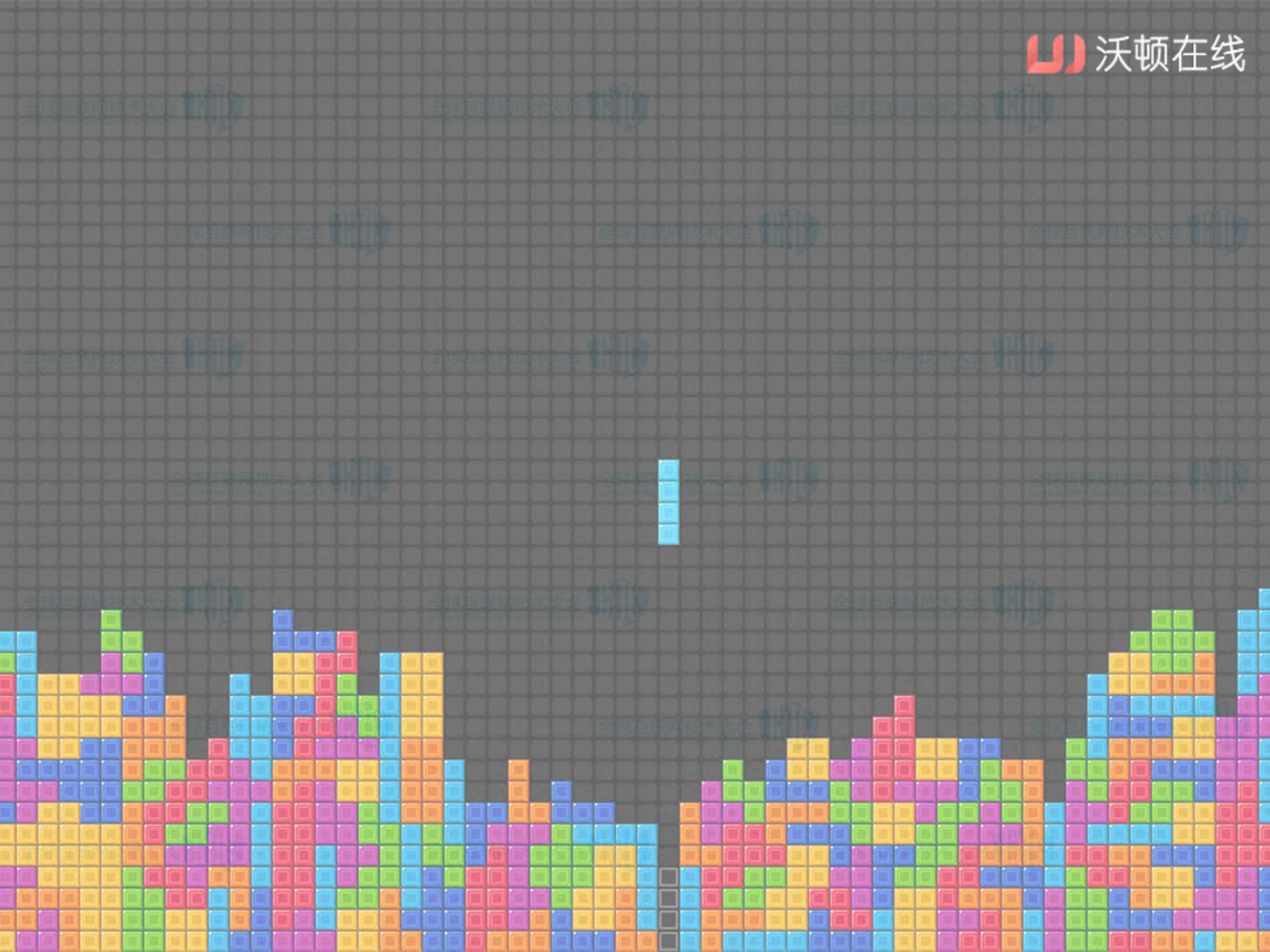
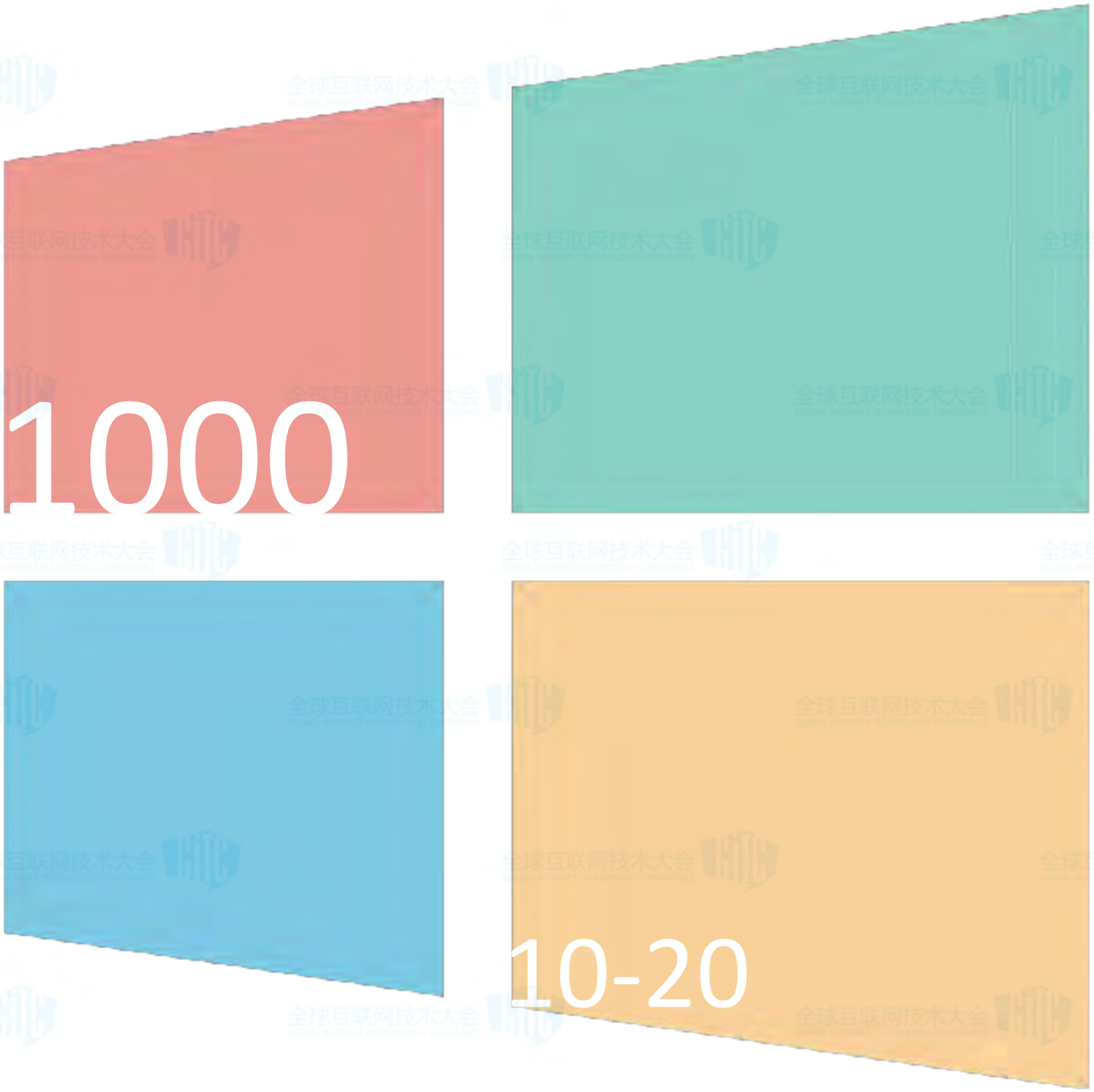
