数字货币交易所

安全白皮书

Helm 区块链安全实验室

2018 年 9 月 5 日

目录

0x01 区块链行业的安全现状

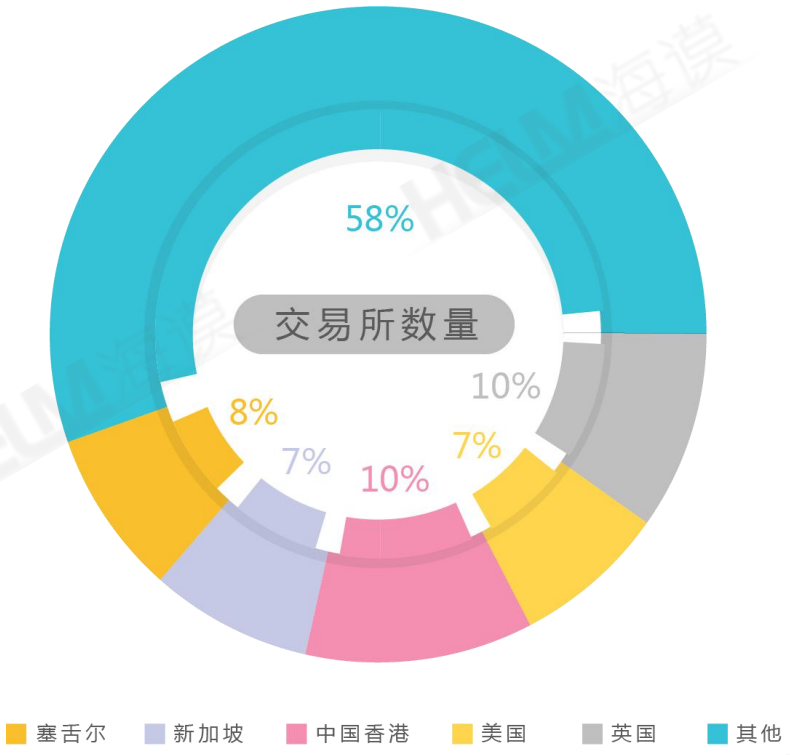
区块链行业目前处于一个发展期，生态系统已延伸到物联网、云计算、大数据、人工智能等多个领域，应用场景也涵盖了金融、投资、监管等机构，引发了新一轮的技术创新和产业变革。由于目前具体化的场景应用落地难，区块链作为一套减少信任成本的小型交易系统目前更多的是发行数字资产。

一直以来，安全问题都是信息产业的重大发展方向，而区块链作为一种新兴技术，安全性威胁是其迄今为止所面临的最重要的问题之一。而除了链上的安全，交易所安全是直接影响用户数字资产的安全的最主要因素。

为全面了解和推动区块链技术和产业发展，解决区块链目前面临的安全问题，保证数字资产的安全，HELM 安全团队根据各成员在交易所安全漏洞挖掘的经验和响应经验，对大多数交易所存在的安全问题进行总结分析，并以部分交易所为案例对交易所安全性作出报告与建议。本报告不针对任何交易所，仅以此份报告解释说明其衍生的排行榜，希望能对行业的区块链安全生态添砖加瓦，对监管单位和数字货币投资者有一定的参考价值。

0x02 交易所的安全现状

拥有主流数字货币的区块链交易所有 270 多家，其中英国 30 家，美国 20 家，中国香港 28 家，新加坡 22 家。其中大多数的东南亚交易所的客户群体为国内客户。具体分布如下图：



在国内有很多的投机投资者，所以继资金盘、p2p 理财之后又一回报比较高的投资方式的出现导致了大量的资金涌入，具一些区块链媒体统计，2017 年币圈的价值约为一个上证的价值。

去中心化的交易所并未出现，人民币与数字货币的兑换还需要交易所充当法币兑换的角色。目前大多

数交易所的安全性令人堪忧，并非没有被曝光漏洞的交易所就是安全的。相反，未曝光漏洞的才是最危险的，可能黑客像一直蚊子一样不知不觉地向交易所吸血。

黑客的目的就是盗取钱包中数字货币，而不管一个漏洞的攻击手法多么低级、不起眼，只要能够让黑客得到了这些数字黄金，它就是一个危害大的漏洞。不能用传统的眼光来看待币圈的漏洞，交易所只要能让资金资产受到威胁，每一个漏洞都是致命的。

