OWASP

Open Web Application Security Project

从软件开发角度解密OWASP TOP 10

应用安全与安全的开发

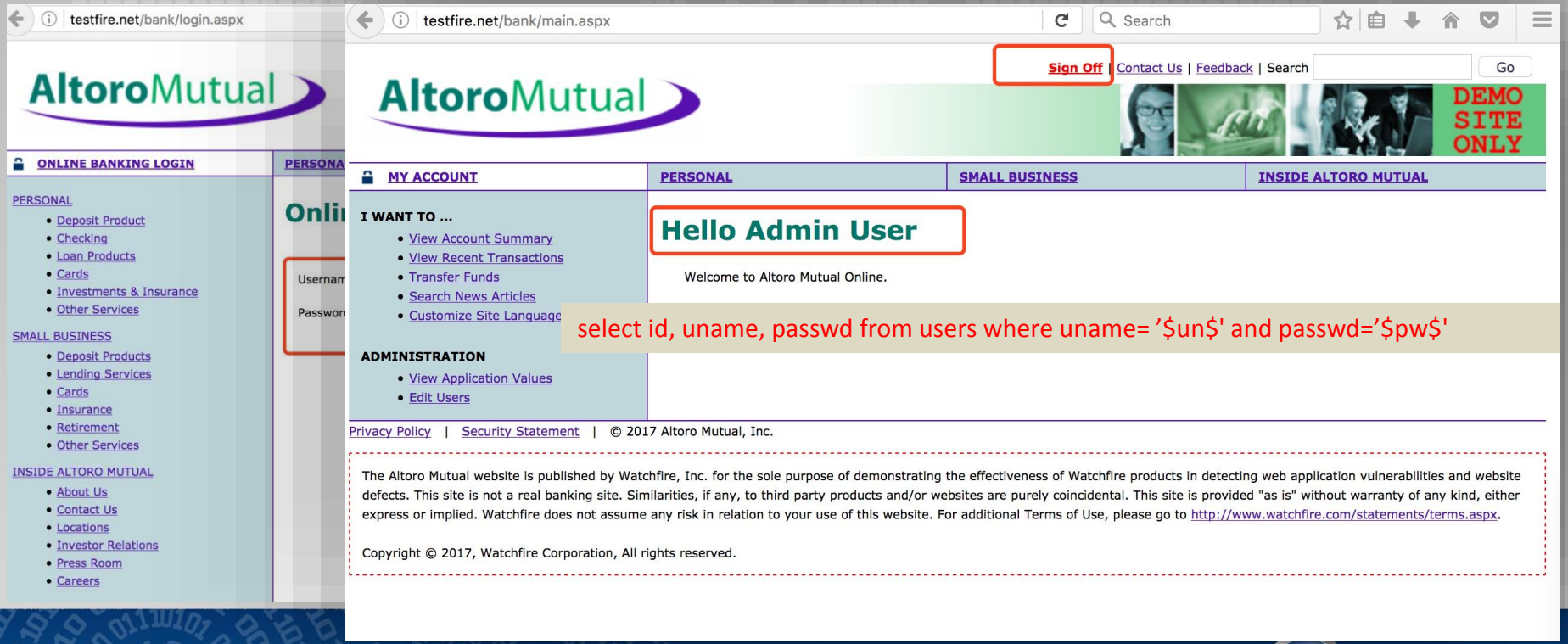
日程

- OWASP TOP 10浅析
- 安全开发演化
- 安全开发现状
- 企业所面临的安全挑战
- S-SDLC落地实现
- 研发视角解决OWASP TOP 10

