TASS®
江南天安

漏洞与数据的奇点临近

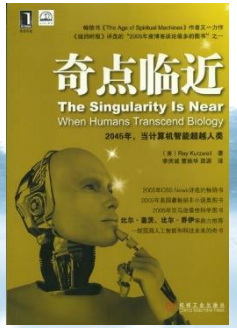
www.tass.com.cn

whoami

- @sm0nk
- 猎户攻防实验室
- 特长：WEB攻防、攻击建模、关联分析

议题简介

- 人类发展及人工智能将有一拐点——奇点
- 漏洞和数据的奇点定义了攻击者和防御者之间的结合点
  - 漏洞的规律特征提供了防御结合点的理论支撑
  - 数据元的关联分析提供攻击与防御的方法模型
- 本议题从漏洞规律入手，寻找防御的关键点，然后依据关联分析去定位分析，例如攻击的自动化、防御的追踪溯源，均落地于漏洞与数据的奇点。



目录

典型漏洞规律特征

漏洞名称	原理概述	加固方法
注入漏洞	携参拼接、构造语句、执行	预编译、过滤
跨站脚本	注入恶意指令代码到网页	过滤（黑白名单）、httponly
文件上传	配置、编辑器、过滤绕过、特性	综合+过滤（白名单、服务端）
文件包含	LFI RFI ,传入文件名校验不足或被绕过（截断）	输入强校验、位置指定
代码执行	危险函数的执行	脚本应用、参数过滤
请求伪造	错把“经过认证的浏览器发起的请求”当成“经过认证的用户发起的请求”	Referer token 验证码
越权访问	未严格权限判断	会话权限校验

一切输入都是有害的

防御：过滤频率最高

WAF

业务漏洞规律特征

漏洞名称	分类概述	加固方法
身份认证	Pwd、Session 、Token、Cookie	强校验
业务一致性	身份对应	权限绑定
业务数据	金额、数量校验	校验、加密、逻辑判断
输入交互	WEB、二次引用、Fuzz	定向、逻辑判断
密码找回	弱凭证、逻辑步骤及判断	Token(匹配)
验证码	猜解、绕过、回显	强化凭证、逻辑判断
业务授权	未授权、越权	权限绑定
业务接口	接口调用（网关、内容）	逻辑限制

原理高频Tips: 认证、会话、控制

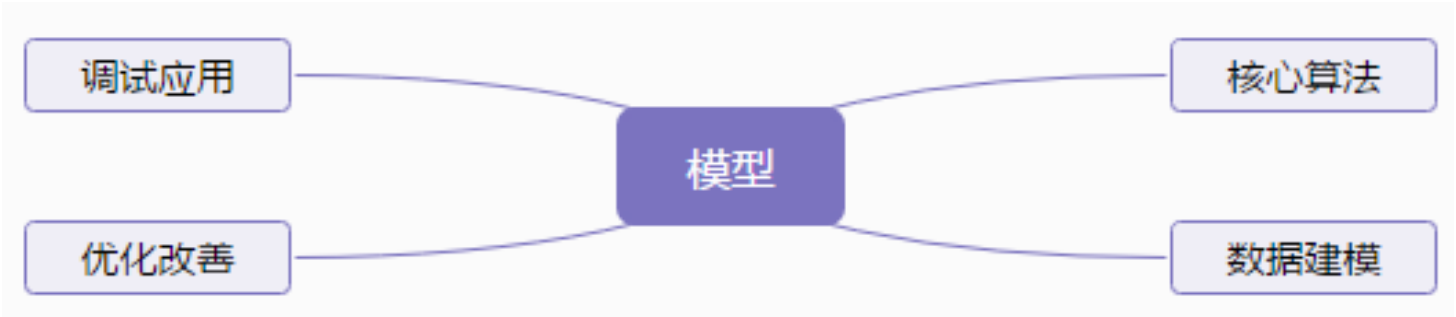
加固高频Tips: 逻辑、校验

关于防护

Web攻击产生的根源是由于程序引用恶意的输入流导致程序内部执行解析而产生的行为。
WAF产品类基本都是在对输入流的控制上做防护；
RASP（Runtime Application Self Protect） 则是在程序执行解析这个流程中做防护。

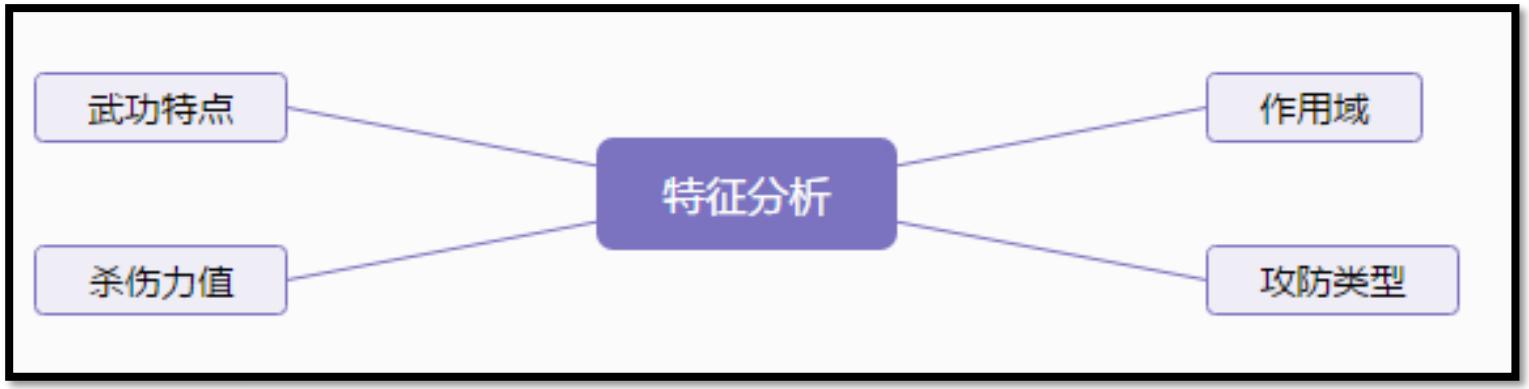
数据与漏洞的博弈

- 数据是防御者的核心（Des）
- 漏洞是攻击者的核心（Sou）
- 分析和归纳漏洞是为了关联分析进而定位保护数据的策略和方法
- 数据与漏洞的奇点——关联分析