根据 HELM 安全团队分析，交易所的主要威胁为：内部员工盗窃、用户信息泄露、越权漏洞、通过金融手段操纵用户拉币价以及拒绝服务攻击。

千里之堤毁于蚁穴，交易所通常都是一些不起眼的漏洞导致了崩盘。相反，很少直接公有链上智能合约的漏洞直接影响某个单一的交易所。

在此，HELM 安全团队列出近几年遭受过攻击的交易所（其中有一些已经向韭菜们告别了）：

2015 之前 攻击者在 Bancor 交易所中实施先行攻击

GATE 交易所遭黑客攻击，RLC 瞬间爆拉百倍

交易所 OKEX 数位用户平台账号被窃取

曾经世界第一的日本交易所 Mt.Gox，导致其最终被迫宣布破产

美国数字货币交易所 Poloniex 被盗

交易所 LocalBitcoins 遭受拒绝服务漏洞攻击

2015-01-05 全球知名的数字货币交易所 Bitstamp 系统管理员被诱导执行恶意文件

2016-01-15 交易所 Cryptsy 被攻击，黑客从 Cryptsy 冷钱包转出小型的数字货币。

2016-05-14 香港数字货币交易所 Gatecoin 遭黑客攻击

2016-08-02 交易所 Bitfinex 遭黑客攻击

2017-06-07 韩国最大交易所 Bithumb 三万用户信息被泄露

2017-12-19 韩国数字货币交易所 Youbite 受到黑客入侵，损失平台内总资产的 17%。

2018-01-26 日本最大的比特币交易所之一 Coincheck 遭黑客攻击

2018-02-13 交易所 BitGrail 被攻击，大量 XRB 被黑客窃取

2018-03-07 币安交易所用户权限被盗

2018-03-18 迪拜某加密货币交易所员工窃取 20 万美元的加密货币供个人使用

2018-04-13 Coinsecure 被盗取 438 比特币，价值超过 300 万美元。

2018-05-28 GATE 交易所遭黑客攻击，RLC 瞬间爆拉百倍

2018-06-11 韩国加密货币交易所 Coinrail 遭黑客入侵，损失价值 4000 万美元的 ICO 代币

2018-06-12 比特儿交易所疑似遭黑客入侵，目前已进入维护状态

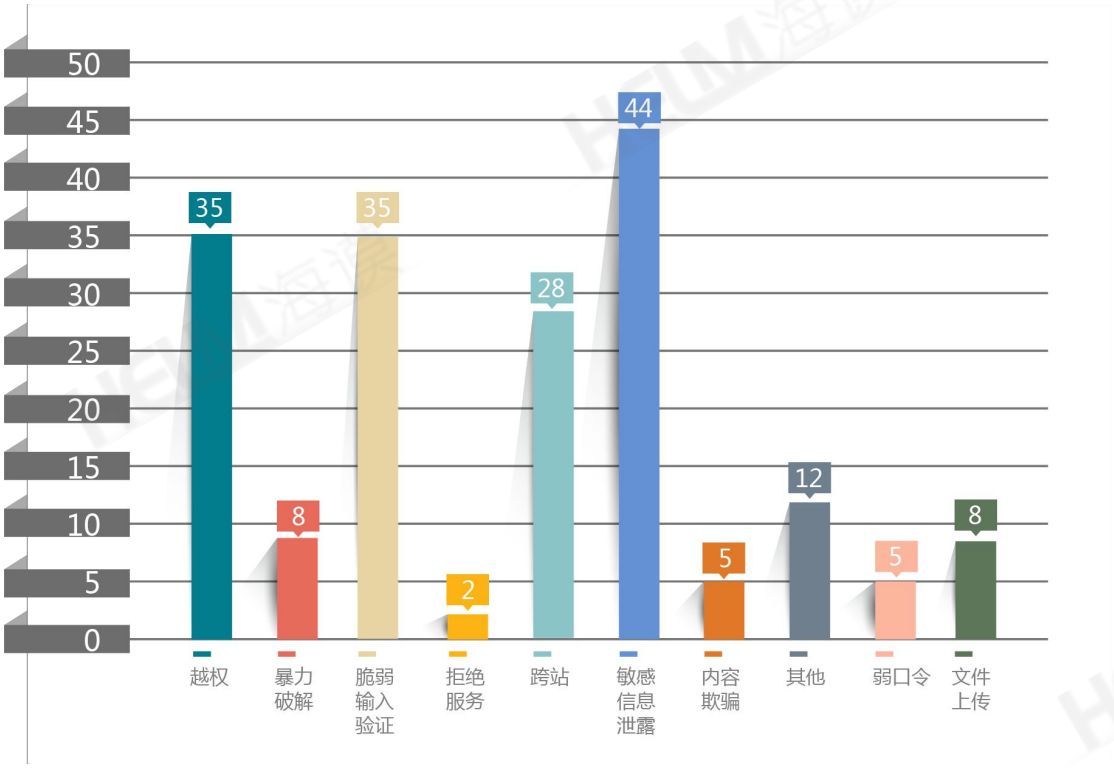
2018-06-28 部分交易所对 USDT 币充值存在校验缺陷，可通过“假充值”导致市场混乱！

2018-07-10 交易所 EXX 称遭黑客频繁攻击

2018-07-12 LBank 交易所移动终端可被中间人攻击提取数字资产

2018-07-23 直布罗陀区块链交易所 RKT 存在上溢漏洞

据 HELM 团队了解，由于被黑客攻击导致破产的交易所超过 10 家，在此 HELM 安全团队对 2018 年交易所受到常见的黑客攻击类型进行统计（截止 7 月），得到以下结果（统计图）：



可见黑客的攻击手法在敏感信息泄露、越权与脆弱输入验证上有比较大的比例，并非交易所不存在高危的漏洞，而是简单看似低危的漏洞攻击成本高，并且更容易成功。往往千里之堤毁于蚁穴，蝴蝶扇动翅膀总能出现风暴。

0x03 交易所的基础安全防护

在币圈有一句话：错过了房地产，错过了牛市，你还要错过了区块链么?

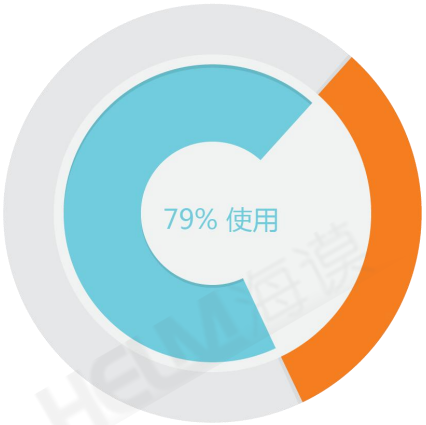
一些团队发链只为了割韭菜，对安全持无所谓态度。一些交易所也如此，没有专门的安全团队，甚至也没有对基础的安全防护，没有对漏洞进行应急响应。

在此，HELM 安全团队对交易所得基础安全防护多维度进行识别统计。

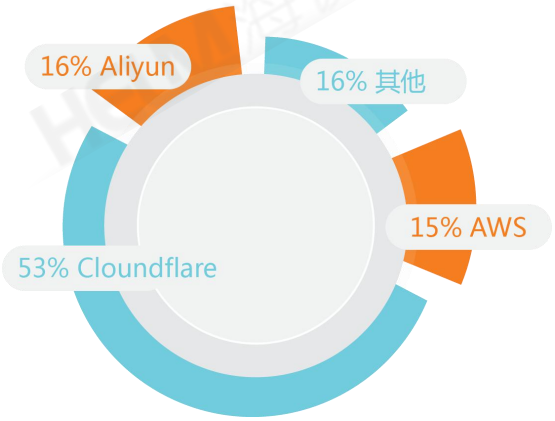
其中有 210 家使用了云服务，使用 Cloundflare 的交易所 111 家，使用 Aliyun 的交易所 34 家，使用 aws 云主机 32 家，使用其他的云主机的交易所 33 家。

