2019 China White Hat Report

中 国 白 帽 子

2019 CHINA
WHITE HAT REPORT

中国白帽子
调查报告

漏洞盒子

114K+

国内白帽子总数

468K+

帮助客户组织修复漏洞

35%

获取漏洞赏金较去年增幅

67.4%

国内白帽子18-25岁占比

SUMMARY

概述

报告背景

随着国内外企业网络安全现状日益严峻，在这场风起云涌的浪潮中，大部分企业（特别是中小企业）仅凭自身安全团队的力量，已经很难支撑其业务或产品的安全性。众测模式、SRC以及Bug Boughty的出现，是企业向外界主动寻求安全能力的明显信号。这几种模式各有特色，但主角毫无疑问都是一群人——那些身怀绝技的白帽子们。

据统计，2019年国内白帽子总数已超过114000人。他们在保护企业安全、防止数据泄露、减少网络犯罪等领域起到了关键作用。截至《2019年中国白帽子调查报告》（以下简称报告）发布前，国内的白帽子们已经帮助超过3000个客户组织发现并修复了超过468000个漏洞，共获取超过1600万元漏洞赏金，相比去年增幅高达35%。

显而易见的是，整个社会正在加速拥抱白帽子们的积极力量。企业之外，上到欧盟委员会、英国国家网络安全中心、新加坡国防部、美国国防部都在积极推动漏洞赏金计划。白帽子驱动安全这一理念在金融服务、银行、保险、医疗等重安全行业中呈明显上升趋势。

近年来，我国国家层面也在积极立法推动行业规范与发展。《网络安全法》正式实施两年来，越来越多的配套法律法规陆续出台。6月18日晚间，工信部一纸《网络安全漏洞管理规定(征求意见稿)》迅速引爆安全圈，引发了白帽子们的广泛关注与讨论。相信随着监管机制愈发成熟透明，我国网络安全市场必将迎来进一步的机遇和发展，为白帽子们提供更加广阔的舞台。

他们是最值得信赖的伙伴，致力于挑战一切看上去不可能完成的任务。他们的故事鼓舞人心，有些甚至将成为传奇。但网络之外，他们也是和你我一样的普通人，有七情六欲，为生活烦恼。

这份报告将尝试为读者们呈现2019年中国白帽子们的真实状况。

关键发现

1、2019年国内白帽子总数已超过114000人，已经帮助超过3000个客户组织发现并修复了超过468000个漏洞，共获取超过1600万元漏洞赏金，相比去年增幅高达35%。

2、国内白帽子群体中，18-25岁的人群占比最多，达到67.4%，平均年龄22.7岁，整体上呈现出年轻化、技术宅、夜猫子、单身比例高等现状。

3、近70%的白帽子都是自学成才，网络资源和大咖博客是他们主要的学习途径。随着国内网络安全重视程度越来越高、教育水平逐渐提升，科班出身的白帽子数量会越来越多。

4、总体上来说，国内白帽子群体的收入区间跨度依然较大，其中部分甚至面临着生存困境。但通过努力充实自己，白帽子显然也可以获得与自身能力相匹配的高额回报。

5、大多数的白帽子是网络世界里的“独行侠”，选择单打独斗。他们偏爱金融、电商、IT/互联网等目标行业，当然，也与这3个行业资源集中、漏洞价值大有关。

6、大多数白帽子们的有效漏洞挖掘数量集中在50-300个，少数大佬提交有效漏洞超过5000个。漏洞提交后，20%白帽子认为企业修复不及时，对漏洞修复的反应速度仍有待提升。

