# 信息安全法律法规

--白帽子黑客

白帽子，描述的是正面的黑客,他可以识别计算机系统或网络系统中的安全漏洞，但并不会恶意去利用，而是将漏洞提交给对应的SRC。这样，系统将可以在被其他人（例如黑帽子）利用之前来修补漏洞；与黑帽子（即黑客）不同。“白帽子”们在漏洞的挖掘上具有公开性和正义性，并不恶意利用，而是以此对抗黑灰产业。

白帽黑客和黑帽黑客的区别：“黑帽黑客”即black hat hacker，也是人们常说的“黑客”或“骇客”了。与白帽黑客相反，黑帽黑客往往利用自身技术，在网络上窃取别人的资源或破解收费的软件，以达到获利，属于非法行为。虽然在他们看来这是因为技术而就得到的，但是这种行为却往往破坏了整个市场的秩序，或者泄露了别人的隐 私。 黑客也分为白帽黑客和黑帽黑客2种，一般我们所看到的相关黑客攻击报道，通常都是指黑帽黑客。由于黑帽黑客主要是为自己谋利，因而广为被媒体报道，而白帽黑客主要是测试安全，为企业或者组织扫描程序漏洞，防止黑帽黑客入侵，一般媒体报道的比较少，因此被网友关注的比较少。

著名案例与白帽黑客：

一：Jack在IOActive Labs安全顾问公司担当软件安全研究员。

他是全球著名的“白帽黑客”（white hat Hacker）之一，最为瞩目两个事件让他的技术受到了全球黑客的认可。首先是发生在2010年BlackHat大会上，他利用自己研发的一款名为“Jackpotting”软件成功侵入装有两种不同系统的ATM机，并当场让这些ATM机吐出钱来。

第二个著名事件发生在2012年，他成功黑掉了多家厂商生产的心脏起搏器，只需十几米之外的一台笔记本电脑，就能让它放出830V的电压，足以致人死地。Jack表示问题在于心脏起搏器和心脏除颤器都是有无线接收装置的，可以调节它们的工作模式；正是这个无线遥控渠道里面存在漏洞。他及时的将这个漏洞告知了多家厂商，并希望这些厂商及时改善提高安全措施。

二：**“变色龙”马克·迈弗雷特**作为顾问，替FBI机构工作。他的专业技能还让他三度面对美国国会的质询。迈弗雷特与别人一起成立了软件安全公司 eEye Digital Security，以曝光微软产品漏洞而赢得职业声誉，比如臭名昭著的“红色警报”蠕虫。

三：**查理·米勒博士**是一位简历上标有政府部门工作经历的黑客——为NSA服务了5年。米勒拥有数学学士和博士学位，带学术背景的黑客技术令他成为了4届Pwn2Own竞赛年度赢家。

米勒的声名来自于对苹果产品漏洞利用的展示。他是黑掉iPhone第一人，在2分钟内黑进了一台 MacBook Air，仅用一条短信就侵入了iPhone。黑进一辆行驶中的吉普切诺基，导致140万车辆被召回后，他得到了Uber工程师的职位。

四：化名为奥尔德森(Elliot Alderson)的法国黑客日前在Twitter上表示，其发现了印度政府“Aarogya Setu”新型冠状病毒追踪APP的安全问题，这可能会危及9000万印度人的隐私。作为一名有良心的黑客，奥尔德森已经将这个问题“标记”发送至印度计算机应急响应小组(CERT)和隶属于印度电子和信息技术部的国家信息中心(NIC)。

奥尔德森早先还曝光了印度政府“mAadhar”安卓应用程序的问题。

中国“白帽黑客”生存现状

频发的系统漏洞隐患也让网络安全问题愈发受到关注，如携程网的安全支付系统存在漏洞，导致用户的支付日志可被轻易下载，使大量用户银行卡信息(包含持卡人姓名身份证、银行卡号、密码等)泄漏和12306网站用户信息外泄（用户账号、明文密码、身份证、邮箱等）泄漏等一些事件。然而发现这些漏洞的，并不是某个人或者某个公司，而是一个被称为“白帽黑客”的群体。

曾经，即便是“白帽黑客”，也带着一层暧昧和隐晦的色彩，部分白帽黑客经常游走在法律边界，一不小心就会“踩线”。为了避免“白帽黑客”踩到雷区，2016年11月全国人民代表大会常务委员会颁布了《网络安全法》，于2017年6月1日开始施行。《网络安全法》的颁布将彻底扭转中国网络安全市场无法可依的窘境，把“挖漏洞”从灰色地带放到光明地带。中国的白帽黑客处于世界较高水平，每年世界上都会有GEEKPWN（黑客赛事平台）、PwN2OWN（全世界最著名、奖金最丰厚的[黑客](https://link.zhihu.com/?target=https://baike.baidu.com/item/%E9%BB%91%E5%AE%A2/118396" \t "https://zhuanlan.zhihu.com/p/_blank)大赛）这样的针对系统、硬件、攻防技术的黑客大赛，主要是微软、谷歌、苹果、Adobe等互联网和软件巨头通过让世界各路“黑客打擂”，找到系统漏洞加以完善，这些大赛上，360安全团队、腾讯安全战队等国内安全厂商都相继取得不俗成绩。“白帽黑客”的生存环境正变得越来越好，创业公司的热情日益高涨，“白帽黑客”这个职业开始逐渐被传播、被尊重。

我对于白帽黑客的见解：

与“黑客”相对，“白帽黑客”是高校培养的网络安全人才，被称为“信息安全保卫者”，他们是互联网世界的“守护者”，也是“互联网+”语境下不可或缺的中坚力量。一名白帽黑客，首先要有强大的技术诉求。在密码、数学、或者IT领域中有一技之长。白帽黑客是合法的黑客，其现实生活中的身份就是安全专业人士，他们的工作是寻找、测试和修补危机计算机的漏洞，让狂野的互联网更加安全。他们中有社会工程学专家、网络专家、硬件和软件工程师，毫无疑问他们对于计算机技术的了解十分深入。需要对计算机技术有着全面的了解，枚举法、社会工程、SQL、木马程序、 蠕虫病毒、以及其他形式的攻击都要烂熟于心，例如分布式拒绝攻击（DDoS）。掌握了全面的技术以后，对白帽黑客来说，道德上的要求和考量也是必须的。因为黑客的背景让你接触到大量的利益和诱惑，有时候你的行为游离在法律的边缘，这时候需要道德对你加以约束。确保自己的技术是为了造福人类本身而不是为了个人利益而发动恶意攻击。最后，白帽黑客作为黑客一族中约束力、自制力最强的团体，代表了人类技术的先驱，同时也在用自己的技术来造福人类。将自己学习或者掌握到的知识分享在网络上，帮助更多的人解决问题。