Web3律师：加密安全公司CertiK与Kraken互撕，白帽也会变黑帽？

加密行业的撕逼真精彩。这不，加密安全独角兽CertiK和美国超级交易所Kraken的掰头，让笔者变成了瓜田的猹。

事情大约是这样的：CertiK在其安全测试过程中发现了一个严重的漏洞，涉及到在Kraken平台上人为增加加密交易账户余额的可能性，并希望通过测试触达Kraken的报警提示阈值。然而，Kraken对此表示，CertiK的行为超出了一般安全研究的范围，涉嫌利用漏洞获利，因此指责CertiK进行了敲诈行为。



根据CertiK的说法，他们的测试揭示了Kraken系统中的多个安全漏洞，这些漏洞未经修复可能导致数亿美元的损失。CertiK强调，他们的行为是为了加强网络安全，保护所有用户的利益，并公开了完整的测试时间线和相关的存款地址，以证明他们的透明度和诚信 。



Kraken及其CSO Nick Percoco则通过社交媒体和公开声明强调，他们的漏洞赏金计划有明确的规则，并要求所有发现漏洞的研究员遵守这些规则。Kraken还表示，CertiK的行为已经构成了对其平台安全的直接威胁，并已向执法机构报告了这一事件 。

这场对峙不仅涉及技术和安全问题，也触及到了法律和道德的边界，特别是关于白帽黑客活动的界限和责任。这为曼昆律师进一步探讨白帽黑客的法律尺度提供了丰富的背景和讨论基础。

### 白帽黑客的行为合法吗？

从严格的行为上而言，白帽黑客的行为和非法侵入计算机系统非常的相似。但在绝大多数情况下是不会给予白帽黑客违法犯罪的法律评价。因为白帽黑客的目的、行为过程使其与违法犯罪行为有着本质区别。

链上的白帽黑客通过发现和修补漏洞，帮助企业和组织建立更安全的网络环境，从而增强网络的可靠性和可信度，为整个链上的安全性和稳定性都做出了积极贡献。

那收取报酬的行为是否会影响对白帽黑客的评价？报酬作为一种有效的激励机制，可以吸引更多人才投入网络安全领域，从而提升整个行业的安全性，对于企业和组织来说，也是一种高性价的漏洞修复方式，同时，也能树立企业重视网络安全的形象。因此，白帽黑客收取合理费用一般属于行业的约定俗成。

### 这一次，CertiK是白帽黑客吗？

在CertiK与Kraken之间的掰扯中，核心问题之一是CertiK的行为边界问题。CertiK的行为，特别是向外部钱包转移300万美元资金的动机和法律性，成为了争论的焦点。

#### 行为并不透明

CertiK是Kraken合作的安全公司，并且明知Kraken设有针对安全漏洞的赏金计划，完全可以在开始测试之前确保获得充分的授权。与此同时，据社区及Kraken披露，CertiK报告漏洞时，并未提及具体转移数量，而是在Kraken发出“退还$3M”后，披露自己“全部测试地址”，以证明自己未转走Kraken指控的金额。

#### 资金转移是事实

根据Kraken以及链上侦探@0xBoboShanti的陈述，早在5月27日就有CertiK安全研究人员进行了探测和测试，这与CertiK的事件时间表产生了矛盾。与此同时，在后续的漏洞测试中，尽管CertiK声称所进行的操作是为了测试Kraken的报警系统是否能及时触发，然而在实际操作时，这种测试不仅仅停留在发现漏洞，CertiK还将金额转移到了独立钱包地址。这一行为超出了常规的安全测试范围。据披露，此前CertiK已经对多个交易所进行了相同操作，并且还使用过Tornado Cash转移资产以及ChangeNOW进行抛售。

以上两个情况大概率已经超越了白帽黑客的行为边界。

### 法律界定成关键

从法律角度来看，白帽黑客的行为通常被视为合法，但前提是这些行为符合一定的规范和条件。

在美国，与白帽黑客活动密切相关的法律主要包括《计算机欺诈与滥用法案》(CFAA)。根据CFAA，任何未经授权访问或超出授权范围访问保护计算机的行为都可能构成犯罪。对于白帽黑客而言，他们的行为通常需要在明确获得授权的范围内进行，否则即便是出于安全测试的目的，也可能违反CFAA。此外，随着技术的发展，一些地区也逐渐形成了更具体的规定来指导和保护白帽黑客的行为。

而在中国，《网络安全法》也明确了增强网络安全防护和加强网络空间管理的总体要求。这意味着网络入侵，即使是出于安全测试的目的，也可能被视为非法行为；同时，安全法强调了个人数据和隐私的保护。任何在网络测试中涉及个人数据的操作，必须确保数据的安全和隐私不被侵犯；发现安全漏洞后，有责任及时向网络安全管理机构和受影响的网络运营商报告。这种报告机制旨在及时修补漏洞，防止漏洞被滥用。

不过在Web3.0行业，部分白帽黑客的测试也会涉及到转移资金的行为，但通常会在项目默许的情况下（比如项目有相关grants），或者将加密资金转移至特定的独立钱包做存储（不再进行下一步操作），进而提报漏洞并获取项目方赠与的报酬，这也算是行业约定俗成的行为。

然而，在CertiK的案例中，资金的实际转移，尤其是后续操作引发了法律上的复杂问题。一方面是CertiK是否因私利动机而进行了资金转移；一方面是CertiK并未遵守Kraken对于白帽黑客的明确要求，而是通过转移资金再次证明同一个漏洞；另一方面是其后续对转账资金的操作，可能被视为非法获利。此外，CertiK在行为后的处理方式，包括与Kraken的沟通和协调，也会影响其行为的法律评估。

### 结论与反思

虽然Kraken和CertiK这场争议完完全全是个美国法律问题，曼昆律师也不好发表美国法下的观点。但假设发生在中国法下，CertiK的行为恐怕也难逃敲诈勒索和非法侵入计算机系统的指控。

确实，白帽黑客在某些情况下也可能“变黑”。即使最初的意图是为了增强系统的安全，但如果他们在没有适当授权的情况下进行测试，或者为了私人利益而利用发现的漏洞，这些行为就已经偏离了白帽黑客的法律以及伦理标准。正如CertiK与Kraken事件所展示的，如果未经授权进行资金转移行为，尤其是在涉及巨额资金时，即便是出于测试目的，也可能被视为黑帽行为。