中国白帽子概况

中国白帽子画像

精彩的故事，一定少不了出众的主角。“黑客”是大众给他们贴的标签，而“白帽子”才是他们真正的名字。

白帽子

一群热爱以创造性的手段，克服智力挑战的人。热衷于挑战未知的漏洞，以降低潜在网络安全风险。

企业SRC

即企业安全应急响应中心，可自主实现漏洞接收与奖励计划，设置漏洞接收范围、定义漏洞评级、并通过漏洞奖金池的形式进行全程管理。

漏洞

可以利用的软件、硬件或在线服务的脆弱点。

CTF

网络安全夺旗赛，白帽子之间进行技术竞技的一种比赛形式。

众测平台

安全测试协作平台，旨在排除企业安全隐患、提升安全能力。众测平台为需求方提供了一个在线发布任务的广阔空间，也为白帽子创造了能将知识转化商业价值和社会价值的机会。

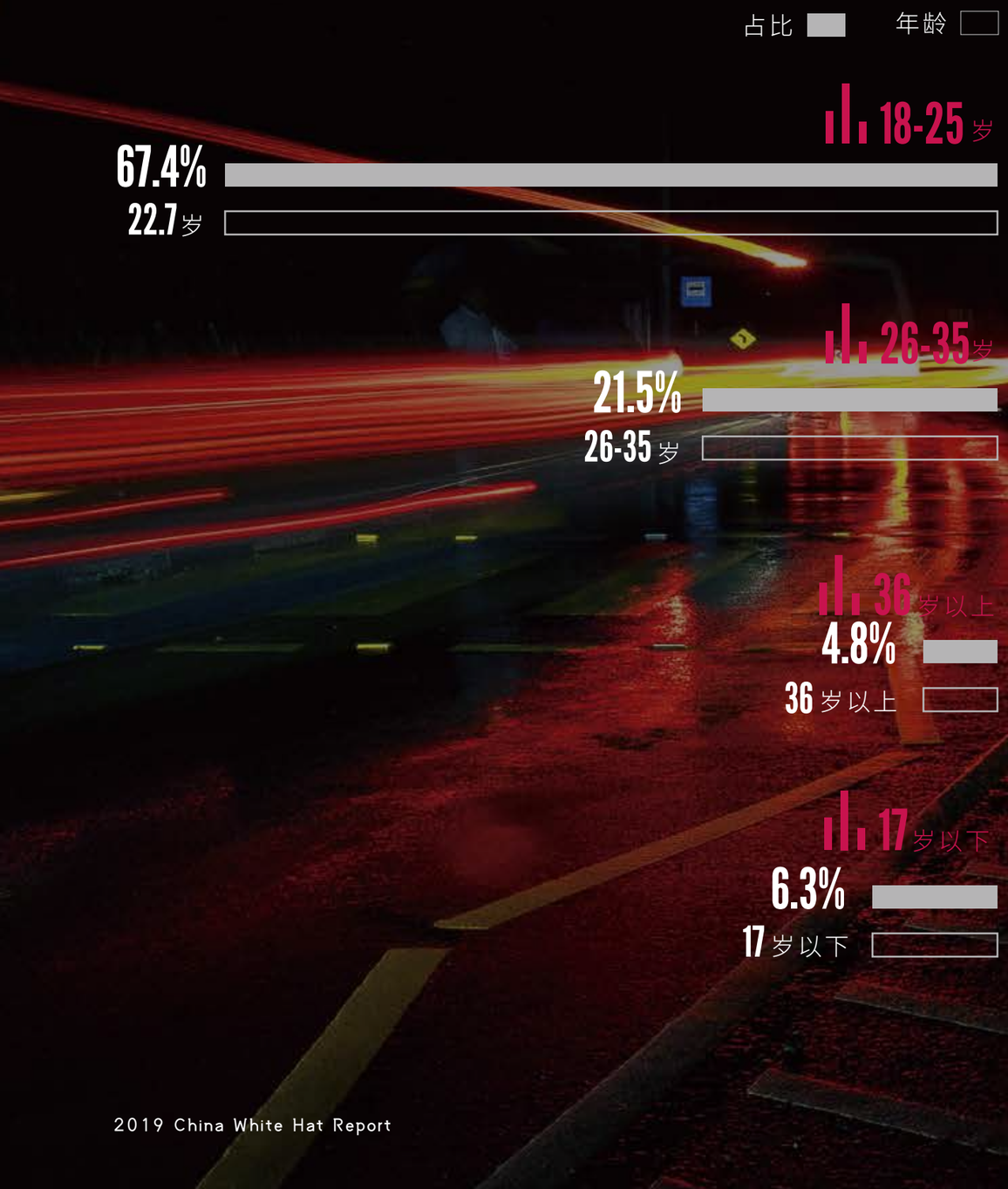
漏洞马拉松

漏洞盒子平台在国内首家发起的线下漏洞挖掘、赏金奖励比赛。

这群网络世界的侠客，在现实生活中到底什么样?他们是跟谢耳朵一样的技术宅，还是如韩商言一般外冷内热的大帅哥?通过近百份问卷以及走访调查，我们绘制了一份真实的中国白帽子画像。

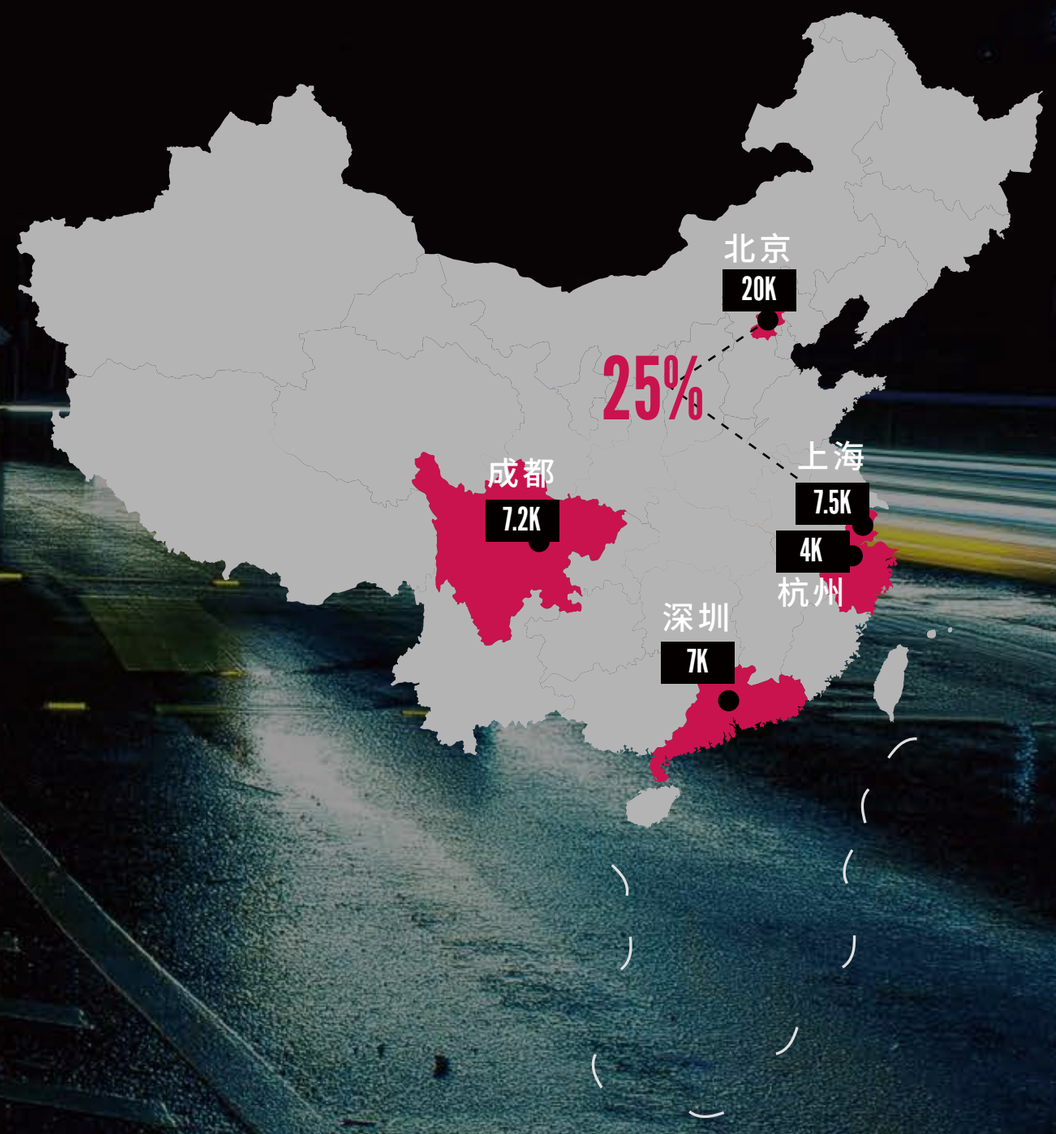
年龄分布

国内白帽子群体中，18-25岁的人群占比最多，达到67.4%，平均年龄22.7岁。26-35岁年龄段的白帽子数量相比去年略有增长，占总数的21.5%。36岁及以上的高龄白帽子比例为4.8%。自古英雄出少年，安全圈也不例外。17岁及以下的高中白帽子，也达到了总人数的6.3%。



他们从哪里来

白帽子们遍布全国各大省市，呈现出广撒网与区域集中化并存的趋势。北京、上海、深圳、杭州、成都在网络安全领域的地位依然无法撼动，是全国白帽子最集中的五大城市。问卷调查显示，仅北京和上海的白帽子人数就占据了总量的25%。



教育情况

69.3%的白帽子达到了本科学历，该结果在教育情况调查中排行最多。接下来是12.4%的专科和8.4%的硕士，博士生占比也达到了0.9%。调查还显示初中及高中在读学生占比约为9%左右。总的来说，国内白帽子高学历人才已经不再稀缺。另一方面，某业内大牛也曾坦言，渗透测试相关的招聘，他不太关注学历。第一看身家是否清白，第二看真实能力水平。