规律特征之关联分析

- 降龙十八掌&九阳神功（未知攻焉知防）
- 斗转星移&乾坤大挪移
- 北冥神功&吸星大法
- 特征分析（线性）&行为分析（非线性）



关联分析方法梳理

详细内容

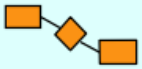
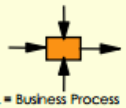
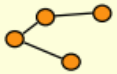
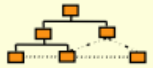
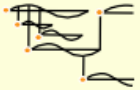
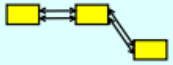
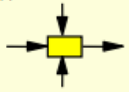
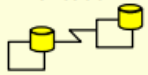
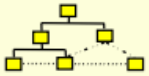
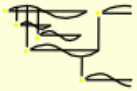
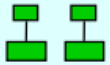
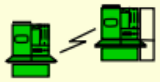
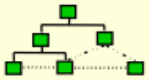
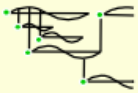
依据6W原则设计

继承关系

概念

逻辑

物理

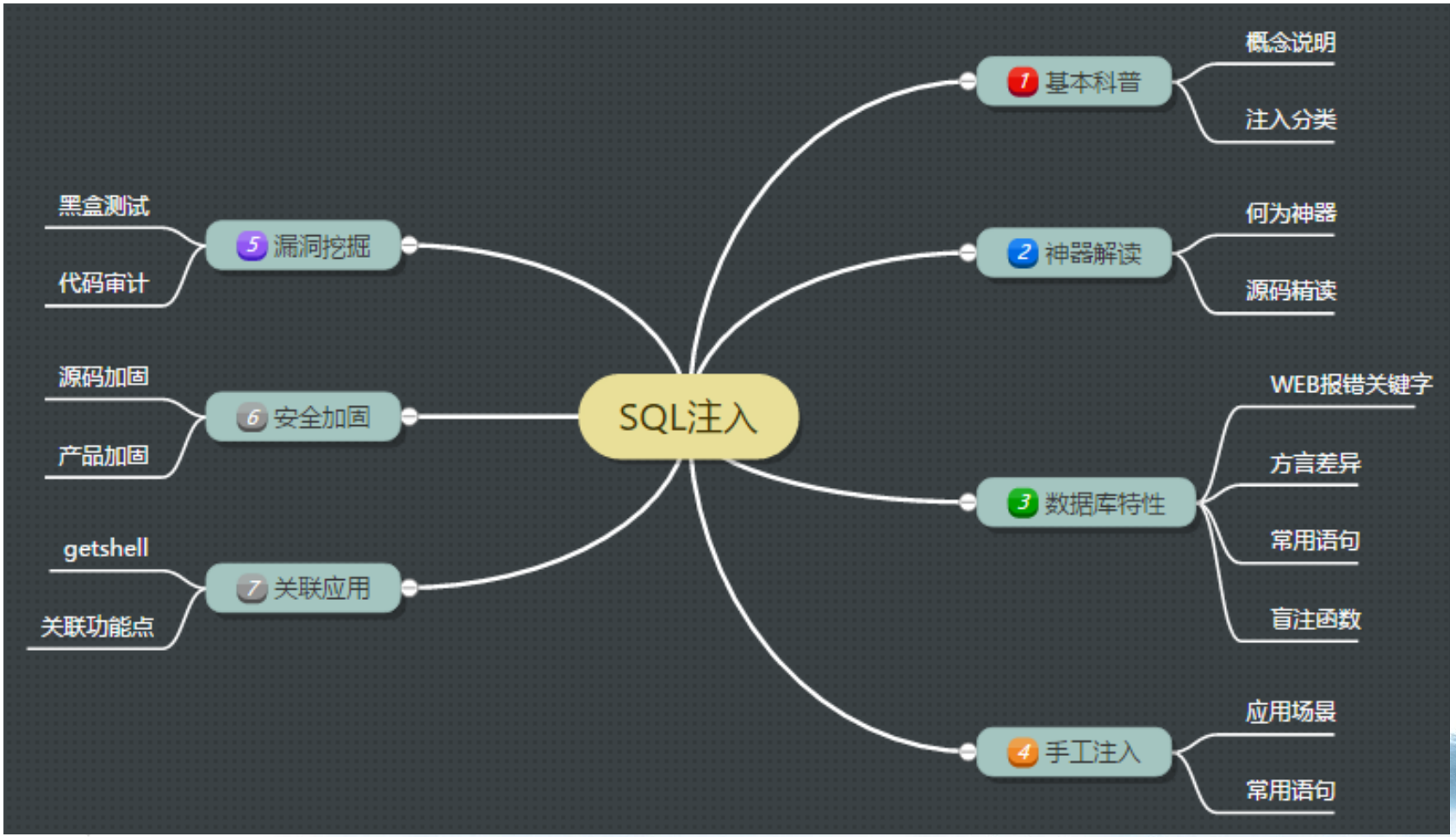
	DATA What	FUNCTION How	NETWORK Where	PEOPLE Who	TIME When	MOTIVATION Why
SCOPE CONTEXTUAL Planner	List of Things Important to the Business  ENTITY = Class of Business Thing	List of Processes the Business Performs  Function = Class of Business Process	List of Locations in which the Business Operates  Node = Major Business Location	List of Organizations Important to the Business  People = Major Organizations	List of Events Significant to the Business  Time = Major Business Event	List of Business Goals/Strat  Ends/Means=Major Bus.Goal/ Critical Success Factor
ENTERPRISE MODEL CONCEPTUAL Owner	e.g. Semantic Model  Ent = Business Entity Reln = Business Relationship	e.g. Business Process Model  Proc. = Business Process I/O = Business Resources	e.g. Business Logistics System  Node = Business Location Link = Business Linkage	e.g. Work Flow Model  People = Organization Unit Work = Work Product	e.g. Master Schedule  Time = Business Event Cycle = Business Cycle	e.g. Business Plan  End = Business Objective Means = Business Strategy
SYSTEM MODEL LOGICAL Designer	e.g. Logical Data Model  Ent = Data Entity Reln = Data Relationship	e.g. Application Architecture  Proc.= Application Function I/O = User Views	e.g. Distributed System Architecture  Node = I/S Function (Processor, Storage, etc) Link = Line Characteristics	e.g. Human Interface Architecture  People = Role Work = Deliverable	e.g. Processing Structure  Time = System Event Cycle = Processing Cycle	e.g. Business Rule Model  End = Structural Assertion Means = Action Assertion
TECHNOLOGY MODEL PHYSICAL Builder	e.g. Physical Data Model  Ent = Segment/Table/etc. Reln = Pointer/Key/etc.	e.g. System Design  Proc.= Computer Function I/O = Data Elements/Sets	e.g. Technology Architecture  Node = Hardware/System Software Link = Line Specifications	e.g. Presentation Architecture  People = User Work = Screen Format	e.g. Control Structure  Time = Execute Cycle = Component Cycle	e.g. Rule Design  End = Condition Means = Action
DETAILED REPRESENTATIONS OUT-OF CONTEXT Contractor	e.g. Data Definition  Ent = Field Reln = Address	e.g. Program  Proc.= Language Stmt I/O = Control Block	e.g. Network Architecture  Node = Addresses Link = Protocols	e.g. Security Architecture  People = Identity Work = Job	e.g. Timing Definition  Time = Interrupt Cycle = Machine Cycle	e.g. Rule Specification  End = Sub-condition Means = Step
FUNCTIONING ENTERPRISE	e.g. DATA	e.g. FUNCTION	e.g. NETWORK	e.g. ORGANIZATION	e.g. SCHEDULE	e.g. STRATEGY