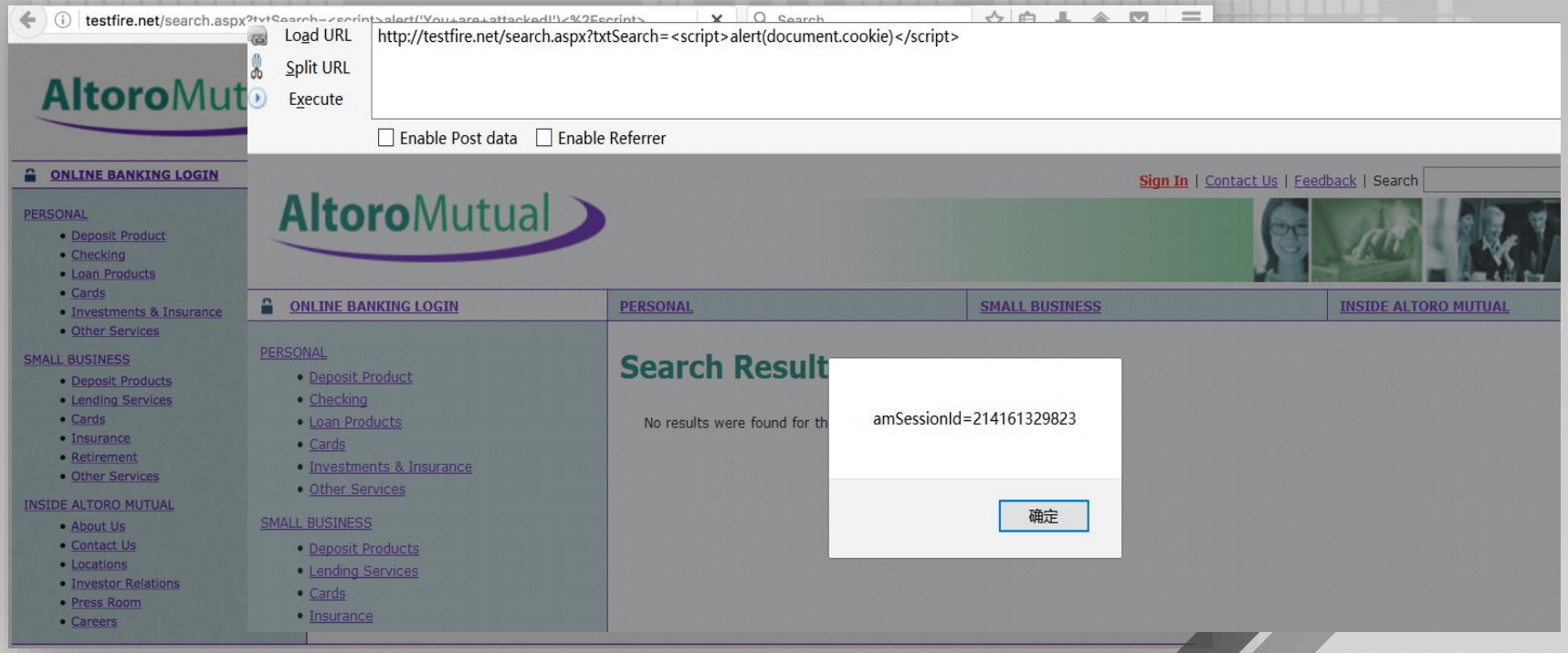
OWASP TOP 10

2013年版《OWASP Top 10》		2017年版《OWASP Top 10》
– 注入	→	A1:2017 – 注入
– 失效的身份认证和会话管理	→	A2:2017 –失效的身份认证
– 跨站脚本（XSS）	↘	A3:2017 –敏感信息泄漏
– 不安全的直接对象引用 [与A7合并]	∪	A4:2017 – XML外部实体（XXE） [新]
– 安全配置错误	↘	A5:2017 – 失效的访问控制 [合并]
– 敏感信息泄漏	↗	A6:2017 – 安全配置错误
– 功能级访问控制缺失 [与A4合并]	∪	A7:2017 – 跨站脚本（XSS）
– 跨站请求伪造 （CSRF）	☒	A8:2017 – 不安全的反序列化 [新，来自于社区]
– 使用含有已知漏洞的组件	→	A9:2017 –使用含有已知漏洞的组件
0 – 未验证的重定向和转发	☒	A10:2017 – 不足的日志记录和监控 [新，来自于社区]

