arXiv:2301.04781v2 [cs.CR] 7 Mar 2023

漏洞猎人对漏洞赏金生态系统挑战与益处的视角

Omer Akgul[◇] TahaEghtesad[*] Amit Elazari[§] Omprakash Gnawali[+] *akgul@umd.edu teghtesad@psu.edu aelazari@berkeley.edu gnawali@cs.uh.edu*

Jens Grossklags[¶] MichelleL.Mazurek[◇] DanielVotipka[‡] Aron Laszka[*] *jens.grossklags@in.tum.de mmazurek@umd.edu dvotipka@cs.tufts.edu laszka@psu.edu*

[◇]马里兰大学 [*]宾夕法尼亚州立大学 [¶]慕尼黑工业大学[§]加利福尼亚大学伯克利分校 [+]休斯敦大学 [‡]塔夫茨大学

摘要

尽管研究人员已从平台和项目的角度对漏洞赏金生态系统进行了描述，但对主要参与者——漏洞猎人的观点，却鲜有研究。要改进漏洞赏金，了解漏洞猎人的激励因素、挑战和整体益处至关重要。我们通过三项研究填补这一研究空白：通过自由列举调查问卷确定关键因素（n=56），通过规模更大的因素评分调查问卷评估各因素的重要性（n=159），并开展半结构化访谈以深入了解详情（n=24）。在漏洞猎人列出的54项因素中，我们发现奖励和学习机会是最重要的益处。此外，我们发现范围是区分不同项目的首要因素。令人意外的是，我们发现获得声誉是对漏洞猎人而言最不重要的激励因素之一。在我们发现的各项挑战中，沟通问题最为突出，例如缺乏响应和争议。我们提出建议，以使漏洞赏金生态系统能够接纳更多漏洞猎人，并最终提升这一利用不足的市场中的参与度。

1 引言

传统上，组织依靠内部安全专家（例如红队）和外聘专家（例如渗透测试）来发现其产品中的漏洞。相比之下，漏洞赏金计划也称为漏洞奖励计划或“众包”安全，通过提供奖励（经济奖励或其他形式的奖励，例如学习机会），激励独立安全专家评估组织产品的安全性并报告漏洞。漏洞赏金计划最初由网景公司于 1995 [26]发起；如今，许多公司（例如谷歌、苹果公司）和政府机构（例如美国国防部）都在运行漏洞赏金计划。

然而，由于采用众包模式，漏洞赏金计划也存在效率低下的问题。漏洞赏金计划可能会收到无效或重复的报告，造成资源浪费，浪费精力 [6, 63]。此外，各计划相互竞争，以吸引高效的漏洞猎人，而较早推出的计划则难以维持猎人群体 [49, 56]。另一方面，漏洞猎人（下文简称漏洞猎人）对自己的发现及奖励感到不确定，而且常常对计划的回应感到失望 [1, 55]。为缓解其中一些问题，Bugcrowd [10] 和 HackerOne [32] 等漏洞赏金平台应运而生，通过市场将漏洞赏金计划与漏洞猎人连接起来。然而，许多问题依然存在。

或许是由于这些问题，尽管漏洞赏金计划益处颇多，但组织对其的采用率仍然相对较低[1]，远低于预测水平（如 [11, 56]所引述）。此外，尽管据 [25, 47, 60] 报告，漏洞猎人人才库看似庞大，但只有少数漏洞猎人能发现大量漏洞 [13, 35]。这些漏洞猎人往往更受生态系统关注，而其他人则遭到忽视 [26]。

识别使漏洞赏金计划具有（或不具有）吸引力和成功率的具体因素，应对最重大的挑战，并巩固漏洞赏金生态系统中普遍享有的益处，有助于吸引更多漏洞猎人、提高他们的投入程度、发现更多漏洞、减少漏洞挖掘和报告中的无效努力，并简化已报告漏洞的修复流程；所有这些都有助于改善许多公司的安全态势，并更广泛地提升软件安全。此外，通过了解漏洞猎人的动机，我们还可以认识漏洞赏金市场对社会的影响，并指导监管机构的工作，确保该市场满足社会更广泛的需求。

要改善漏洞赏金生态系统，我们必须首先了解漏洞赏金如何运作。事实上，已有不少研究尝试朝这个方向探索 [24, 28, 44, 45, 47,49, 56, 60, 62]。然而，一个常见的局限是，研究人员只从漏洞赏金计划的视角考察所收集的数据（例如漏洞报告和付款）。因此，他们对漏洞

[1]两个最大型的漏洞赏金平台上托管着 ~3，300 个（全球）漏洞赏金计划 [13, 35]；相比之下，仅美国就有超过 10,000 家“软件发行商”和 60,000 家“定制计算机编程服务”机构 [15]。《福布斯》500强中，大多数（80%）都没有漏洞披露计划 [7]。

猎人的工作只关注最终成果，却忽略了猎人的动机以及他们面临的挑战。

近期研究开始广泛考察漏洞发现中的决策过程 [30, 57, 58]；但这些研究都没有专门关注漏洞赏金，只在参与者提及时顺带讨论。此外，这些以黑客为重点的研究都没有通过实证评估影响漏洞猎人选择评估哪些软件的因素。

漏洞赏金平台自身也发布了几份关于漏洞猎人动机的报告 [12–14、34–36]。然而，这些简短的报告并未关注漏洞猎人面临的挑战，似乎是出于营销目的，且未经独立验证。

其他研究工作通过访谈漏洞披露过程中的各类利益相关者（包括漏洞赏金计划的相关人员），探讨零工工作模式的缺点 [26]以及整个漏洞发现生态系统所面临的挑战 [3]。我们以这些宽泛的定性研究为基础，采用更大的混合方法样本，明确且系统地识别并量化影响漏洞猎人参与漏洞赏金计划的因素。不同于先前研究，我们要求漏洞猎人量化各个因素的重要程度，使利益相关者能够了解应优先关注哪些因素。例如，与其他研究人员一样 [26, 60], ，我们发现声誉是一个激励因素；然而，我们能够证明，事实上它是重要性最低的激励因素之一（§5.1）。

我们的具体研究问题如下：

RQ1： 漏洞猎人在参与漏洞赏金活动时会考虑哪些因素，又会面临哪些挑战？**RQ2：** 这些因素对漏洞猎人有多重要？为什么？

我们从四个方面探讨这两个问题：(1) 选择具体计划时考虑的因素，(2) 面临的挑战，(3) 漏洞赏金总体上带来的益处，以及 (4) 漏洞赏金平台的实用功能。

我们开展了三项研究（§3）来回答研究问题：首先进行因素识别调查（n=56），列出其中的主要因素（RQ1）；然后进行更大规模的调查（n=159），了解各因素的重要性（RQ2）；最后开展半结构化访谈研究，探究这些因素为何重要（n=24）。

正如预期，我们发现最显著的益处是金钱回报，无论是在选择计划时，还是作为普遍的动机，都是如此（§5.1）。选择计划时，漏洞猎人会考虑一些启发式方法（例如范围），以提高发现漏洞的概率（§5.3）。除了金钱回报，漏洞猎人也非常看重学习机会（§5.2）。与先前研究 [25, 56, 60],的直觉相反，我们发现他们对声誉的重视程度远低于其他因素。

我们发现，漏洞猎人的主要挑战是与负责评定报告并决定奖金支付的漏洞赏金计划管理员沟通不畅。具体问题包括响应不佳、漏洞评级争议，以及对调解和平台分流的不满（§5.4）。

我们还发现，漏洞赏金的零工工作模式给漏洞猎人带来了独特的挑战。虽然这种模式提供了灵活性，但也可能造成压力和不确定性（§5.5）。

我们讨论了漏洞猎人认为最有用的漏洞赏金平台功能：公开仪表板，以及便于报告漏洞和收取付款的流程（§5.6）。

接下来，我们的研究结果表明，在多种情境下，法律安全港对漏洞猎人都至关重要（§5.7）。

论文最后讨论了我们的研究结果如何拓展我们对漏洞赏金的益处与挑战的理解，并提出建议，旨在打造一个更有利于漏洞猎人、公司以及整体软件安全的漏洞赏金生态系统（§6）。

2 相关工作

研究人员尝试通过对市场行为进行实证分析，以及直接向漏洞猎人开展调查和访谈，来了解他们的动机。

市场行为 为了解漏洞猎人如何选择漏洞赏金计划，研究人员对漏洞赏金计划产生的实证数据（例如漏洞报告和付款）进行了研究 [2, 28, 40, 48, 49, 53, 56, 60, 64]。这些研究考察了漏洞猎人活动与各种计划特征之间的关系，并指出可能反映其动机的相关性。例如，研究人员发现，漏洞猎人对计划的选择与预期金钱奖励和计划存续时间有关 [45, 49]。这些结果与对 Google Chrome 和 Mozilla Firefox 漏洞赏金计划公开报告的类似研究 [28] 以及 HackerOne 公开数据的研究 [49]相符。尽管我们的研究也发现了一些重叠因素，但视角有很大不同：我们直接调查漏洞猎人，让他们直接说明自己的优先考虑事项，而不是通过推断得出结论。

漏洞猎人自我报告的动机 其他出版物利用调查来描述漏洞猎人的人口统计特征和动机。这方面最突出的例子是 HackerOne [35,36] 和 Bugcrowd [12–14],这两个最大的漏洞赏金平台每年发布的营销材料。两家公司都会对参与其平台的漏洞猎人进行调查，收集人口统计信息，并了解漏洞赏金参与者的总体动机（例如，金钱、教育）。然而，与我们的研究相比，这些调查对漏洞猎人动机的探究不够深入，也没有关注漏洞猎人面临的挑战。

或许与我们的研究最为相关的是一家非营利研究组织对漏洞赏金生态系统利益相关者开展的访谈研究，旨在了解他们的经验 [26]。作者提出了漏洞猎人面临的若干益处和挑战，但并未对其进行系统定义，且主要着眼于批评零工工作模式。我们的研究则采用混合方法，系统地识别、定义并量化与漏洞赏金相关的因素，涵盖四个方面：在漏洞赏金计划之间进行选择、漏洞赏金带来的挑战、漏洞赏金带来的益处，以及漏洞赏金平台的实用功能

。我们对相关因素的量化，有助于漏洞赏金生态系统的利益相关者——包括漏洞赏金平台、漏洞猎人、希望提升安全性的公司，以及可能关注安全问题的监管机构或标准组织——做出更明智的决策。

一项更全面的研究考察了整个漏洞披露流程，发现沟通往往是一个问题 [3]。Fulton 等人探讨了边缘化群体（例如女性、有色人种）在漏洞发现领域面临的问题 [30]。虽然这两项研究都简要涉及了漏洞猎人对漏洞赏金的看法，但这与其研究主题只是间接相关。

3 方法

我们设计并开展了三项研究，以探讨研究问题：首先进行自由列举研究，确定其中的影响因素（RQ1）；接着进行因素评分研究（RQ2）；最后进行访谈研究（RQ2）。前两项研究帮助我们了解漏洞猎人的动机与挑战，而访谈研究则为这些结果提供背景。

我们所在机构的伦理审查委员会批准了全部三项研究。参与者在数据收集前签署了知情同意书，其中详细说明了研究计划和参与者的权利。只有伦理审查中列明的作者才能访问可识别身份的数据。