未使用云主机者的交易所有 57 家，并且据 HELM 安全团队统计，未发现此些未使用云主机的交易所有独立的安全团队或使用 WAF。

是否使用云主机

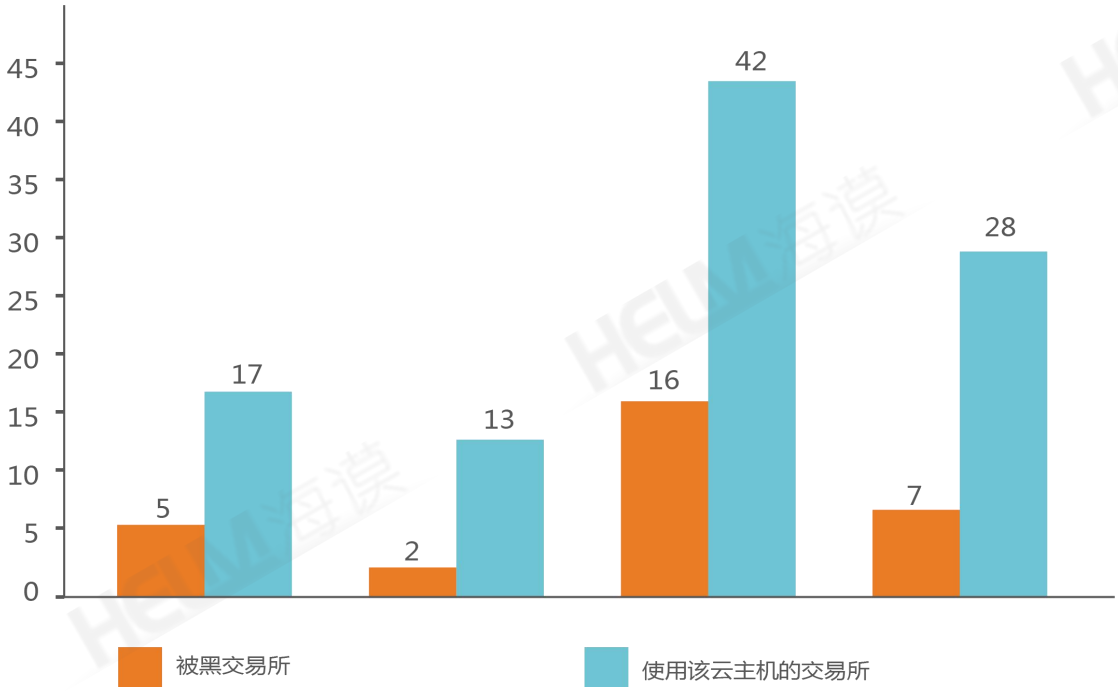


交易所云主机使用分布

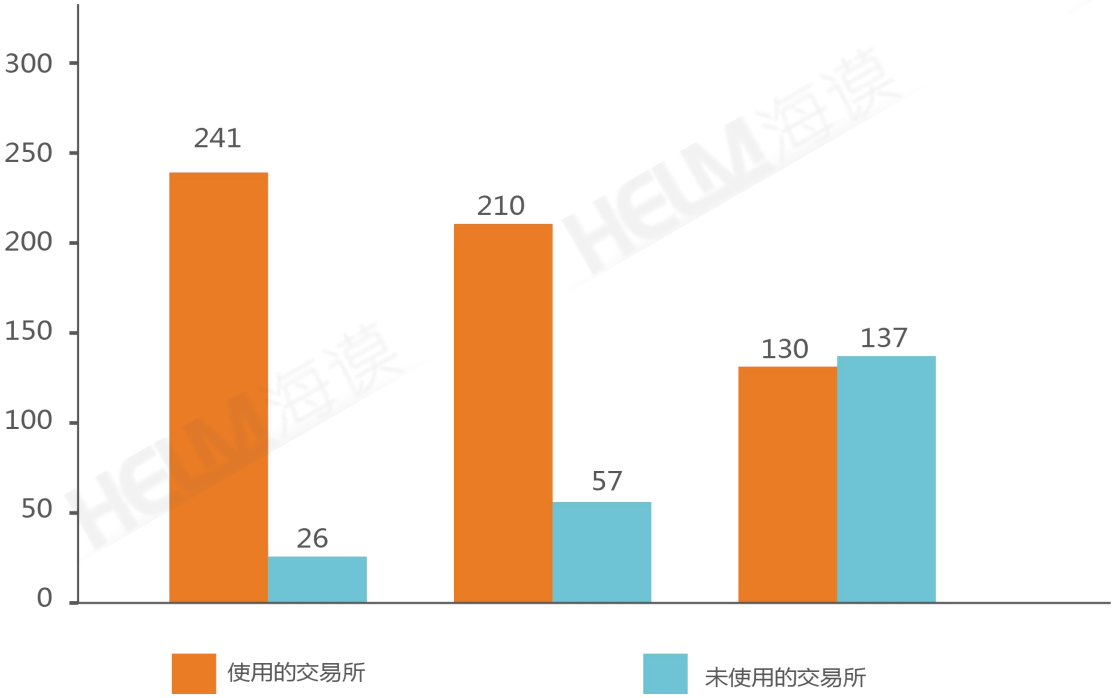


非小号上排名前 100 的交易所，根据已被曝光的消息，被攻击过的有 30 家，未被攻击的有 70 家。其中使用阿里云的交易所有 13 个 ,被攻击的有 2 个 ;使用 aws 的交易所有 5 个 ,被攻击的 5 个 ;使用 cloudflare 的交易所有 42 个，被黑的有 16 个；未使用云服务器的有 28 个，被黑的交易所有 7 个。

对比统计结果，可知基础安全防护对交易所的重要。



根据 HELM 安全团队的 HELM 引擎分析 ,其中有 241 家交易所使用 CDN ,26 家交易所未使用 CDN ；有 210 家具有抗 DDOS 能力，57 家交易所不具备抗 DDOS 能力；有 WAF 的交易所有 130，无 WAF 的有 137 家，统计结果如下图。



虽然 WAF、CDN 不能从根源上杜绝恶意攻击，但是可以对一部分攻击进行防护，降低安全防护的成本。

抛开是否为三流的交易所 ,市面上的交易所大多数没有良好的风控措施 ,并基本存在传统的 web 漏洞，有些交易所目的放在的自动交易机器人的开发，并未在安全投入太大的精力，但是有时候一个简简单单的越权就可以操纵整个交易所的资金，直接导致交易所破产。

0x04 交易所的漏洞情况

HELM 安全团队从一些交易所中选取常见且对业务有较大影响的漏洞进行分析 ,抛开 SQL 注入与文件上传等从技术角度危害重大的漏洞，在交易所中，只要涉及金钱资产问题，哪怕是一个小小的越权漏洞、敏感信息泄露漏洞可能也是致命的问题。