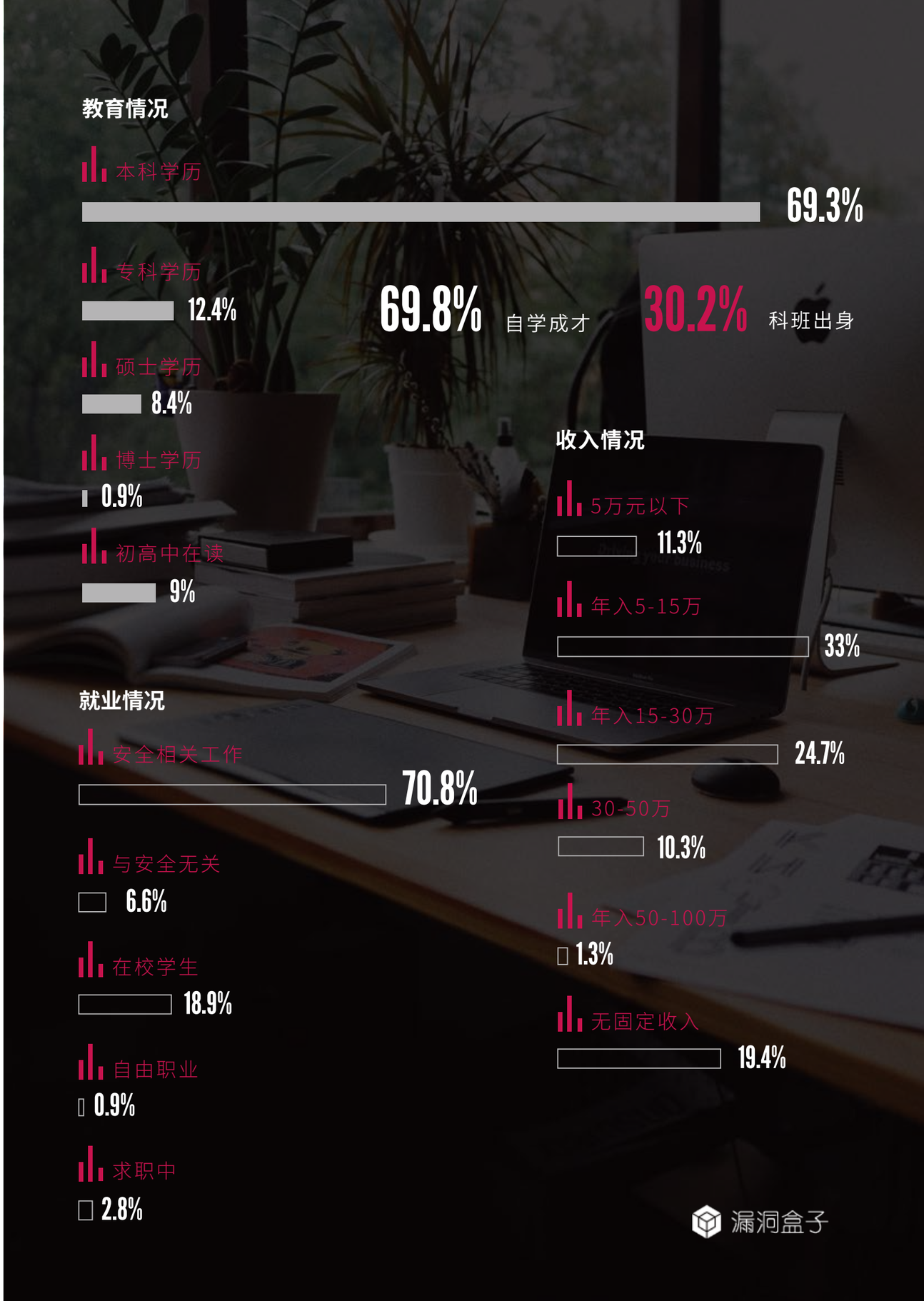
此外，参与调查的白帽子们当中，近七成为自学成才，网络资源和大咖博客是他们主要的学习途径。只有30.2%的白帽子是信息安全专业科班出身。随着国内网络安全重视程度越来越高、教育水平逐渐提升，相信这一数字也会逐年增长。

就业情况

从就业情况来看，七成以上的白帽子正在从事安全相关的工作，本职工作与安全无关的则占6.6%。另外，参与调查的白帽子当中还有18.9%的在校学生和0.9%的自由职业者，剩下的2.8%为求职中。

收入情况

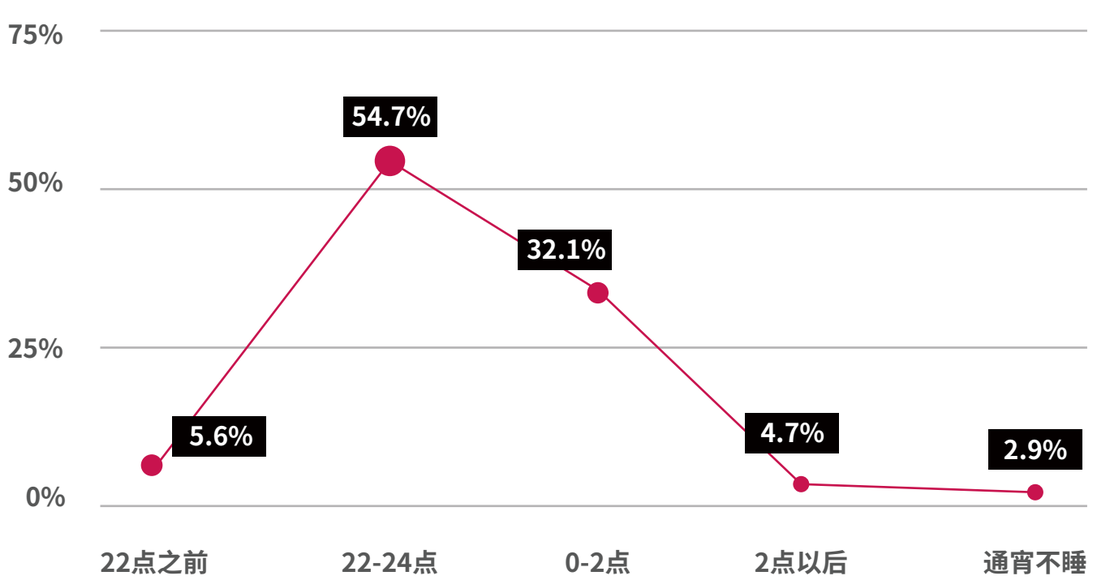
年收入5-15万元的白帽子占比最多，达到33%。其次是年收入15-30万元的群体，占比为24.7%。有19.4%的白帽子反馈并没有固定收入，这与前文中提到的在校学生占比基本吻合，而年收入范围在50-100万的占比仅为1.3%。总体上来说，国内白帽子群体的收入区间跨度依然较大，部分白帽子甚至面临着生存困境。另一方面，通过努力充实自己，白帽子显然也可以获得与自身能力相匹配的高额回报。



