

企业安全合集—第四期:春秋技术专题

转载

[chengman3837](#) 于 2017-02-09 14:03:00 发布 73 收藏

文章标签: [系统架构](#) [网络](#) [web安全](#)

原文链接: <https://my.oschina.net/ichunqiu/blog/834641>

版权

前言

本着知识分享,聚合优质内容为大家提供方便的原则,我们将每周为大家做一期技术专题,论坛本身的内容有限并且带有天然的局限性,不得已很多内容都是外部转载来的,在此并无侵权的意图,为大家更好的去学习,如有作者或网站不同意分享到本社区的,可私信我来解决,感谢大家的支持!

这次专题从防御切入,其实就像老话说的,知攻则知防,当你了解一种攻击手法及其所有的变种时,那么你就对如何防御想必已经有了个模糊的概念。但将对防御的想法应用在企业之中时总是会出现各种各样的问题,难保不会有那么一天,你的同行好基友在朋友圈开着嘴炮,骂着你做的防御体系**无比。

真正的问题在于,环境总是在快速变化的,业务的研发走了一个又一个,系统架构改了一遍又一遍,你午睡个两小时的时间公司已经有那么几个岗位换人了。所以才会出现所谓动态防御,自适应防御的概念。就像长亭科技,还有其他一些企业在防御web问题所做的产品,通过机器学习结合waf的思路,降低跟随变化的成本,去逼近最后一公里的问题。

当你为业务系统构建了个比如强大的安全体系时,你又会发现隔壁的小王因为12345的弱密码导致了你们几百万的直接损失,人是安全最核心的问题,这句话这么说一点不为过。比如我刚才说的几百万损失,是个实际案例,所以[安全培训](#)也成为了甲方必做的功课。

总而言之是个苦逼的岗位,好好努力,早日转行。

以上个人观点,谨慎吸收

参考

[《互联网企业安全高级指南》](#)

[OWASP 安全编码规范快速参考指南](#)

[集团web安全标准](#)

[唯品会信息安全培训体系](#)

文章合集

[网站安全](#)

[如何打造一款可靠的WAF \(Web应用防火墙\)](#)

[Web应用防火墙 \(WAF\) 竞品分析](#)

走进科学之WAF(Web Application Firewall)篇

开发安全指南：如何安全地储存用户密码

基础安全

一起写一个 Web 服务器

Linux强化论：15步打造一个安全的Linux服务器

一次服务器被入侵后的分析

Linux服务器应急事件溯源报告

云服务器安全设计

业务安全

美团风险控制系统综述

解析P2P金融的业务安全

互联网业务安全之通用安全风险模型

i春秋学院视频推荐

网络安全之弱口令

网络数据包分析从入门到精通

安全开发

构建企业代码安全保障体系

安全产品原理

基于入侵检测的追踪溯源

转载于:<https://my.oschina.net/ichunqiu/blog/834641>