3.1 自由列举研究（RQ1）

为了找出影响参与漏洞赏金的因素，我们对漏洞猎人进行了一项在线调查n=56。

调查问卷 调查问卷首先提出开放式问题，请参与者列出在五种（后来减少为四种，见§3.1末尾）情境中影响他们的因素（我们称之为因素组）：（1）在不同漏洞赏金计划之间进行选择时的因素；（2）退出漏洞赏金计划的原因；（3）参与漏洞赏金的益处；（4）普遍面临的挑战；（5）漏洞赏金平台的实用功能。

对于每个问题，我们都强调，初始研究的参与者应列出所有可能考虑的因素，即使他们认为某个因素并非每次决策都会涉及。此外，我们还请初始研究的参与者，如果觉得可能还有更多因素可以想起，就花些时间回忆。与列举练习中常见的做法一样，这一提示有助于我们引出不那么显而易见的因素 [8]。我们采用一种开放式列举方法，称为自由列举；在人类学研究中，当研究领域尚未得到充分了解时，这种方法很常见 [8]。这种方法有助于全面 eliciting 所有可能因素。

接下来，我们请参与者自行报告其漏洞赏金经验（见 表 1）和技能。最后，我们通过标准的人口统计问题（见 表 1）了解样本群体的情况。我们还询问参与者是否愿意接受联系，以参与后续研究。完整的调查问卷见 附录 B。

试测 我们通过私人关系招募了三位经常参与漏洞赏金项目的安全专家。我们向他们发送了调查问卷，并在线上焦点小组会议中讨论了他们的回答。待问题清晰且具备良好的表面效度后，我们便开始收集数据 [31]。

招募 我们通过社交媒体（作者的账号）、邮件列表以及漏洞猎人使用的 Slack 频道发布招募信息。我们总共收到了 61 份完整的调查问卷回答。由于回答质量较差（内容难以理解、完成时间短得不合理或存在重复漏洞），我们剔除了 5 份回答，最终留下 56 份用于分析。回答收集时间为2019年5月至12月。

在最后收到的 15 份回答大体上印证了前 41 份回答中识别出的因素，表明概念饱和 [16]后，我们结束了数据收集。

数据分析 我们使用探索性开放编码 [54]分析了开放式调查问卷回答。由于计划在因素评分研究中直接使用识别出的因素，因此我们计算了评定者间信度 [50]。

有时，列出的因素存在多义性。对于这些回答来自同意接受访谈的参与者的情况，我们会请求对方澄清（n=7）。

我们使用前 41 份回答（占全部回答的 73.2%；每个问题列出的所有因素中占 64.0–78.2%）开发了编码手册并建立信度[2]。三位研究人员使用 10 份回答（当时回答总数的 25%；列出因素的 15.3–28.0%）编制了初版编码手册。随后，其中两位研究人员尝试通过每次独立编码一批 10 份回答来建立良好的信度，并在每批编码后解决分歧、更新编码手册。新回答已经用尽，但我们仍未能达到可接受信度的门槛（Cohen's $\kappa > 0.8$）。然而，28 天后，研究人员修订了编码手册，并对 41 份回答中的 16 份进行了独立重新编码（~40占当时回答总数的 %；占列出因素总数的 27.0–38.3%），达到了"几乎完全一致"的 [43] 信度（Cohen's $\kappa > 0.8$ 适用于所有因素组；为 0.81–0.91）。最后，在信度确立后，一位研究人员对其余回答进行了重新编码。最后收到的 15 份回答是在信度确立后提交的，并由一位研究人员完成编码。最终的编码手册涵盖五个因素组中的 78 个因素。

精炼因素我们的列举练习发现了许多因素，因此在因素评分研究中，要求参与者逐一直接回应并不切实际。此外，我们注意到两个因素组之间存在显著重叠：退出漏洞赏金计划的原因，以及更广泛地说，在漏洞赏金情境中面临的挑战。为减少问题数量，我们将两者合并，最终得到四个因素组中的54个因素（见表2）。

[2]根据一条回答中列出的因素数量对回答进行单元化处理（即，为单个因素而非整条回答分配代码）。

3.2 因素评分研究（RQ2）

自由列举研究找出了漏洞猎人所考虑因素的完整集合，但未确定这些因素的相对重要性。因此，我们设计了第二项研究，请参与者评定每个因素对他们个人而言有多重要。

调查问卷 第二份调查问卷从让参与者对 54 个因素逐一进行七点李克特量表评分开始。[3] 与前一份调查问卷一样，我们要求参与者结合各自所属的因素组进行评估：选择计划时考虑的因素、漏洞赏金带来的挑战和益处，以及实用的漏洞赏金平台功能。为进一步了解漏洞猎人的背景，我们提出了一个开放式问题，询问他们是如何开始参与漏洞赏金计划的。和之前一样，我们最后询问了参与者的漏洞挖掘经验和人口统计信息。我们再次询问参与者是否愿意接受后续研究的联系。完整的调查问卷见附录 C。

试测 我们邀请五位漏洞猎人试测调查问卷，重点了解参与者对所提供的修订后因素列表的理解程度。根据他们的反馈，我们对 54 个因素的名称和说明做了少量修改。最终待评估的因素列表见表2。

招募 除了自由列举研究中采用的方法外，我们还联系了 586 名漏洞猎人。他们在 2020 年上半年曾在 HackerOne 或 BugCrowd 上发布公开漏洞报告，列出了自己的 Twitter 账号，并允许任何人向其发送私信。绝大多数回复很可能是通过这种方式获得的。此外，我们还在 reddit.com/r/bugbounty 上发布了招募信息。在收到的 161 份已完成调查问卷中，我们剔除了两份在多个开放式问题中回答不合常理的问卷，最终留下 159 份用于分析。我们估计自由列举研究和因素评分研究之间有 4–6 名参与者重合。

数据分析 分析哪些因素最重要，一个简单（且常见）的方法是将参与者的李克特量表选项转换为数值，并计算简单平均值。尽管这种方法看起来直观，但统计学家已对其提出批评并不建议使用 [21, 46, 61], ，因为它做出了一个值得质疑的假设：参与者选择的有序选项之间距离相等（例如，“极其重要”与“非常重要”之间的距离，与“非常重要”与“中等重要”之间的距离相同）。因此，我们采用基于比较的技术，只考量一个因素的评分是否高于另一个因素。具体而言，我们使用对数线性 Bradley-Terry（LLBT）模型，综合得出 价值 估计值（π），以表示各因素（f）对参与者的相对重要性，并采用偏好量表 [21, 23]。其概率一个因素优于另一个因素的概率由下式给出：

$$p(f_j > f_k|\pi_j,\pi_j) = \frac{\pi_j}{\pi_j + \pi_k}$$

其中 j,k 表示所考虑因素的索引 [22].[4]

3.3 访谈

我们邀请所有同意参与且回答有效的自由列举研究参与者参加远程半结构式访谈。我们询问这些因素对他们是否重要，以及重要的原因。访谈（n=8）首先询问参与者是如何开始接触漏洞赏金及安全领域的。接着，我们解释每个因素组以提供背景，然后请参与者选出最重要的因素并说明选择理由。最后，我们询问他们是否会继续参与漏洞赏金活动，以及会如何继续。

同样，我们邀请了同意接受访谈的因素评分研究参与者，并对访谈方案做了少量修订。具体而言，我们使用了修订后的因素列表（54 项），并直接询问参与者（n=16）他们在调查问卷回答中评分较高的因素。在两轮访谈中，我们都在调查招募仍在进行时启动访谈，以提高参与者留存率。

访谈不可能涵盖全部 54 项因素。因此，我们重点讨论参与者最在意的因素；如果时间允许，再询问其他因素。访谈人员谨慎避免提出重复问题，因为围绕某一因素的讨论常常会延伸到其他因素。

要涵盖 54 项因素，而且许多漏洞猎人表达了各自独特的考量，因此要让参与者对每项因素的看法都达到饱和并不现实；我们转而致力于收集足够的数据，以便为调查结果提供背景。

我们总共访谈了 24 人，每次访谈平均为 43 分钟。虽然调查问卷参与者没有获得报酬，[5] 受访者则获赠了一张价值 20 美元的礼品卡以示感谢。

分析 我们再次采用探索性开放编码来分析访谈 [54]。两名研究人员对三次访谈进行编码，编制了初版编码手册。随后，他们每次独立编码三次访谈，并会面讨论访谈内容、解决分歧并更新编码手册。所有访谈均完成编码和讨论后，最终版编码手册随之定稿。研究人员使用最终版编码手册重新编码访谈，最终在这 24 次访谈中共得到 1004 个编码片段。我们没有寻求评定者间信度指标，因为我们认为访谈主要是为自由列举研究和因素评分研究的结果补充背景信息 [50]。

[3]“极具挑战性／重要”至“完全没有挑战性／不重要”，或“极其有用”至“极其无用”（视情况而定）。

[4]我们使用的 LLBT 版本要求将数据转换为明确的成对比较。对于我们的高维数据而言，不进行这种转换的方法在计算上不可行 [21, 38]。开发这些统计方法的研究人员确认，我们采用的方法是恰当的 [29]。[5]我们采用了多种招募方法，参与者来自不同国家，而且调查问卷相对较短，因此在后勤安排上难以提供补偿。

3.4 局限性

我们的方法主要基于自我报告数据，而这类数据存在众所周知的局限性。自我报告数据往往噪声较大，因此仅凭一次测量无法确保得出确切答案。因此，我们通过三项不同的研究来探究总体研究目标，并记录了其中出现的少数不一致之处。

自由列举可能会受到记忆缺失的影响 [4]。我们要求参与者尝试回忆所有可能的因素，只有在再也想不出任何因素时才转到下一个问题，这是自由列举回忆的最佳实践 [8]。

漏洞猎人可能将自己描述得比实际情况更成功。同样，我们提供的礼品卡激励可能对那些在漏洞赏金计划中收入较低的访谈参与者最具吸引力，这或许是因为他们的技能或经验较少。对此，我们采取了一定的应对措施：自由列举研究的大多数参与者来自非公开的猎人消息渠道，而因素评分研究的参与者则是公开披露漏洞的漏洞猎人，这意味着他们具备一定程度的专业领域知识。此外，我们收集的指标表明，各种技能和经验水平的参与者分布相对均衡（见 表 1）。

另一方面，我们很可能没有涵盖那些希望参与漏洞赏金、却完全无法参与的人。这种幸存者偏差问题可能无法避免，因为没有明确的方法招募那些对漏洞赏金感兴趣、但并未实际参与其中的人。不过，我们预计，部分漏洞赏金参与程度较低的参与者也会有类似经历。

此外，与所有自我报告研究一样，我们的三项研究 [9], 都存在一些抽样和选择偏差。我们的样本很可能能够较好地代表当前的黑客群体（§4），且参与者所在地、教育、经验和技能各不相同，这意味着我们的研究结果很可能适用于一般漏洞猎人。然而，猎人群体本身在人口统计方面存在偏斜（例如，年轻、白人或东南亚人，以及男性 [13, 14, 35]），这可能会引入固有偏差（例如，受到关注的公司和漏洞）。关于边缘化群体的讨论，请读者参阅 Fulton 等人的研究 [30]。

最后，为了最大限度地确保表面效度，我们对研究的每个阶段都进行了严格的试点测试，并根据反馈修订了流程。

4 参与者

表 1 总结了参与者自我报告的人口统计信息和经验。自由列举研究有 56 名参与者，因素评分研究有 159 名参与者，另有 24 名访谈受访者。参与者主要来自北美、南亚和欧洲；年龄较轻，且绝大多数为男性。

