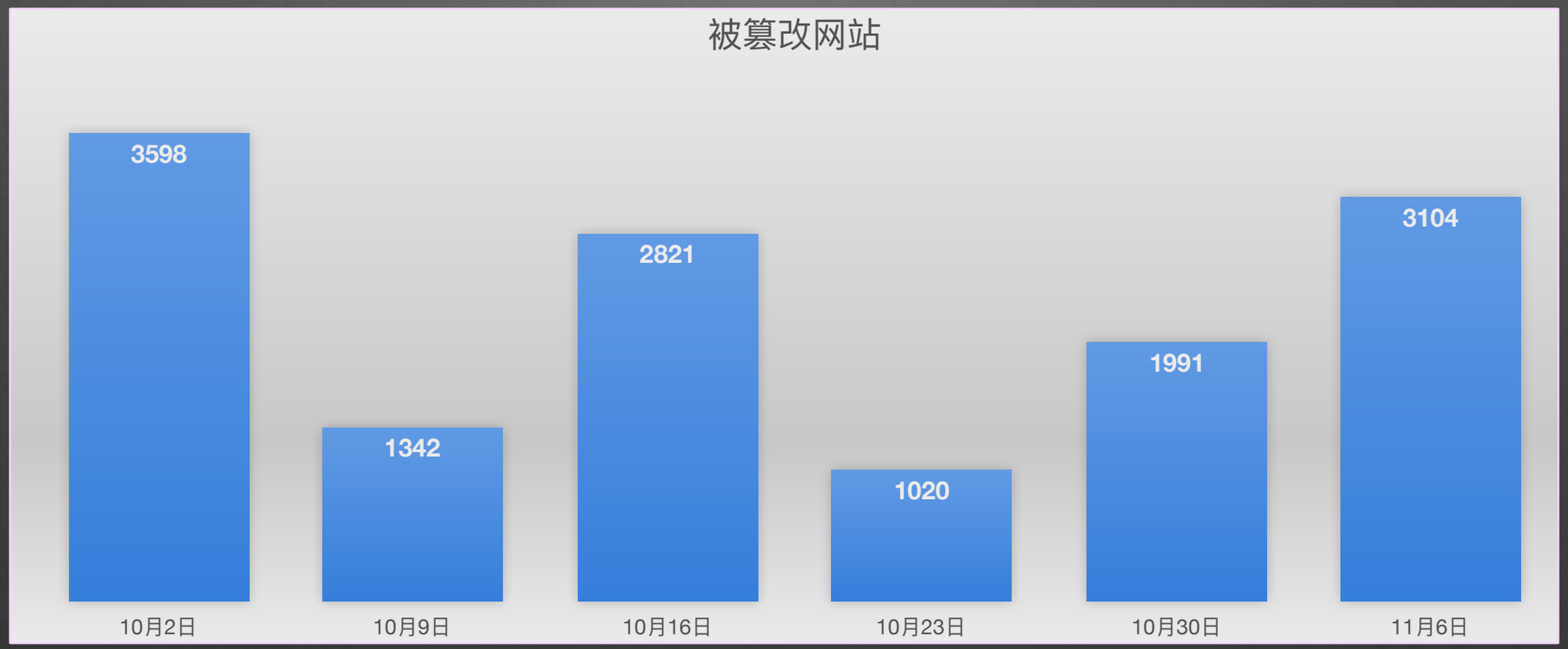
敏捷开发中的安全实践

郭洋 青松云安全

安全重要么?

网络安全的现实



数据来源：CNCERT互联网安全威胁周报

OWASP TOP10

- A1 SQL注入
- A2 失效的身份认证和会话管理
- A3 跨站脚本（XSS）
- A4 不安全的直接对象引用
- A5 安全配置错误
- A6 敏感信息泄露
- A7 功能级访问控制缺失
- A8 跨站请求伪造（CSRF）
- A9 使用含有已知漏洞的组件
- A10 未验证的重定向和转发

安全开发所面临的困难

开发的不同阶段漏洞的成本

编写代码 | 集成构建 | QA | 交付发布

$80/漏洞 | $240/漏洞 | $960/漏洞 | $7600/漏洞

数据来源：checkmarx

安全开发所面临的困难

- 对于安全没有认知
- 不知道如何将安全和开发结合起来
- 不知道如何编写安全需求，如何做安全测试
- 项目紧急，时间不够
- 安全是安全专家的职责，不是程序员负责的

如何兼顾敏捷开发同时还保证安全?

1，统一团队认知，明确职责

- 团队需要安全专家，但安全由团队一起负责
- 安全相关的用户故事需要针对性编写
- 安全专家对代码进行安全评审
- 安全专家组织安全代码开发培训
- 安全专家帮助QA进行安全测试

如何兼顾敏捷开发同时还保证安全?

2，完善流程

- 遵循编码规范(PHP-PSR，PEP8，OWASP)
- 使用框架开发，使用开源组件
- 在敏捷开发中使用安全工具
- 使用持续集成系统

如何兼顾敏捷开发同时还保证安全?