安全情报分析中的钻石模型

在钻石模型中，分析依赖的主要是活动线（Activity Threads）以及活动－攻击图（Activity－Attack Graphs）。活动线和Kill-Chain紧密结合，描述了对一个特定受害者执行的恶意活动，可以支持假设事件，也可以利用水平分组来获得不同活动线之间的相关性。

而通过活动线和面面俱到列举攻击对手可能路径的攻击树进行叠加，不但保持了两种图形的信息，同时更突出了攻击者的喜好，并考虑到对手的反应及替代战术，从而得到更好的应对策略；同时也可以是正在进行的事件调查更准确，更快的生成假设。

关联分析之线性雪球技术



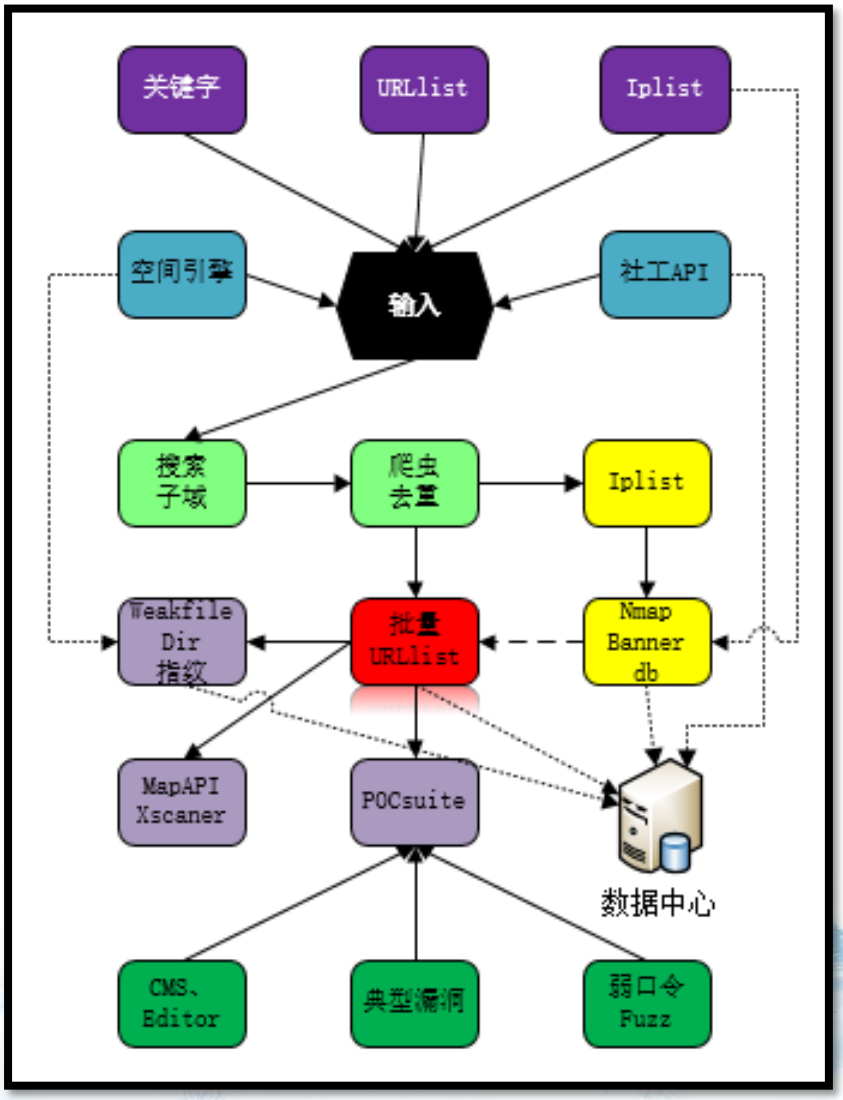
归纳渗透方法

阶段	内容	key
信息收集	关键字、配套服务、C段子域名、协议端口、目录、弱文件、弱口令、指纹、社工、源码收集	GIT、GHDB WEBServer、Middleware Nmap、 Dic (type)、weakfile
漏洞扫描	已知漏洞的扫描；典型漏洞的验证	AWVS、Pocsuite
暴力破解	(字典积累)（字典分层）、Fuzz	Htpwdscan Hydra Fenghuangscan burp
注入上传 典型漏洞	有注入看权限找管理找上传 漏洞库（看积累看经验有思路） 结合收集的信息去搞	Wooyun、 top 10、webshell、 JAVA、PHP、bypass、 SQLMAP(API)、Burp
WEB前端	Js、XSS、CSRF、SSRF、蠕虫、点击劫持	Exp&bypass Platform
业务逻辑	注册、验证、Top 10；逻辑、权限	Burp Fiddler APP
Getshell 内网渗透	挂代理、找密码、看数据、扫内网、翻滚吧	Socksproxy 、Chopper 、Conner、 nmap、3389 22 21..