漏洞猎人的确切人口统计信息尚不清楚；不过，除教育程度较低外，我们的参与者与知名漏洞赏金平台所报告的群体相似。据报告，这些平台的样本中，77–85% 的人年龄为 < 35 岁，90–96% 为男性，19–34% 拥有研究生学位，37–67% 每天投入 < 10 数小时进行漏洞赏金活动 [13, 14, 35]。HackerOne 的样本是唯一报告漏洞猎人经验的营销调查，其经验水平与我们的相似（即，47% 的人有 <三年漏洞猎人经验） [35]。

		FL	FR	I
性别	Male	51	147	24
	女性	2	2	0
	自我描述	1	2	0
Age	18-29	34	124	16
	30-39	16	27	7
	40-49	4	3	0
	50-59	2	0	0
居住地	北美	21	22	3
	南亚	14	64	7
	欧洲	14	23	9
	东南亚	2	14	0
	中东	0	18	0
	其他	5	11	4
教育	≤高中毕业	18	53	11
	贸易／技术／职业教育	1	3	0
	上过大学，未取得学位	13	17	2
	副学士学位	3	5	1
	学士学位	15	56	3
	专业学位／硕士学位／博士学位	5	19	4
每周工作小时数 g	<5	13	34	3
漏洞赏金	5-10	18	53	8
	10-20	12	40	8
	20-30	8	18	2
	30-40	1	13	2
	>40	4	3	0
漏洞总数	<10	6	39	2
发现	10-99	18	65	10
	>= 100	12	52	8
从事漏洞研究的年数	<1	2	3	1
悬赏金	1-2	18	87	12
	3-5	15	46	4
	6-9	6	14	4
	>= 10	0	5	0
技能	1 - 基础	3	9	1
	2 - 新手	8	23	3
	3 - 中级	23	68	9
	4 - 高级	10	48	6
	5 - 专家	12	13	4
年收入来自	<$999	10	33	3
漏洞赏金的年收入	$1,000 - $29,999	19	57	9
	$29,999 - $74,999	5	13	2
	>= 75,000美元	10	12	3

表 1：各项研究的参与者人口统计信息和经验。不同研究中的问题相似，但并不完全相同。FL：自由列举。FR：因素评分。I：访谈研究。

5 个因素

我们在四个因素组中识别出 54 个影响人们参与漏洞赏金生态系统的因素。完整列表见表2。先前研究报告了其中一些因素；如表2所示，尚无研究系统性地识别出所有因素，而且大多数研究侧重于益处，

因此对挑战以及哪些平台功能最有用的探讨仍有不足。此外，我们首次对各因素的重要性进行了深入排名。

在访谈中，我们归纳出七个共同主题，用来串联相互关联的因素；我们以这些主题为框架组织讨论。为求简洁，我们主要讨论最受关注的因素；更多细节见 附录 A。我们报告了访谈中提出某项观点的参与者人数（I）、在自由列举研究中列出某项因素的参与者人数（FL），以及因素评分研究得出的因素相对重要性（价值估算）(π)。[6]

需要注意的是，由于每位受访者只有时间评论部分因素，因此访谈中的参与者人数仅供参考，不能据此判断这些因素的普遍程度。

5.1 获得奖励

尽管奖励看起来似乎是显而易见的动机 [13,14, 26, 34–36, 62], 漏洞猎人表达了更细致、 nuanced 的看法。

奖励方面的考量 不出所料，金钱奖-励 是自由列举研究参与者常列出的因素，也是因素评分研究参与者高度重视的因素，既是选择漏洞赏金计划时的考量（FL=36, π=0.120），也是漏洞赏金计划的首要益处（FL=42, π=0.191）。漏洞猎人同样优先考虑漏洞严重程度与奖励之间的对应关系（即漏洞赏金表, FL=16,π=0.117）。非货币奖励 （例如周边商品；FL=4, π=0.013）也是激励因素 [26], , 但重要性排名最低。

在访谈中，漏洞猎人表达了对如何确定和管理悬赏金的细致看法。许多漏洞猎人（I=9）认为，悬赏金应与所发现漏洞的严重程度相关；这与行业惯例十分吻合 [5]。其中三人特别提到，应根据漏洞被利用后可能给公司造成的损失来评估其价值。三位专攻高严重性漏洞的漏洞猎人提到，这类漏洞应获得高额奖励，而对不那么关键的漏洞，奖励则不那么重要。

相比之下，三位漏洞猎人在选择漏洞赏金计划时，主要考虑低严重性和中严重性漏洞的支付金额，这主要是因为他们认为发现更关键漏洞的可能性不大。一位漏洞猎人表示，只有在计划长期参与某项计划时，才会考虑高严重程度漏洞的支付等级。其他漏洞猎人（I=7）则认为，付款应与漏洞猎人的付出成正比，而不应仅取决于结果。

一些人（I=7）认为，漏洞赏金表并不能很好地预测他们参与计划后预期获得的付款，因为这主要取决于诸如他们预计能找到多少漏洞、可能获得的额外奖金（例如，对写得好的报告给予的奖金），以及多次获得付款的可能性（例如，重新利用先前已打上补丁的漏洞）。一位受访者表示，更喜欢这样一种计划："奖金支付不会特别高，但.....你很可能因此获得更多，因为你实际上会提交更多漏洞，因为你对它更熟悉。"

有趣的是，八位受访者表示，相较于金钱奖励，还有其他更重要的动机。一位通常以尽可能多地发现漏洞为目标的漏洞猎人指出："我有时会尝试寻找这类不提供金钱奖励的项目.....从这类项目中发现漏洞很容易。"另一位则表示，无论是否获得付款，他们都会报告漏洞，因为"我只是想让公司更安全。"

正如先前研究所指出的，作为金钱奖励的替代 [26],, 少数受访者满足于仅获得声誉提升（I=3）；更多人（I=5）则认为商品已是足够的补偿。然而，因素评分研究的参与者普遍认为，声誉和非货币奖励是最不重要的动机。

5.2 学习机会

三项研究都强调了漏洞猎人对学习机会的重视。漏洞猎人表示，他们会通过多种方式学习，例如从公开披露的漏洞和社区互动中学习。

学习的重要性 学习 新的黑客攻击技术，是自由列举研究中最常被列为益处的因素之一；因素评分研究的参与者（FL=32,π=0.170）则认为它是第二重要的益处。尽管这一点并非那么显而易见，但漏洞猎人对学习的重视，也体现在其他几个经常被讨论的相关因素上。

谈到漏洞赏金项目提供的学习机会，大多数受访者表示，学习是这一过程不可或缺的一部分：漏洞猎人要么在过程中自然而然地学习，要么就必须学习新技术，才能保持竞争力（I=12）。具体而言，三位受访者解释说，在寻找某些漏洞时，需要学习新技术和方法。一位漏洞猎人回忆说，为了找到一个漏洞，自己不得不学习 GraphQL："我当时想，先来了解一下吧。于是我开始学习 GraphQL，包括它的结构、编写方式、如何获取响应，以及会得到什么样的响应。"

三位漏洞猎人指出，漏洞赏金也提供了练习技能的机会，而练习是学习不可或缺的一部分 [59]。

相较之下，三位漏洞猎人指出，持续学习带来的压力可能令人难以承受。"无论你的经验有多丰富，每天都得学习新东西。我认为，这是让漏洞挖掘变得有些困难、有些棘手的原因之一。如果你停止学习，就会失去[手感]。为了找到漏洞，你必须在社区中及时了解最新动态，学习新东西。"

从公开报告中学习我们的受访者证实了先前关于公开披露对学习过程重要性的推测 [62] 。学习作为一项

[6]价值估算只有在各因素组内部才有意义，才能进行比较；这些因素组是分别分析的。表2列出了完整清单。

	因素	定义	相关工作	FL	价值(π)
Choosing a program	范围	计划中包含的域名或资产。	[14]	28	0.156
	奖励	预期的货币或非货币奖励。	[14, 28, 35, 45, 62]	36	0.120
	漏洞赏金表	不同漏洞类型对应的奖励规则和范围。	[28]	16	0.117
	技术熟悉度	熟悉资产所采用的技术（例如熟悉 Web 或 iOS）。	[14]	22	0.113
	法律安全港	包括承诺不对遵守规则的黑客提起法律诉讼。 [26]		4	0.098
	项目声誉	在社区中以合作愉快而享有良好声誉。	[35]	15	0.086
	学习机会	对资产技术缺乏熟悉程度，以及学习的兴趣。	[35]	1	0.064
	私有或公开	私人计划（仅限受邀者参与）与公开计划（任何人都可以参与）。	[35]	4	0.048
	对公司的熟悉程度	计划背后的公司广为人知；你或你的同行使用其产品。 [35, 62]		15	0.047
	饱和	收到的报告数量或参与该计划的黑客人数。		8	0.047
	职业机会	未来在负责该计划的公司获得职业发展的机会。	[35]	3	0.027
	公开披露	漏洞修复后通常允许公开披露漏洞。		6	0.027
	Age	该计划已运行多长时间。	[49, 56, 60]	6	0.023
	业务领域	计划背后公司的业务领域（例如：医疗保健、零售）。 [56, 62]		2	0.021
	国家	计划背后的公司所在的位置。		1	0.006
Challenges of bug hunting	响应不佳	项目管理人员未回复或回复缓慢。	[13, 14, 28, 36]	30	0.130
	对响应不满	奖励低于预期（例如下调严重程度、影响）。	[26]	26	0.120
	范围不明确	计划范围定义不清晰。		3	0.082
	平台支持不佳	对平台处理问题的方式感到不满，例如调解。		1	0.079
	重复漏洞	太多报告被标记为重复漏洞。	[26]	4	0.078
	超出专业范围的资产	资产超出了专业领域，且缺少某些所需技能。		11	0.068
	安全资产	发现漏洞太难了。		5	0.064
	压力与不确定性	担心倦怠、工作时社交孤立、收入不稳定等。	[26]	5	0.062
	劳动工作过多	琐碎任务（例如验证码、超时、代码混淆、设置测试账户）。		12	0.050
	无聊	厌倦了参与该计划，或者有更有趣的计划启动了。	[26]	8	0.050
	缺乏代表性的声誉系统	黑客的声誉积分无法反映其实际经验。		1	0.047
	与管理者合作困难	与管理者合作困难（例如，受到不尊重、被要求承担额外工作）。	[26, 36]	23	0.044
	时间不足	没有足够的时间参与漏洞赏金活动。		2	0.043
	有限的漏洞披露	限制严格的漏洞披露政策和保密协议可能会阻止您发布信息。 [26]		2	0.041
	法律威胁	担心面临法律后果（民事或刑事）的威胁。		2	0.028
	沟通或语言	由于语言技能不足、沟通焦虑等造成的沟通困难。		2	0.014
Benefits of bug hunting	金钱奖励	金钱补偿。	[13, 14, 26, 34–36, 62]	42	0.191
	学习	学习或提升技能。	[13, 14, 26, 34–36]	32	0.170
	乐趣	白帽黑客活动带来的乐趣或挑战。	[14, 26, 34–36]	20	0.140
	法律安全港	只要遵守规则，就可以进行黑客攻击而不必担心遭到法律诉讼。		4	0.118
	灵活性	（相较于传统雇佣）工作时间安排和地点灵活性。	[13, 26]	16	0.095
	职业发展	与公司建立关系，以获得就业和其他机会。 [26, 34–36]		11	0.091
	社区	漏洞赏金构建了一个黑客社区。	[26, 35]	3	0.071
	利他主义	提升网络安全，帮助他人，保障互联网安全。	[13, 14, 26, 34–36]	5	0.062
	声誉	赚取平台声誉积分、积累关注者等。	[26, 34, 35, 60]	14	0.048
	非货币奖励	非货币补偿（例如周边商品、硬件、订阅）。	[26]	4	0.013
Useful platform features	支付便利性	以标准化、无繁琐步骤的方式收取付款。		12	0.156
	报告便利性	轻松生成、提交报告并追踪其状态。		16	0.142
	查看已披露的漏洞	平台提供的界面，可查看他人发现的漏洞。	[62]	15	0.137
	私人计划邀请	访问平台上的私人计划。		5	0.107
	计划目录	在一个地方列出许多项目，并提供统计数据、详情等信息。		17	0.068
	标准化规则	平台对范围、奖励、严重性等的定义进行标准化。		3	0.063
	社区	平台努力打造黑客社区。	[26]	11	0.057
	平台奖励	例如，平台周边礼品和资助差旅。	[26]	1	0.054
	调解	平台解决黑客与项目之间的争议。		13	0.051
	平台管理的披露	平台提供用于公开披露已修复漏洞的工具/机制。		6	0.050
	学习资源	平台提供关于如何进行黑客攻击的免费资源（例如 Bugcrowd University）。	[36]	2	0.047
	声誉系统	平台为黑客管理的声誉系统。		6	0.043
	平台分流	由平台负责分流（例如，由 HackerOne 而非 Uber 对你的报告进行分流）。		5	0.023