一、账号体系脆弱

（一）场景

1.在短信验证中，若不对短信验证码的有效期做限制或者验证接口做限制，很容易短信验证码被破解；

2.若登陆接口未做请求限制，攻击者可以通过大量的密码字典来暴力破解某个账户的密码。又或者说，攻击者可以通过大量的用户名字典来暴力破解密码为某个值的用户，比如密码为 123456、qwe123 的用户；

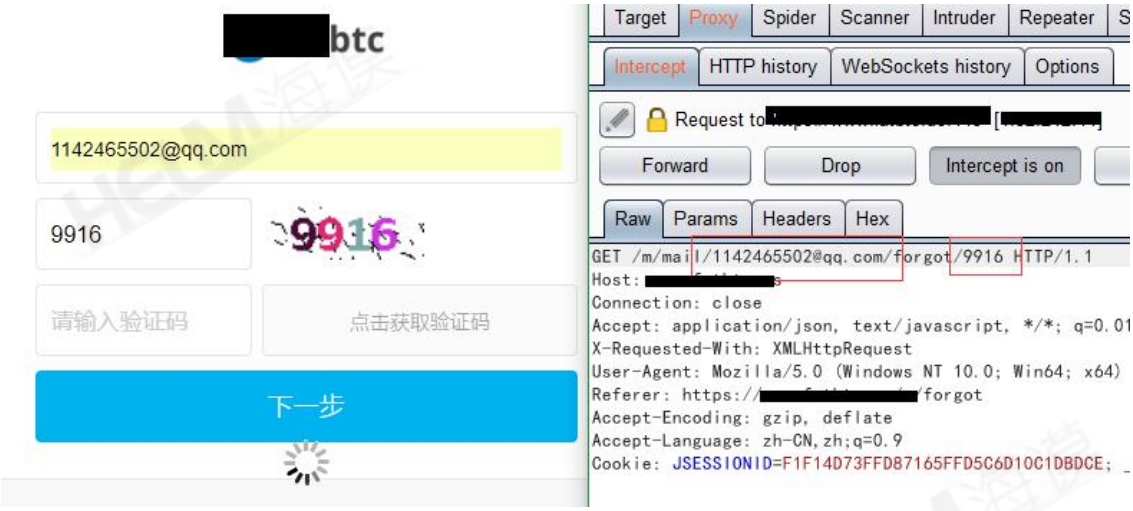
3.绕过二级保护验证，对某账户的密码进行重置。

（二）案例

一、重置任意用户密码

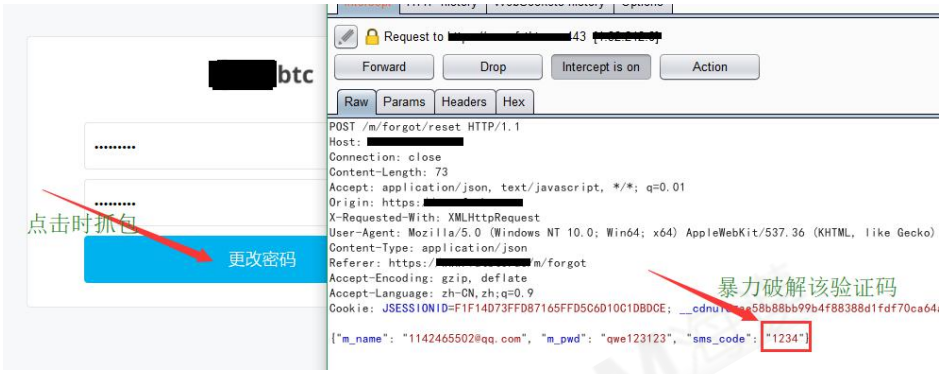
1.重置被害者 1142465502@qq.com 账户的密码：

2.点击获取验证码，这里也需要先获取。

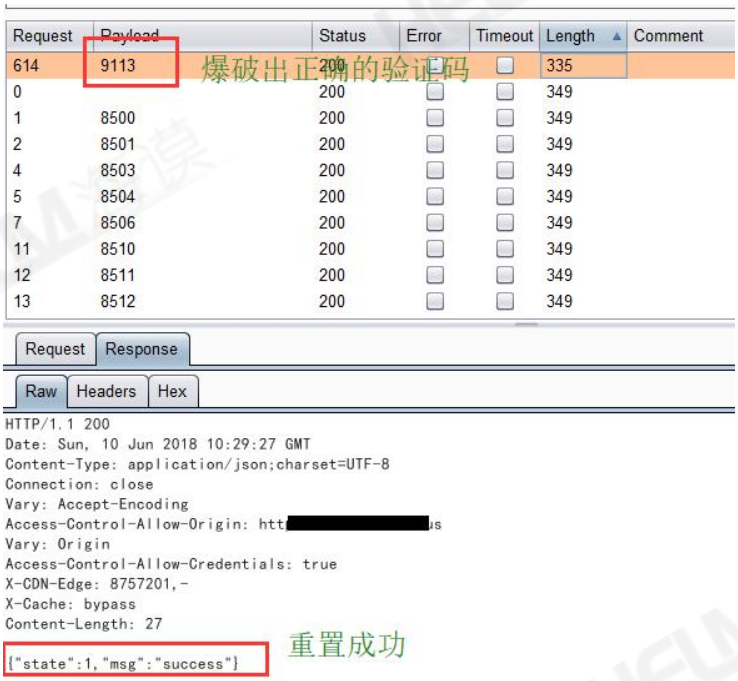


3.但是我们并不知道验证码是多少，于是我们直接随便填写验证码，点击“下一步”时抓取数据包。虽然服务器端返回的状态是表示不通过的-1，但是我们这里把-1 改成 1，让客户端误认为验证码正确而发起下一步的请求：

