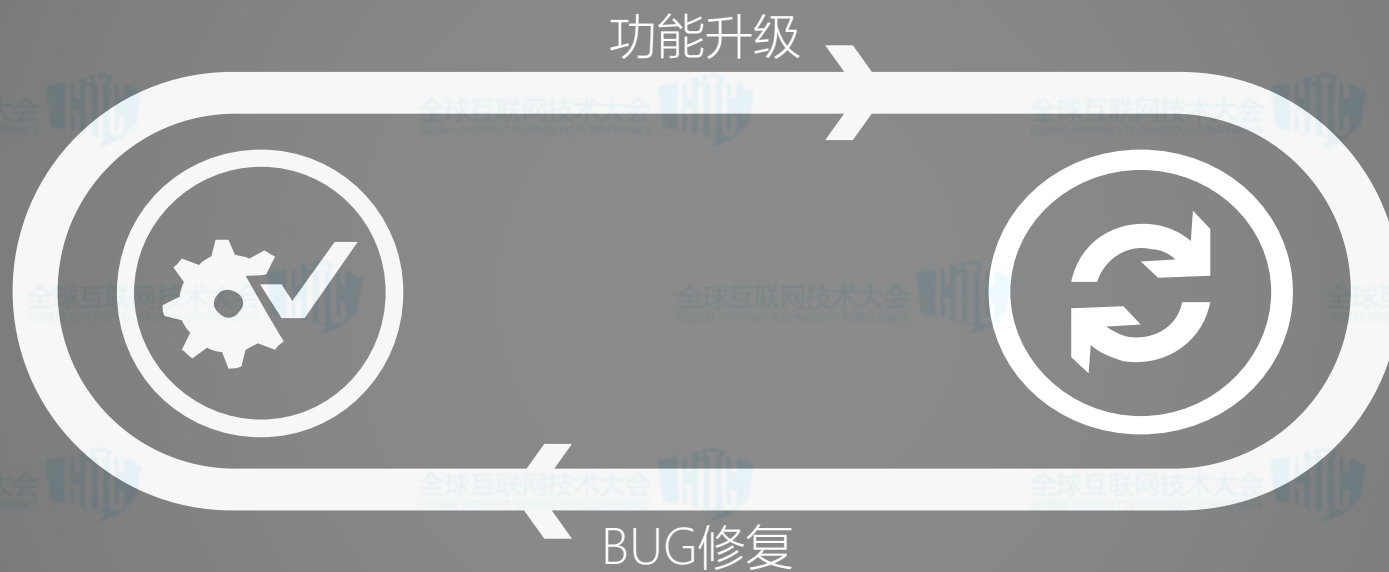




1000

10-20



漏洞消消乐

沃顿在线 · 朱磊

讲师简介



朱磊

- 沃顿在线 执行总裁（邦德）
- 复旦大学MSE 外聘主讲、顾问
- GITC 演讲嘉宾、专家团成员
- WOT 演讲嘉宾、联合出品人
- 完美世界优秀讲师
- 京东技术学院金牌讲师
- 天融信 CISP讲师
- ISO 27001 Foundation

运维

安全

研发



VS.



VS.