作息时间

国人对极客型宅男的印象可能有一大半都来自《生活大爆炸》：兴趣独特、女生苦手、夜猫子、技术大神……虽然这代表了大多数人的刻板印象，但与白帽子的生活轨迹确实有些许重合之处。调查显示，22点之前就上床睡觉的白帽子仅有5.6%。绝大多数人选择在22-24点之间休息，占比达到54.7%。受访者中第二大的群体是在0-2点间睡觉的熬夜党，32.1%。2点以后才睡与通宵党则分别占据4.7%与2.9%。或许只有在深夜时候， 白帽子们才能发挥出100%的潜能吧。他们不是英雄，是悄无声息的卫士，是时刻警惕的守护者。

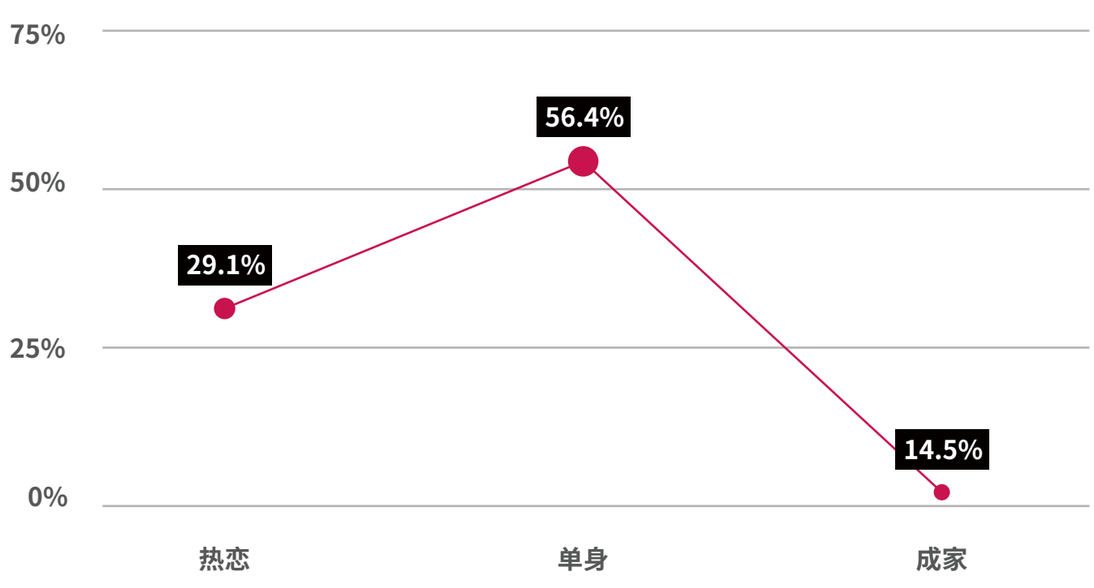
是暗夜中的骑士。

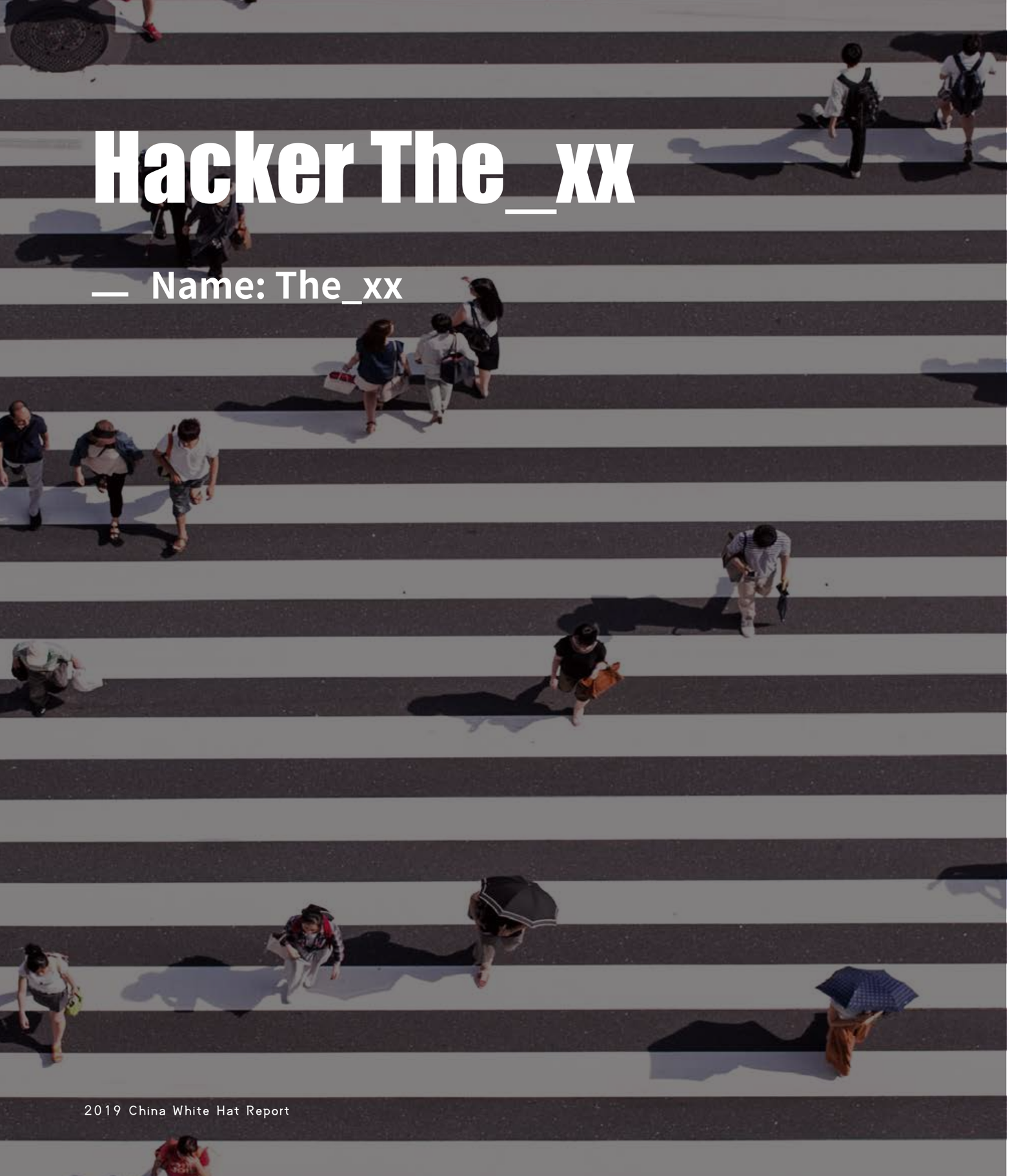


感情状态

谈朋友？不存在的！妹子哪有挖洞好玩~受访的白帽子群体单身狗比例较高，超过56.4%的白帽子目前还是单身状态；虽然也有近三成的白帽子正在热恋中，但真正步入婚姻殿堂，已经成家立业的群体比例则为14.5%左右。也许这并不能直接归结为技术宅们是暗夜中的骑士。性格内向、不善言辞等刻板印象，而是与目前我国青年群体的整体状况，如工作压力加大、更加注重个人生活品质、爱好更加广泛从而缺乏恋爱向往等因素都密切相关。