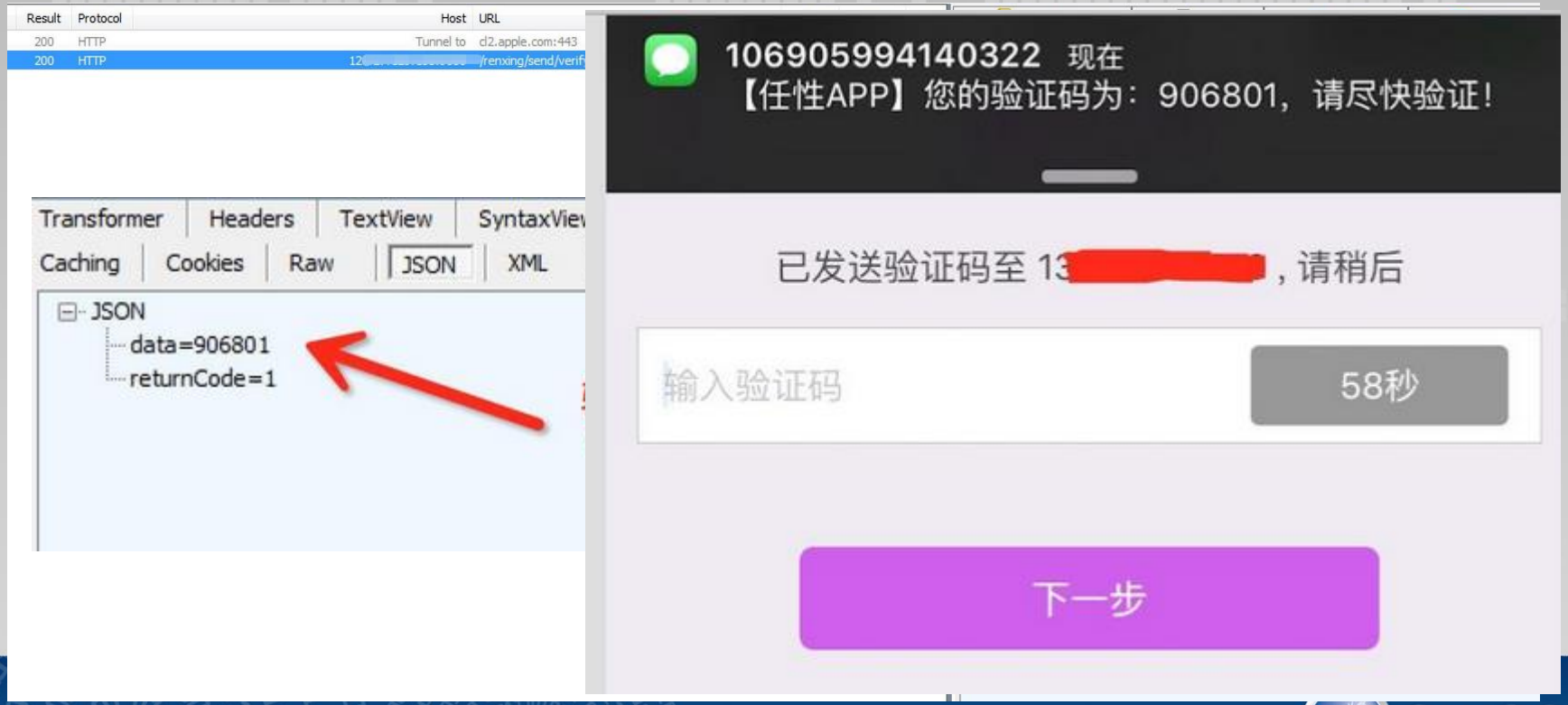
SQL Injection



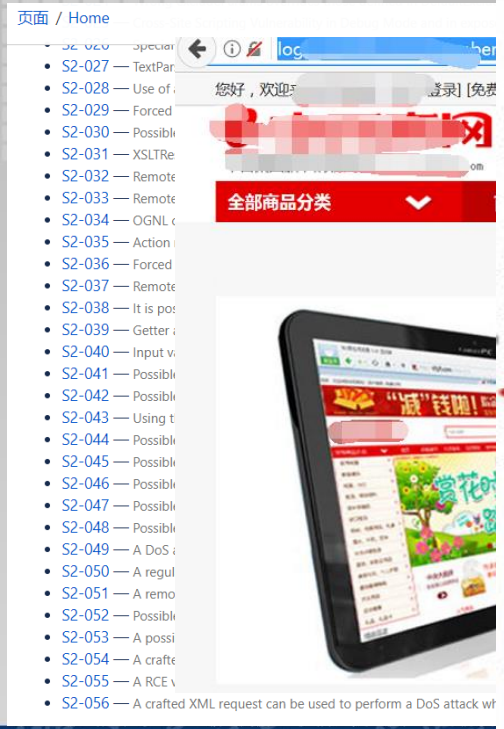
XSS



业务逻辑


Result
Protocol
Host
URL
200
HTTP
Tunnel to
cl2.apple.com:443
200
HTTP
/renxing/send/verif
Transformer
Headers
TextView
SyntaxVie
Caching
Cookies
Raw
JSON
XML
JSON
data=906801
returnCode=1
106905994140322 现在
【任性APP】您的验证码为：906801，请尽快验证！
已发送验证码至 13
，请稍后
输入验证码
58秒
下一步