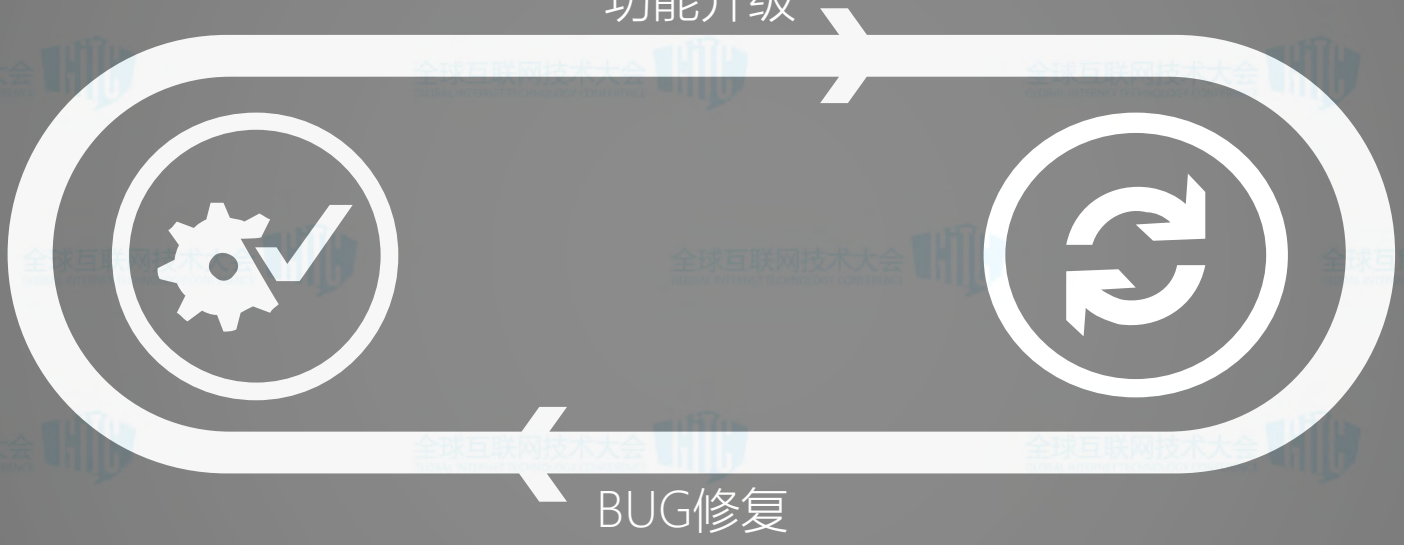


