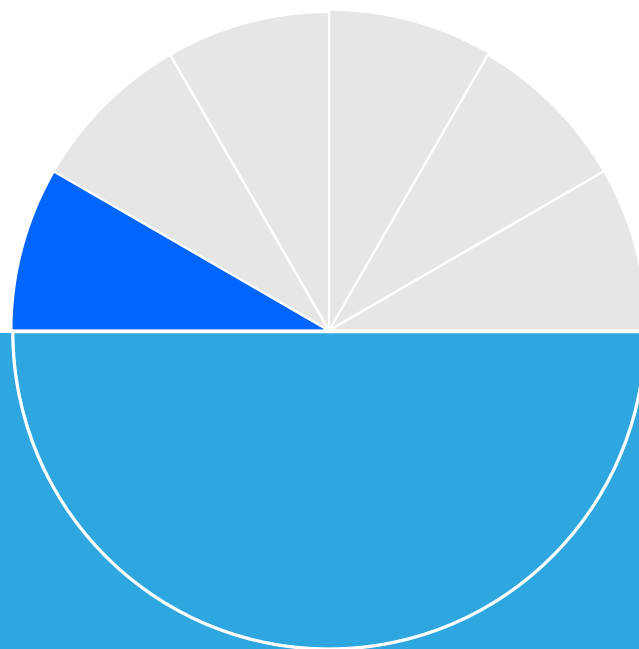


网络尖刀团队

在线旅游的安全现状

吴永丰

知安天下、网络尖刀创始人、同程旅游安全工程师



第一章

免费入住五星级酒店？

后台发码

- 找到漏洞，渗透后台，熟悉业务流程，并



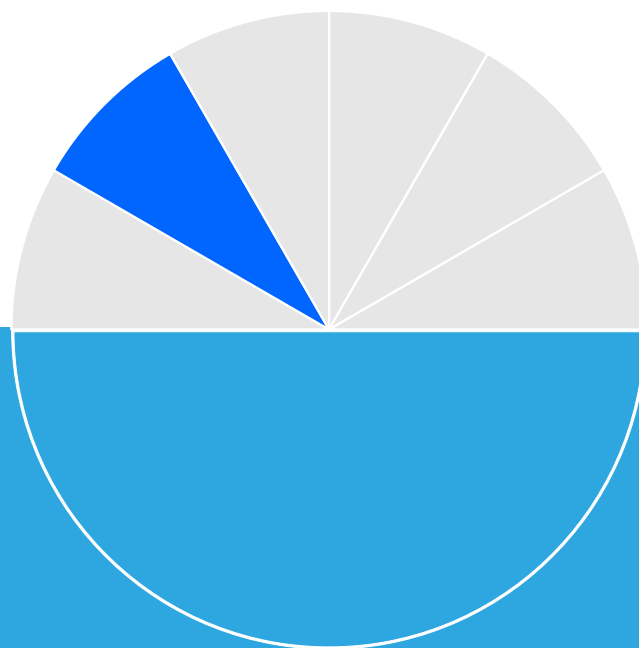
电话预约



免费入住



啪啪啪啪



第二章

在线旅游行业的安全现状

漏洞列表：漏洞列表：漏洞列表：

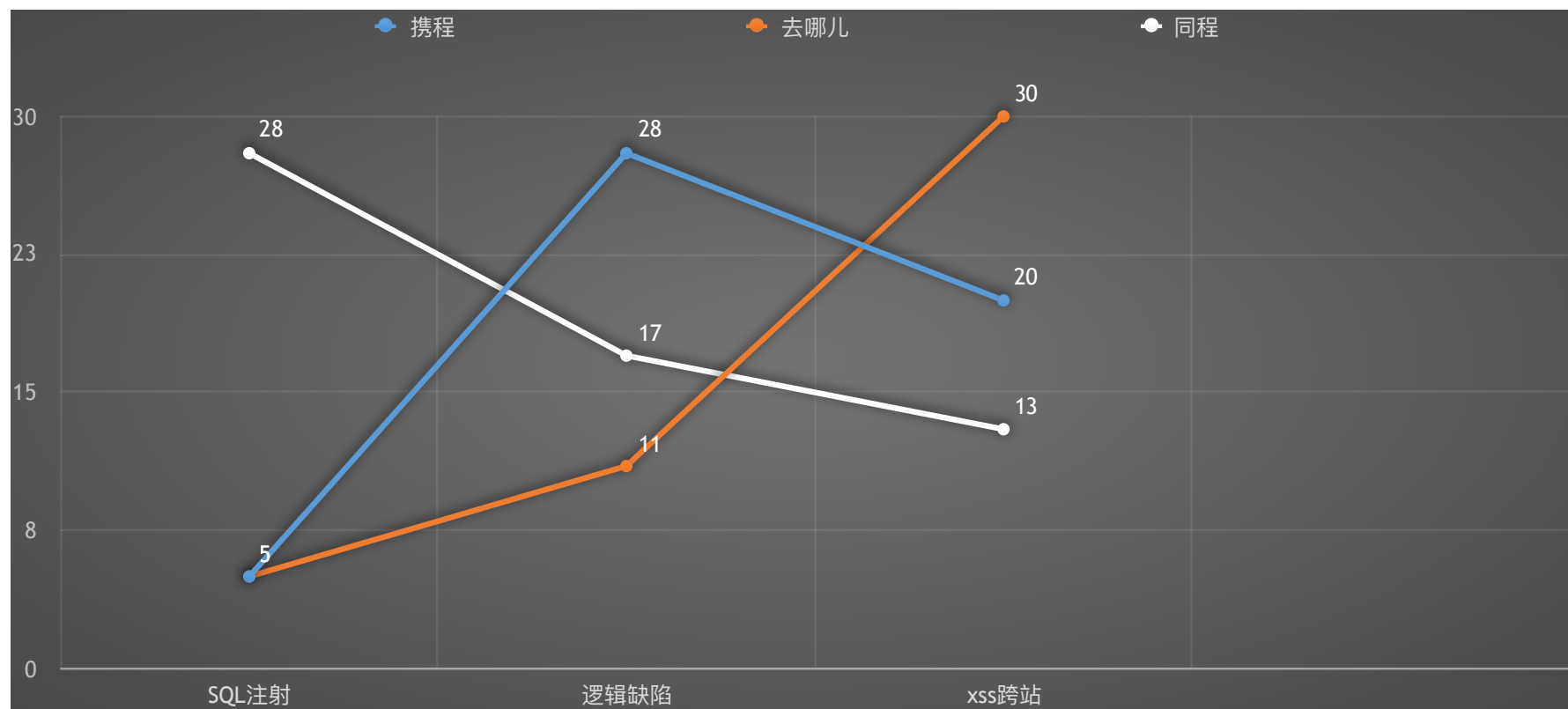
提交日期	提交日期	提交日期	漏洞名称	状态	作者
2015-10-10	2015-10-20	2015-10-26	同程csrf修改任意用户资料	已确认	路人甲
2015-09-09	2015-09-13	2015-10-14	同程旅游网某接口可取消任意订单	已确认	Focusstart
2015-08-31	2015-08-20	2015-10-05	同程全资子公司某系统存在通用型SQL注入(DBA权限)	已确认	YY-2012
2015-08-27	2015-07-29	2015-10-05	同程客户端拒绝服务两处	已忽略	昊昊
2015-09-07	2015-07-07	2015-09-23	同程旗下某app一元住酒店	已公开	路人甲
2015-07-05	2015-05-29	2015-09-09	同程网某站Getshell已入内网(影响内部网络\信息安全)	已公开	if、so
2015-07-01	2015-05-10	2015-09-07	旅游业安全之同程旅游网某站SQL注入	已公开	管管侠
2015-06-26	2015-03-22	2015-09-07	同程旅游客户端设计不当可实现钓鱼攻击	已确认	Moonight
