”Hacking自动化就是好玩“星球未来规划：安全工具与自动化bugbounty

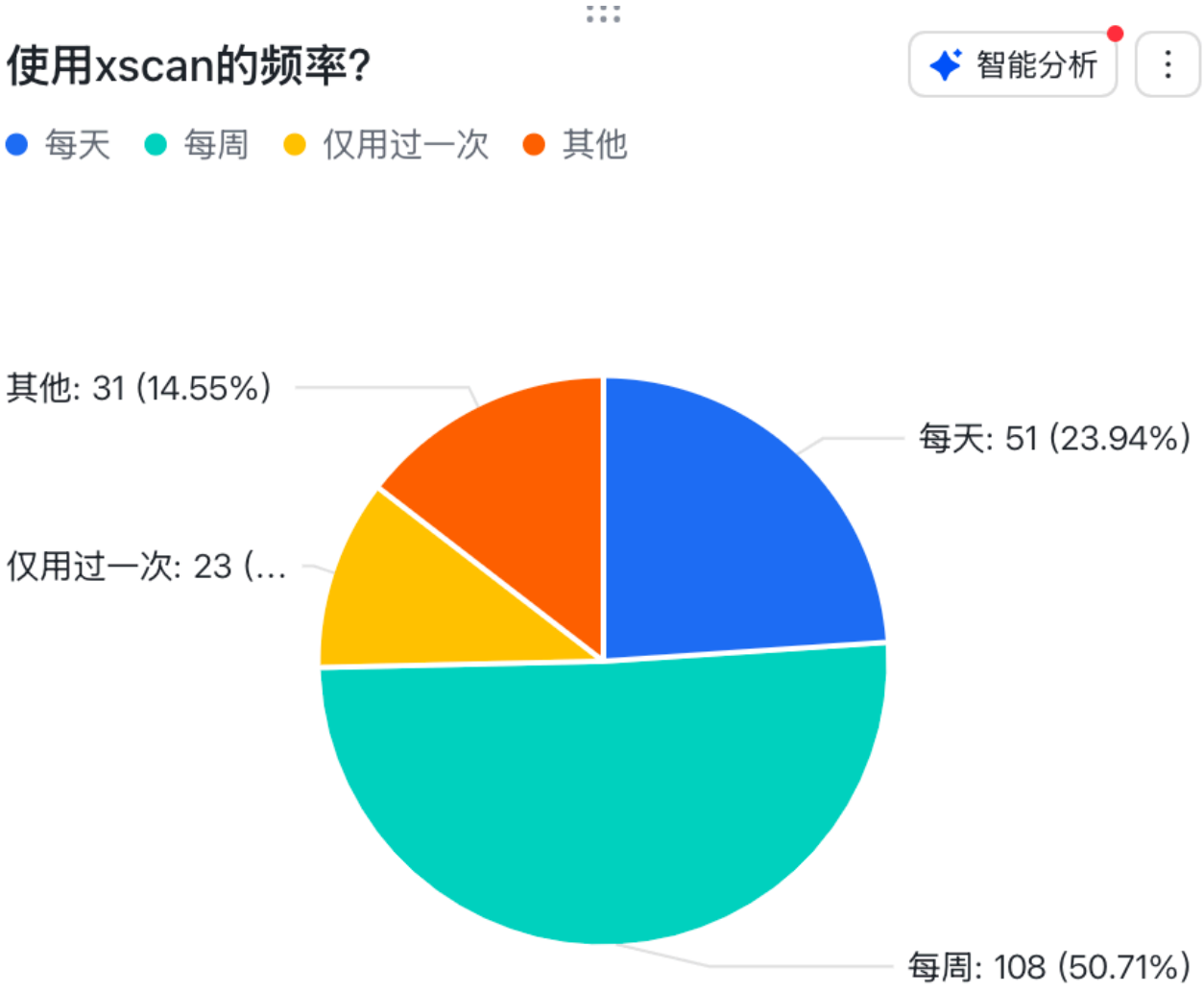
各位星球的大佬们，

感谢大家因为信任而加入星球。首先想和大家道个歉，最近半年，我的生活发生了两大变化：一是换了新工作，大量内容需要保密，新活不多了，二是家里迎来了新生命，需要有更多时间照料他。这两件事挤占了大量时间，所以最近知识星球的更新比较零碎，很多大家的问题也没来得及回复，我知道关于星球的未来的规划必须和大家好好聊聊。