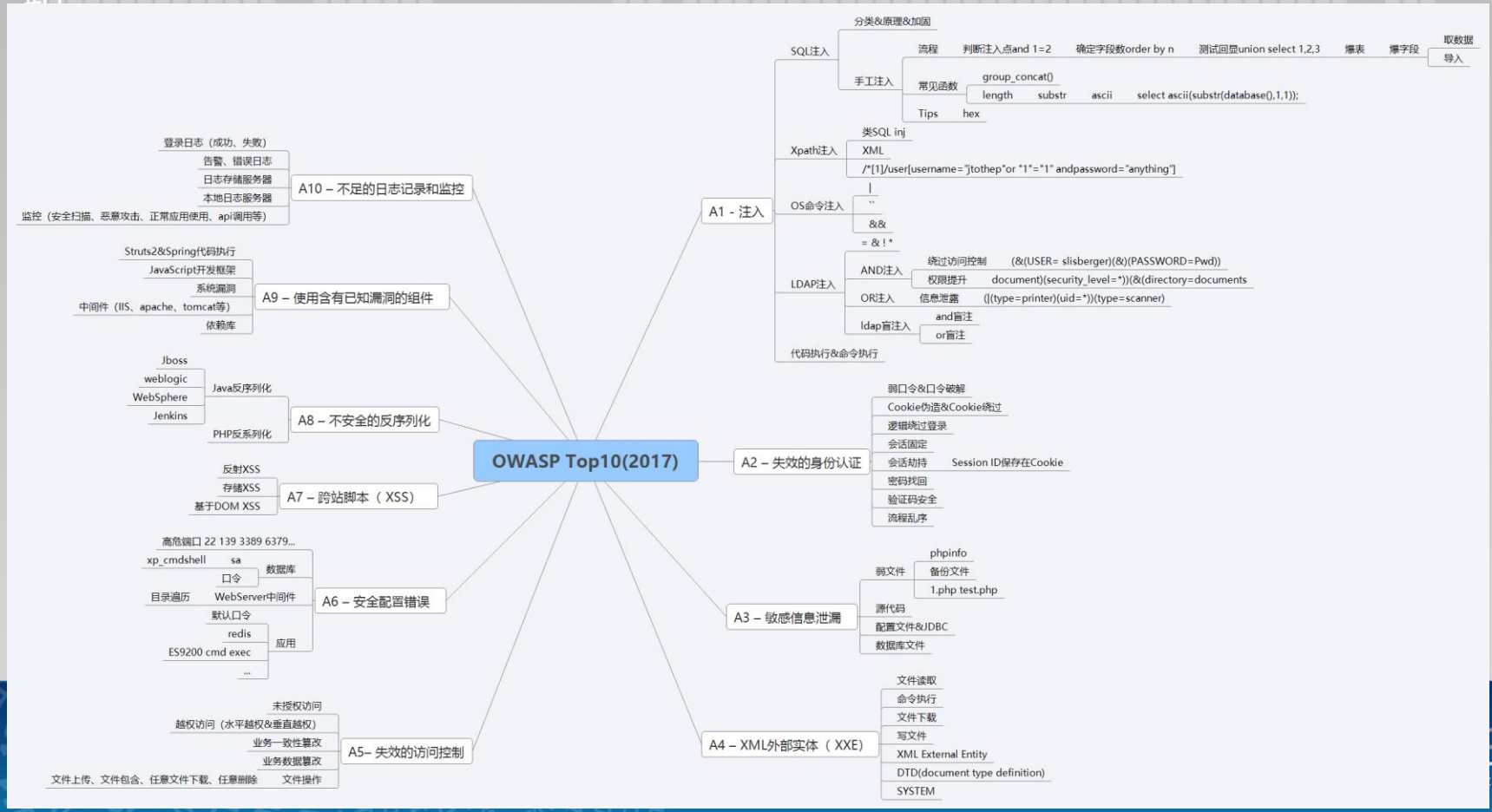
第三方插件


页面 / Home
S2-027 — TextPar
S2-028 — Use of
S2-029 — Forced
S2-030 — Possibl
S2-031 — XSLTRe
S2-032 — Remote
S2-033 — Remote
S2-034 — OGNL
S2-035 — Action
S2-036 — Forced
S2-037 — Remote
S2-038 — It is pos
S2-039 — Getter
S2-040 — Input v
S2-041 — Possibl
S2-042 — Possibl
S2-043 — Using t
S2-044 — Possibl
S2-045 — Possibl
S2-046 — Possibl
S2-047 — Possibl
S2-048 — Possibl
S2-049 — A DoS
S2-050 — A regul
S2-051 — A remo
S2-052 — Possibl
S2-053 — A possi
S2-054 — A crafte
S2-055 — A RCE
S2-056 — A crafted XML request can be used to perform a DoS attack wh
全部商品分类


首页
微博正文
公开
EOS博士
5-30 01:08 来自iPhone客户端 已编辑
+关注
BM刚刚在eos开发者群里对360今天的发布做出了回应：今天中国的漏洞新闻是一个FUD即制造恐慌，因为该漏洞早在被发布前就已经修复了，而且是一个较为常见的漏洞，但是bm称该漏洞并不能改写可执行内存，且不能获得root权限，除非部署节点时就已经是以root用户身份来运行。同时bm表示对这种将该已知已修复漏洞在系统测试期间同时是美国团队需要至少几小时才能回复的情况下大肆报道的行为表示不赞同。另外团队已基本修复了目前所有被发现的漏洞，大部分漏洞是来源于第三方代码库而非eos核心代码。最后bm表示欢迎广大程序猿继续提交发现漏洞赢得赏金，但是那些制造恐慌传播FUD的提交者将失去获取赏金和认可的资格。eos
we have one crash in our unit tests in wavm that we are fixing
that chiense report is FUD, it was fixed before it was even published
what bugs?
Can we get a post mortem on the fixes?
in this case it was a copy/paste assert from binaryen code that
so far the vast majority of reported bugs have actually been in 3rd party libraries we build on
it is one thing to over-write memory, but they wouldn't over-write executable memory
and they wouldn't get root access
and they likely wouldn't even get the transaction broadcast


