**信息安全法律法规大作业（一）**

学号： 姓名：

白帽子，亦称白帽黑客、白帽子黑客，是指那些专门研究或者从事网络、计算机技术防御的人，他们通常受雇于各大公司，是维护世界网络、计算机安全的主要力量。很多白帽还受雇于公司，对产品进行模拟黑客攻击，以检测产品的可靠性。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。

要说白帽子的发展，那就不得不提中国网络安全形势的大发展。最开始对网络安全工作者的区分是“黑客”和“红客”，具备鲜明的政治色彩。打击美国帝国主义的就是红客，红客以让五星红旗飘扬在国外网站上为荣，而此时被划分为黑客的人更多的从事无差别攻击。而伴随着苏联解体，全球化多极化的发展，中国网络安全工作的政治色彩逐渐减弱。正此时，被称为“世界头号黑客”的凯文·米特尼克被逮捕，《黑客帝国》发行并爆火，基于对米特尼克和尼奥的崇拜，大家开始区分“黑客”和“骇客”。黑客是好人，是正义有能力的化身，而骇客形容的是攻击，渗透，木马，破坏者的概称。之后，XCON大会允许被召开，黑客技术培训也登堂入室。此时的黑客开始被国家“特殊关照”，有些黑客违反法律被抓，或因为特殊能力而被招安；而骇客们形成了地下产业链，从事灰色产业。再往后，“黑客”升级成了“极客”，参加各种PWN大会，秒杀谷歌、微软、苹果的新应用、新系统，获得国际赞誉无数。

因此，其实直到“白帽子”一词的出现以前，类似“白帽子”的群体一直存在。但是由于互联网行业和网络安全形势的发展，网络安全工作者被划分为“白帽子”、“黑帽子”和“灰帽子”。渐渐的，白帽子们形成一个社区——wooyun。而自从乌云论坛出现，白帽子开始抱团，并开始在乌云论坛上面上传各种平台的漏洞。因为发掘漏洞必须要对网站的数据进行爬取和分析，并且法律法规并未对此行为进行明确规定，因此这也为以后白帽子和各大平台的冲突埋下了祸根。

白帽子一直游走在法律的灰色边缘，这是因为，其工作属性要求其不可避免地须进入互联网网站，并和黑客使用同样的工具软件，查看、分析、提取、测试数据，从而发现网站漏洞。这一系列的动作其实早已是悬在白帽子头上的达摩克利斯之剑，随时会落下。而这首先是因为对于数据的爬取本身就会造成一定的风险，对于发掘漏洞过程中白帽子接触到的数据，其泄漏问题以及滥用问题，除了发掘漏洞的白帽子本人，谁也说不清楚。其次是大多数时候，白帽子对于企业漏洞的挖掘是并未经过企业的正式授权的，而此时法律就相当于发掘出平台漏洞的白帽子和平台之间的窗户纸，平台有权利捅破“窗户纸”，利用已有的法律要求白帽子为“恶意入侵”、“窃取数据”付出代价。就比如被世纪佳缘送入牢狱的白帽子袁炜，在发现世纪佳缘的网站BUG以后反手被世纪佳缘控诉被捕。

尽管白帽子群体的初心是：“我们有着足够强大的技术力量能够帮助企业发现问题，并协助企业解决问题。也希望企业能够信任我们，支持我们的行为。我们并不求任何回报，不过有一定的回报我相信我们能配合的更深入更好”，但实际上，在现有的法律框架下，想要实现这个初心，大多数时候需要白帽子和平台双方实现“心照不宣”，且尽量在《中华人民共和国刑法》、《中华人民共和国网络安全法》、《网络安全等级保护制度2.0》等等的法律框架下行事。白帽子值得大家共同保护，但目前不论是司法实践，还是理论研究，都没有十分关注这一类型的案件。然一万年太久，我们只争朝夕，白帽子应当抬头看看那把达摩克利斯之剑，从刑法条文中分解整理，并打开自己的保护伞。

除了社会的关注和注意法律边界以外，白帽子本身也应当注意自我规范：

1. 白帽子要依托安全的平台

这类平台国内的包括CNNVD：中国国家漏洞库（中国国家信息安全漏洞库）、CNVD：中国国家信息安全漏洞共享平台（国家信息安全漏洞共享平台）、WooYun：乌云安全漏洞报告平台等，国际上如CVE、NVD、SecurityFocus、Secunia及OSVDB等。

1. 寻找漏洞时要区别友商对象

重点值得注意的对象，例如国家事务、国防建设、尖端科学技术领域、金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统。针对这类网站，除非获得友商的书面合同或授权，否则白帽子不要轻易出动，因为我国刑法对该类网站的保护程度是“只要侵入就犯罪”，而不论白帽子是否进行数据读取、篡改、删除。而所谓的侵入，指未取得国家有关主管部门合法授权或批准，通过计算机终端访问国家重要计算机信息系统或者进行数据截收的行为。

1. 寻找漏洞要区别数据源类型

《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释〉明确规定了“获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组”，或其它“身份认证信息五百组以上的”，则构成犯罪，因此，身份认证信息是白帽子须努力避免触碰的信息，特别是以下载的方式直接存放到本地电脑上，更是一种赤裸裸的“数据获取”形式。

最后，我认为安全平台对白帽子也应当起到保护作用。

1. 企业公关保护

对于在平台上提交的BUG，要进行正确的舆论引导。避免被发现BUG的企业利用舆论引导对发现BUG的白帽子进行反讹诈。

2. 白帽子安全保护

平台要对漏洞检测方面的具体情况与企业进行合理沟通，并一定将具体情况和相关细则告知白帽子，避免白帽子抓取沟通范围以外的数据，导致白帽子遭到企业控诉。

在互联网领域，暴露在阳光下白帽子和阴暗处的黑帽子正在斗智斗勇，如果把暴露在阳光下的白帽子一刀砍杀，不免让人寒心。因此我们呼吁为互联网中的这群特殊群体，建立更加透明、规范的体制，建立白帽子认证体系，为白帽子的漏洞寻找之旅铺平道路，莫让为众人抱薪者暴毙风雪之中。