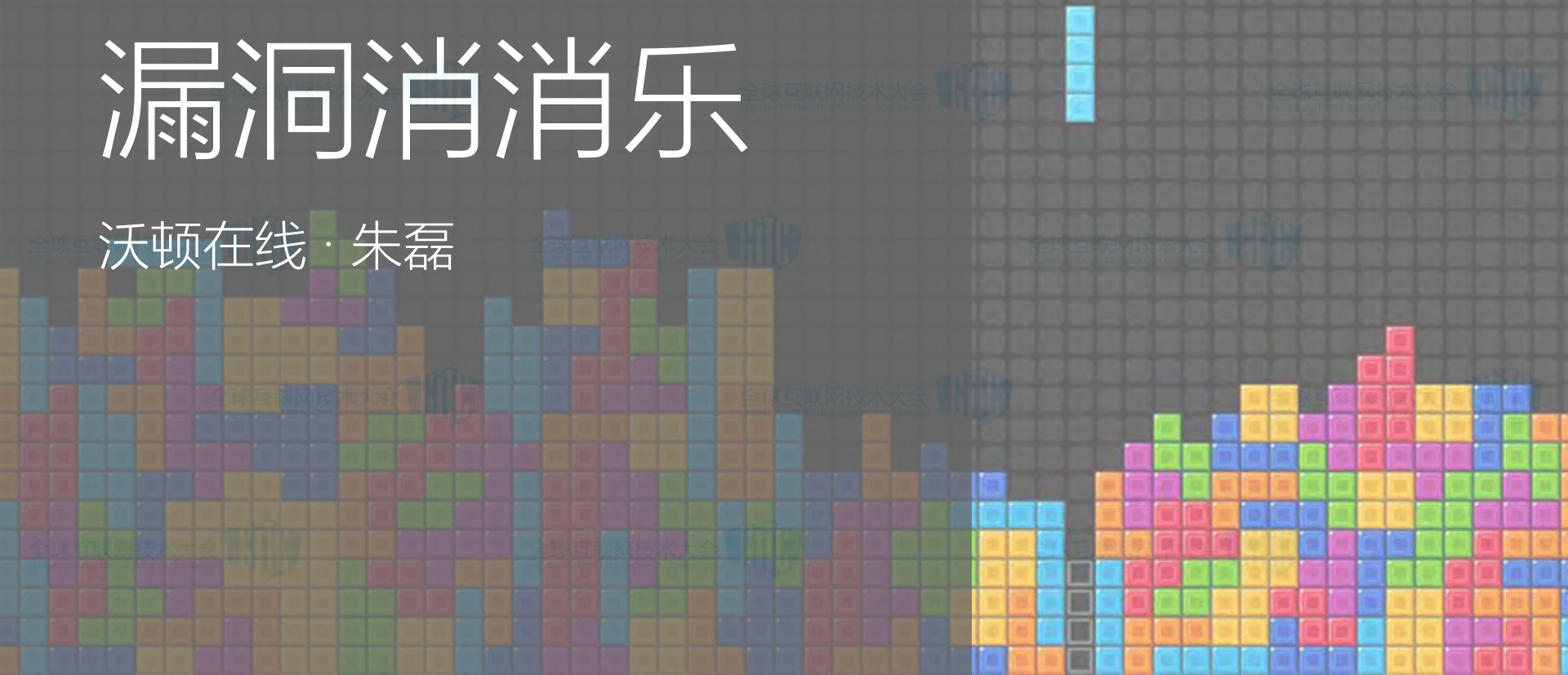

1000
10-20


功能升级
BUG修复

沃顿在线

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

vs.