例

逻辑漏洞

命令执行

XSS跨站

配置错误

例

逻辑漏洞

用户注册
用户登录
订单系统
活动系统
积分系统
短信接口
业务接口

命令执行

应用框架

XSS跨站

用户资料
用户注册
收获地址
用户评论

配置错误

传输过程
应用配置
服务配置
错误页面

输入输出

文件上传

认证与会话

登录与注册

权限控制

开源框架



- 跨站脚本攻击
- 注入攻击
- 跨站伪造请求
- 篡改请求信息

输入输出

文件上传

认证与会话

登录与注册

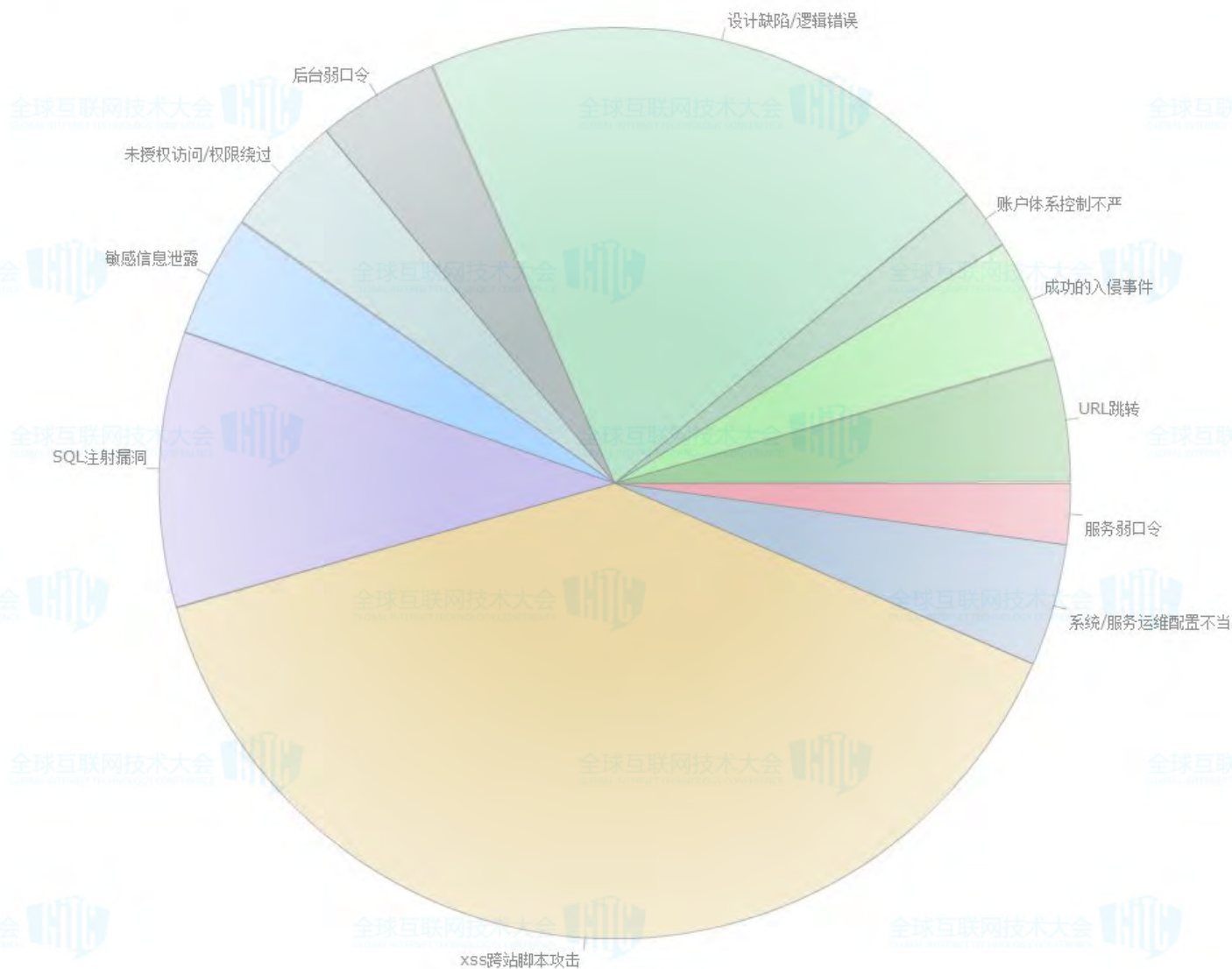
权限控制

开源框架

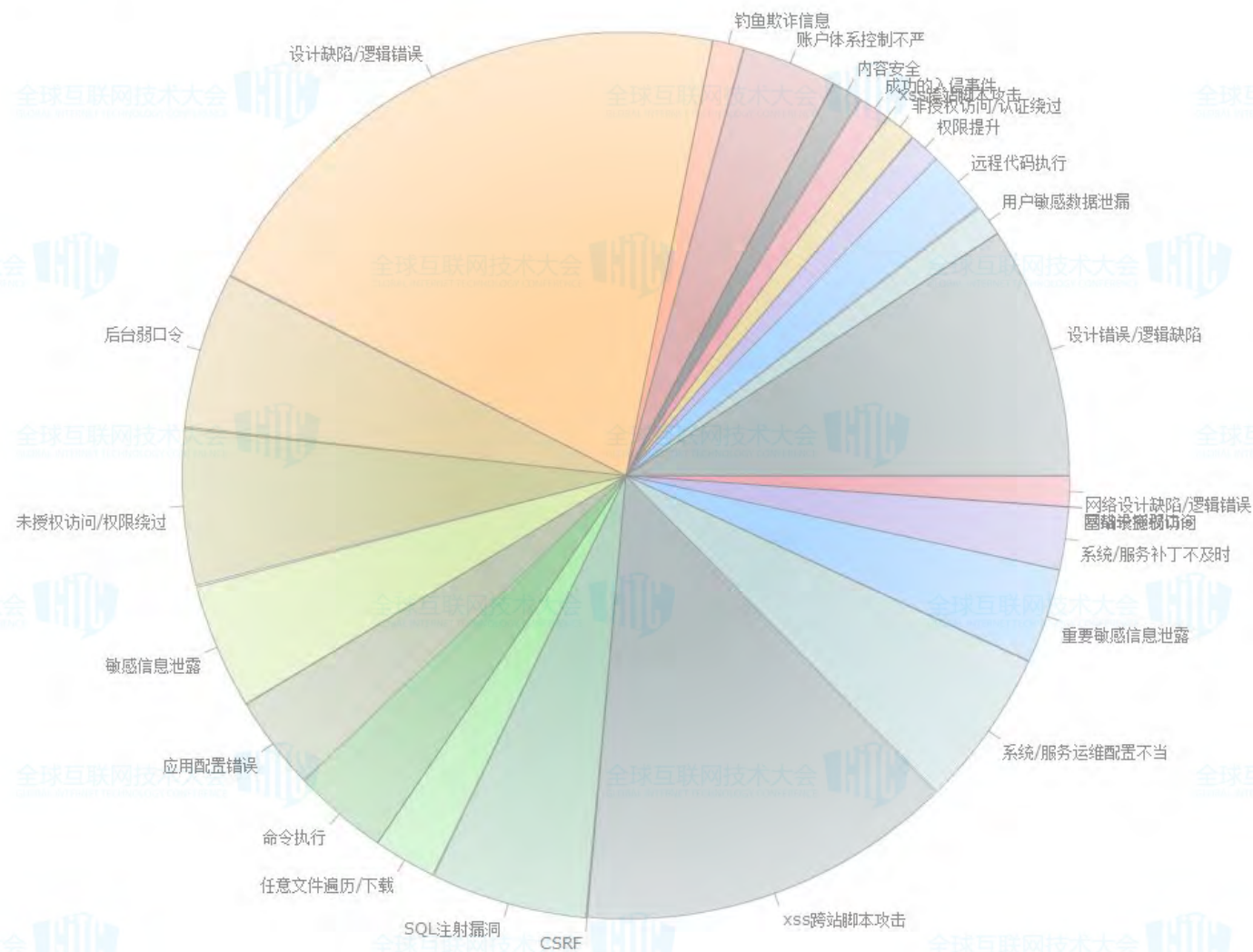


- 上传WEB脚本
- 修改上传POST包
- 伪造合法文件头

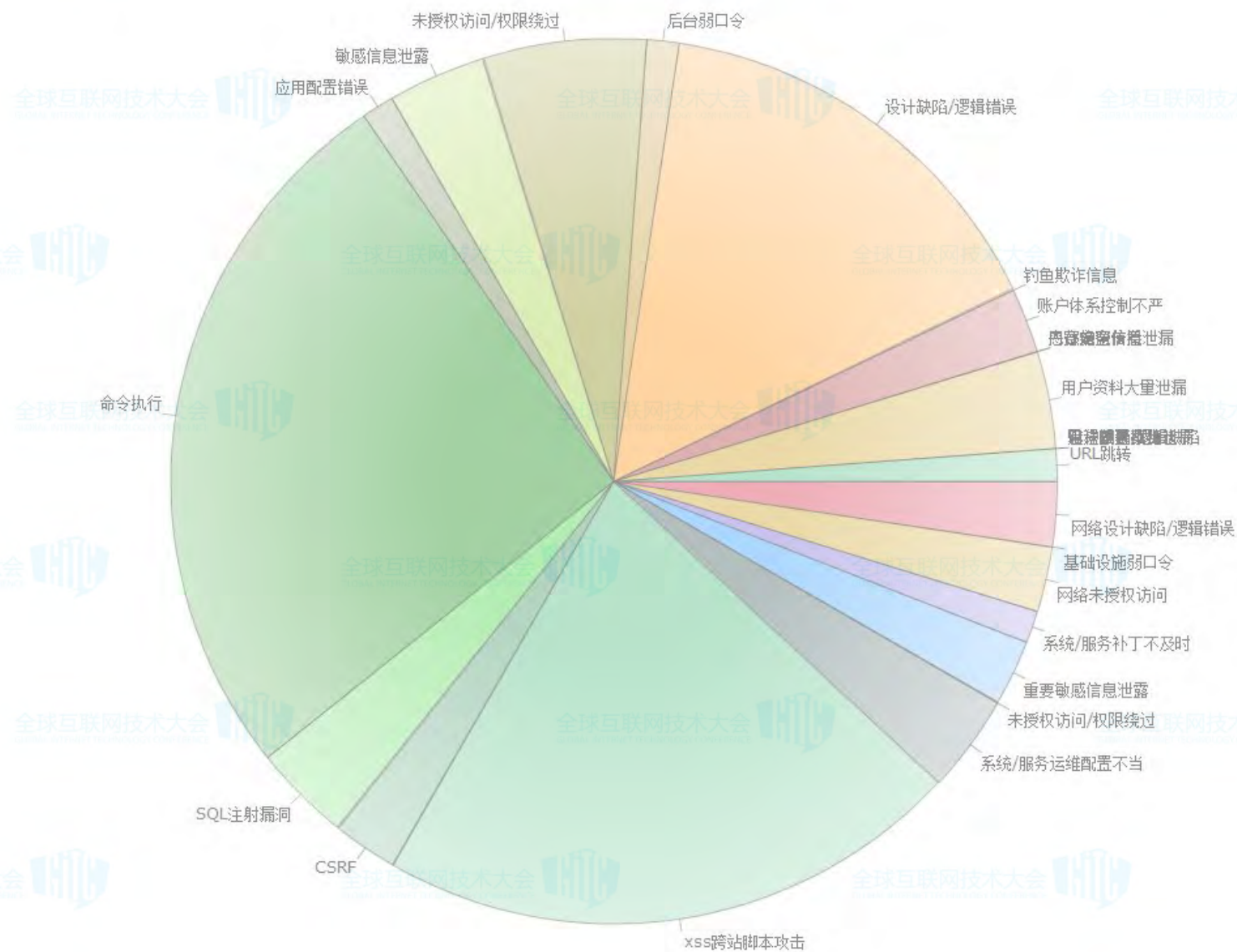