表2：因素评分研究中使用的因素，按因素组整理。佛罗里达州：在自由列举研究中列出该因素的参与者人数。价值(π)：因素相对重要性的估计值（数值仅在比较时有意义，详情见§3.2）。为节省空间，描述已缩短；完整版本见附录 D。引文标明了先前研究中发现的因素。

主要益处，漏洞猎人自然认为公开披露是一种学习机会。虽然因素评分研究的参与者他们并未像重视其他因素那样，直接看重计划是否愿意披露（佛罗里达州=6, π=0.027），但他们确实认为

查看已披露的漏洞是平台第三有用的功能（佛罗里达州=15, π=0.137）。这一结果为先前研究 [25], 增添了细微差别：尽管漏洞猎人不需要某个特定的漏洞赏金计划对披露持开放态度才会参与其中，但他们更希望整个生态系统都如此。这进一步印证了这样一种观点：漏洞猎人主要将公开披露作为学习资源，而建立声誉的重要性较低。相反，学习资源漏洞赏金平台所提供的学习资源并未被评为有用（佛罗里达州=2, π=0.047），这表明仍有改进空间。

查阅公开披露的漏洞是漏洞猎人最常提到的学习方法（I=18）。这些报告向漏洞猎人展示了同行如何处理问题（I=9）：“关键在于思考过程。”报告中的漏洞也可能直接在其他项目中复现（I=4）。一位漏洞猎人对此这样描述：“大家都会从报告中借鉴漏洞利用或攻击向量，然后都尝试在不同项目中找到同一个问题。”

公开披露不仅能让人学习新的黑客技术；漏洞猎人还指出，披露也有助于评估漏洞赏金计划（I=10），尤其是分诊团队的质量（I=3）（参见 §5.4）。正如一位漏洞猎人所说：“我会阅读 HackerOne 上所有已披露的报告，看看他们如何与研究人员沟通。”此外，两位漏洞猎人认为，公开披露为项目提供了宣传机会。他们浏览平台的已披露漏洞列表时（例如 Hacktivity 和 Crowdstream [19, 37]），这些披露吸引了他们的注意。这些披露表明，公司认真对待其漏洞赏金计划，因此更值得合作。

社区的影响 自由列举研究的参与者报告称，漏洞猎人社区是漏洞赏金的一项益处（FL=3）。尽管其评分不如其他因素高（π=0.071），但我们发现，社区是学习不可或缺的一部分。这个社区通过社交媒体上的互动自然形成，但许多漏洞猎人（FL=11, π=0.057）也指出，漏洞赏金平台有所贡献（例如，现场黑客活动）。

几乎所有受访者都指出，漏洞猎人社区成员经常彼此交流、分享信息，从而营造出一种学习氛围（I=22）。这包括漏洞猎人披露漏洞，以此“回馈社区”（I=5）、提供具体的技术知识（I=7），以及回答问题（n=5）。一位漏洞猎人赞赏博客文章作者的响应度：“如果你有任何疑问，只要联系他们就行了……大家都很乐于助人。社区氛围很好。”在漏洞赏金这个竞争激烈的世界里，资源共享（通常免费提供（I=1））尤为引人注目（也就是说，每个漏洞只有一名漏洞猎人能获得报酬）（I=2）。

漏洞赏金社区还让人们能够通过与其他漏洞猎人建立关系来学习。许多参与者提到，他们结识的业内人士对其职业发展有所帮助（I=8），其中五人指出，这些人脉促成了漏洞发现合作。还有几人强调了参与社区所带来的社交益处（I=7），这可以减轻远程、独自工作带来的孤独感（I=2）。尤其是线下活动，能让人感受到归属感。一位漏洞猎人解释说：“你能结识很多人，也会拥有很多机会。大家似乎都认识你，每个人都想做你的朋友，而你也想和每个人交朋友。”

并非所有人都认为社区是有用的学习工具。五位受访者指出，社区成员并不总是分享有用的知识，还有两位表示，分享知识是近来才出现的现象。一位受访者指出：“网络喷子有点太多了，但通常来说，[普通漏洞猎人] 都很乐于助人，这确实能促进交流。”

与技术熟悉度的对比 自由列举研究的参与者指出，选择漏洞赏金计划时，技术熟悉度 很重要（FL=22）；在因素排名中，参与者也将其评为重要因素（π=0.113）。

大多数受访者表示，他们更喜欢自己熟悉相关技术的计划，因为这能让他们更容易找到漏洞（n=15）。具体而言，一些受访者（n=5）指出，熟悉相关技术（有时会具体提到某些库：“比如你熟悉 Django，可能也熟悉 Flask 之类的，那么你就可以去搜索看看版本有没有更新。”）有助于他们运用已有技能。正如一位受访者所说：“……如果你想找到漏洞，就需要熟悉相关技术……”三位漏洞猎人表示，熟悉技术有助于他们发现高危漏洞；另有一位表示，这有助于他们找到“唾手可得的成果”。

表面上看，这似乎与强调现有技能、专注于学习的观点相矛盾。然而，访谈显示事实并非如此。参与者表示，即使是已有的技能也需要练习（I=3）[59]，而且无论目标是什么，漏洞猎人都会学习新技术。因此，我们认为，漏洞猎人选择自己更熟悉的技术，并不一定会限制他们的学习。相反，专注于熟悉的技术有助于漏洞猎人开始寻找漏洞，并为他们提供了解新变体或相关模块的机会，还能通过练习精进技能。

5.3 预测发现漏洞的可能性

许多参与者指出，与发现漏洞的概率相关的因素是重要的考量。这些因素包括计划范围、年龄和饱和度、计划是公开还是私有、出现重复漏洞的可能性，以及漏洞猎人的声誉所产生的影响。对于某一因素的哪些方面有利或不利，大家几乎没有达成共识。

计划范围的广度与明确性 自由列举研究中有一半的参与者认为，范围 ——它决定了可以调查哪些资产，以及会接受哪些漏洞类型——是选择漏洞赏金计划时的重要因素（佛罗里达州=28）。因素评分研究的参与者将范围评为最重要的因素（π=0.156）。有趣的是，这一发现此前仅在

营销材料中提及 [14]。

许多漏洞猎人认为，范围有助于预测他们预计能发现多少漏洞。大多数受访者更喜欢较大的范围（I=15），他们认为，更大的攻击面应当意味着存在更多潜在漏洞。例如，一位漏洞猎人解释说："美国国防部是范围很大的一个好例子.....那里有很多系统，你可以在其中识别漏洞，因此有很多机会发现问题。"

较大的范围也让漏洞猎人能够全面评估一款产品（就像恶意行为者可能做的那样）；有两位受访者表示，更好地了解资产的整体架构，最终能提高发现漏洞的可能性。一位受访者解释说："我只想知道对手能否拿到客户数据。而他们 [对手] 没有范围限制，只会直接攻击目标，我也想这么做。"

相应地，范围狭窄也有重要缺点（I=5）。首先，这会增加发现范围外漏洞的风险（I=3）。此外，一位受访者认为，在高度互联的产品中，漏洞赏金计划无法充分隔离出范围较小的部分："他们有一长串范围外的项目，.....所以我去访问他们的网站，进入一个范围内的目标，结果它就开始到处触及这些范围外的目标。"范围狭窄也会增加漏洞赏金计划趋于饱和（定义见下文）的可能性，因为每个目标可能有更多漏洞猎人（I=3），相应地，发现漏洞的难度也会增加（I=2）。

相反，少数受访者并不认为范围广是一个主要因素。两位受访者指出，与有经验的人相比，范围对初学者更重要，因为技能会随着经验增加："也许如今情况不太一样了，因为我现在经验更丰富了，但至少在刚开始时，范围很重要。"

参与者认为，范围不明确是漏洞赏金中的一大问题（佛罗里达州=3，π=0.082）。许多受访者回忆起因范围描述不准确而感到沮丧的经历（I=10），其中包括范围含糊不清（I=5）或已过时（I=2）的情况。两位受访者提到，他们不得不与管理者沟通以寻求澄清。范围不明确在许多情况下属于沟通问题；我们将在§5.4中讨论与沟通相关的主要挑战。

年龄与饱和度参与者表示，漏洞赏金计划的存续时间——即自启动以来经过的时间——会影响他们选择哪个漏洞赏金计划（佛罗里达州=6, π=0.023）。一个密切相关的因素是饱和度：相对于范围，一个计划已受到多少关注，以及有多少漏洞猎人正在积极参与其中（佛罗里达州=8, π=0.047）。11 位参与者将计划存续时间作为饱和度的代理指标，通常认为较新的计划中还有更多未发现的漏洞。因此，12 位受访者更倾向于选择较新的计划。较早启动的计划确实会定期推出新代码（I=3），从而创造新的机会。

然而，在这一点上并未达成共识。这似乎与先前研究相矛盾 [49, 60],六人更偏好较早的计划，因为他们在处理漏洞报告方面经验更丰富（I=2），并且能提供更多公开信息（I=1）。一位参与者说："关于那个[较年轻的]计划，报告会更少，所以你也学不到那么多。"

公开项目与私有项目公开项目会公开宣传，任何人都可以参与。相比之下，私有项目仅允许受邀者参与。几位受访者在选择项目时，会根据其公开或私有状态来判断找到漏洞的机会；不过，这并非首要考虑因素（FL=4, π=0.048）。受访者的偏好各占一半（私有：I=11；公开：I=9）。

据报告，私有项目中的漏洞猎人较少（I=9），这表明其饱和度较低。相反，有三人表示，私有项目的饱和程度与公开项目不相上下："大多数项目通常都有相当多的黑客。"此外，三人指出，公开项目的范围通常更广。除饱和度外，一些人还将项目的公开或私有状态作为判断项目年龄（I=1）、响应度（I=1）以及是否可能公开披露（I=2）的经验法则。

重复漏洞的可能性报告重复漏洞——即此前已报告过的漏洞——往往得不到奖励，这让漏洞猎人感到沮丧。受访者将其列为第四大问题（FL=4, π=0.078）。他们认为，重复漏洞与漏洞赏金计划管理员未能及时修补漏洞（I=6）以及项目较为老旧（I=2）有关："如果你是最早参与该项目的人之一，我认为.....遇到重复漏洞的机会就会降低。"三人认为，重复漏洞主要发生在漏洞猎人专找较容易发现的漏洞时，而避开"唾手可得的成果"便可以减少这种情况。