4.填写密码，点击“更改密码”时抓取数据包，于是我们暴力破解此处的验证码：



5.暴力破解得到正确的验证码，于是重置密码成功：

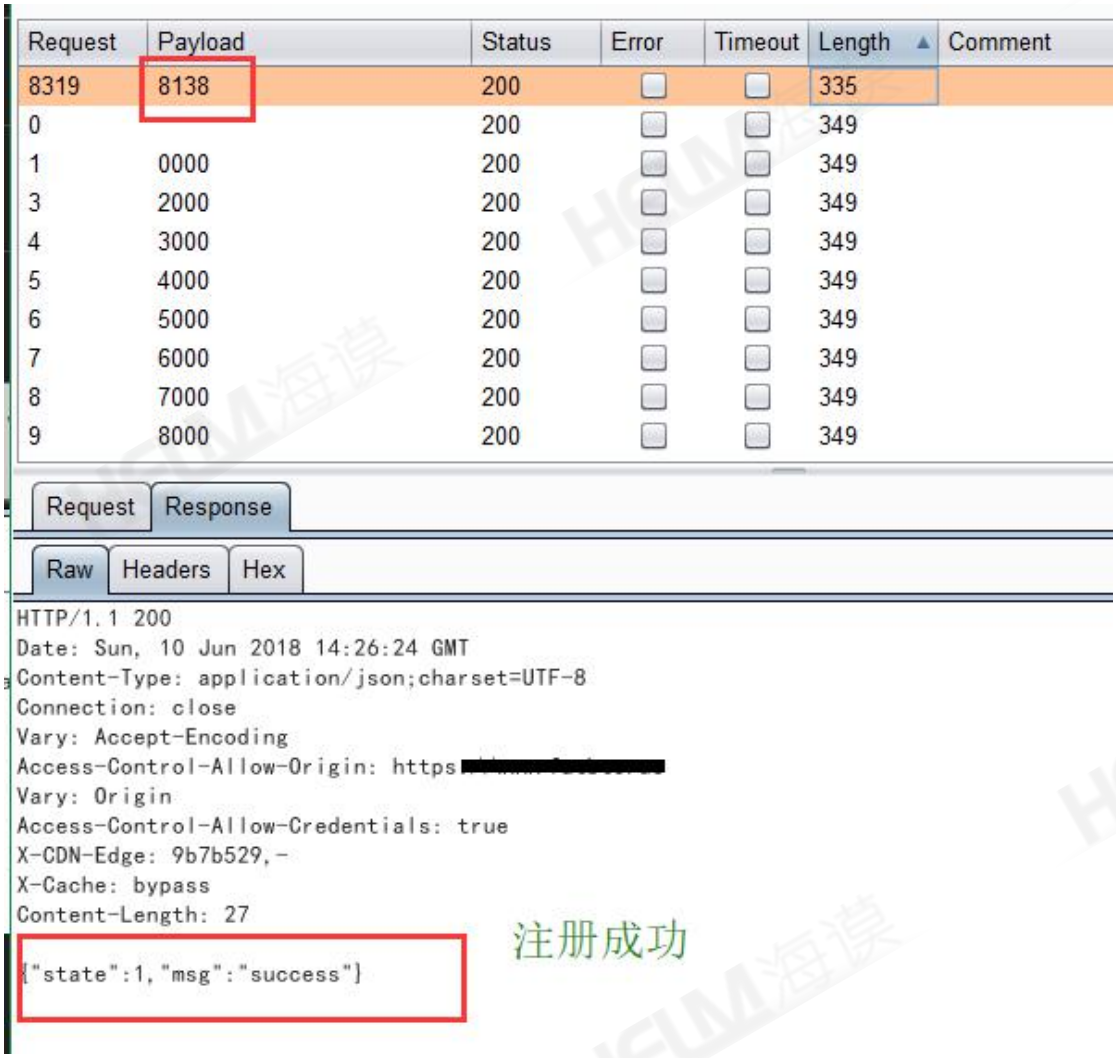


二、任意手机号注册

1.注册页面，填写注册信息：

2.任意填写验证码，点击“注册”时抓取请求数据包，然后把该数据包加入暴力破解，暴破 sms_code 参数：

3.以下是利用工具暴力破解的结果，暴力破解成功后，账号注册成功：



脆弱的账户体系会导致交易所任意密码被修改，用户数字货币被盗取。结合社工的手段可造成大量的数字资产损失。

二、越权漏洞

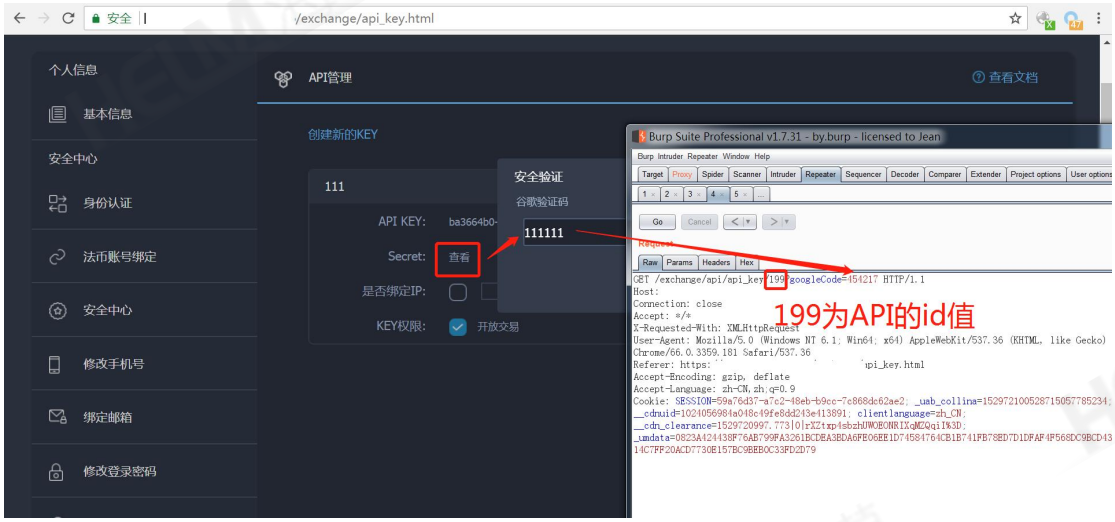
（一）场景

1、普通用户对管理垂直越权，导致整个交易所的权限沦陷；

2、普通用户之间越权，可操纵其他用户，如：越权操纵用户资产管理权限、API 信息等。

（二）案例

某非小号排名 top30 的交易所越权漏洞，访问页面 www.xxx.helm/exchange/api_key.html。



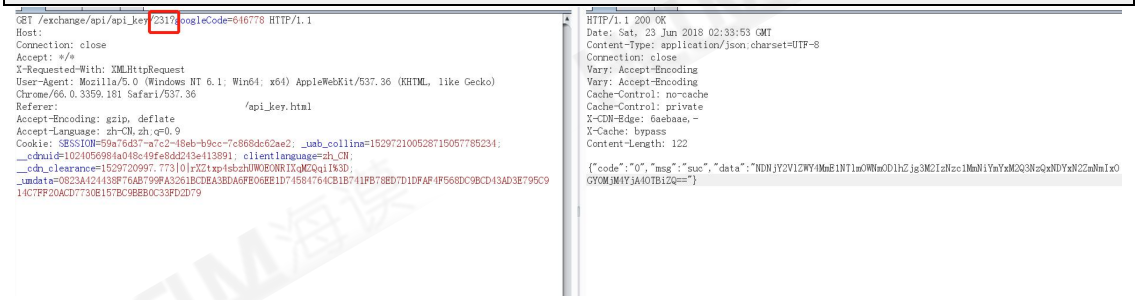
这里只要保证输入的 GoogleCode 是正确的，然后替换前面的数字，即可越权查看别人的 API 秘钥。