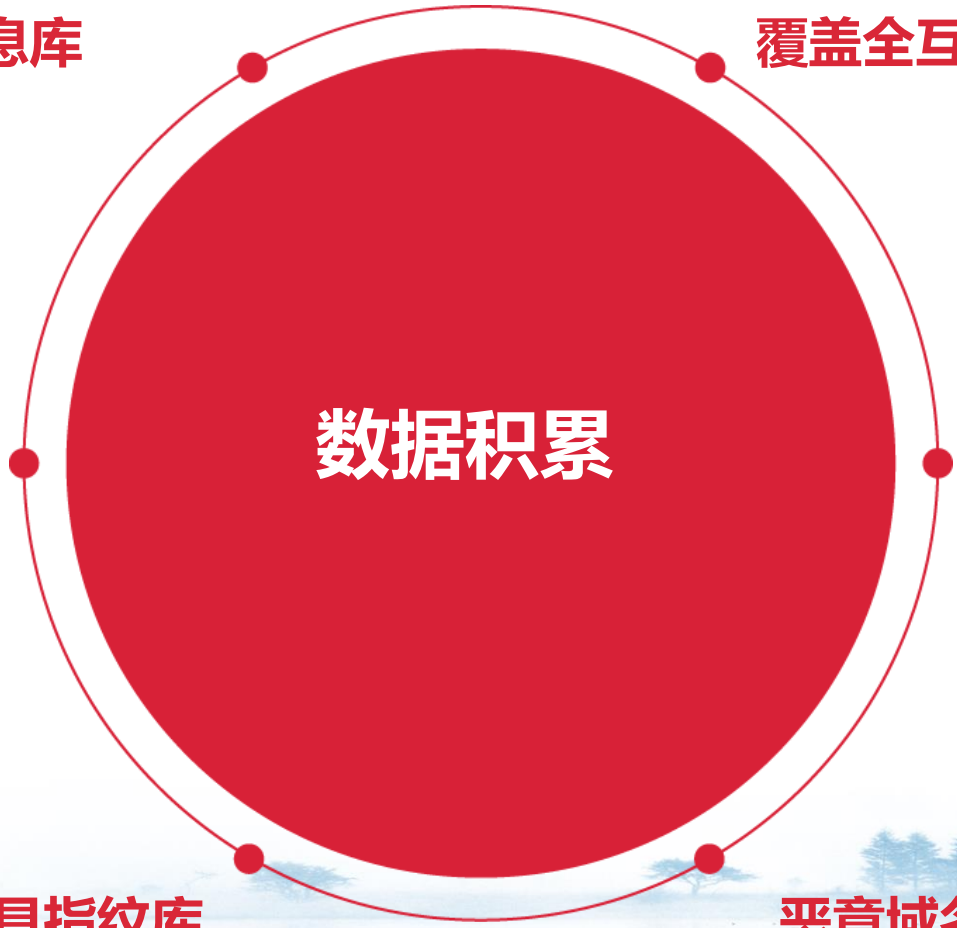
方法中寻找规律来完成自动化

渗透：运气+积累+思路（猥琐）

基于攻击模型的自动化平台-轩辕剑



攻防积累—DT—基于数据的溯源防御

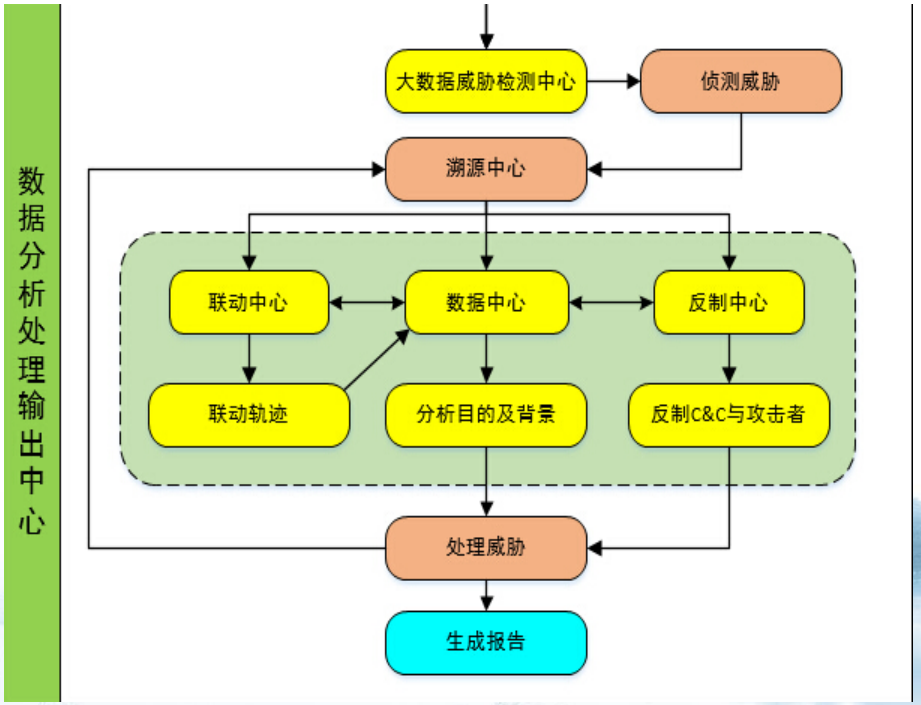


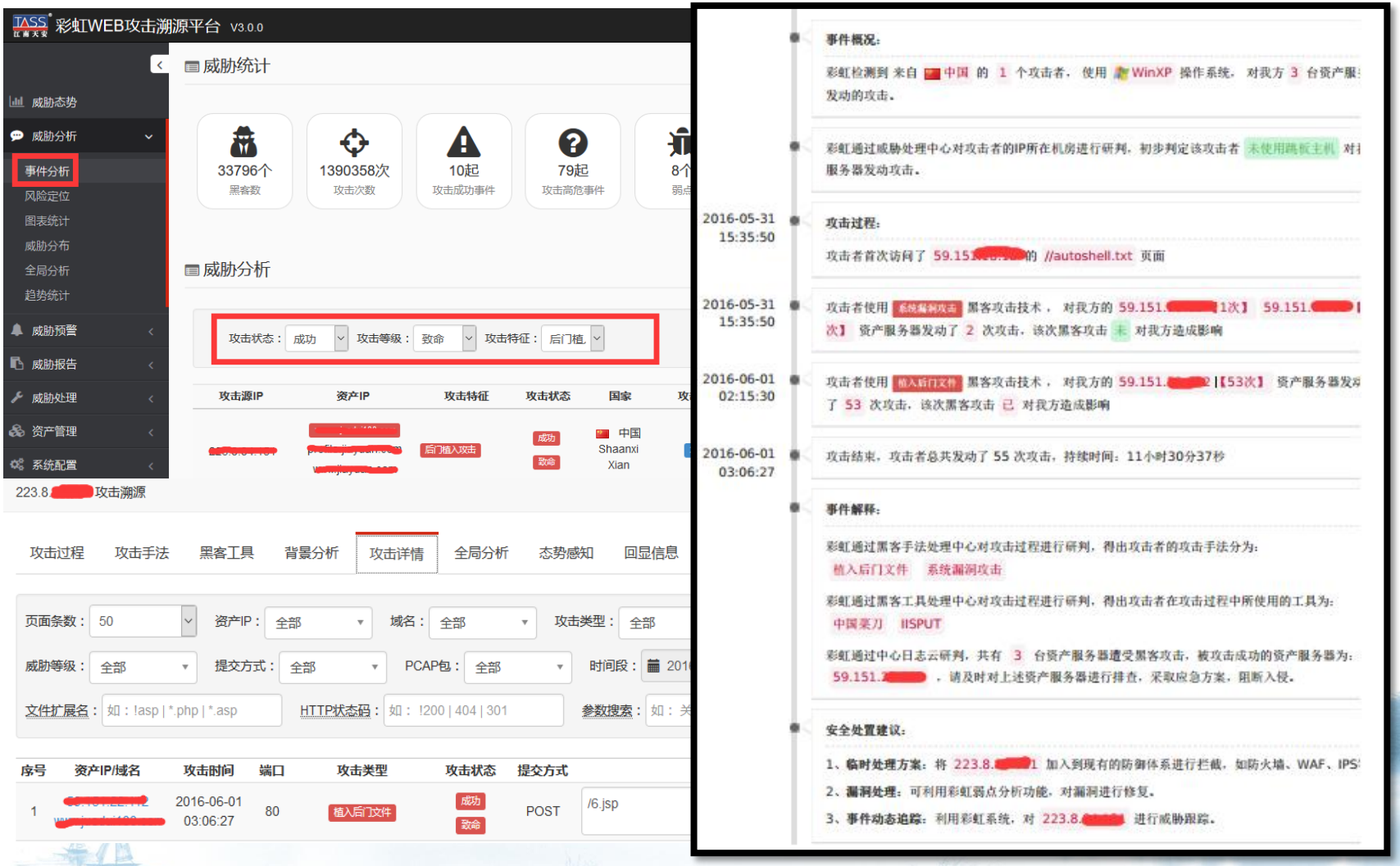
BIG DATA

利用大数据对确切的攻击行为进行分析