2，完善流程

SAST

工具：Fortify，ZAP，Dependency-Check
RIPS，Burp Suite，Brakeman

DAST

工具：AppScan，WebInspect，Arachni
SQLmap

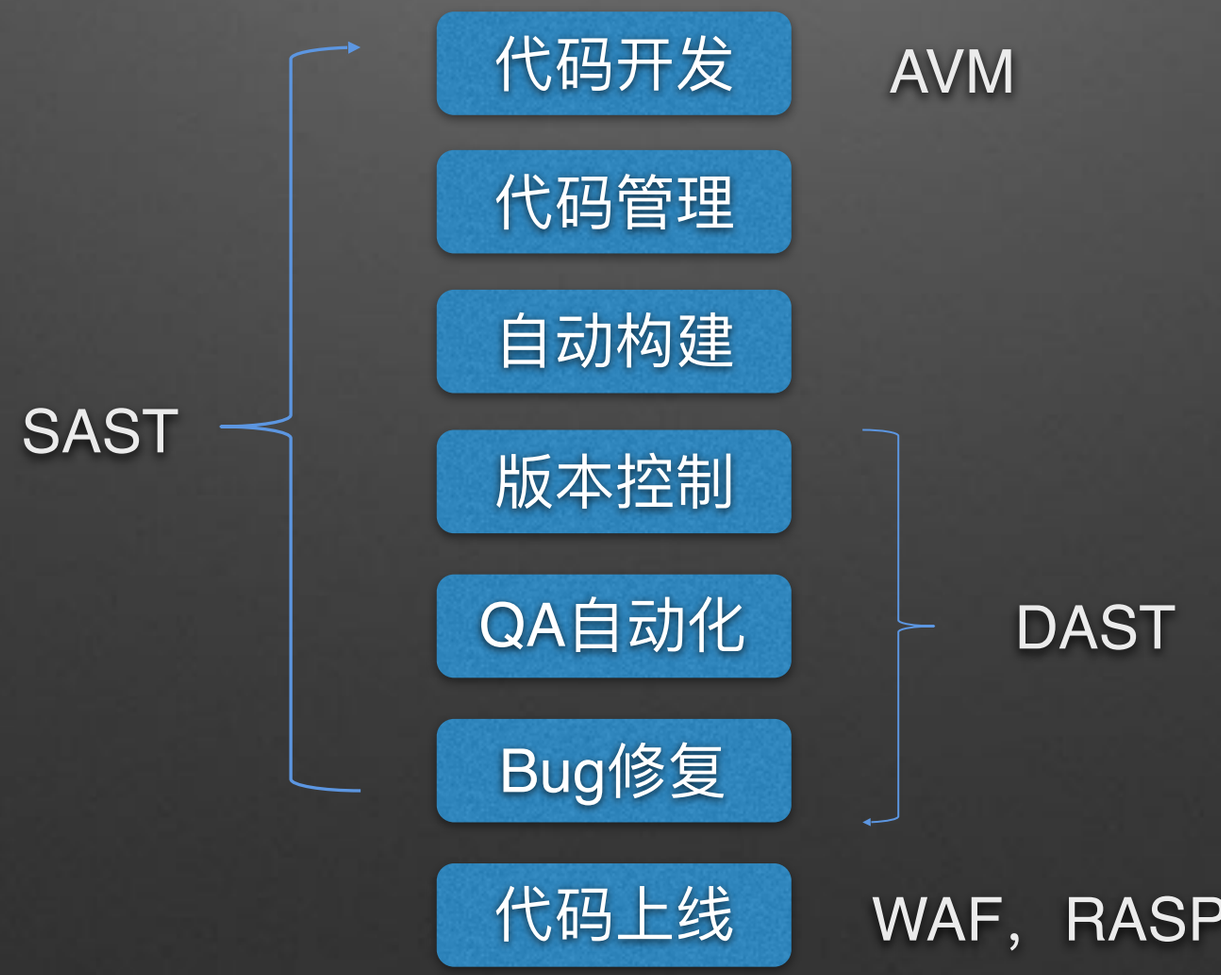
如何兼顾敏捷开发同时还保证安全?

3，结合敏捷开发流程的安全

故事分析	编写安全验收标准，安全专家，客户，QA
故事启动	确定安全验收标准，安全专家，开发，QA
故事开发	编写安全代码，开发，QA
故事验收	按安全标准验收，安全专家，开发，QA
故事测试	进行安全测试，安全专家，QA
故事演示	展示上线产品，团队，客户

如何兼顾敏捷开发同时还保证安全?

3，结合敏捷开发流程的安全



如何兼顾敏捷开发同时还保证安全?

4，敏捷和开发的平衡

- 根据规范编写安全代码
- 安全测试手工发现
- 工具自动化批量
- 结合CI/CD自动化

如何提高人的安全意识?

对于安全意识的提高，举一个例子
SSRF（Server-side Request Forgery）

危害:
URL为内网IP，直接访问内网资源
URL中包含端口，可用于扫描

```
guoyang@rMBP(09:47):~$ ping -c 1 012.0.0.1
PING 012.0.0.1 (10.0.0.1): 56 data bytes
^C
--- 012.0.0.1 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
guoyang@rMBP(09:47):~$ ping -c 1 0xa.0.0.1
PING 0xa.0.0.1 (10.0.0.1): 56 data bytes
^C
--- 0xa.0.0.1 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
guoyang@rMBP(09:47):~$ ping -c 1 167772161
PING 167772161 (10.0.0.1): 56 data bytes
^C
--- 167772161 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
guoyang@rMBP(09:47):~$ ping -c 1 10.1
PING 10.1 (10.0.0.1): 56 data bytes
^C
--- 10.1 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
guoyang@rMBP(09:47):~$ ping -c 1 0xA000001
PING 0xA000001 (10.0.0.1): 56 data bytes
^C
--- 0xA000001 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
```

如何提高人的安全意识?

HOST获取绕过

1. 如何正确的匹配出URL中Host?
2. 只要不是内网IP地址就可以吗?
3. 只要Host指向的IP不是内网IP即可吗?

1. http://233.233.233.233@10.0.0.1:8080/
2. http://127.0.0.1.xip.io/
3. HTTP 30X 跳转

总结

人，认知，规范，流程，工具

感谢

青松云安全

www.qssec.com

抗DDoS，WAF

SFDC SegmentFault Developer Conference