一些受访者（I=4）认为重复漏洞是不可避免的："重复漏洞总是你必须习惯的事情。"不过，也有几位（I=9）描述了应对方法：三人表示，知道自己发现的漏洞已得到确认会有所帮助；四人表示，被加入报告中（即使没有奖励）也能让他们确信漏洞赏金计划管理员没有撒谎；还有两人表示，他们不会去追查自己认为在社区中很热门的漏洞。

声誉的影响漏洞猎人是否会获得奖励，取决于多个因素，其中之一就是漏洞猎人的声誉。声誉可以通过官方平台声誉系统建立，也可以通过发布已发现漏洞的基本宣传材料（如技术分析文章）来建立。高声誉和低声誉的漏洞猎人（I=9）都表示，由于缺乏声誉，他们在报告漏洞时不会受到重视，或者过去没有受到重视；然而，声誉通常是通过报告有效漏洞获得的，这使初学者很难起步。同样，五人指出，漏洞猎人的声誉有助于他们获得私有项目邀请，"以确保我的声誉始终足够高，让他们继续邀请我并向我发出私有邀请。"四位参与者还提到，声誉也有助于获得其他安全研究人员的重视（I=3）。

尽管有 14 名自由列举研究参与者提到了声誉是整体上的一项益处，但因素评分研究的参与者认为其重要性有限，将其评为倒数第二重要的益处（π=0.048）。同样，声誉系统所

提供的漏洞赏金平台被评为倒数第二重要的特征（佛罗里达州=6， π=5）。我们推测，尽管声誉是漏洞赏金中非常显眼的一面，但最终并不像其他因素那样有益。这一发现与先前研究相矛盾；先前研究假设，声誉的重要性可能高于或相当于金钱补偿 [25, 56, 60]。

5.4 沟通、争议与调解

自由列举研究揭示了与漏洞猎人和漏洞赏金计划管理员之间沟通有关的多个因素，包括响应不佳、粗鲁或不合理的漏洞赏金计划管理员，以及对报告的意外回应。尽管先前研究已经讨论过其中一些问题（见 表2），但其他重要问题（例如调解流程）此前并未得到探讨。

响应不佳 在自由列举研究中，多数参与者（佛罗里达州=30）提到了响应不佳：漏洞赏金计划管理员未能有效地与漏洞猎人沟通。因素评分研究的参与者也将响应度评为漏洞赏金中的首要挑战（π=0.130）。先前研究 [26] 和营销材料 [14] 都曾简要指出这一问题的重要性。我们的受访者（I=17）进一步阐释了何为及时响应，包括首次响应时间（I=1）、严重程度判定所需时间（I=1）、奖金支付所需时间（I=5）和／或补丁所需时间（I=1）。这份多样化的定义清单表明，漏洞赏金计划应致力于改善所有指标，而不是只挑选其中一项。

有些人（I=5）讲述了令人沮丧的经历：漏洞悬赏计划的项目管理人员完全不回应他们或其他人的沟通尝试。一位受访者说："有时，有些项目不修复那些确实成立的问题，却以不适用为由将其关闭，而且不作任何解释。我对此发表评论后，他们也不回应，完全无视我的评论。"

许多受访者提出了让对方不回应变得更容易接受的方法，但意见并不一致。有些漏洞猎人希望在奖金支付延迟时能收到频繁更新（I=4），因为"只要他们持续提供更新，延迟就是可以接受的"。两位受访者表示，面对高危漏洞，他们可以等得更久；而另一位受访者则认为，高危漏洞应该更快得到解决。

与管理者／分诊人员合作困难尽管对方不回应往往是最令人沮丧的沟通问题，但并非唯一的问题。值得注意的是，许多自由列举研究的参与者（FL=23）提到了与管理者合作困难。然而，这一因素在挑战性排名中靠后（π=0.044），可能是因为我们将其与密切相关的因素"对响应不满"（下文讨论）区分开来。

六位受访者提到，漏洞赏金计划管理员在沟通时并非总是专业；他们可能会出言不逊（I=3），或以其他方式表现出轻蔑（I=2）。正如一位漏洞猎人所说："和一个侮辱你、对你粗鲁或诸如此类的人共事，其实一点也不愉快。"

尽管大多数漏洞猎人将沟通困难归咎于项目管理人员，但有九位受访者也责怪漏洞猎人。六人表示，漏洞报告有时不够清晰。对此，一位漏洞猎人正努力改进："我们现在也一直在努力做的一件事是……尽可能让报告的质量高、内容清晰。"两位受访者表示，漏洞猎人偶尔会言辞无礼，应当表现得更加专业（n=2）。

潜在冲突的另一个来源是平台分诊人员；自由列举研究的五位参与者提到了这一点，但将其评为最没用的平台功能之一（π=0.023）。一些漏洞赏金计划从漏洞赏金平台雇用分诊人员，而不是组建自己的团队。几位漏洞猎人（I=2）认为，开发团队之外的分诊人员会加剧沟通困难。两人表示，受雇的分诊人员在漏洞猎人与负责修复漏洞的团队之间设置了不必要的障碍；另一人指出，由于公司作出最终的奖金支付决定，分诊人员的严重性评级并不重要。

相反，五位受访者对平台分诊人员有过积极的经历。他们指出，平台分诊人员专门负责与漏洞猎人打交道，因此比漏洞赏金计划管理员更容易合作。一位参与者很赞赏平台分诊人员会在漏洞报告提交给漏洞赏金计划管理员之前协助澄清报告内容；另一位表示，平台分诊人员帮助他们信任自己并不认同的决定（例如，将其判定为重复漏洞）。两位参与者回忆起了与没有平台分诊人员的项目合作时的负面经历。

在被问及对管理者不满时，两位漏洞猎人明确表示没有什么大问题；其中一位说："总体而言，我的体验一直非常好。"

意料之外的回应 与前一个因素密切相关，对响应不满 也是一个常被提及、令人极为沮丧的问题（FL=26, π=0.120）。

大多数受访者回忆说，他们曾不同意漏洞赏金计划管理员对漏洞的评估（I=16），分歧通常涉及漏洞适用性和严重性级别、重复状态，以及是否允许公开披露。

八位受访者表示，漏洞赏金计划管理员会因误解提交的报告而犯错：要么没有仔细阅读报告（I=2），要么不理解其中的技术细节（I=4）。相反，一位受访者指出，漏洞猎人也可能没有完整阅读计划说明："老实说，我有时会忘记读完整个项目范围，有时会提交一些不在范围内的漏洞。"

令人担忧的是，与此前在类似情境中的发现一致 [3]，，两位漏洞猎人指出，他们可能会为了避免与漏洞赏金计划管理员就范围产生分歧，而不报告潜在漏洞。

有五位漏洞猎人更加悲观，认为公司可能会欺骗漏洞猎人，以此逃避支付报酬。一位漏洞猎人回忆道："有时，计划从你这里拿到所需的一切后，……他们就会把状态设为 [to] needs more……接着，漏洞被修复了……严重程度被调低，你得到的奖励也比预期的少。然后，他们

突然就不再回复你的评论了，而这种情况经常发生。”

争议和响应度问题在极少数情况下可能导致极端后果。一名参与者被一家大型漏洞赏金平台封禁。另一名参与者指出，当他们对漏洞赏金计划感到沮丧时，直接利用漏洞会变得更有吸引力。

尝试解决争议争议发生时，漏洞猎人可能会请漏洞赏金平台充当表面上公正的调解方，尽管平台通常无法推翻漏洞赏金计划管理员的最终评估 [33]。虽然许多人在自由列举研究中将其列为一项益处（FL=13），调解并未被评为漏洞赏金平台的一项顶级功能（π=0.051）。同样，平台支持不佳（包括调解支持不佳）被视为漏洞赏金领域面临的最大挑战之一（FL=1，π=0.079）。

受访者对平台调解的反应有正面（I=8）和负面（I=5）之分。从正面来看，一些人指出，调解有助于向漏洞赏金计划管理员澄清技术问题（I=5）。一位受访者解释说：“最大的益处之一.....是他们确实会促成对话.....主要是帮助非技术背景的计划经理理解漏洞的影响。”一名参与者表示，知道“.....平台会支持他们。大多数情况下如此”，让自己感到安心。

然而，其他参与者认为，调解本质上存在偏见，因为漏洞赏金平台会偏袒付费请它们托管项目的公司（I=4）。两人回忆称，曾遇到漏洞赏金平台未回应调解请求的情况；另外两人虽听说过此类问题，但没有亲身经历。一位漏洞猎人描述了自己申请调解的经历：“然后什么也没发生。每两周才能收到一次回复，因为你只能每两周联系他们一次，而且完全看不出事情有任何进展。这简直是个天大的笑话。”

5.5 零工工作的益处与弊端

我们发现的多个因素都与漏洞赏金生态系统的零工工作性质有关。这种模式有其益处（例如灵活性），但也存在严重弊端，包括压力与不确定性。值得注意的是，尽管 Ellis 和 Stevens 并未正式界定并衡量各类问题的普遍程度，但漏洞赏金的这一方面已受到他们的严厉批评 [26]。

灵活性 零工工作模式中一个常被提及、排名居中的益处（FL=16, π=0.095）是灵活性：可以随时随地工作，工作时长也可自行决定，并且能够完全自主地选择工作内容。

大多数受访者都提到了灵活的工作时间（I=14）。三位受访者强调，这样可以避免截止期限和压力：“相比之下，我之前的开发工作完全以项目为导向，都有截止期限.....而做这个没有任何截止期限。”其他人则提到了可以自行选择要攻击的目标（I=2）、能够远程工作（I=2），以及入门门槛相对较低（不需要正式职位或事先批准，I=1）。

一些漏洞猎人指出，灵活性也有一些缺点。一位受访者提到，自己安排工作时间可能很棘手。另一位受访者则表示，对于基本上全职从事漏洞狩猎的人来说，能够自行选择工作时间意义不大：“我想什么时候做都可以.....如果你唯一的工作就是全职从事漏洞赏金狩猎，这可能就更难了。”

此外，受访者认为，入门门槛低只是表象：两位受访者表示，他们花了好几年培养技能，才能有效参与其中。

零工工作的负面方面 漏洞赏金通常只会为被认定为独特且有效的漏洞向漏洞猎人发放奖励。因此，漏洞猎人可能投入大量精力却得不到报酬，进而产生压力与不确定性 (FL=5, π=0.062)。在许多情况下，这种压力源于我们在前文小节中指出的关键因素，例如范围不明确或出现重复漏洞的可能性。

最常见的不确定性来源是付款（I=9）。漏洞猎人不知道自己什么时候可能发现漏洞、漏洞何时（以及是否）会得到认可，也不知道管理者什么时候会决定付款。四位参与者指出，当漏洞赏金是主要收入来源时，收入不稳定尤其令人压力重重：“有时我连续几天甚至几周都找不到一个漏洞。我觉得这挺令人沮丧的，可以说，这是整个故事阴暗的一面。”

付款的不确定性因寻找漏洞的竞争而加剧，“因为漏洞赏金本质上是一场竞争，先到先得。”三位漏洞猎人指出，限时活动会加剧这种竞争感。

即使漏洞猎人最先发现漏洞，仍必须说服漏洞赏金计划经理确认漏洞有效，才能收到付款。正如第 5.4 节所述，这可能因多种原因而颇具挑战，进而带来额外的压力与不确定性。