- ✓关联分析
- ✓攻击来源
- ✓身份背景
- ✓攻击路线
- ✓攻击目的
- ✓数据损失

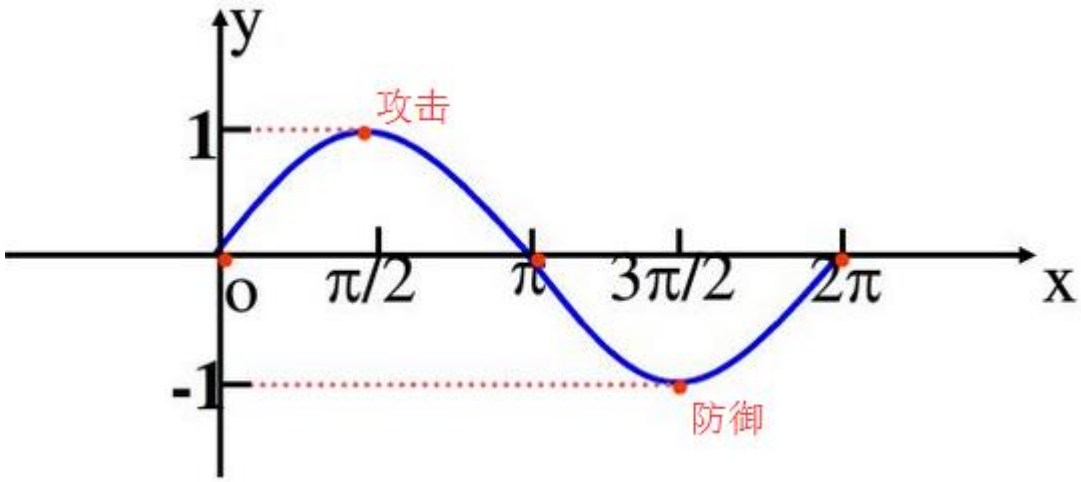
入侵事件的处理模型





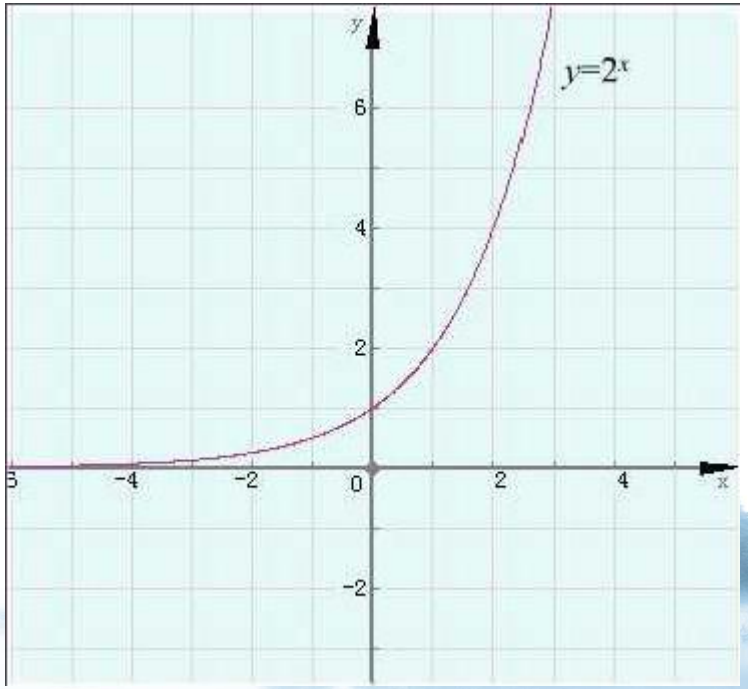
漏洞和数据的结合点-临界

- 攻击离不开漏洞（轩辕剑）防御离不开数据（彩虹）
- 百分百攻击的概率
- 百分百防御的概率
- 平衡态