安全

vs.

研发

例 | 逻辑漏洞 | 命令执行 | XSS跨站 | 配置错误

例	逻辑漏洞	命令执行	XSS跨站	配置错误
	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	应用框架	用户资料 用户注册 收获地址 用户评论	传输过程 应用配置 服务配置 错误页面

输入输出

- 跨站脚本攻击
- 注入攻击
- 跨站伪造请求
- 篡改请求信息

文件上传

认证与会话

登录与注册

权限控制

开源框架

输入输出

文件上传

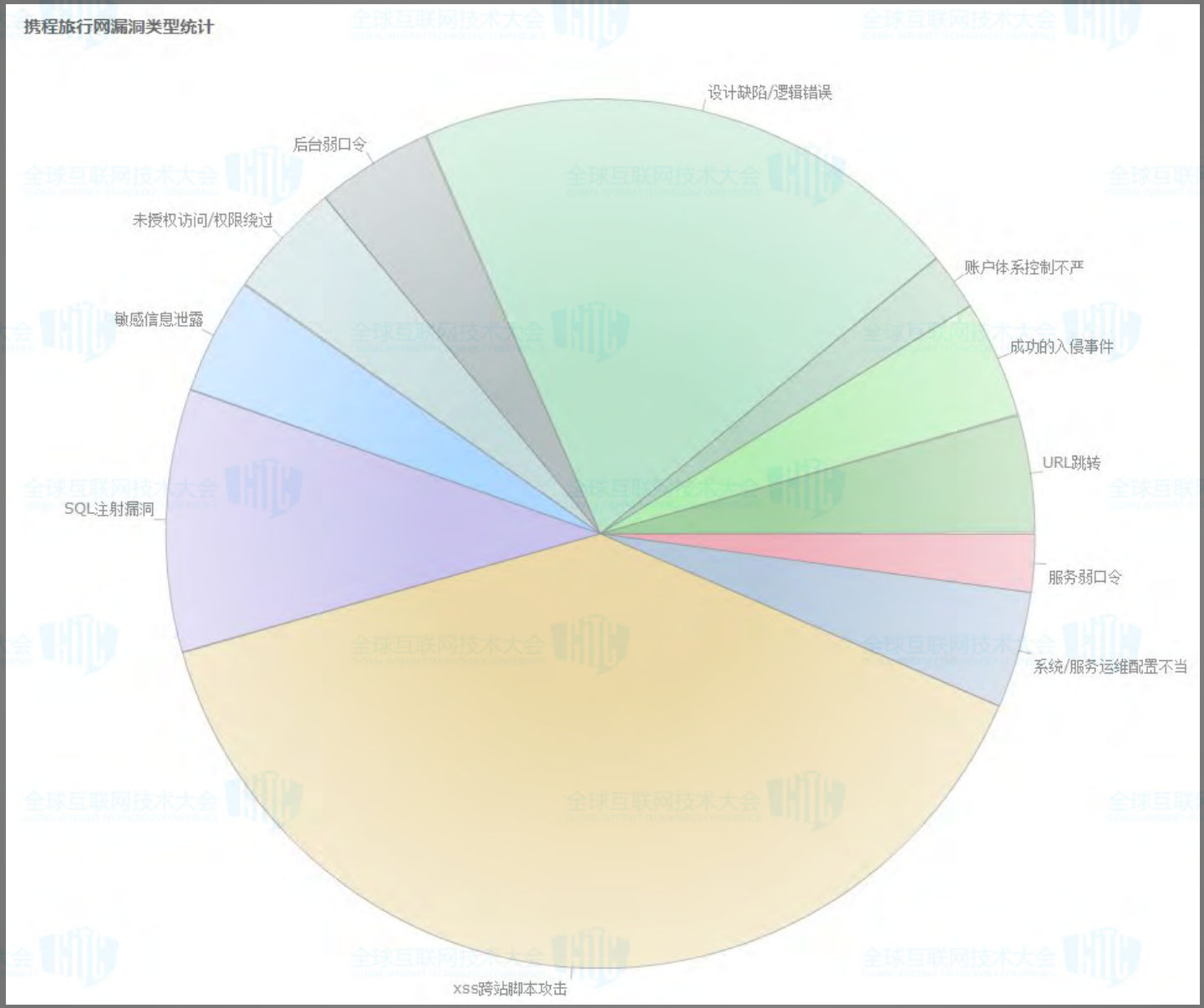
认证与会话

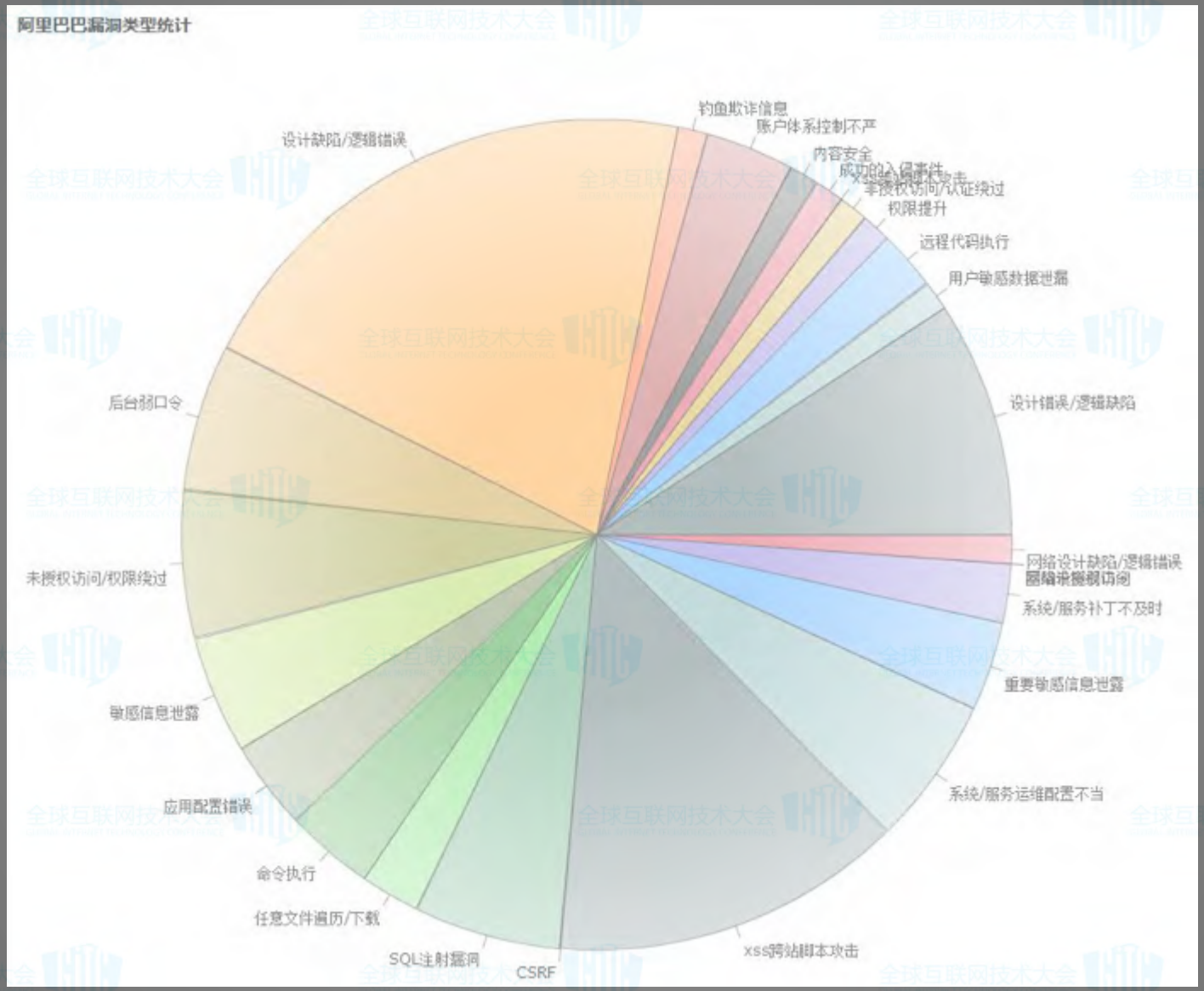
登录与注册

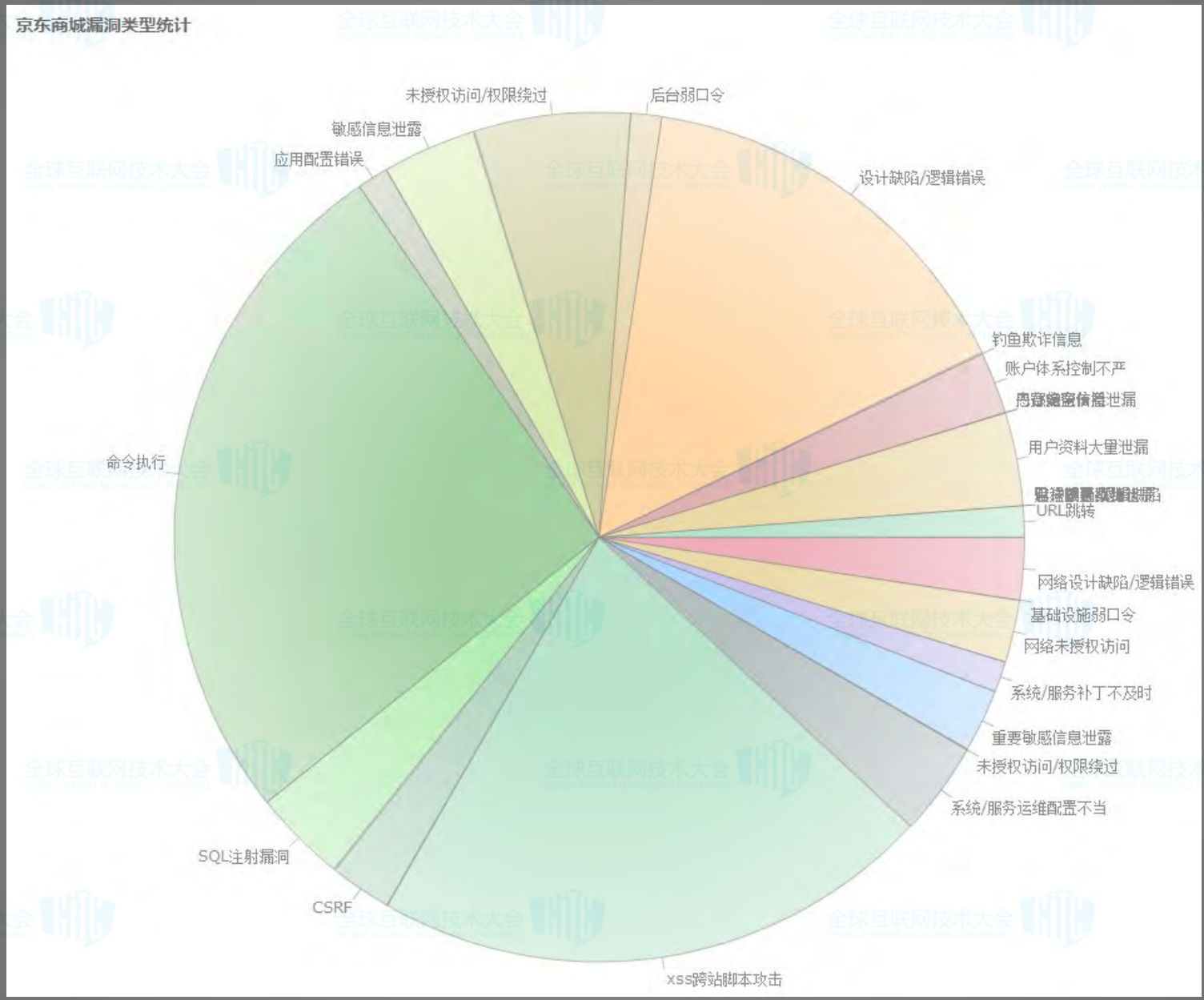
权限控制

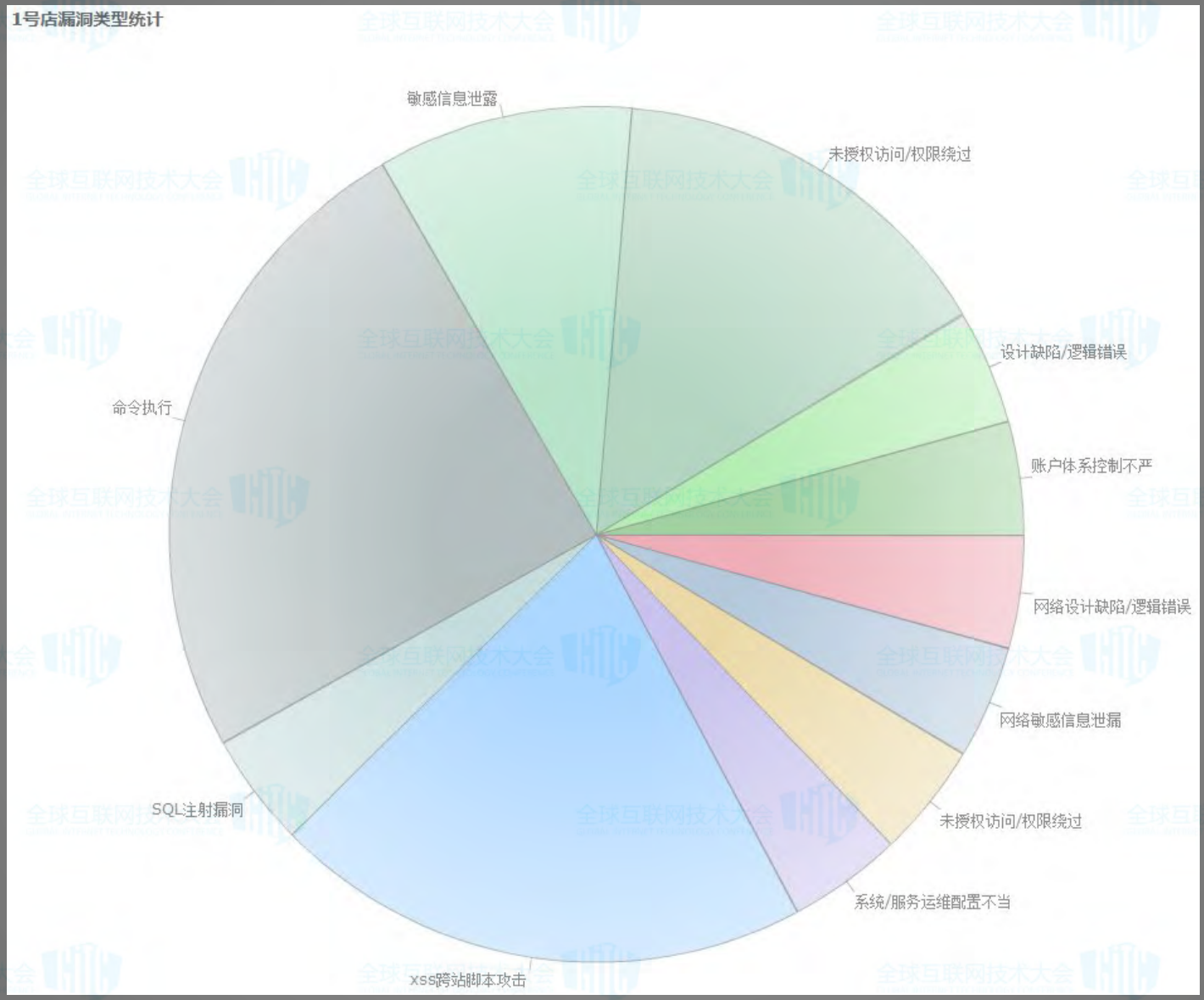
开源框架

- 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
设计缺陷/逻辑错误
后台弱口令
未授权访问/权限绕过
敏感信息泄露
SQL注射漏洞