访问

```
GET /exchange/api/api_key/231?googleCode=646778 HTTP/1.1
Host: www.xxx.helm
Connection: close
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (K
HTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
Referer: https:// www.xxx.helm/exchange/api_key.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: SESSION=59a76d37-a7c2-48eb-b9cc-7c868dc62ae2; _uab_collina=1529721005287
15057785234; __cdnuid=1024056984a048c49fe8dd243e413891; clientlanguage=zh_CN; __
cdn_clearance=1529720997.773|0|rXZtxp4sbzhUWOEONRIXqMZQqiI%3D; _umdata=0823A424438
F76AB799FA3261BCDEA3BDA6FE06EE1D74584764CB1B741FB78ED7D1DFAF4F568DC9BCD43AD3E795C91
4C7FF20ACD7730E157BC9BEB0C33FD2D79
```

返回私钥

{"code":"0","msg":"suc","data":"NDNjY2V1ZWY4MmE1NT1mOWNmOD1hZjg3M2IzNzc1MmNiYmYxM2Q3NzQxNDYxN2ZmNmIxOGY0MjM4YjA4OTBiZQ=="}



由于越权造成的 API 泄露会造成巨额的账户资产损失，黑客可以遍历整个交易所的所有 API，利用大户们 API 上巨额的资金拉升某个币种，攻击手法相对传统的提币、提现等留下的痕迹更少。甚至甚至可以采用长期持有某个币种的手段，一点点蚕食用户炒币的收益。

0x05 交易所风控能力

（一）场景

1、部分平台没有热钱包，提币的时候人工审核。但是业务人员安全意识低下，没有严格地对黑客账户放行（进行限制）；

2、提币自动审核，但是无风控验证，一旦出现漏洞导致热钱包钱被盗；

3、冷钱包存储不当受黑客攻击；

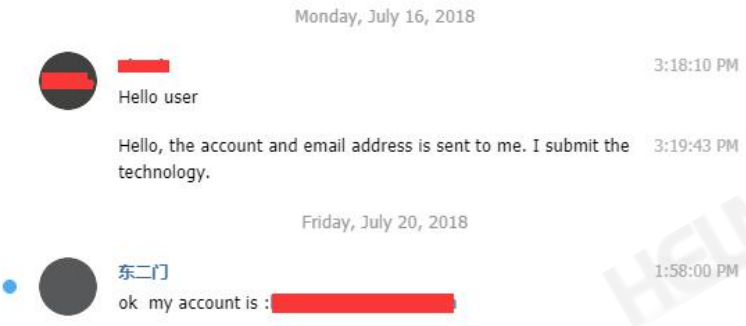
4、没有控制好官方资讯、交流渠道。出现假冒官方人员钓鱼、钓币人员，出现假的官方消息等；