不过好在这个群体也足够年轻，有的是时间体验生活，改变世界，不是么？





Hacker The_xx

Name: The_xx

进入安全行业也并非一帆风顺，辛辛苦苦挖到的漏洞被忽略，有时也会让他感到沮丧。The_xx的父母并不知道他在网络安全圈，每次打电话也只是问问学习情况、专业上没有什么困难之类。面对挫折和不理解，他认为这些不会成为自己的障碍。坚持下去，不断提升自己，目前碰到的问题总会迎刃而解。

2016年进入安全行业，目前是一名安全服务工程师

孩子上大学是否会建议选择络安全相关专业？

会	27.3%
不会	4.7%
看TA个人兴趣吧	68.0%

白帽子挖洞技能

白帽子挖洞往往基于兴趣，而后再慢慢转向专业的众测平台，通过挖洞不仅为网络安全出力，而且满足自己的乐趣并获得漏洞奖励。

漏洞情况

大多数的白帽子是网络世界里的“独行侠”，选择单打独斗。他们偏爱金融、电商、IT/互联网等目标行业，当然，也与这3个行业资源集中、漏洞价值大有关。

绝大多数的白帽子（87%）喜欢从Web应用中查找漏洞，他们擅长的漏洞类型多样，而XSS漏洞依旧最为热门，其次集中在注入、逻辑漏洞、弱口令等漏洞类型。

据统计，大多数白帽子有效漏洞挖掘数量集中在50-300个，少数大佬提交有效漏洞超过5000个。而在漏洞提交后，20%白帽子认为企业修复不及时，对漏洞修复的反应速度仍有待提升。

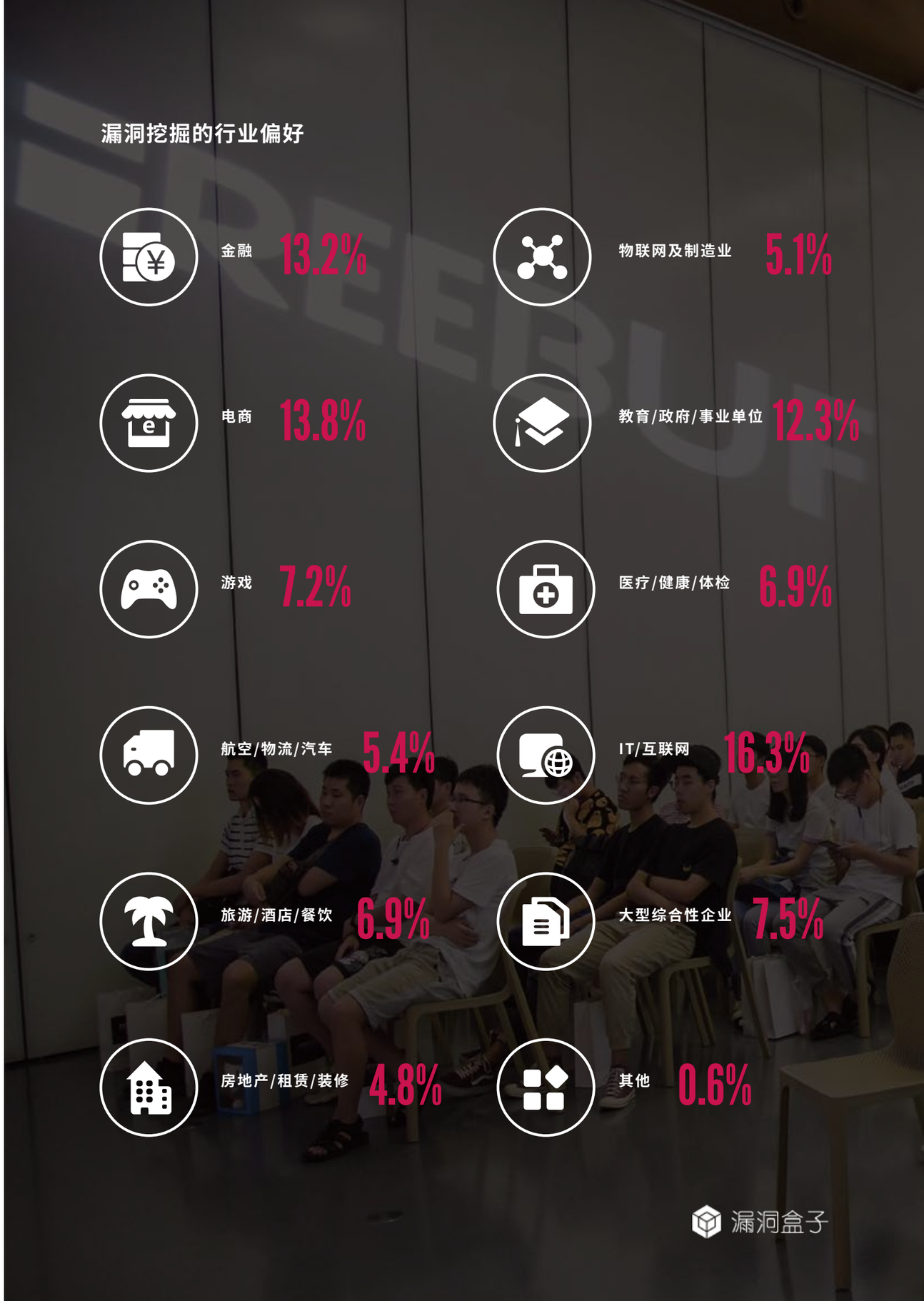
有趣的是，尽管热爱并投入挖洞事业，但只有超过20%的白帽子认为自己非常熟悉与漏洞挖掘相关的法律法规。近年来漏洞挖掘的法律边界问题逐渐成为社会关注热点，这也驱使白帽子不断学习相关法律法规，保障自身利益。

技能提升

挖洞对白帽子的专业技能水平提出了要求，但调查发现，绝大多数的白帽子都是自学成才。

70%的白帽子是非科班出身（计算机相关但非网络安全方向专业，甚至非计算机专业），他们将网络资源、技术论坛/网站等作为主要的学习资源，只有极少数的白帽子经过正规培训，这个比例不到3.8%。

在自学的道路上，约三分之一的白帽子愿意为了自己的技术能力提升投入数千元的成本，报名培训班、购买网络课程和书籍等。虽然有些白帽子处于求学或求职状态中，还没有固定的收入，但他们依旧愿意为学习投入高额支出。