帮助中心
在线客服
购物车结算
新用户，免费注册>
忘记密码？
登 录
支付宝
网易
360

OWASP TOP 10攻击思路



安全离我有多远？

日程

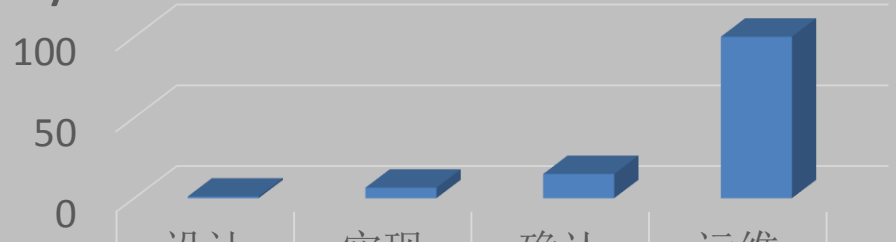
- OWASP TOP 10浅析
- 安全开发演化
- 安全开发现状
- 企业所面临的安全挑战
- S-SDLC落地实现
- 研发视角解决OWASP TOP 10

日程

- OWASP TOP 10浅析
- 安全开发演化
- 安全开发现状
- 企业所面临的安全挑战
- S-SDLC落地实现
- 研发视角解决OWASP TOP 10

安全开发现状

IBM System Science Institute



	设计	实现	确认	运维
修复缺陷的相对成本	1	6.5	15	100

日程

- OWASP TOP 10浅析
- 安全开发演化
- 安全开发现状
- 企业所面临的安全挑战
- S-SDLC落地实现
- 研发视角解决OWASP TOP 10

有安全问题，当然要解决，问题是：
1. 请问题一次性告诉我，我好统筹解决
2. 谁能告诉我们如何解决才是最正确的，我经常遇到解决的问题被打回重新解决？
3. 我要保证产品交付，我不想做没有证据证明确实有安全问题的情况下来解决那些不明确的问题

企业面临的安全挑战-研发团队

绝大多数安全问题是由研发团队写代码写出来的，我们需要制订各种规范，让所有的人遵守：

- Java安全开发规范
- C、C++安全开发规范
- Struts安全开发规范
- Spring安全开发规范
- Web安全开发规范
- Desktop Software安全开发规范
- Server Side Software安全开发规范
- 敏感信息保护策略
- 加密算法安全使用指南
- ……

