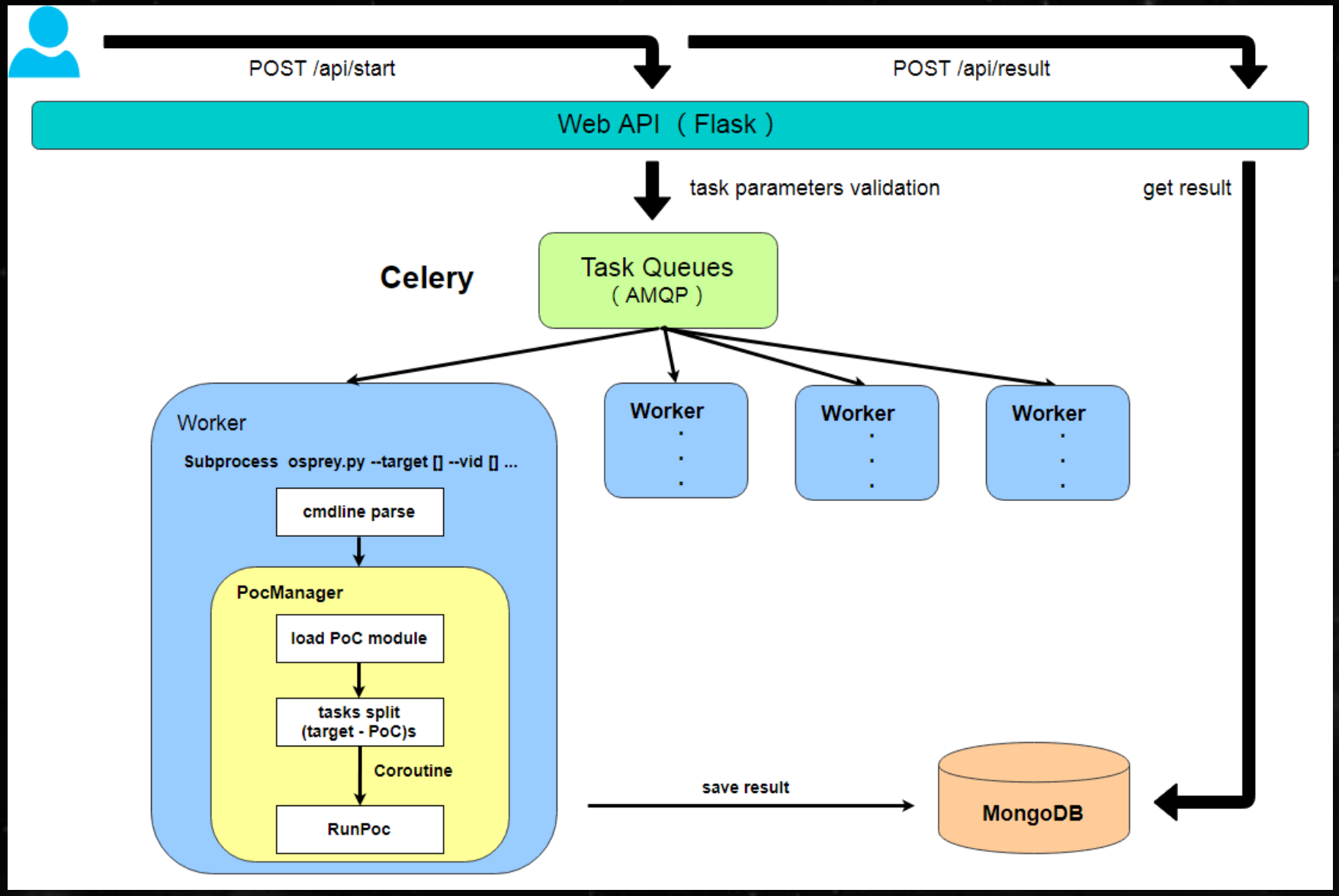
- 命令行与交互式Console：快速检测漏洞，输出结果
- Web API接口：构建自己的漏洞扫描器

FREEBUF

需求与难点

- 对单个目标的单个漏洞做检测
- 对多个目标的多个漏洞做全检测
- 不同PoC检测逻辑和结果的差异
- 任务的下发、调度、管理、任务执行结果的存储与取用
- 运行速度、性能、容错
- ……

构建一个以Flask为轻量级Web API接口，以Celery和RabbitMQ作为队列的任务调度和管理，以多进程和协程结合的执行方式作为Worker消费任务，以MongoDB存储任务执行结果的分布式漏洞检测框架