携程旅行网漏洞类型统计



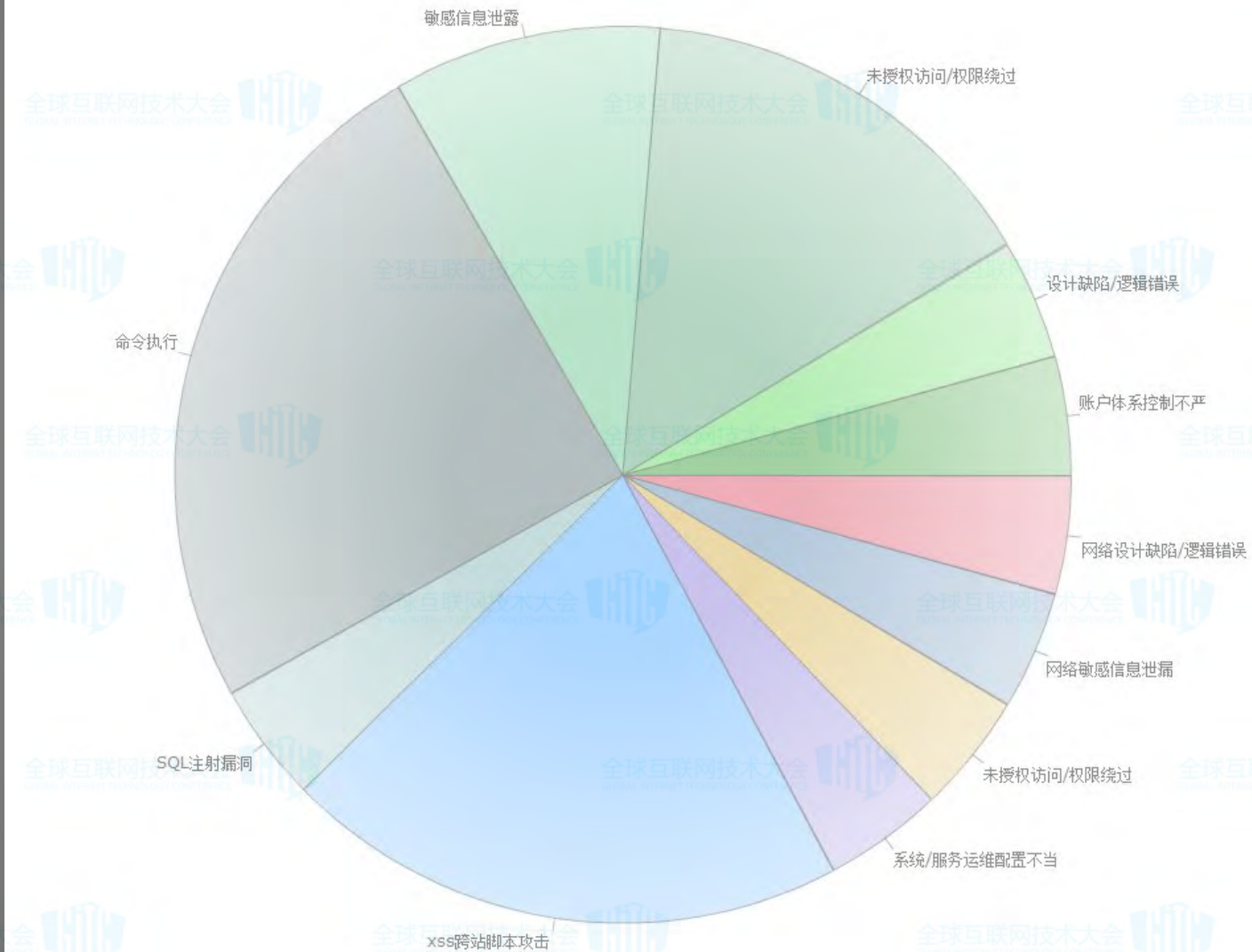
阿里巴巴漏洞类型统计



京东商城漏洞类型统计



1号店漏洞类型统计



阿里巴巴

逻辑漏洞

设计缺陷

XSS跨站

SQL注入

京东商城

逻辑漏洞

命令执行

XSS跨站

SQL注入

携程网

配置错误

命令执行

XSS跨站

SQL注入

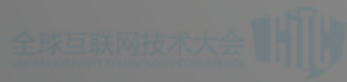
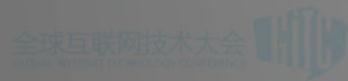
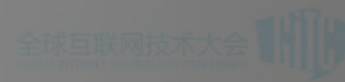
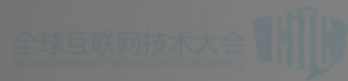
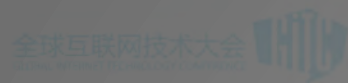
1号店