擅长的漏洞类型

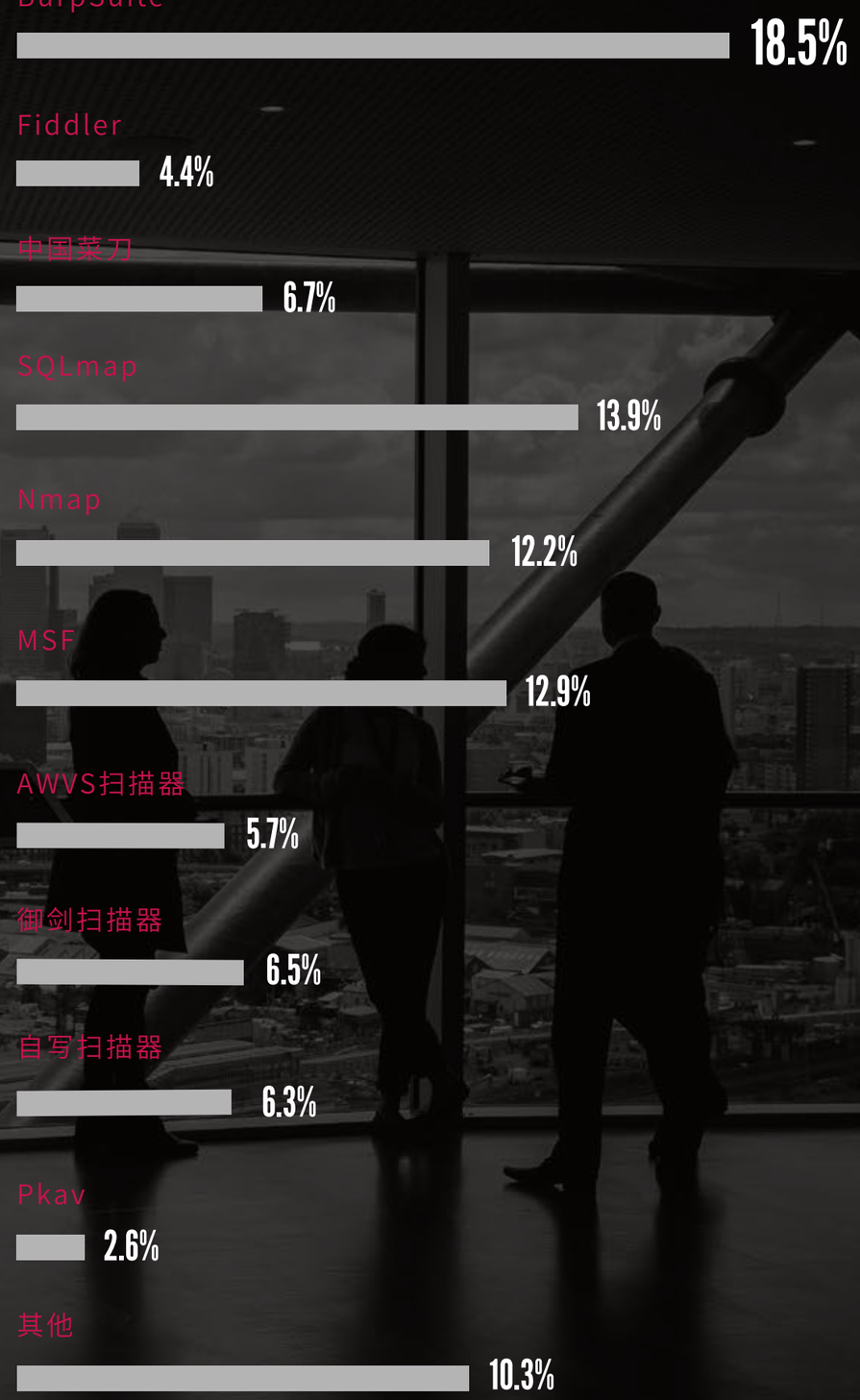
XSS	8.0%	代码执行	3.6%	CSRF	4.8%	客户端信息泄露	0.8%	权限提升/绕过	1.6%
注入	7.1%	信息泄露	6.0%	疑似入侵/存在后门	2.2%	硬编码敏感信息	0.7%	拒绝服务	1.0%
逻辑漏洞	8.1%	文件包含	4.0%	本地拒绝服务	1.4%	AllowBackup	0.4%	数组越界访问	0.5%
权限控制缺失	4.3%	任意文件操作	3.8%	组件暴露/权限漏洞	1.5%	Activity劫持	0.6%	内核提权	0.7%
支付漏洞	4.4%	上传漏洞	4.8%	客户端本地SQL注入	1.3%	DLL劫持	0.8%	智能硬件	0.5%
认证缺陷	3.2%	URL重定向	3.9%	WebView命令执行	0.6%	溢出	1.1%	其他	0.1%
弱口令	7.0%	XXE	3.1%	SSL证书验证错误	0.5%	释放重引用	0.7%		
条件竞争	2.8%	SSRF	3.1%	不安全存储	0.6%	双重释放	0.4%		

有效挖洞数量

20%白帽子认为企业修复不及时，对漏洞修复的反应速度仍有待提升

科班出身比例

常用的安全工具



最爱的安全工具

2019年，越来越多的白帽子开始使用第三方本地代理工具。BurpSuite成为使用最多的工具，SQLmap、Nmap、MSF和中国菜刀分列第二至五位。另外，超过9%的白帽子喜欢自写扫描器。

白帽子最爱的五大工具：

01 BurpSuite

Web安全渗透不可或缺的工具，作为一个集成平台，汇集了可用于攻击Web应用程序的工具，而这些工具具有许多接口，共享更具可扩展性的框架。

02 SQLmap

一款开源的渗透测试工具，拥有非常强大的检测引擎、多种特性的渗透测试器，白帽子测试必备。

03 Nmap

一个网络连接端扫描软件，可以用来探测工作环境中未经批准使用的服务器。

学校专业课
2.8%

有大神带
6.6%

公司培训
0.9%

网络课程/书籍
28.3%

报名培训班
3.8%

经常泡安全技术论坛/网站
53.8%

其他
3.8%

04 MSF

Metasploit Framework（MSF）是2003年以开放源代码方式发布、可自由获取的开发框架，这个环境为渗透测试、ShellCode编写和漏洞研究提供了一个可靠的平台。

