



企业SDL实践与经验

美图安全经理、Security Paper发起人

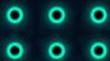


标准化





1. 安全培训
2. 需求评估
3. 产品设计
4. 代码编写
5. 渗透测试
6. 上线发布
7. 应急响应





WEB安全培训

- 针对服务端开发
- 哪里容易出现漏洞
- 怎么写会更安全

APP安全培训

- 针对APP开发
- 数据加密存储
- 不应该存储敏感数据

安全意识

- 针对全体项目成员
- 敏感数据处理办法
- 如何发送敏感数据





后门参数

部署安全检查

身份认证逻辑安全

数据访问机制

集中验证

外部一体化

入口点

外部API

应用系统自身架构安全

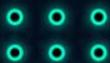
应用系统软件功能安全设计要求

应用系统存储安全设计要求

应用系统通讯安全设计要求

应用系统数据库安全设计要求

应用系统数据安全设计要求



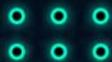


危险函数

安全配置

框架安全

常见安全问题代码示例





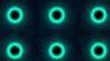
渗透测试 — 速度&深度

IT 2019

自动化扫描

常见场景快速测试点

代码安全检查

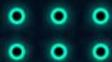




上线发布

FIT 2019

1. 安全嵌入上线流程
2. 安全准入
3. 安全检查





应急响应

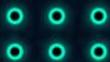
应急响应方案

确保方案落地到人

有电话号码

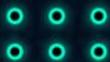
遏制

复盘



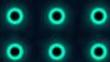


为什么流程这么难推动？



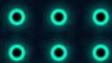


君子协定到底可以不可以？





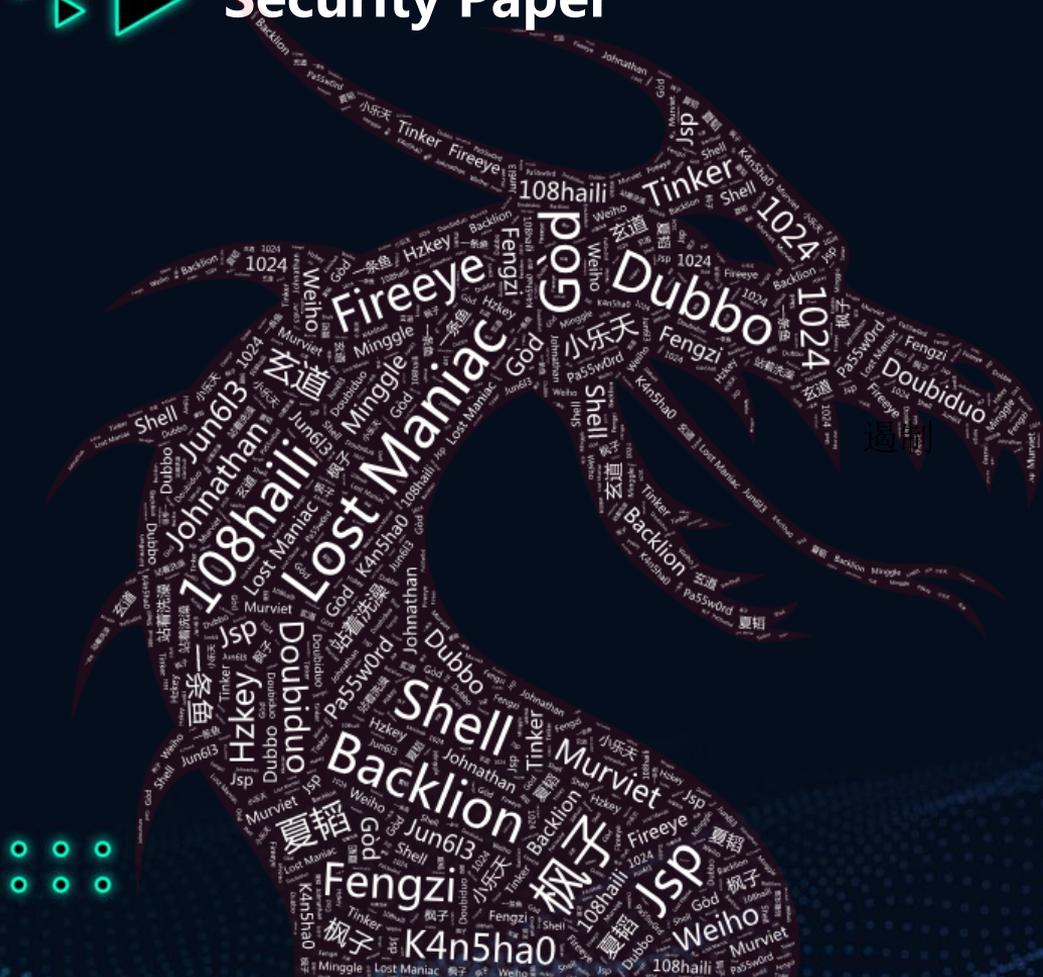
金杯共饮之 白刃不相饶！





Security Paper

IT 2019





REEBUF | 

THANKS