企业面临的安全挑战-安全团队

#1

最近 业界安全事件频发，我们公司全线产品的安全状态是什么？CTO/ CSO，明天给我一份安全现状评估报告给我！

高层领导

#2

老大，这些信息得从研发团队搜集，否则很难得到反应真实状况的数据！

CSO

#3

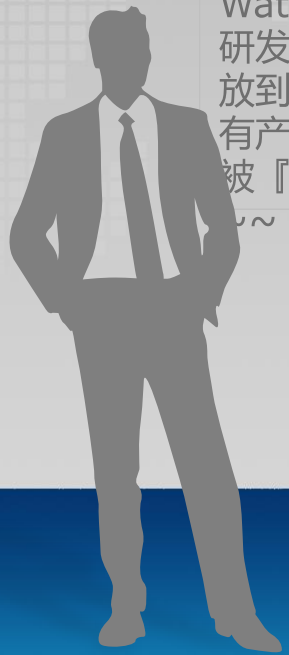
你们不是全程跟踪安全相关的事务的吗，怎么会没有数据？

CTO

企业面临的安全挑战-
CSO/CTO/Highlevel

企业面临的安全挑战-开发流程

Agile:
安全开发流程涉及的工作刚展开，一个Sprint已经结束了~~



Waterfall:
研发团队总是习惯于将安全问题放到Release的末尾，最终如果有产品交付时间冲突，安全将会被『和谐』掉，最终成为烂尾楼了~~

企业面临的安全挑战-工具的利与弊

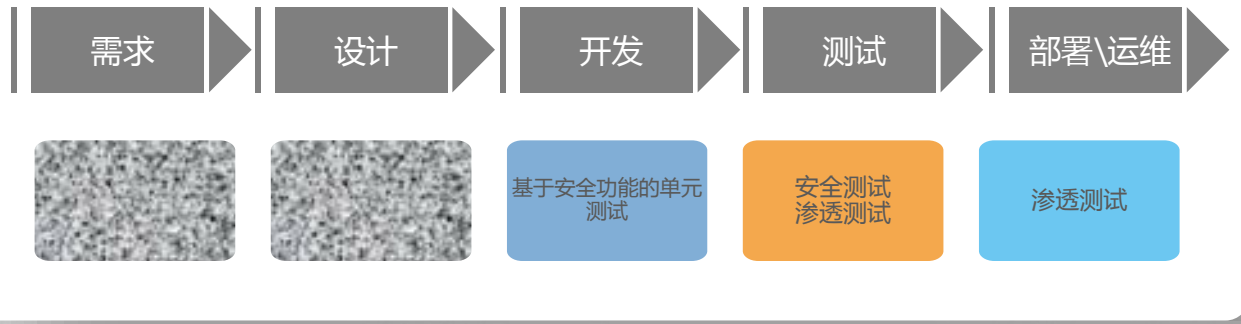
日程

- OWASP TOP 10浅析
- 安全开发演化
- 安全开发现状
- 企业所面临的安全挑战
- S-SDLC落地实现
- 研发视角解决OWASP TOP 10