05 中国菜刀

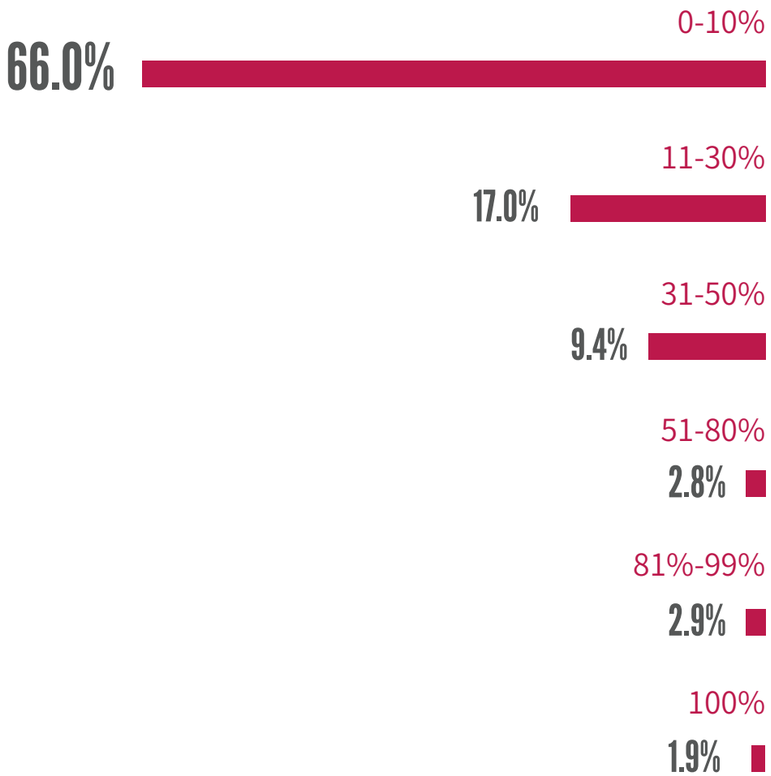
如果说Metasploit是美国黑客的代表工具，那中国菜刀就是白帽子心中的骄傲。作为一款专业的网站管理软件，只要支持动态脚本的网站，都可以用菜刀进行管理。

Hacker Lz12

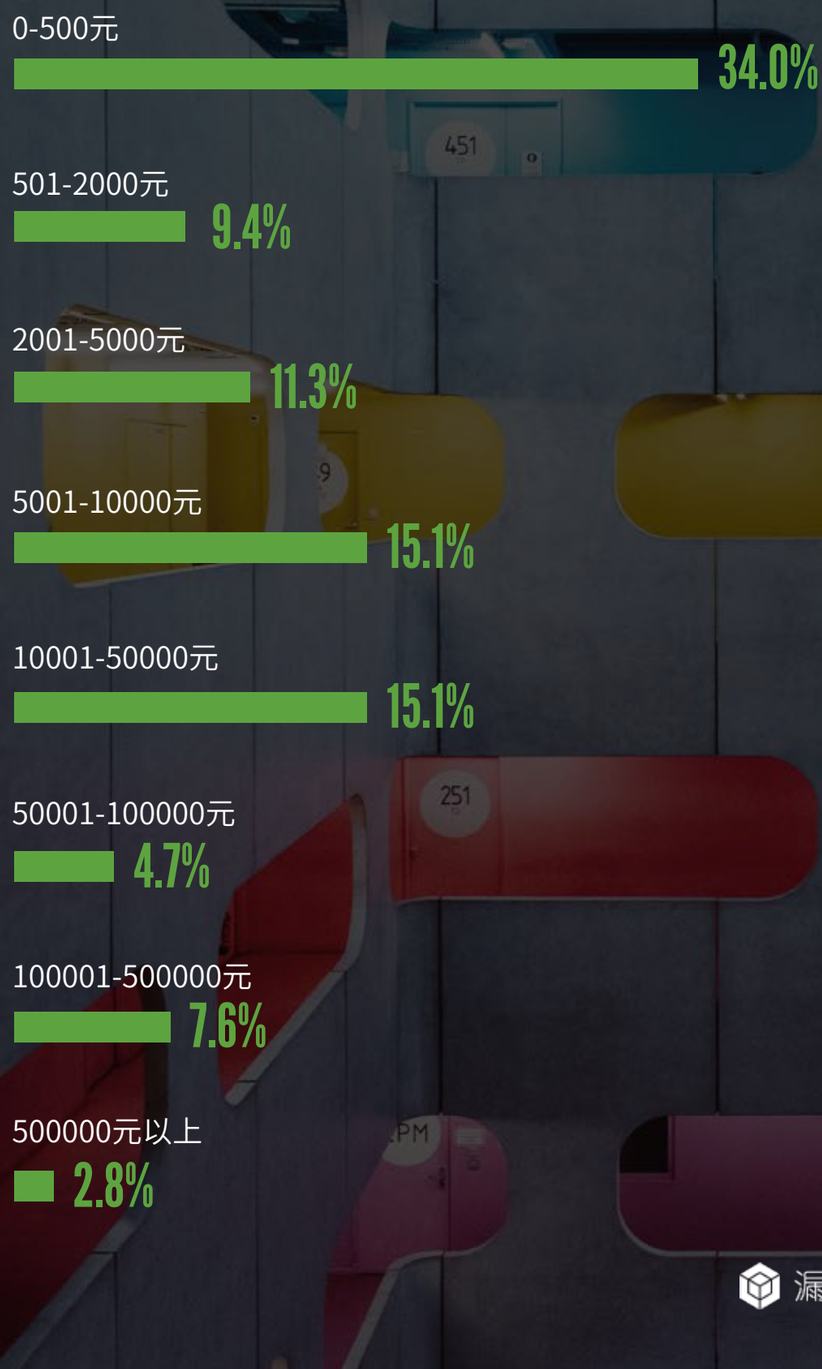
令Lz12印象最深的，是第一次挖到的任意账号密码重置逻辑漏洞。他表示当时的自己真的很激动，手在颤抖，脑海中的思路也如喷泉一样涌现。注册五六个账号反复验证后，他写了一篇长文报告提交漏洞盒子，并得到高危定级和人生的第一笔漏洞赏金。作为正式踏入白帽子群体的第一战，Lz12称从那以后再也没有漏洞可以让他这么激动了。

2017年进入安全行业，某公司安全服务工程师

平均每年获得的漏洞赏金占总收入的比例



已获得的所有漏洞奖励换算为现金，总额为



真实的CTF长啥样

今年，一部青春偶像剧《亲爱的，热爱的》从饭圈火进了安全圈，面对剧中在线恋爱的白帽子主角，坐着电竞椅、戴着耳机，用WASD来打CTF的队友，让人不禁发问：真实的CTF是这样的吗？

Capture The Flag，俗称夺旗赛，在网络安全领域中特指白帽子之间进行技术竞技的一种比赛形式。

1996年，CTF起源于DEF CON全球黑客大会，用竞技代替了之前通过互相发起真实攻击进行技术比拼的方式。发展至今，已经在全球范围网络安全圈内流行，并且有了相对成熟的竞赛模式。

由于CTF中几乎含有所有的信息安全知识，白帽子打比赛往往压力很大。

01 解题模式

与信息学奥赛比较类似，参赛队伍通过互联网或者现场网络参与，以解决网络安全技术挑战题目的分值和时间来排名。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

02 攻防模式

参赛队伍在网络空间互相进行攻击和防守，依赖挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御而避免丢分，比赛情况通过得分实时反应出来。

03 混合模式

结合解题模式与攻防模式，譬如参赛队伍不仅可以通过解题获取一些初始分数，还能通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。