FREETALK
2017深圳站
FREEBUF

神马？？漏洞无回显？？PoC写不了？？

后台XSS、命令注入、SSRF……
有payload也没L用？？！

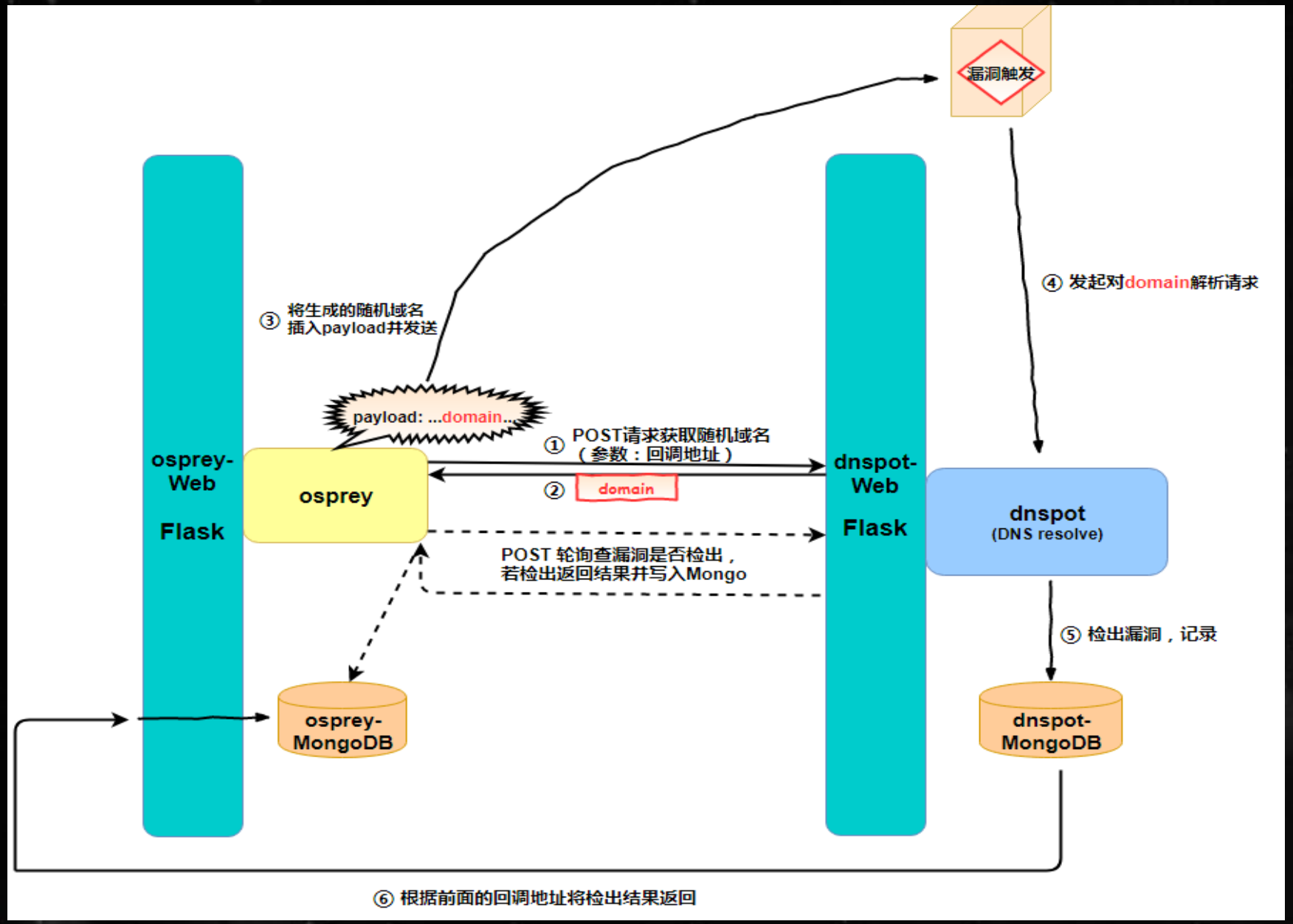
osprey + dnspot = 漏洞无所遁形

利用DNS做盲检测

- 利用DNS域名和解析做无回显漏洞的盲检测，将带有特定标识的域名作为payload的一部分，如在命令注入漏洞的检测中，使用“curl http://1234567abcdefg.blind.vulbox.com/”作为PoC的payload，当在你的名称服务器上收到对该域名的解析请求时，说明漏洞被触发了

dnspot

- TCC的另一个开源项目，实现了一个DNS解析和记录服务器
- 实现：一个域名 + 一台公网服务器 + 将该域名的Name Server配置为该台服务器 + 部署dnspot于服务器上
- 通过osprey.utils提供的接口，可以非常方便的联动dnspot，在PoC中简单的通过方法调用就能实现无回显漏洞的盲检测



FREETALK
2017深圳站
FREEBUF

视频演示

FREETALK

2017深圳站

FREEBUF

FREETALK

2017深圳站

osprey在手，漏洞跟我走

https://github.com/TophantTechnology/osprey

FREEBUF

FREETALK

2017深圳站

Thanks

FREEBUF