初识S-SDLC

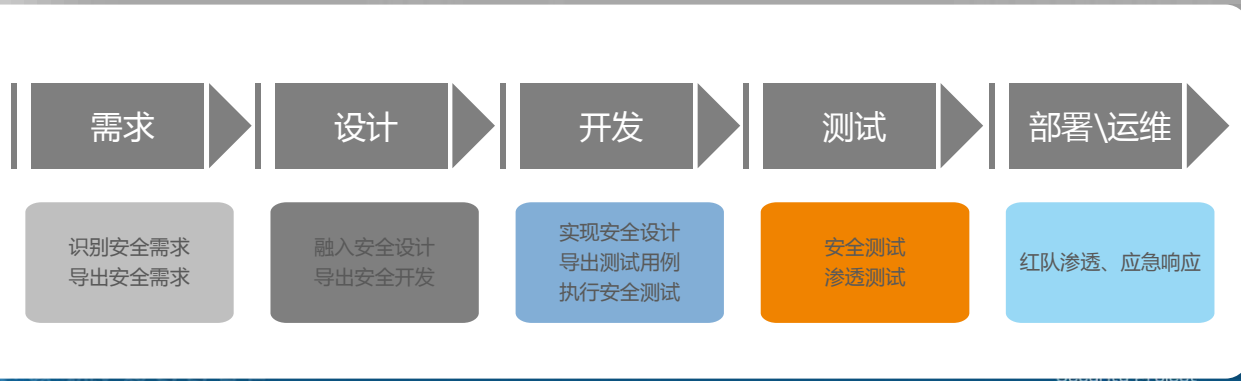
传统的

安全开发过程



S-SDLC

安全开发过程



S-SDLC流程关键要素

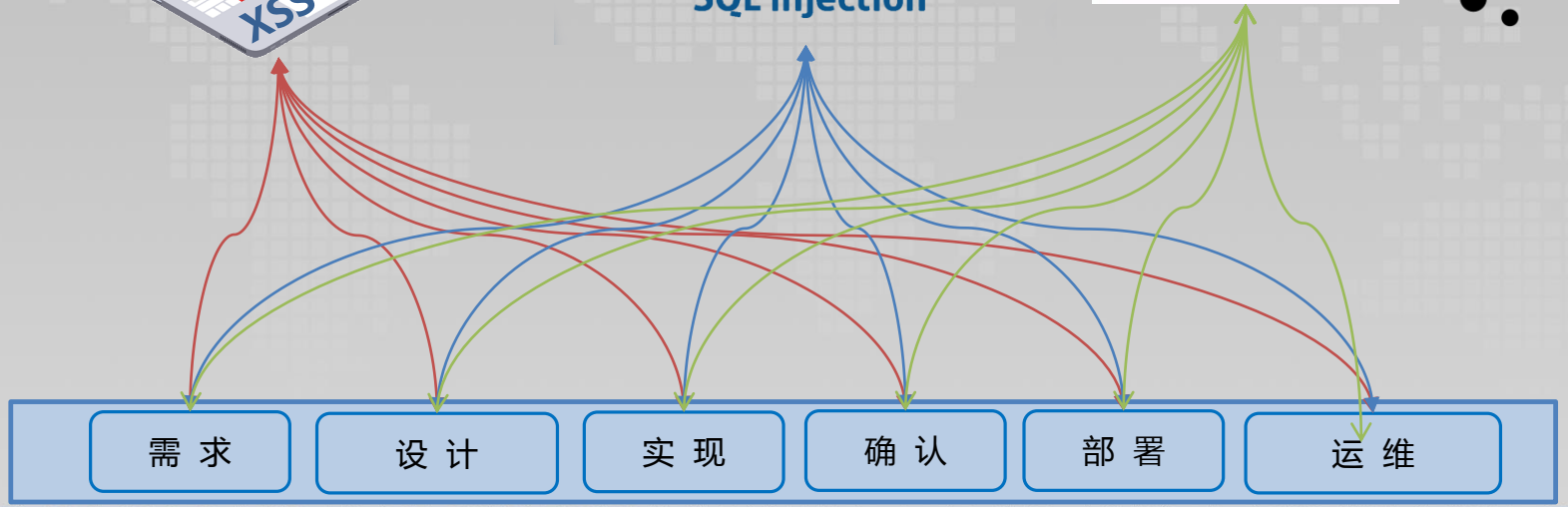
- 1、企业必须自上而下推行S-SDLC实施，且有相应的组织结构支撑
- 2、S-SDLC要与企业的质量管理体系相结合
- 3、建立合适的人员培训体系
- 4、用度量体系将S-SDLC实施效果可视化
- 5、产品的安全目标决定S-SDLC的过程
- 6、威胁模型可以使产品避免大的设计风险
- 7、安全特性组件化可尽量避免编码漏洞
- 8、管理第三方软件的风险
- 9、安全服务化和自动化是实施DevSecOps的基础
- 10、S-SDLC工具链

日程

- OWASP TOP 10浅析
- 安全开发演化
- 安全开发现状
- 企业所面临的安全挑战
- S-SDLC落地实现
- 研发视角解决OWASP TOP 10

OWASP TOP 10解决

Struts



S-SDLC 云平台容器

服务
持续集成
报告中心

知识积累和资源管理平台

项目团队安全培训
需求安全评估
安全设计（TMT）
安全实现（IAST）
安全部署（安全配置）
安全运维（RASP）
需求安全分析报告
安全威胁分析报告
自动、人工代码审核报告
渗透、安全测试及确认报告
安全部署报告
安全运维报告

专业性极强的平台技术支撑团队

安全领域全栈专家
威胁分析专家