2015-06-24	2014-11-21	2015-08-28	同程旅游网移动端某接口泄漏（可查询订单/机票/酒店/电影等部分信息）	已公开	1937nick
2015-06-23	2014-11-11	2015-08-27	同程旅游网某开发人员测试平台暴露在外网	已公开	正义的伙伴
2015-06-22	2014-11-09	2015-07-14	旅游业安全之同程旅游网某重要系统敏感信息泄露可登录酒店管理系统	已公开	管管侠
2015-06-17	2013-11-15	2015-07-01	同程旅游网邮箱伪造漏洞	已公开	Aerfa21
2015-06-11	2013-10-23	2015-06-16	同城旅游某处泄露大量用户信息	已公开	机器猫
2015-06-10	2013-10-22	2015-06-05	旅游业安全之同程旅游网某业务SQL注入	已公开	管管侠
2015-06-09	2013-10-14	2015-06-05	同程某分站撞库（大量数据信息为证）	已公开	Me_Fortune
2015-05-25	2013-10-11	2015-06-03	同程旅游网某站绕过waf继续注入	已公开	杀器王子
2015-05-18	2013-09-10	2015-05-06	同程旅交汇旅行社注册过滤不严，可插入XSS代码，通过构造可盗取用户cookie	已公开	纳米翡翠
2015-05-18	2013-07-17	2015-05-06	同程旅游Android客户端拒绝服务漏洞	已公开	Zhe
2015-05-14	2013-06-13	2015-05-04	苏州同程旅游某站点SQL盲注（非MySQL测试代码）	已公开	loopx9
2015-05-11	2013-06-08	2015-05-04	同程某处用户登录可撞库无需验证码	已公开	路人甲