xss跨站脚本攻击
系统/服务运维配置不当
服务弱口令
URL跳转
成功的入侵事件
账户体系控制不严


阿里巴巴漏洞类型统计
钓鱼欺诈信息
账户体系控制不严
内容安全
成功的入侵事件
权限提升
远程代码执行
用户敏感数据泄露
设计错误/逻辑缺陷
网络设计缺陷/逻辑错误
系统/服务补丁不及时
重要敏感信息泄露
系统/服务运维配置不当
xss跨站脚本攻击
CSRF
SQL注射漏洞
任意文件遍历/下载
命令执行
应用配置错误
敏感信息泄露
未授权访问/权限绕过
后台弱口令
设计缺陷/逻辑错误


京东商城漏洞类型统计
未授权访问/权限绕过
后台弱口令
敏感信息泄露
应用配置错误
设计缺陷/逻辑错误
钓鱼欺诈信息
账户体系控制不严
用户资料大量泄漏
URL跳转
网络设计缺陷/逻辑错误
基础设施弱口令
网络未授权访问
系统/服务补丁不及时
重要敏感信息泄露
未授权访问/权限绕过
系统/服务运维配置不当
xss跨站脚本攻击
CSRF
SQL注射漏洞
命令执行


1号店漏洞类型统计
敏感信息泄露
未授权访问/权限绕过
设计缺陷/逻辑错误
账户体系控制不严
网络设计缺陷/逻辑错误
网络敏感信息泄露
未授权访问/权限绕过
系统/服务运维配置不当
xss跨站脚本攻击
SQL注射漏洞
命令执行