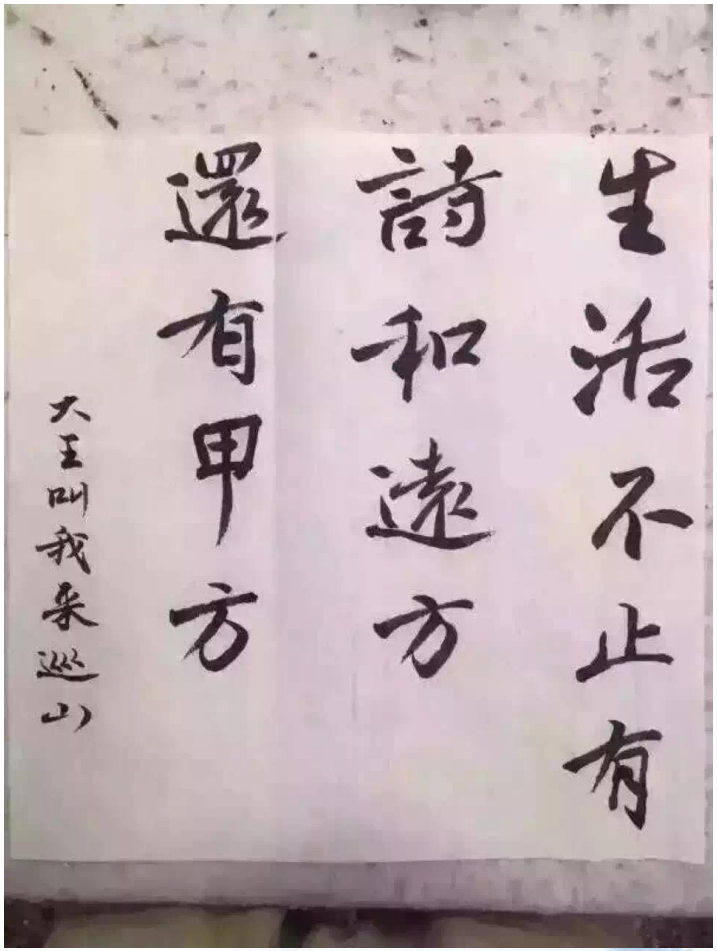


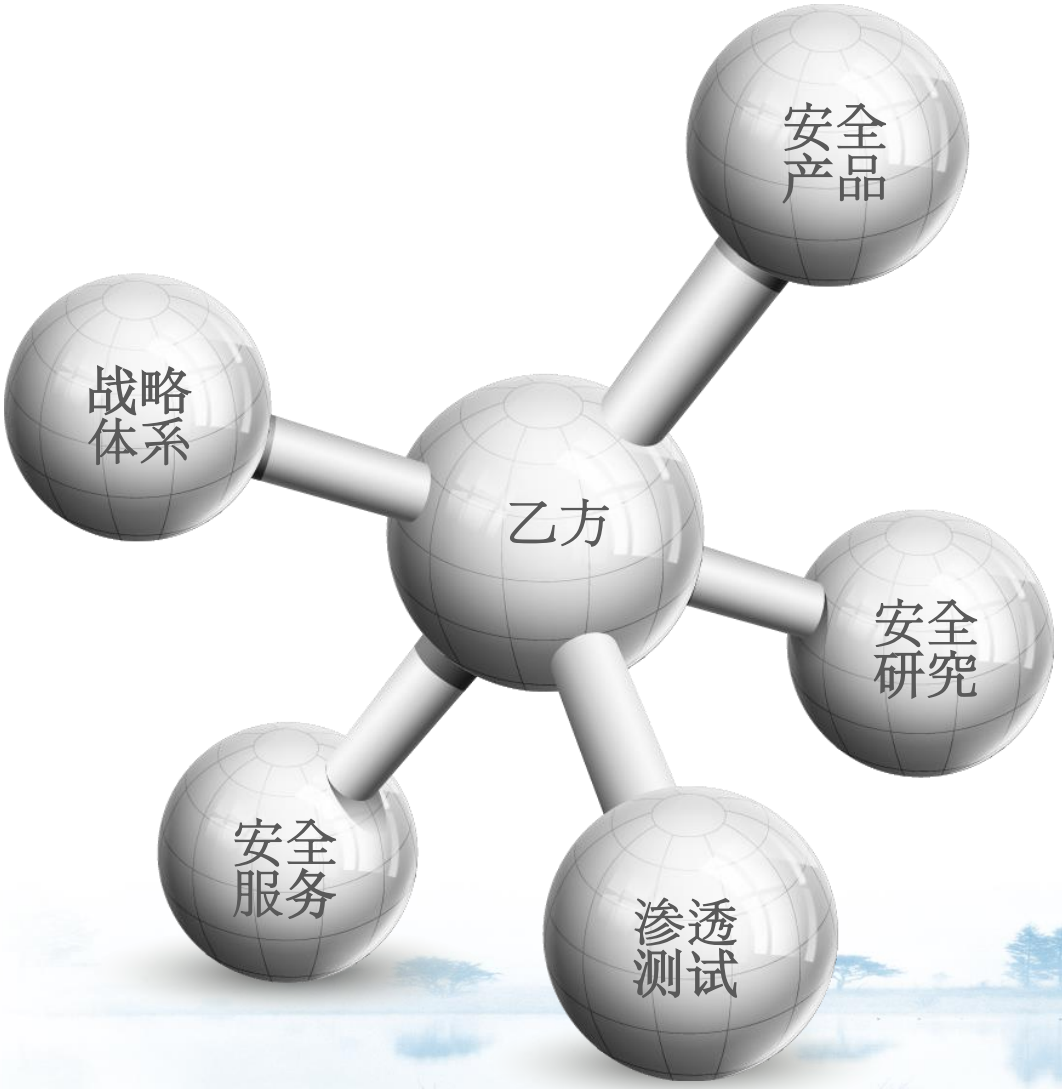
未来玄学拐点——奇点

- X=0 year=2045
- 用奇点主义解释人类的未来
- 用思想的力量迎接临近的挑战



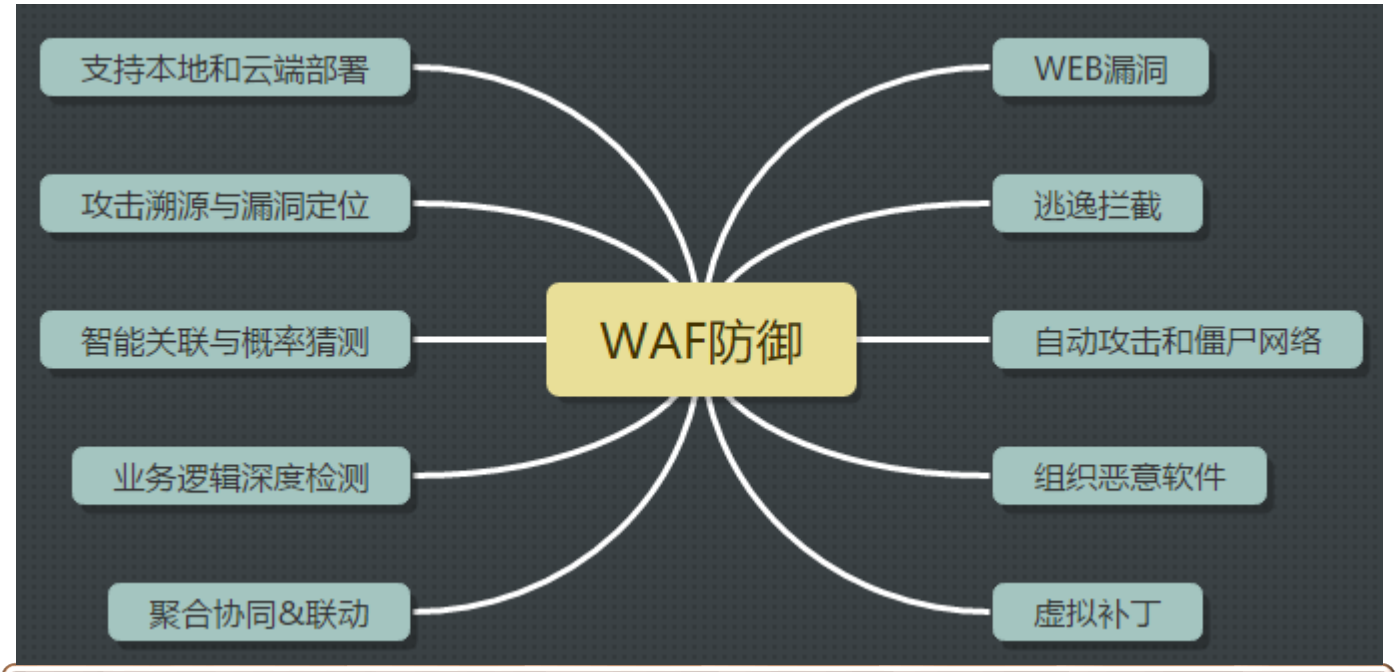
奇点之前的趋势——Web安全形式




安全产品
战略体系
乙方
安全研究