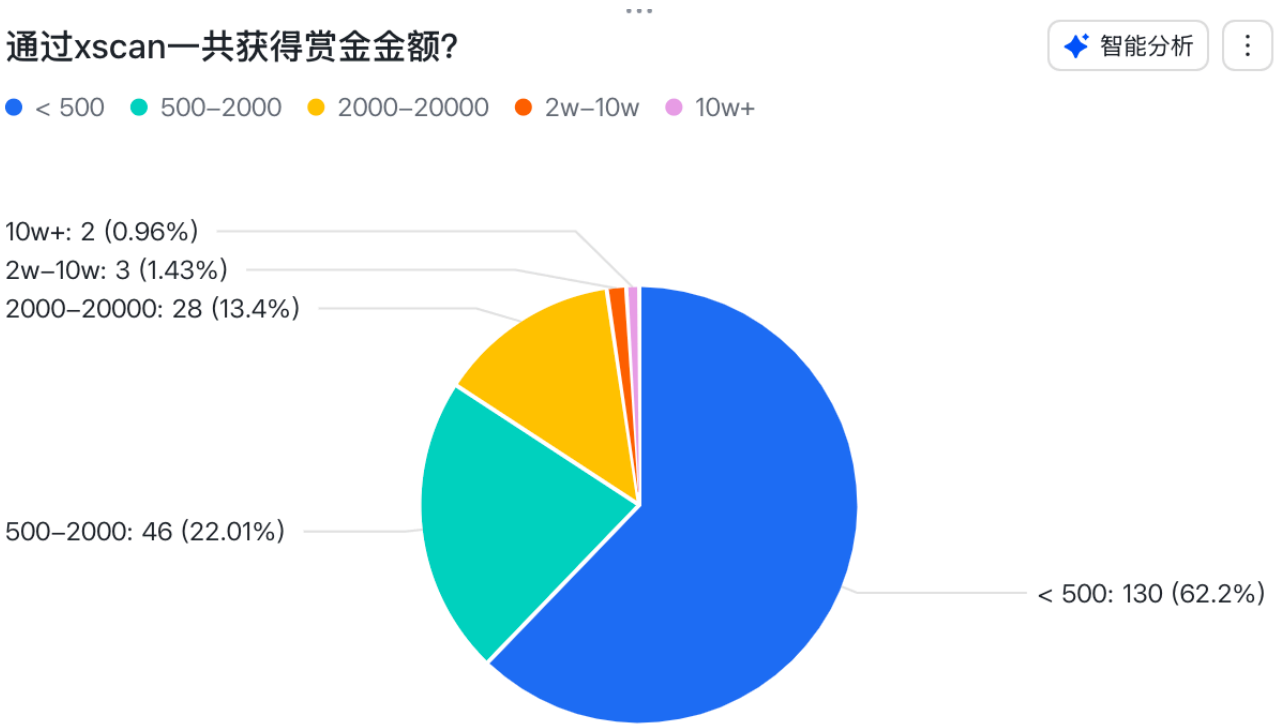
XSCAN的反馈

上周发起的xscan工具调研结果让我既惊喜又感到压力倍增，共209人填写问卷，大家对xscan的效果非常满意，对功能上有很多改进需求：

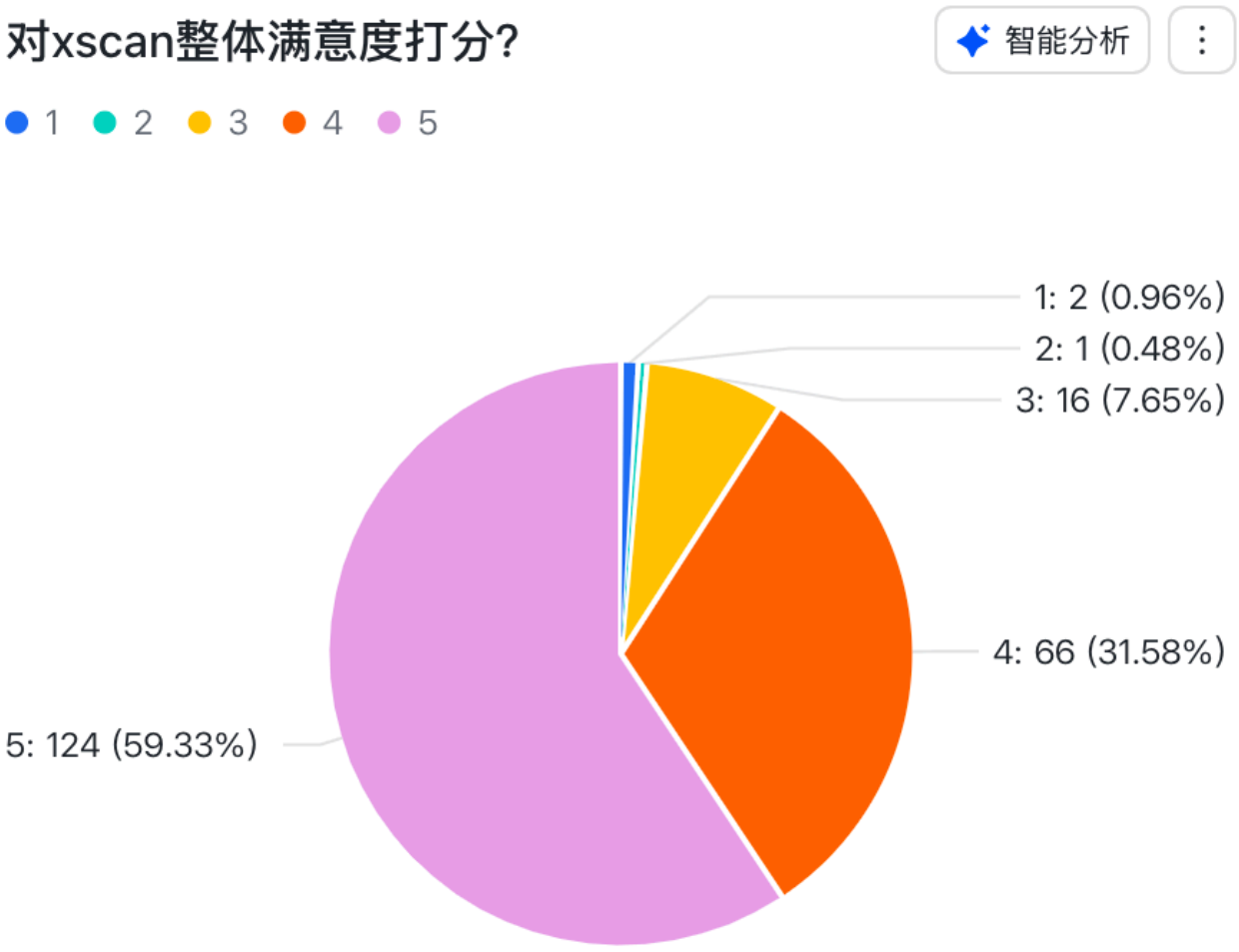
- **使用频率**：25%每日使用、50%每周使用，其他使用主要在演练，集成到工具和内部甲方使用中。