受访者介绍了自己应对这种不确定性的方法。与先前研究一致 [26]，四人表示，为了保持财务稳定，他们会在漏洞赏金生态系统之外从事一份全职工作。一人说：“我有一份全职工作，这让我的收入稳定得多。但我想，如果我全职做漏洞赏金.....可能会影响我的心理健康。”另有三人表示，他们会通过休息来应对漏洞赏金带来的压力：“每当我觉得自己倦怠了，就会去做点别的事。我会提供培训.....或者出去散散步。”

五位受访者表示，这种不确定性让他们无法全职从事漏洞赏金。一位受访者特别指出，即使收入可能很高，也不值得承受这种不稳定性：“通过漏洞赏金，我有可能赚到超过 15 万.....如果我投入时间的话，但收入到账的时间和金额参差不齐，这就是个问题。所以，如果你真的打算全职做这个，就得有一些储蓄.....以备不时之需。”相反，一位参与者主动表示自己是一名全职漏洞猎人，另一位则认为，漏洞赏金本身就可以成为一项可行的职业发展途径。

5.6 平台基础功能

在自由列举研究中，漏洞猎人列出了多项有用的漏洞赏金平台功能。这些功能大多独立于漏洞赏金平台而存在，并已在前文各节中讨论过。这里，我们将讨论其中少数专属于漏洞赏金平台、且对漏洞猎人很重要的功能。

支付便利性 现金奖励是重要的激励因素，因此漏洞猎人也很关注付款是否便利（FL=12, π=0.156）。漏洞赏金平台付款最常被提及的优点是提供了多种选择（I=7）。例如，有六位受访者更愿意以国际货币收款，另有三位更喜欢以加密货币收款。一位受访者解释说："我更喜欢比特币，因为以前用 PayPal 时遇到过问题。"一些漏洞猎人喜欢漏洞赏金平台付款方式简单（I=6）："我只需输入一次支票账户号码，之后就再也不用操心了。"最后，一位受访者喜欢平台支持在合作者之间拆分悬赏金，另一位则喜欢能够追踪自己获得的所有悬赏金。

报告便利性 许多自由列举研究的参与者都赞赏标准化报告、提交和通信功能（FL=16）。事实上，这项功能被评为平台所提供的第二重要功能（π=0.142）。

受访者大多提到了报告界面的实用性(I=9)，包括报告撰写指南、格式化工具（如 Markdown）以及视觉内容支持（如视频）。漏洞猎人也认可用于追踪漏洞处理进度的界面(I=5)，其中包括与漏洞赏金计划管理员的通信以及他们采取的行动。

少数人认为仍有改进空间(I=6)，包括提高报告和附件的大小限制、加强不同漏洞赏金平台之间报告界面的一致性，以及建立更正式的沟通流程。

计划目录 计划目录可以说是漏洞赏金平台的主要功能，让漏洞猎人能够发现各种计划，并在一个地方比较这些计划的多个方面(I=12)。一些可用指标反映了漏洞猎人最关注的内容（如预期悬赏金、响应度）。因此，大多数自由列举研究的参与者(FL=17)都提到了这一功能，而因素评分研究的参与者则认为它相对重要(π=0.068)。

少数受访者认为仍有改进空间，例如发布更多统计数据（I=3），并为每个项目提供漏洞猎人反馈（I=1）。

查看已披露的漏洞 或许是因为这些内容对学习（一个重要的激励因素）至关重要，漏洞猎人（I=11）很喜欢能够通过平台轻松查看某个计划已披露的漏洞 （例如，HackerOne 上的*Hacktivity*）（FL=15, π=0.137）。访谈表明，平台是获取已披露报告的主要渠道。少数人（I=5）提到，他们会寻找独立的分析文章（例如，博客文章）；不过，更多漏洞猎人提到了通过漏洞赏金平台发布的漏洞披露（I=11）。

5.7 法律安全港

法律安全港 是公司作出的承诺：对于遵守规则的漏洞猎人，不会对其采取法律行动，从而允许漏洞猎人攻击真实世界目标。自由列举研究的参与者在多个因素类别下都提到了漏洞赏金的这一法律层面：选择项目、挑战和益处。然而，先前研究经常忽略这一点。

尽管自由列举研究中的许多人并未将法律安全港列为一项益处（FL=4），但它的排名仍相对靠前（π=0.118）。同样，许多人没有将安全港列为选择新项目时的考量因素（FL=4），但它的排名依然相当靠前（π=0.098）。

大多数受访者（I=16）表示，没有安全港的漏洞赏金风险很高；有六人表示不会考虑没有安全港的项目。这或许能部分解释为何自由列举研究期间，人们不一定会首先想到法律安全港：它可能并不显眼，但缺失时却会引人注意。

有些人的标准较宽松，他们表示只会避开曾起诉过漏洞猎人的项目（I=4）。"我只需要在任何实际上不会起诉人的项目上测试漏洞，这样我的生活就轻松多了。"有八人回忆起曾对漏洞猎人采取法律诉讼的案例，另有两人警告说，没有安全港政策的公司很可能会提起诉讼。

作为另一项微妙的益处（I=2），安全港表明漏洞猎人并非如人们通常描绘的那样怀有恶意 [17]。一位受访者说："正因为有了这个 [安全港]，.....大家都认同：'这些黑客是好人黑客。'"

并非所有漏洞猎人都认为法律安全港不可或缺（I=5），这或许与法律威胁被视为第二不重要的挑战有关（FL=2, π=0.028）。受访者解释了原因：他们居住地的法律已经提供了保障（I=1）；所有 HackerOne 项目本来就应该包含安全港，因此无需再次核查（I=1）；而且法律威胁很少见（I=1）。四人表示，确保自身活动合法是漏洞猎人的责任。一人补充道："我了解自己作为研究人员的权利。即使没有法律安全港，他们也必须证明造成了某种损害。"

6 讨论

当生态系统运作良好时，漏洞赏金有望以较低成本提升组织（商业或政府组织）的安全态势 [56, 60]。同时为漏洞猎人带来诸多益处。然而，漏洞赏金的采用率较低，只有部分开展漏洞赏金计划的组织能够持续收到高质量的漏洞报告 [49, 56]。对于漏洞猎人而言，尽管报告中提及的从业者群体规模庞大，但只有少数人能获得承诺的全部益处 [26]。从本质上说，漏洞赏金不仅未得到充分利用，

当前生态系统的益处在组织和漏洞猎人之间的分配也存在不平等。

本节列出了对漏洞赏金计划、平台和政策制定者的建议，旨在缓解我们发现的重要挑战，同时支持并扩大漏洞猎人最为看重的益处。我们希望这些建议能够推动更多组织采用漏洞赏金计划，提升其安全性，并确保更多漏洞猎人充分获得这一市场的益处。

漏洞赏金计划可以采取的措施 排名最高的两个因素是范围和奖励，而这两者都在计划的直接控制之下，但要扩大它们都需要投入额外资源。奖励与资金直接相关，而扩大范围可能会增加人员配置需求；我们建议未来的研究探索扩大范围所涉及的细节。在可行的情况下，扩大范围也可能缓解漏洞猎人的一些其他顾虑，例如重复漏洞、饱和，以及所用技术种类繁多的问题。与范围大小密切相关的是，范围的清晰度也被视为一个重要问题。确保范围清晰且及时更新，成本相对较低，也有助于减少漏洞猎人因遇到意料之外的超出范围问题和无效响应而产生的挫败感。

漏洞猎人报告的最突出挑战都与沟通有关。要解决响应度这一首要挑战，增加人员配置可能是最有效的方案[26]。如果无法增加人员配置，较为经济的选择是频繁、透明地更新漏洞报告的处理状态，以减少不确定性（§5.4）。

总体改善沟通也能减少意料之外的回复。漏洞赏金计划可以从尽可能清晰地说明范围和赏金表入手，或许还可列举按每个（公开披露的）漏洞支付奖金的示例，并提醒大家注意常见的超出范围提交和容易踩中的陷阱。计划也可以培训管理者，帮助他们改善与漏洞猎人的沟通，并避免在解读漏洞报告时常见的错误。

漏洞赏金平台可以采取的措施 平台支持不足（即调解）是最突出的平台问题，而对平台或计划回复不满（进而引发争议，并可能导致调解）则是总体上第二重要的挑战。几位参与者抱怨调解员偏袒漏洞猎人。平台可以更清楚地说明其商业模式，以此应对这一问题——平台要正常运作，漏洞猎人与漏洞赏金计划同样不可或缺；平台还可以通过发布有关调解结果的定期报告，提高透明度。

更广泛地说，平台还可以采纳我们上述的一些建议来改善沟通问题，包括在可能的情况下增加工作人员以减少延误，并为报告提交提供指导。平台还可以根据平台上以往的案例，为参与计划的项目提供培训，教他们如何与漏洞猎人沟通以及如何解读漏洞报告。

我们还建议平台探索如何减少漏洞猎人面临的不确定性。平台可以评估实施保险政策是否有用，以确保即使漏洞赏金计划不愿接受调解结果，漏洞猎人仍能获得付款；或者采取更积极的做法，试图削弱漏洞赏金计划作出最终裁决的权力。例如，平台可以考虑承担更多分诊流程的管理工作，甚至决定最终付款。

学习被视为漏洞赏金的第二大重要益处，也可能是将高产漏洞猎人纳入劳动力的主要途径。目前，只有少数漏洞猎人能够享受漏洞赏金生态系统的全部益处；然而，提高漏洞猎人的技能水平可以缩小这一差距，同时也能促使总体上发现更多漏洞，从而有望普遍提升软件安全性。遗憾的是，漏洞赏金平台提供的学习资源重要性排名倒数第三，表明这方面仍有改进空间。我们建议将学习材料与此前已披露的漏洞（平台第三有用的功能）更好地整合，以使这些材料更具实用性和相关性。

除了改进不太受欢迎的方面，漏洞赏金平台也不应忽视其最受欢迎的功能：提供多种支付机制（例如方便国际漏洞猎人），统一各项目之间的界面，并允许漏洞猎人评价漏洞赏金计划（以及阅读其他人对这些计划的评价）。

漏洞赏金平台还可以通过推广那些关注度较低、但维护良好或对社会具有重要意义的项目，帮助分散漏洞猎人在各漏洞赏金计划之间的注意力，不过这可能需要由外部方提供激励（正如我们将在下文讨论的那样）。

立法机构和政策制定者可以做些什么漏洞赏金计划能带来重要的安全益处，对许多公司都可能有所帮助。然而，我们的结果表明，漏洞猎人通常会优先关注资源最丰富的计划（例如，金钱奖励丰厚、范围广泛的计划）。大型公司（例如谷歌）若能持续投入漏洞赏金计划，便具备充分条件从中获益；而小型公司及其计划可能无法做到这一点，即使这些公司身处关键行业，对安全有着重要需求。更糟的是，小型公司遭受网络犯罪造成重大损失的风险更高[39, 56]。

目前，多个政府机构建议公司采用漏洞赏金计划[42, 52]。这是一个良好的开端，但我们的研究结果表明，如果没有额外支持，这反而会加剧安全不平等。政府机构还可以提供资助，帮助安全预算和人员配置较少的公司负担得起持续运行漏洞赏金计划的费用：扩大范围、改善人员配置并提高悬赏金。资助（例如[18]）可以与改善漏洞赏金生态系统的优先事项挂钩，例如公开报告（让漏洞猎人能够评估各项计划）、吸引人们关注不太热门但对安全至关重要的行业（例如医疗保健、金融[56]），或改善教育资源[59]。