安全实现技术解决方案专家
渗透、安全测试及确认专家
安全配置专家
安全运维专家

思考-S-SDLC支撑平台

AST技术比较	IAST（VulHunter）	SAST	DAST
开发流程集成度	无缝集成开发和测试阶段，零成本完成安全测试	开发阶段，成本较高	测试阶段，成本较高
误报率	较低	较高	最低
测试覆盖度	高，受功能测试覆盖度保障	高	低
检测速度	准实时，和应用程序复杂度无关	非实时，和应用程序复杂度相关，随代码量增加呈指数增长	非实时，和应用程序复杂度相关，程序越复杂，测试用例越多，速度越慢
支持检测的漏洞类型	最多	部分	部分
第三方软件及其漏洞检测	完全支持	有限支持	非常有限
漏洞信息丰富程度	动态数据流+请求和响应信息+配置文件+...	只有静态数据流	只有请求和响应信息
“脏”数据影响	无	无	有
多项目并发	完全支持多应用进行检测	非常有限，通常一个扫描引擎只能同时扫描一个应用	非常有限，扫描器较为耗费资源
部署和使用	简单	复杂	复杂

CWASP CSSP ?

CWASP CSSD ?

CISP ?

CISSP ?

(ISC)² ™

International Standard for Information Security

中国信息安全测评中心

China Information Technology Security Evaluation Center

思考-培训

OWASP

Open Web Application Security Project

谢谢