5、没有设置提现阀值，当被黑客入侵时没有办法及时止损，无法防止大幅度洗钱。

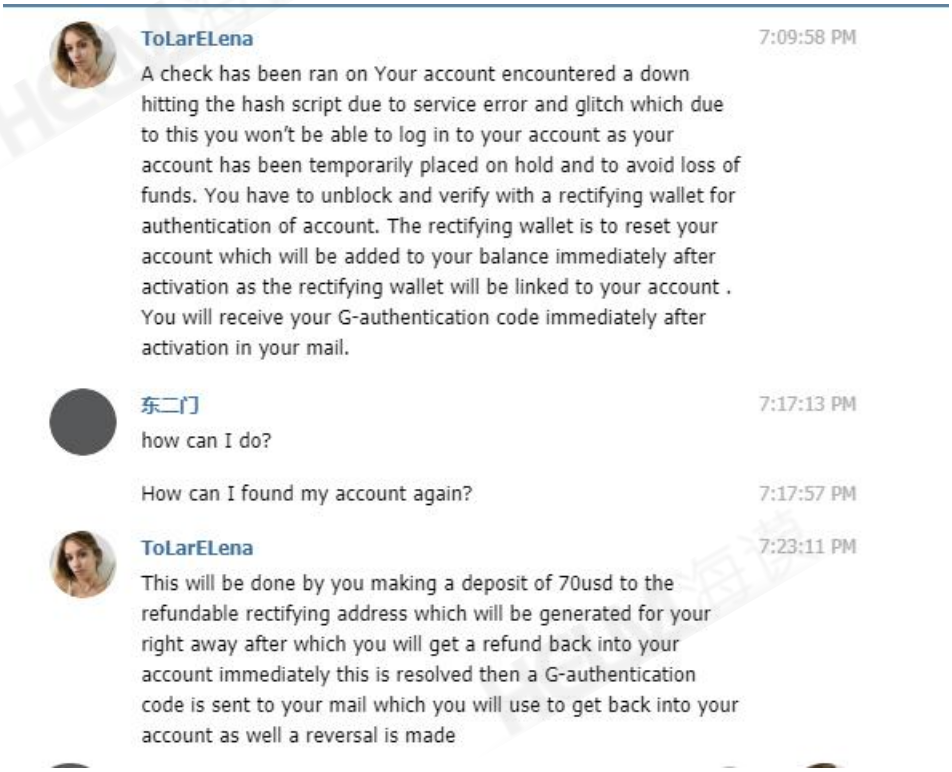
（二）案例

某非小号交易量排名前二十的交易所出现了如下风控问题：

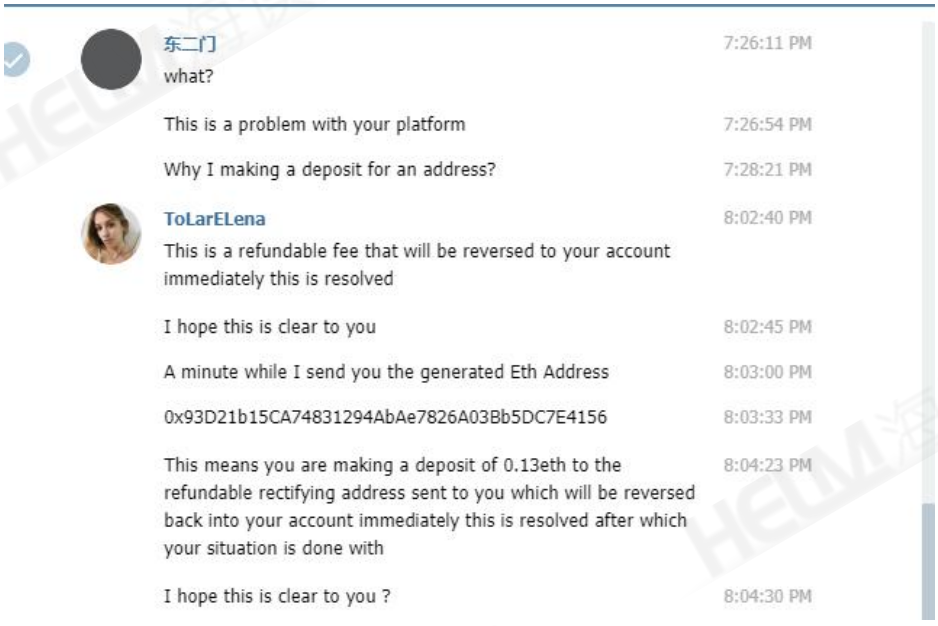
由于网站出现了滑动验证码的 bug 以及其他一些网站问题导致了无法登录与提现，在官方修复此 bug 的时候，15000 人左右的电报群出现了假冒的客服和技术人员、用户。



其中电报群里面有 5 个自称是客服的成员，他们将 telegram 的账户换成与官方客服相似的昵称与头像。然后在系统 bug 期间，利用用户焦急提取数字资产的心理去钓鱼 ETH。



在笔者取材时，此用户已经将昵称头像换回去。不过我们已获知此恶意用户的钱包地址。



此期间，官方未对这些钓鱼人员清理，只是出现“客服”与“客服”的互怼信息。因此造成的客户财产损失官方应该负责任。

某交易所无二次验证，只要是后台提币，确认后自动从热钱包转币：

ID	会员ID	会员手机	会员邮箱	币种名称	转入钱包地址	转出数量
		1398	@qq.com		7d9389bd0)c086774bb	1.0
		1887	@qq.com		5Qu1CEhW 3UCHv9iEe\	70
		1305	q.com		81970a7db :9c8e65efb	7.2
		1313	@qq.com		vLBbztRCfsl nMTDVo1Z	0.0
		1305	4@qq.com		81970a7db :9c8e65efb	1.6
		1845	5@qq.com		81970a7db :9c8e65efb	7.7
		1350	@qq.com		MggS1YMI 27B3Wgu3z	39
		1870	163.com		81970a7db :9c8e65efb	7.6
		1887	@qq.com		5Qu1CEhW 3UCHv9iEe\	56
		1850	@qq.com		YJCrYtfCX :t74xEhAq	4.0

风险点：

1、无对提币发起来源进行判断，审核前应该做如下判断，如：是否常用 IP 登录、是否常用的钱包地址、是否由系统正常发起等；

2、无二次验证，只要收到了提币申请就给予放行，应当做二次电话、邮件确认等。

0x06 从金融角度看交易所安全

（一）场景

1、黑客提前布局，不直接提币，以玩家的身份拉升某个币的价值；

2、交易所身份认证安全问题；

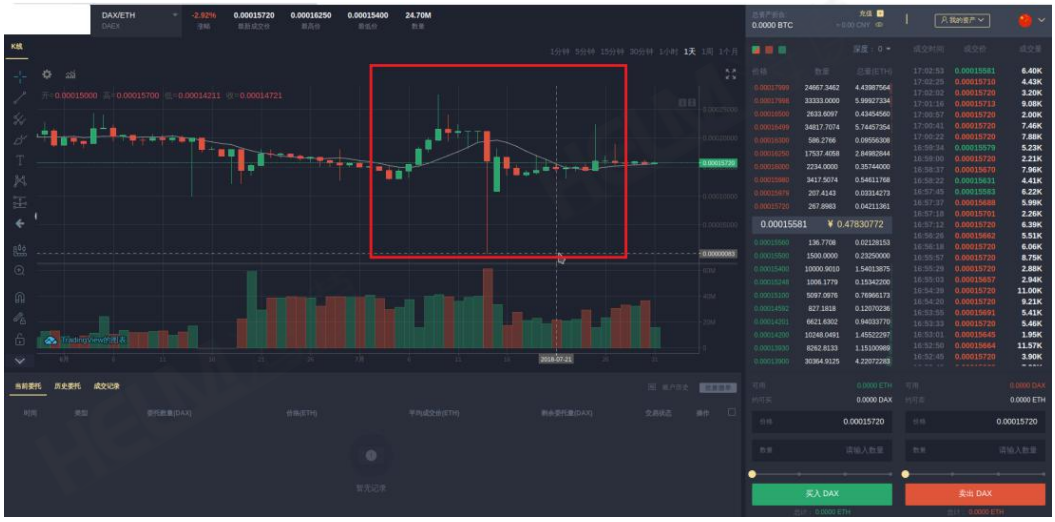
3、交易所自动交易机器人的策略问题；

（二）案例

（1）黑客拉升某个数字代币

1、X 安网 SYS 数字代币一天被拉几百万倍

2、某 top20 交易所代币被拉升上百倍



在许多交易所都能找到一些代币被夸张拉升的案例，其中可能是操盘手行为，也不乏是黑客。

（2）交易所认证问题

许多交易所存在身份认证不严的问题。其一，交易所存在形态法律无明文规定，无法可依，认证没有达到有效的效果，对用户个人信息保护也不全；其二，交易所都用户真实信息判别不严格。造成认证不用自己真实的信息也可完成注册，或是在认证流程存在漏洞。

（3）对资金来源流向模糊

许多交易所对资金的流入流出无监管，不知其来源，也不知其去处，这也为了洗钱滋生了土壤。

0x07 对交易所安全的总结建议

在此，我们列出了交易所客户碰到的历史问题以及需要防范的纬度。

1、从漏洞方面，交易所应该有专门的安全团队或者与安全团队厂商达成合作。交易所应该有自己的漏洞悬赏计划、SRC 或与第三方漏洞平台合作，刺激白帽子的积极性以达到安全生态良好的循环；