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

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）

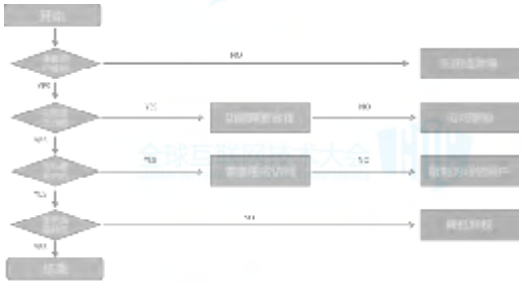
基于业务的风险检测方法

开发

代码级解决方案

- 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

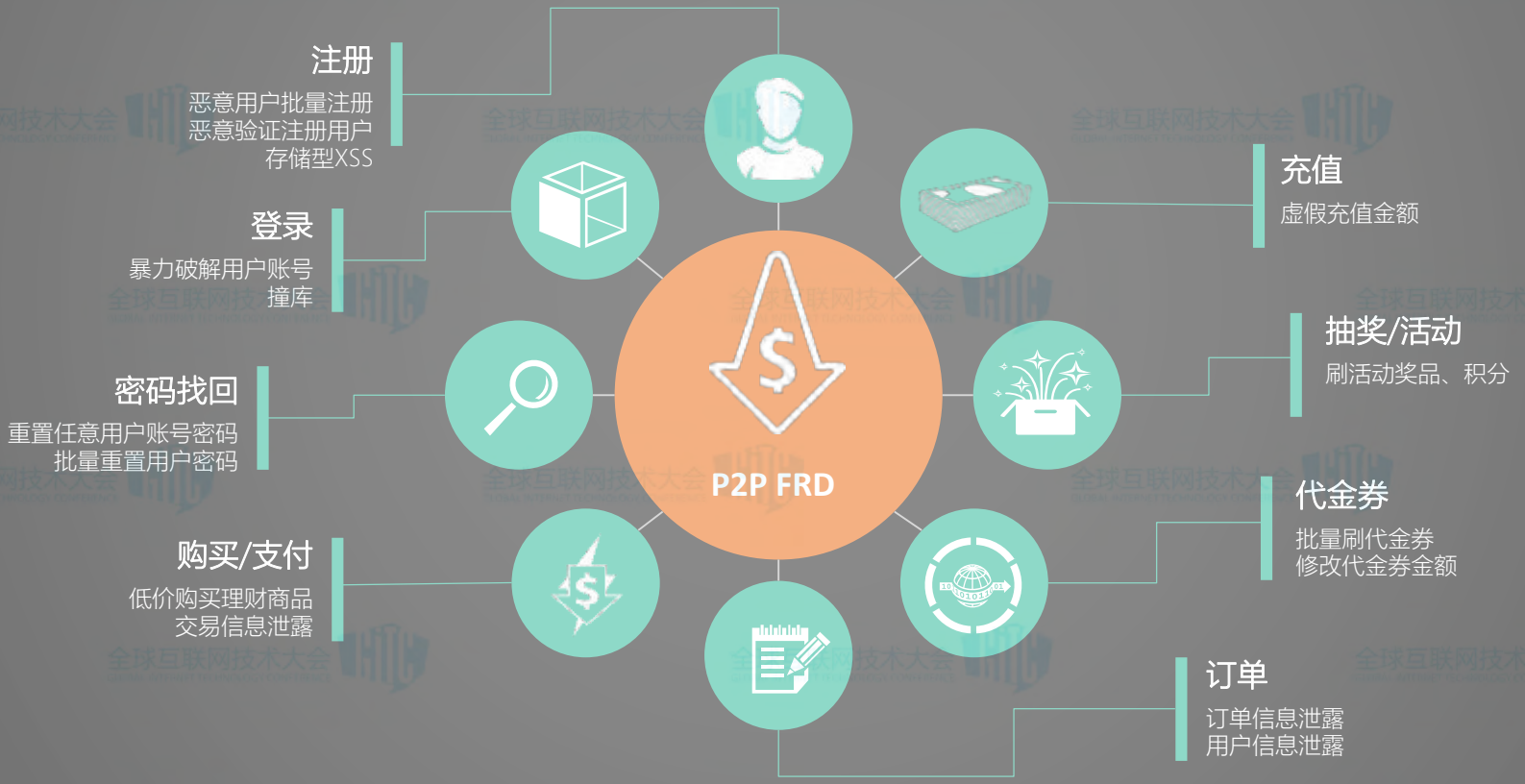
设计



威胁建模

需求

P2P FRD（P2P Finance Risk Detection）



ECRD（Electronic Commerce Risk Detection）

注册

恶意用户批量注册
恶意验证注册用户
存储型XSS

登录

暴力破解用户账号
撞库
手机号撞库
验证码绕过
验证码爆破

密码找回

重置任意用户账号密码
批量重置用户密码
新密码劫持

抢购活动

低价抢购
刷单

抽奖/活动

刷活动奖品、积分

支付/购买

低价购买商品
交易信息泄露


漏洞发现
技术支持
沉淀
归类
时间管理
培训

THANKS – THE EDN