除了模式有些许差异，比赛的大致流程都为白帽子之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。

在CTF的联结下，白帽子走到线下、相互协作。传说中的“漏洞王”可能是大一新生，膜拜的技术帝其实是小公司的螺丝钉。精心设计的题目、几十或几百支参赛的白帽子战队，不断地解题，得分，利用漏洞对攻……在CTF比赛中，大多数白帽子都觉得时间不够用，恨不得一天有48小时地打，压力很大但是也很有趣。

国内部分CTF比赛介绍

01 相关协会指导的权威CTF

XCTF全国联赛，由中国网络空间安全协会竞评演练工作组主办，称得上是国内最权威、最高技术水平与最大影响力的网络安全CTF赛事平台。全国大学生信息安全竞赛创新实践能力赛线上赛，覆盖面广，质量级别最高，被参赛选手称作CTF的国赛。

02 以BAT为代表的企业CTF

百度杯CTF夺旗大战，由百度安全应急响应中心和i春秋联合举办，是国内现今为止首次历时最长（半年）、频次最高的CTF大赛，而且赛题丰富，突破了技术和网络的限制。此外，还有阿里巴巴组织，面向在校学生的AliCTF，腾讯主办的腾讯信息安全争霸赛TCTF，字节跳动主办的Byte CTF字节跳动网络安全攻防大赛等。

03 各大高校CTF

HCTF，由杭州电子科技大学信息安全协会承办组织的HCTF，协会内部成员由热爱黑客技术和计算机技术的一些在校大学生组成，研究方向丰富，涉及渗透，逆向，内核，Web等。ISCC，北京理工大学组织的传统网络安全竞赛，但最近几年已经逐渐转向CTF赛制。以及由西安电子科技大学组织举办XDCTF等。

漏洞马拉松

漏洞马拉松是漏洞盒子平台在国内首家发起的线下漏洞挖掘、赏金奖励比赛。活动至今已经成功举办三期，吸引了来自全国各地的顶尖白帽。这是一场拼技术、脑力、体力的比赛盛宴。选手需要针对企业提供的业务环境，24小时不间断地进行漏洞挖掘比拼。比赛采用积分制模式，根据挖掘出来漏洞高低等级累计积分排行。与传统CTF不同的是，由于挖掘对象是企业提供的真实业务环境，一切漏洞均是未知，没有固定答案，实战性更强。

Hacker Yu

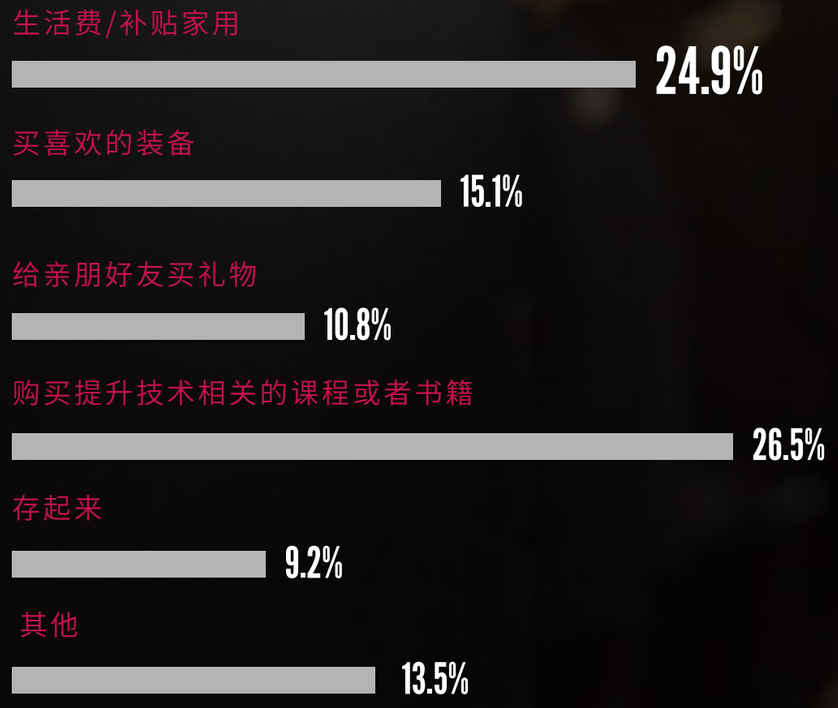
“

羽抱着学习的心态参加了上一届漏洞马拉松。说到原因，他表示一方面可以和大佬们一起挖洞，一睹他们的风采；另一方面也可以检验一下自己的真实水平。另外，比赛现场也不像电视剧里那样，灯光、舞台和欢呼声交相辉映，那只是戏剧化的虚构。24小时挖洞战场其实很安静，即使有人说话也是轻声交流，真正丰富多彩的是选手们的内心圣殿，脑力激荡中的搏杀，目前的国产剧真的拍不出来。

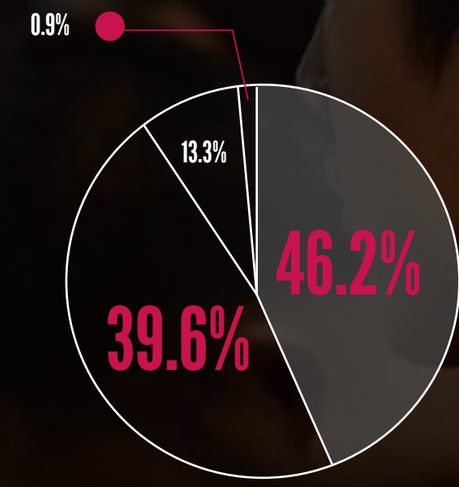
研究生，表示今年的漏洞马拉松会继续参加

”

所获得的漏洞赏金如何使用



你认为给予的漏洞赏金是否达到预期



比预期低一点 46.2%

远远没有 39.6%

差不多 13.3%

超出预期 0.9%

漏洞盒子

附录

漏洞盒子期望借由《2019年中国白帽子调查报告》，反映国内相关行业的真实现状，为大家呈现真实的白帽子生活群像，了解并认可他们为国内网络安全事业所做出的努力与贡献。

再次感谢大家的阅读，并期待您的宝贵意见！

Thank you again for reading and looking forward to your valuable comments!

01 用于支撑本次报告的研究方法和信息来源包括

2019年8月份，我们对来自数百家公司的共500多名受访者进行了详尽的问卷调查，整合超过数千条资料数据，并对之进行深入分析。此外，漏洞盒子也为本次研究报告提供了大量数据支持。

02 关于漏洞盒子

漏洞盒子，高效的互联网安全测试众测平台，国内安全众测模式的创新者和领导者。连接全球安全专家资源与自有团队，通过再现真实环境进行漏洞挖掘，为企业用户提供高效、透明的互联网安全服务平台。

截至2019年10月，漏洞盒子注册白帽子已达6万余名，发现漏洞数超过39万个。被国家计算机网络应急技术处理协调中心（CNCERT）、国家信息安全漏洞库（CNNVD）、上海市委网信办分别评定为网络安全应急服务支撑单位（省级）、优秀技术支撑单位、和网络安全技术支撑单位。

漏洞盒子