政府在改善漏洞猎人的处境方面还可以发挥其他作用。法律学者提议立法，为任何善意的安全研究人员（包括漏洞猎人）提供法律安全港 [27]，，司法政策制定者也已采取措施朝这一方向推进 [51]。我们的研究为这项值得推进的工作提供了证据：漏洞猎人重视法律安全港，并会据此区分不同计划（§5.7）。因此，普遍适用的安全港可以激励目前未提供这项保障的公司吸引漏洞猎人参与。此外，劳动监管机构可以考虑如何更好地保护漏洞猎人，避免他们遭受零工工作所带来的不确定性乃至侵害（§5.5, [26]），并制定适当的沟通乃至付款标准，从而帮助更多漏洞猎人留在生态系统中。

致谢

我们感谢所有参与者，没有他们，这项研究便无法完成；也感谢帮助完善本文分析和论述框架的评审。我们还要感谢 Jack Cable、Julien Ahrens 和 Nathan Reitinger 提供的帮助与见解。

本材料所述工作由美国国家科学基金会资助，资助编号为 CNS-1850510 和 CNS-1801545。本材料中表达的任何观点、发现、结论或建议均属于作者，并不一定反映美国国家科学基金会的观点。本研究还获得了谷歌的捐赠支持。

参考文献

[1]Reed Albergotti。苹果公司向发现其软件漏洞的黑客支付六位数报酬，却对他们的发现置之不理。《华盛顿邮报》，2021 年。https://www.washingtonpost.com/technology/2021/09/09/apple-bug-bounty/。

[2]Nikolaos Alexopoulos、Andrew Meneely、Dorian Arnouts 和 Max Mühlhäuser。《谁是漏洞报告者？关于自由/开源软件的大规模实证研究》。载于第*15*届*ACM/IEEE*实证软件工程与度量国际研讨会（*ESEM*）论文集，2021年。

[3] Noura Alomar、Primal Wijesekera、Ed ward Qiu 和 Serge Egelman。"你已经有了一份不错的漏洞清单，接下来怎么办？"现实环境中的漏洞发现与管理流程。载于第*16*届可用隐私与安全研讨会（*SOUPS*）。USENIX 协会，2020年。

[4] John Annett. 层次任务分析。《认知任务设计手册》，2，2003。

[5]苹果公司。示例付款。https://developer.apple.com/security-bounty/payouts/。

[6] Soodeh Atefi、Amutheezan Sivagnanam、Afiya Ayman、Jens Grossklags 和 Aron Laszka。漏洞发现与漏洞赏金计划的益处：Chromium 和 Firefox 的案例研究。载于*2023* 年 *ACM* 万维网大会（*WWW*），2023 年 5 月。

[7]Tod Beardsley、Bob Rudis、Tom Sellers、Curt Barnard 和 Kwan Lin。2021年行业网络暴露（ICER）：财富500强报告，2020年。https://www.rapid7.com/research/report/2021-industry-cyber-exposure-report/。

[8] H. Russell Bernard。 人类学研究方法：定性与定量方法。Rowman & Littlefield，2017年。

[9] Casey Breen、Cormac Herley 和 Elissa M. Redmiles。针对个人的网络犯罪大规模测量。载于*2022*年*CHI*计算机系统人因大会，第1–41页，2022年。

[10] Bugcrowd。https://www.bugcrowd.com。

[11] Bugcrowd。Bugcrowd在2018年上半年创下增长纪录，2018年。https://www.bugcrowd.com/press-release/bugcrowd-achieves-record-growth-in-first-half-of-2018/。

[12] Bugcrowd。漏洞赏金现状，2018年。https://www.bugcrowd.com/resources/reports/state-of-bug-bounty-2018/。

[13] Bugcrowd。黑客的内心世界，2020年。https://itmoah.bugcrowd.com/。

[14] Bugcrowd。《黑客的内心世界》，2021年。https://www.bugcrowd.com/resources/report/inside-the-mind-of-a-hacker/。

[15]美国人口普查局。按企业行业划分的2019年SUSB年度数据表，2020年。https://www.census.gov/data/tables/2019/econ/susb/2019-susb-annual.html。

[16] Kathy Charmaz。建构扎根理论：定性分析实用指南。Sage Publications，2006年。

[17]Mitchell Clark。《密苏里州州长威胁揭露州政府网站泄露私人信息的记者》，2021 年。https://www.theverge.com/2021/10/14/22726866/missouri-governor-department-elementary-secondary-education-ssn-vulnerability-disclosure。

[18] 欧盟委员会。小型企业资金申请机会。
h
t
t
p
s://
commission.europa.eu/funding-tenders/how-apply/eligibility-who-can-get-funding/funding-opportunities-small-businesses
en。 _

[19]Crowdstream。https://bugcrowd.com/crowdstream。

[20] Fred D. Davis。 用于实证检验新型终端用户信息系统的技术接受模型：理论与结果。博士论文，麻省理工学院，1985 年。

[21] Regina Dittrich、Brian Francis、Reinhold Hatzinger 和 Walter Katzenbeisser。《运用配对比较法分析李克特量表回答集合》。统计建模，7(1)，2007年。[22] Regina Dittrich 和 Reinhold Hatzinger。《使用 R 软件包 prefmod 拟合用于配对比较的对数线性 Bradley-Terry 模型（LLBT）》。心理测验与评估建模，51(2)：216，2009年。[23] Regina Dittrich、Reinhold Hatzinger 和 Walter Katzenbeisser。《在配对比较研究中对受试者特定协变量的影响建模，并将其应用于大学排名》。英国皇家统计学会杂志：*C*辑（应用统计），47(4)，1998年。[24] Amit Elazari。《塑造网络安全政策的私人规制：漏洞赏金案例》。本文经编辑的最终版本，载于《重塑：网络安全治理》，*Ryan Ellis* 和 *Vivek Mohan* 编。*Wiley*，2019年。[25] Ryan Ellis、Keman Huang、Michael Siegel、Katie Moussouris 和 James Houghton。《填补漏洞：漏洞劳动力市场》。载于《网络安全的新解决方案》，第129–159页。麻省理工学院出版社，2018年。[26] Ryan Ellis 和 Yuan Stevens。《万物皆可悬赏：黑客与全球漏洞市场的形成》。可见于 *SSRN 4009275*，2022年。[27] Daniel Etcovitch 和 Thyla van der Merwe。《走出寒冬：为安全研究人员提供免受《计算机欺诈与滥用法》和《数字千年版权法》第1201条追诉的安全港》。伯克曼·克莱因互联网与社会中心研究出版物，（2018-4），2018年。[28] Matthew Finifter、Devdatta Akhawe 和 David Wagner。《漏洞奖励计划的实证研究》。载于第*22*届 *USENIX* 安全研讨会（*USENIX* 安全）。USENIX 协会，2013年。[29] Brian Francis、Regina Dittrich 和 Omer Akgul。私人沟通，2022年。

[30] Kelsey R. Fulton、Samantha Katcher、Kevin Song、Marshini Chetty、Michelle L. Mazurek、Chloé Messdaghi 和 Daniel Votipka。《人人都能发现漏洞：漏洞发现中的边缘化经历》。载于即将发表于第*32*届 *USENIX* 安全研讨会（*USENIX* 安全）。USENIX 协会，2023年。

[31] Frederick J. Gravetter 和 Lori-Ann B. Forzano。行为科学研究方法。圣智学习，第 6 版，2018 年。

[32] HackerOne。https://www.hackerone.com。

[33]HackerOne。黑客调解。
https://docs.hackerone.com/hackers/hacker-mediation.html。[34] HackerOne。黑客驱动的安全报告：2019年，2019。
h
t
t
p
s://
w
w
w.
h
a
c
k
e
r
o
n
e.
com/sites/default/files/2019-08/hacker-powered-security-report-2019.pdf。
[35]HackerOne。2020年黑客报告，2020年。
h
t
t
p
s://
w
ww.hackerone.com/sites/default/files/2020-04/the-2020-hacker-report.pdf。
[36]HackerOne。2021年黑客报告，2021年。
https://www.hackerone.com/resources/reporting/the-2021-hacker-report。
[37] Hacktivity。https://hackerone.com/hacktivity。[38] Reinhold Hatzinger 和 Regina Dittrich。Prefmod：一个基于成对比较、排名或评分对偏好进行建模的 R软件包。《统计软件杂志》，48：1–31，2012年。[39] Nicolas Huaman、Bennet von Skarczinski、Christian Stransky、Dominik Wermke、Yasemin Acar、Arne Dreißi- gacker 和 Sascha Fahl。关于中小企业信息安全及其遭受攻击的大规模访谈研究。载于 第*30*届 *USENIX* 安全研讨会（*USENIX Security 21*）。USENIX 协会，2021年8月。[40] Keman Huang、Michael Siegel、Stuart Madnick、Xiao- hong Li 和 Zhiyong Feng。海报：多样化还是集中化？黑客跨多个漏洞赏金计划开展工作的策略。载于 第*37*届 *IEEE* 安全与隐私研讨会（*S&P*），2016年。[41] Muhammad Ikram、Narseo Vallina-Rodriguez、Suranga Seneviratne、Mohamed Ali Kaafar 和 Vern Paxson。对获准使用Android VPN权限的应用的隐私与安全风险进行分析。载于 *2016*年互联网测量会议（*IMC*），2016年。

[42] Christopher C. Krebs。具有约束力的操作指令 20-01——制定并发布漏洞披露政策。2020年。https://www.cisa.gov/sites/default/files/bod-20-01.pdf。

[43] J. Richard Landis 和 Gary G. Koch。《分类数据的观察者一致性测量》。*Biometrics*，33(1)，1977 年。

[44] Aron Laszka、Mingyi Zhao 和 Jens Grossklags。在漏洞赏金平台中消除用于验证报告的激励错位。载于第 *21* 届欧洲计算机安全研究研讨会（*ESORICS*），第 161–178 页，2016 年。[45] Aron Laszka、Mingyi Zhao、Akash Malbari 和 Jens Grossklags。漏洞赏金计划的交战规则。载于第 *22* 届金融密码学与数据安全国际会议（*FC*）。施普林格，2018 年。[46] Gitta H. Lubke 和 Bengt O. Muthén。将适用于连续结果的多组验证性因子模型应用于李克特量表数据，会使有意义的组间比较变得复杂。*Structural Equation Modeling*，11(4)：514–534，2004 年。[47] Donatello Luna、Luca Allodi 和 Marco Cremonini。漏洞赏金计划中的生产力与活动模式：对 HackerOne 和谷歌漏洞研究的分析。载于第 *14* 届可用性、可靠性与安全性国际会议（*ARES*），2019 年。[48] Ana Magazinius、Niklas Mellegård 和 Linda Olsson。关于漏洞赏金计划，我们了解些什么——一项探索性系统映射研究。载于安全与信任社会技术方面国际研讨会（*STAST*）。施普林格，2019 年。[49] Thomas Maillart、Mingyi Zhao、Jens Grossklags 和 John Chuang。只要有足够多的眼睛，所有漏洞都浅显易见？借助漏洞赏金计划重新审视 Eric Raymond。*JournalofCybersecurity*，3(2)，2017 年。[50] Nora McDonald、Sarita Schoenebeck 和 Andrea Forte。定性研究中的信度与评定者间信度：计算机支持的协同工作和人机交互实践的规范与指南。美国计算机协会人机交互论文集，3（计算机支持的协同工作专刊），2019 年。[51]美国司法部。司法部宣布针对《计算机欺诈与滥用法案》案件的新起诉政策，2022 年。https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act。