安全服务
渗透测试

Web安全防御趋势-奇点与结合点

- UTM类
- SOC类
- WAF类



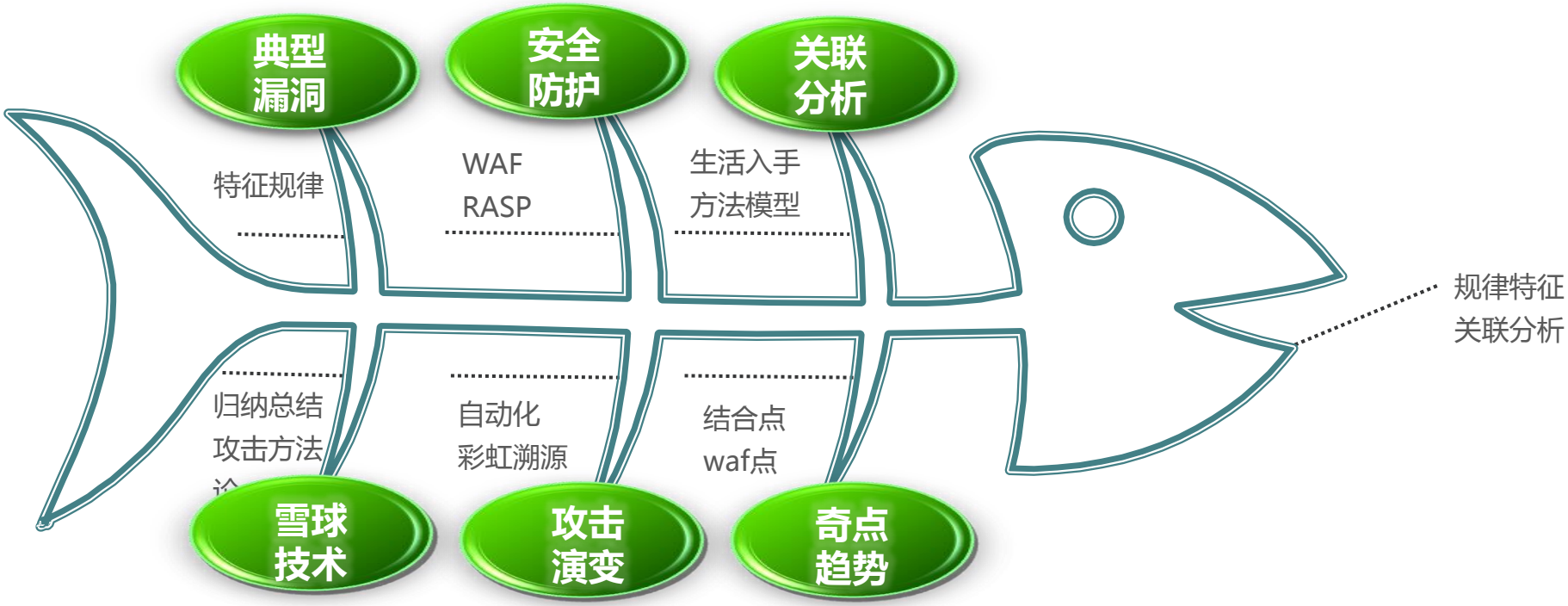
以WAF为核心的轴对称产品：聚合&协同

Think different

- 客观规律（流程和标准）
- Think different （对于创新而言，流程和价值观是阻碍作用）

- 虽然这个世界以确定的规则为基础，但本质上这个世界是不可预知的。
- 理智的人总在适应这个世界，不理智的人总是试图让世界适应自己，然而世界的进步总是取决于那些不理智的人。（By乔治.伯纳德.肖）

议题回顾


典型漏洞
安全防护
关联分析
特征规律
WAF
RASP
生活入手
方法模型
规律特征
关联分析
归纳总结
攻击方法
自动化
彩虹溯源
结合点
waf点
雪球技术
攻击演变
奇点趋势

江南天安

JIANGNAN TASS TECHNOLOGY

专业安全服务商

www.tass.com.cn