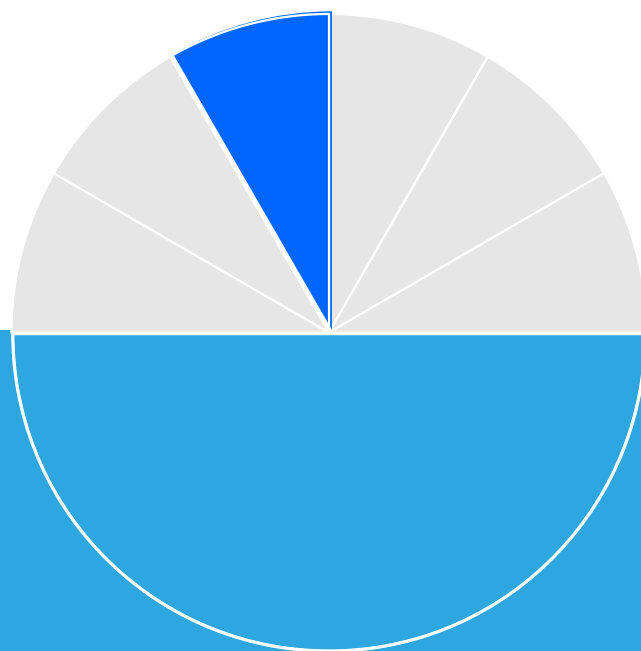


漏洞盒子
WWW.VULBOX.COM

酒店信息安全报告

根据漏洞盒子平台[安全报告](#)，知名连锁酒店桔子、锦江之星、速八、布丁；高端酒店万豪酒店集团（万豪、丽思卡尔顿等）、喜达屋集团（喜来登、艾美、W酒店等）、洲际酒店集团（假日等）存在严重安全漏洞，房客开房信息一览无余，还可对酒店订单进行修改和取消。





第三章

在线旅游行业的漏洞经典回顾

漏洞概要

关注数(266) [关注此漏洞](#)缺陷编号: **WooYun-2014-54302**

漏洞标题: 携程安全支付日志可遍历下载 导致大量用户银行卡信息泄露(包含持卡人姓名身份证、银行卡号、卡CVV码、6位卡Bin) ⚡

相关厂商: [携程旅行网](#)漏洞作者: [猪猪侠](#) ✓

提交时间: 2014-03-22 18:18

公开时间: 2014-09-26 12:38

漏洞类型: 敏感信息泄露

危害等级: 高

自评Rank: 20

漏洞状态: 厂商已经确认

漏洞来源: <http://www.wooyun.org>Tags标签: [目录遍历](#) [敏感信息泄露](#) [错误信息未屏蔽](#)分享漏洞: [分享到](#) [☆](#) [👁](#) [🐾](#) [🔗](#) 7832人收藏 [收藏](#)

漏洞概要

关注数(36) ✓已关注 [取消关注](#)

缺陷编号: **WooYun-2014-88773**

漏洞标题: 同程旅游某服务配置不当getshell入内网并泄露内网结构

相关厂商: [苏州同程旅游网络科技有限公司](#)