- **赏金统计**：80%用户已通过XScan找到漏洞，62%用户赚到第一笔赏金（≤500美元），22%斩获500-2000美元，更有5位大佬累计收入超2万美元



- **企业级应用**：多家甲方将XScan集成到内部安全平台，甚至有团队用它做SRC众测的自动化验证工具
- **满意度统计**：4分和5分加起来超过90%



也接收到了很多对xscan的功能建议：

- **漏洞手册需求**：对于报告部分想查看类似案例，希望有一本xscan漏洞结果使用手册，提供漏洞参考或验证poc，来更好利用结果。（已经有规划）
- **正则功能回归**："怀念老版本的自定义规则功能，上次用它扫到了AWS密钥泄露"（已经有规划）
- **DOMXSS&能力增强**：不少人肯定了对xss扫描的能力，不少人希望希望增强domxss的检测能力，而且觉得功能性有点单薄，也可以扫描一些其他的漏洞，不少漏洞可以配合xss来升级危害。（已经在升级JS引擎了）
- **SaaS化和License**：大部分人接受xscan的saas和绑定license，很多人希望绑定license来保护加入星球的人的权益。（已经有规划）
- **AI加持**：报告的漏洞，写报告等等可以用AI加持。（已经有规划）

星球专属的自动化bugbounty平台

最近发现知识星球上线了**「成员身份验证API」**（每月成本100+，这钱我掏了！）。有了它我准备建设星球专属的漏洞赏金平台。规划有以下功能：

🚀 **平台核心功能**

- **赏金平台情报**：自动抓取HackerOne/Bugcrowd等平台的资产变更（新上线的项目最易挖！）
- **License统一管理**：用星球ID作为XScan/W15Scan/XProxy的激活密钥，方便管理。
- **实战知识库**：收集各类bugbounty漏洞文章

- **赏金项目监控**：用户自由添加赏金项目，自动收集域名，监控更新，html，js变化等等

安全工具路线图

未来也会在星球更新优化各类工具，主要三大类：

XSCAN

- 本地版
  - 持续优化xss核心扫描技术和附属漏洞检测
  - 增加 license
- 高级版
  - WEBUI，本地化部署，支持资产添加→扫描→报告闭环

W15SCAN

w15scan定位是攻击面管理平台，我知道这个项目鸽了太久（鞠躬道歉！），之前小范围内测过，效果有点不理想，而且项目复杂性有点超出预期，对前端，后端，扫描端有很高要求，一直在改bug。争取今年面向星球成员开放首批测试。

演示视频：https://mp.weixin.qq.com/s?__biz=MzU2NzcwNTY3Mg==&mid=2247485195&idx=1&sn=25007f5e1bc5fe2375842a769e5393cc&chksm=fc986e2ccbefe73a1f3003bf50b5e5d6033b764e075267b19872b5d54ba70a3bf06629d9310f&token=520476794&lang=zh_CN#rd

XPROXY

用cursor做了一个burp like的前端，发现很好看，准备以此为基础做第二个版本的burp，纯爱好，会以免费版和星球版推出。

图：https://mp.weixin.qq.com/s/e4QCRUQWzMJaW3flF-SiJw

写在最后

以上是在周末写的对与未来星球的规划，未来星球也会涨价（毕竟开始支出API成本了），我也无法承诺每个项目具体的时间，但可以保证：

- 每月至少发布一个工具的重要更新
- 遇到有意思的内容也会发星球
- 平台和工具对星球成员免费开放，不会二次收费
- 你的每条建议都会进入需求池

所谓星辰大海，不过是一群人不肯熄灭对技术的好奇心。

感谢你们照亮这个星球，更感谢你们，让我始终相信技术人的浪漫。