2、在金融方面，应该对自动交易机器人的安全性进行专门的测试，防止黑客从金融的手段对交易所发送”操盘攻击”；

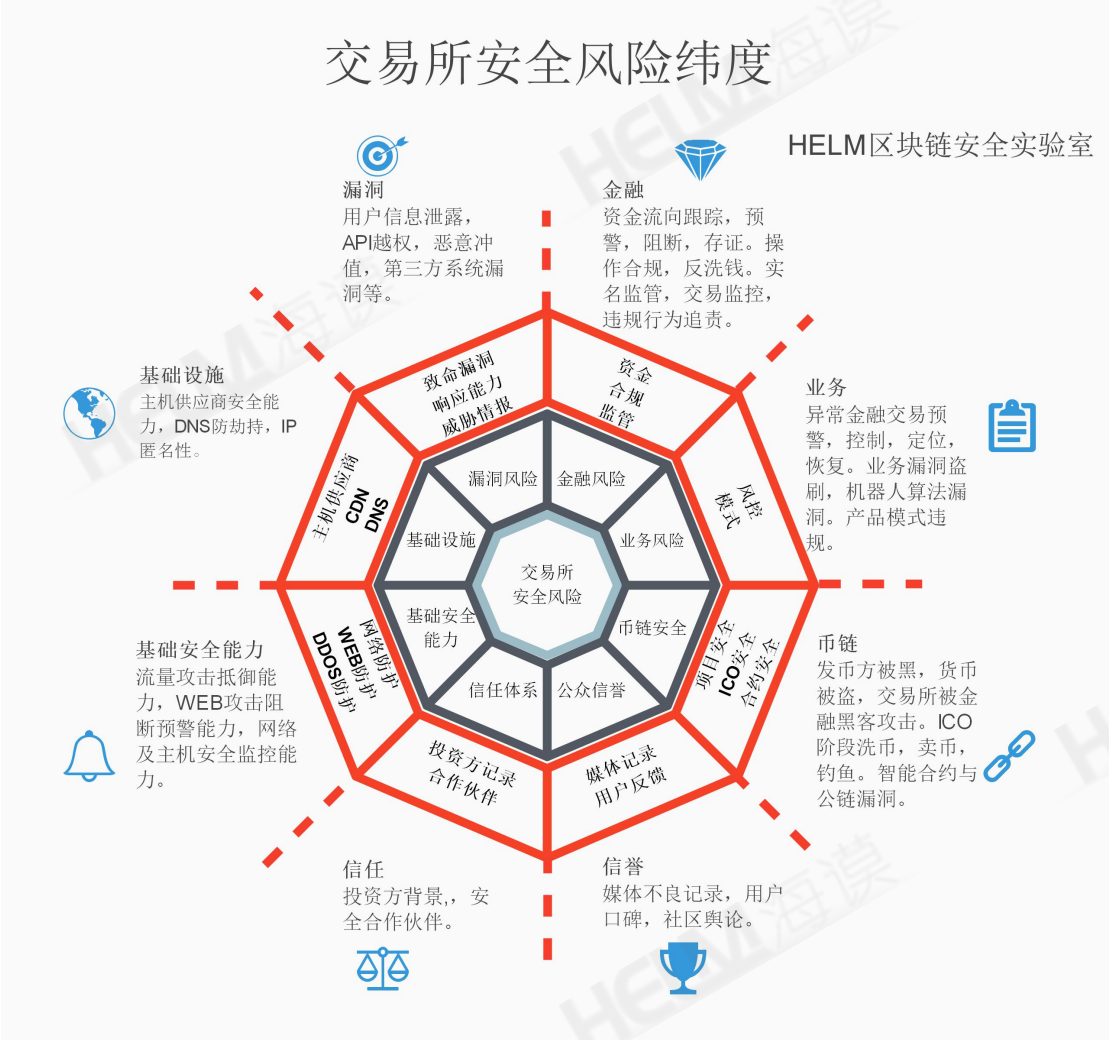
3、在风控方面，对一些资金异常的账户应当监控与报警，防止恶意洗钱行为或者黑客攻击行为。对交易的量、充值数字货币的量应当有一定的计算分析，设立阀值，如果超过阀值，则设立大型交易账户的阀值额度提升制度（如：银行卡、信用卡额度信用卡提升机制），通过在大型交易账户超过一定阀值的提币、提现应当通过电话等联系方式进行二次确认，否则提示暂停提现；

4、在币链方面，每一个交易所都会在自己的平台主推平台币或者主推一些上链的与平台合作的小型 token，应当对每种 token 进行智能合约审计，应该避免此币种影响整个交易所；

5、在基础安全方面，量级较小的交易所应该重视基础安全，那怕没有多余的资源投入设立安全团队。至少要对用户安全负责；

6、在公众信任方面，应该积极应对监督，处理负面的质疑，对用户财产保持保持负责的态度。

HELM 安全团队以我们对交易所安全的经验在此分享交易所安全应该注意的纬度（如下图）：



根据各维度的理解和评估，HELM 安全团队推出的数字货币交易所风险感知排行榜如下（详情请访问 http://helmbc.io/#index/situation）：

数字货币交易所风险感知排行榜

通过salins引擎，通过6个维度：基础设施健壮性、基础安全防护、风控能力、漏洞风险水平、金融风险、投资、合作方威胁性、公众信誉。及120个评分点以及安全专家对交易量排名前50的交易所进行评估而成。若有疑问意义请咨询：mkt@helmbc.io

更新时间：2018年9月03日

排名	名称	基础设置风险	基础防护风险	风控能力风险	漏洞风险	金融风险	合作方风险	媒体风险	安全风险指数
01	Ibank	高	低	高	高	高	低	低	高
02	ZB网	高	高	中	高	高	高	低	高
03	币安网	中	中	高	中	高	高	高	高
04	Exmo	高	高	高	中	高	高	中	高
05	澳洲U网	中	高	高	中	高	高	中	高
06	HitBTC	中	低	高	高	高	高	中	高
07	Allcoin	高	高	中	中	高	高	中	高
08	Bitstamp	高	中	高	中	高	高	高	高
09	Zaif	低	中	高	中	高	高	高	高
10	B网	高	低	高	中	高	高	中	高
11	AEX	高	中	高	中	高	中	中	高

扫描二维码关注我们

邮箱：

mkt@helmbc.io