漏洞作者: [杀器王子](#) ▼

提交时间: 2014-12-26 14:36

修复时间: 2015-02-03 13:53

公开时间: 2015-02-03 13:53

漏洞类型: 系统/服务运维配置不当

危害等级: 高

自评Rank: 20

漏洞状态: 厂商已经修复

漏洞来源: <http://www.wooyun.org>

Tags标签: 无

分享漏洞:  分享到      0

8人收藏  收藏

漏洞概要

关注数(69) ✓已关注 [取消关注](#)

缺陷编号: **WooYun-2015-139097**

漏洞标题: 看我如何进入途牛内网访问大量内部系统与权限

相关厂商: [途牛旅游网](#)

漏洞作者: [if、so](#) ✓

提交时间: 2015-09-05 11:27

公开时间: 2015-10-20 12:10

漏洞类型: 系统/服务运维配置不当

危害等级: 高

自评Rank: 20

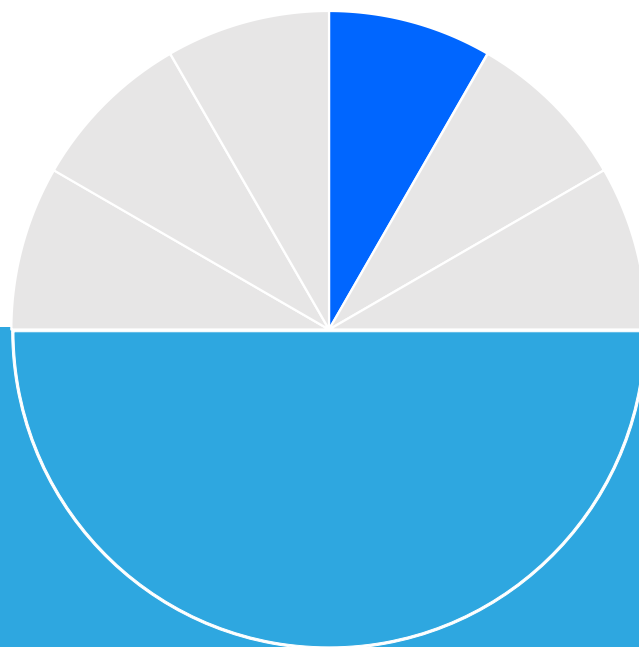
漏洞状态: 厂商已经确认

漏洞来源: <http://www.wooyun.org>

Tags标签: 无

分享漏洞: [分享到](#) [☆](#) [👁](#) [🐾](#) [🔗](#) 0

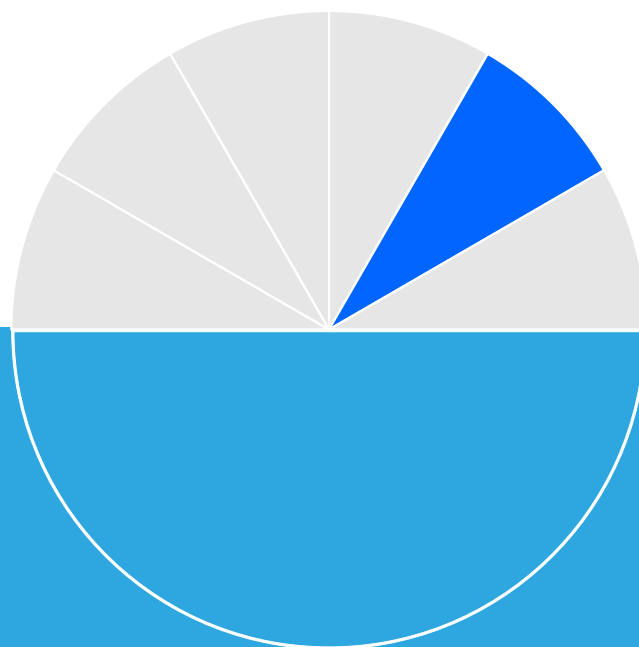
20人收藏 [收藏](#)



第四章

需要我们解决的问题是什么？

在企业，安全人员要有上帝视角！



第二章


我们团队在做些什么有趣的事？

感谢聆听



 Madmaner@Knowsafe.com

 <http://www.knowsafe.com>

 @疯子_Madmaner