配置错误

命令执行

XSS跨站

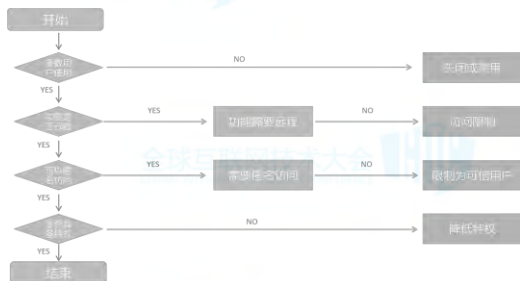
权限绕过



效率为王

基于业务的风险检测方法

- Blog Archive » 利用HTTP Basic认证进行钓鱼攻击.pdf
- Blog Archive » 逻辑问题合集.pdf
- Blog Archive » 权限控制之水平权限案例.pdf
- Blog Archive » 任意文件读取案例.pdf
- Blog Archive » 支付安全那些事.pdf
- Blog Archive » 撞库与黑客攻击知多少.pdf



发布

周期例行

测试

- P2P FRD (P2P Finance Risk Detection)
- ECRD (Electronic Commerce Risk Detection)
- GSRD (Government Service Risk Detection)
- IRD (Internet Risk Detection)

开发

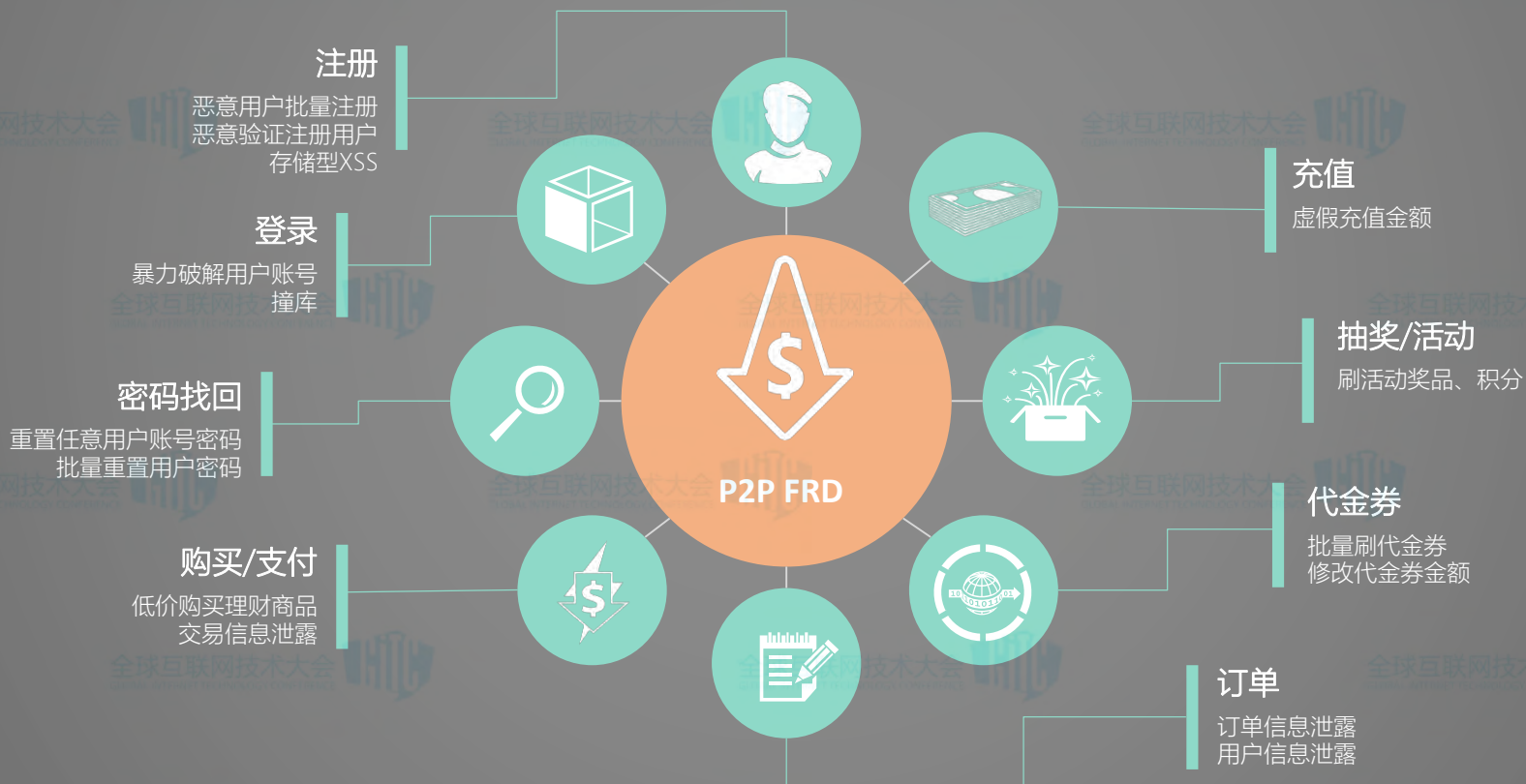
代码级解决方案

设计

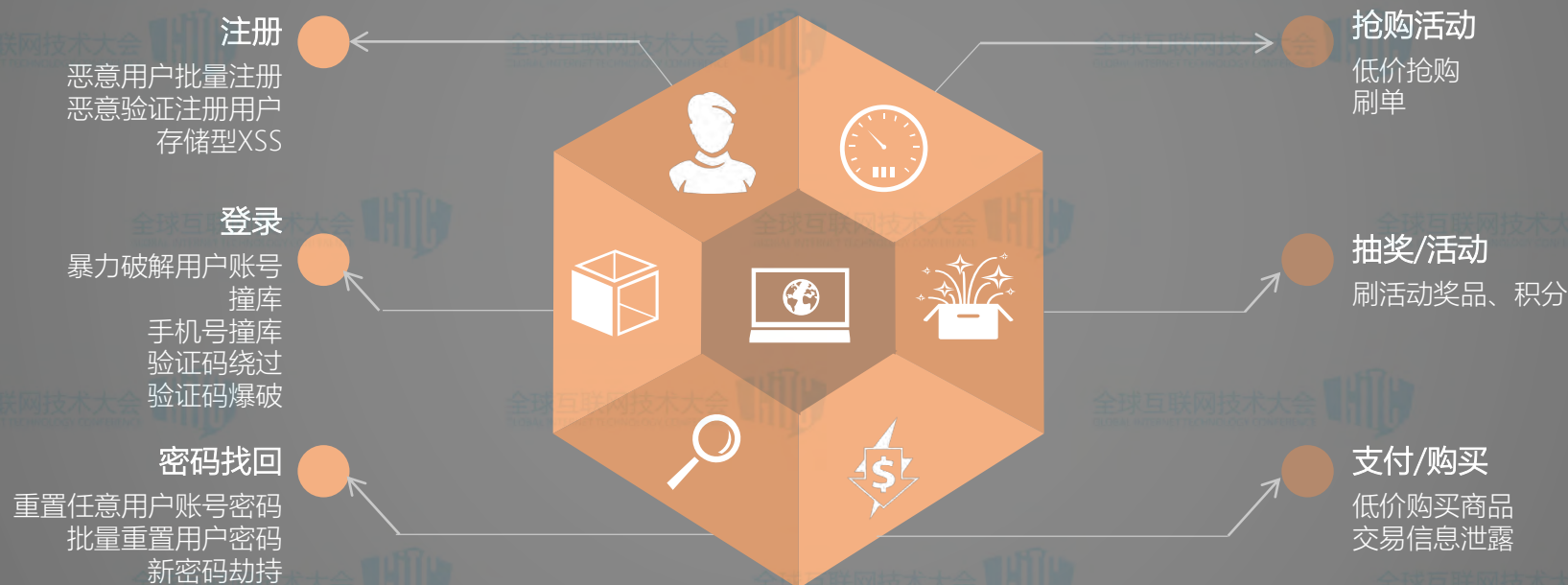
威胁建模

需求

P2P FRD (P2P Finance Risk Detection)



ECRD (Electronic Commerce Risk Detection)



漏洞发现

技术支持

沉淀
归类

时间管理

培训

THANKS – THE EDN