[52]美国国家标准与技术研究院。信息系统与组织的安全与隐私控制。RA-5：245，2020 年。https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf。[53] Jukka Ruohonen 和 Luca Allodi。从漏洞赏金的视角看网络漏洞披露。arXiv 预印本 arXiv:1805.09850，2018 年。[54] Johnny Saldaña。《定性研究人员编码手册》。定性研究人员编码手册，第 1–440 页，2021 年。[55]Jim Salter。对苹果公司漏洞赏金计划感到失望的研究人员披露了三个 iOS 零日漏洞，2021 年。https://arstechnica.com/information-technology/2021/09/three-ios-0-days-revealed-by-researcher-frustrated-with-apples-bug-bounty/。[56] Kiran Sridhar 和 Ming Ng。为善而黑客攻击：利用 HackerOne 数据构建漏洞赏金经济模型。Journal of Cybersecurity，7(1)，2021 年。[57] Daniel Votipka、Seth Rabin、Kristopher Micinski、Jeffrey S. Foster 和 Michelle L. Mazurek。对逆向工程师工作流程的观察性调查。载于第 29 届 USENIX 安全研讨会。USENIX 协会，2020 年。[58] Daniel Votipka、Rock Stevens、Elissa Redmiles、Jeremy Hu 和 Michelle Mazurek。黑客与测试人员：软件漏洞发现流程的比较。载于第 39 届电气电子工程师学会安全与隐私研讨会（S&P），2018 年。[59] Daniel Votipka、Eric Zhang 和 Michelle L Mazurek。遭到黑客攻击：对在线漏洞发现练习的教学分析。载于 2021 年电气电子工程师学会安全与隐私研讨会（S&P）。电气电子工程师学会，2021 年。[60] Thomas Walshe 和 Andrew Simpson。漏洞赏金计划的实证研究。载于第 2 届电气电子工程师学会智能漏洞修复国际研讨会（IBF），2020 年。[61] Chien-Ho Wu。将李克特量表数据转换为数值分数的实证研究。Applied Mathematical Sciences，1(58)：2851–2862，2007 年。[62] Mingyi Zhao、Jens Grossklags 和 Peng Liu。网络漏洞发现生态系统的实证研究。载于第 22 届 ACM SIGSAC 计算机与通信安全会议（CCS），2015 年。[63] Mingyi Zhao、Aron Laszka 和 Jens Grossklags。为漏洞赏金平台和安全漏洞发现制定有效政策。Journal of Information Policy，7，2017 年。

Pu发表于第32届 USENIX 安全研讨会论文集（USENIX Security ’23）。

[64] Mingyi Zhao、Aron Laszka、Thomas Maillart 和 Jens Grossklags。《众包安全漏洞发现：漏洞赏金计划的建模与组织》。发表于第*4*届 *AAAI* 人类计算数学基础研讨会（*HCOMP*），2016。

A 其他因素

接下来，我们将讨论漏洞猎人在参与漏洞赏金计划时会考虑的其他因素。

A.1 其他益处

乐趣 对漏洞猎人而言，排名靠前的一项益处，就是参与漏洞赏金计划本身带来的乐趣（FL=20,π=0.140）。具体来说，受访者提到了智力刺激（I=3）："攻破某个东西很有趣.....这就像一项挑战，就像一道谜题。"还有人提到击败开发团队的快感（I=1）、将漏洞挖掘作为放松方式（I=1），甚至是享受不确定性的刺激（I=1）。"这就像赌博，我常用这个来打比方。你根本不知道下一笔奖金会不会到手。我想，这同时也正是它有趣的原因。"一位参与者特别指出，漏洞赏金只有作为一种爱好时才有趣；如果变成全职工作，就会失去吸引力。

利他主义 自由列举研究中的少数参与者表示，他们参与漏洞赏金活动是出于利他主义 原因（FL=5）。但因素评分研究的参与者并未将利他主义列为主要益处（π=0.062）。四位漏洞猎人认为，漏洞赏金活动让他们有机会为其他用户打造更安全的互联网。一位受访者说道："我认为，利他主义和为善而进行黑客攻击，是漏洞赏金平台乃至道德黑客行为存在的主要目的之一。"一位受访者认为，分享知识以帮助其他漏洞猎人也体现了利他主义。四位受访者表示，无论是否能得到报酬，他们都会报告漏洞；还有一位表示，愿意帮助无力支付费用的公司："我不介意做无偿工作，但这通常只会发生在人们确实完全付不起费用的时候。"不过，同一位受访者指出，这类公司通常"还不够成熟，无法[采纳] 我给他们的建议，这有点可惜。"其他受访者（I=4）将自己的利他工作与犯罪黑客造成的危害作了对比。

A.2 其他挑战

语言障碍 一位自由列举研究的参与者指出，漏洞猎人与漏洞赏金计划管理员之间的语言障碍是另一个沟通问题。我们的受访者无人提及这一点；不过，我们注意到，所有受访者都必须具备足够的英语流利程度，才能接受访谈。由于我们能够用英语采访所有受访者，因此他们可能并非具有代表性的样本。

太多琐碎劳动 在自由列举研究中，12 位参与者提到，他们对漏洞赏金计划管理员通常要求完成的重复性琐碎任务感到厌烦。受访者指出了两大挫折来源：公司的网络架构，以及必须使用的测试账户或凭证。

谈到网络架构，受访者抱怨说，他们需要绕过内容分发网络（I=2）、防火墙（I=2）或验证码（I=1）。漏洞猎人觉得，漏洞赏金计划把绕过这些（通常经过加固的）工具与在目标本身发现漏洞混为一谈，这令人沮丧："我很乐意评估 Web 应用防火墙，但你们要我评估的是网站。..... 如果他们用 CloudFlare [来设置防火墙], , 那我是在绕过 CloudFlare 吗？我可不觉得，刚绕过 CloudFlare 控制器就能从 Barry 的蛋糕店拿到合适的奖励，还能拿到一个价值 500 美元的跨站脚本攻击漏洞。实际上，绕过 CloudFlare 对 CloudFlare 的价值可能更高。"

要求使用测试账户，尤其是虚拟专用网络，会引发隐私顾虑（I=2）："我不喜欢连接到虚拟专用网络，让它们监控我的流量.....我可以接受使用代理.....绕过 Web 应用程序防火墙。这还算合理，但把所有流量都通过虚拟专用网络传输，就有点让人反感了。"值得注意的是，先前的研究表明，虚拟专用网络具有欺骗性，并且会损害隐私 [41]。其他人（I=2）指出，设置测试账户可能是一项繁琐又容易出问题的手动工作。例如，一位漏洞猎人回忆说，他难以从一家社交媒体公司获取测试账户："我在 [网站],上发现了一些漏洞，但他们的自动防火墙一直拦截我.....所以我就不再在他们的网站上做研究了。"

最后，两位漏洞猎人提到了地理位置带来的不便；其中一位指出，尽管一些网站的漏洞赏金计划面向国际用户，但这些网站却不允许国际用户注册。有趣的是，另一位黑客抱怨了因地区而异的格式问题："这就是让我开始测试更多 [本地]计划的原因。例如，有个范围我在美国时从未测试过，因为我需要一个地址，而我用了那个地址生成网站。不知为何，有些信息无法使用。"

相比之下，两位漏洞猎人认为琐碎任务很有用。一位表示，配置流程（包括设置测试账户）能让漏洞猎人熟悉系统；另一位则认为，这些琐碎任务本身也可以成为可行的攻击目标，从而实质上扩大范围。第三位则认为测试账户必不可少："你可以入侵很多不同的网站。但如果没有以正确的方式利用漏洞，就很容易搞垮网站。"

A.3 公司内在因素

漏洞猎人考虑的一些因素，源自那些举办漏洞赏金计划的公司本身。虽然没有任何一项被评为首要区分因素，但我们在自由列举研究中识别出三个此类因素：公司的业务领域（FL=2, π=0.021）、公司所在的国家（FL=1, π=0.006），以及公司的知名度（FL=15,π=0.047）。

业务领域 公司所属的业务领域（电子商务、

加密货币、政府等）被两名自由列举研究参与者列为选择参与哪个漏洞赏金计划时考虑的因素。

受访者在解读漏洞赏金计划的业务领域时，通常会考虑实际因素或情感因素。 [20] 从实际角度来看，一位受访者更愿意攻击金融企业，因为他们认为这些企业有更多损失，因此漏洞影响也更大。另一位受访者则避开政府国防部门、执法机构和情报机构；他们认为，这些机构会调查任何参与其项目的漏洞猎人："我倾向于避开中央情报局和联邦调查局这类政府目标……我不想在边境遭到盘问，所以通常会避开它们。"第四位列举实际原因的受访者则不愿攻击区块链公司。这位受访者有几个不这么做的理由："这项技术对我来说没意思……因为这些公司成立时间很短，在如何回应 [沟通] 方面还不够成熟……他们会用加密货币付款……由此产生的税务成本，实在一点都不值。"

在列举情感层面的原因时，一位黑客提到，出于道德原因不愿为航空业工作："我可以告诉你，比如我拒绝为航空公司工作。这是出于道德原因……我坚信我们需要减少对环境的影响。我认为人们应该减少乘飞机出行。"另一位黑客则避开带有社会污名的公司："是的。我觉得真正会带来负面污名的项目只有少数几个，至少在我看来是这样。比如 PornHub 或 Roblox。"

国家 自由列举研究中的一位参与者表示，他们会考虑公司的总部所在国家（例如，Uber 是一家总部位于美国的公司）。受访者中有一人指出，与自己国家的公司合作能带来竞争优势："我觉得这是因为搜索的人比较少，不是因为地点本身，而是因为……巴西以外的人更难注册账号、准备好文件以及完成其他必要事项，才能进入某些地方。"另一位受访者表示，他们更愿意攻击来自自己国家（印度）的项目，因为（1）这些项目的漏洞更多；（2）公司总部设在自己的国家。总的来说，一些漏洞猎人似乎更青睐特定国家的漏洞赏金计划，因为他们认为这样能获得个人优势，而这种优势往往来自地理邻近。

相反的观点是，漏洞悬赏属于远程工作，因此你身处世界何处并不重要。

对公司的熟悉程度 熟悉某家公司或其产品，是选择参与哪些漏洞赏金计划时较常被提及的因素之一（FL=15）。

在谈到这一因素的受访者中（I=9），大多数人表示，他们重视这一点，因为熟悉相关产品有助于他们侦察漏洞赏金计划所涵盖的资产

所涵盖的范围（I=8）。一位漏洞猎人解释说："我喜欢按照网站或应用程序原本的使用方式来使用它……这样就会让你想到可以如何滥用它，或者哪些功能没有按预期运行……如果你已经很熟悉它，这一步就可以跳过。"两位漏洞猎人采取了更具体的策略，会追踪公司的收购。他们认为，新收购的公司最终会被纳入漏洞赏金计划的范围。通过追踪新收购，漏洞猎人可以抢先调查新目标，在这些目标被公开纳入范围之前做好准备。一位漏洞猎人以谷歌漏洞奖励计划[7]为例解释道："谷歌会为其收购的公司支付悬赏金，只要这些公司被收购已满六个月。因此，你可以进行大量侦察，甚至发现漏洞，或者找到你怀疑是漏洞的问题。等它们被收购满六个月后，你就可以提交报告。"最后，一位漏洞猎人提到，他们更喜欢攻击自己亲自使用的产品——并最终确保这些产品的安全。

B 自由列举研究调查问卷

[参与者会通过招募材料进入研究流程，材料中会说明本研究。]展示同意书。[如果未获得同意，则不要继续。]

[主要测量问题：]

- 选择参与哪些漏洞赏金计划时，你会考虑哪些因素？请列出你考虑过的所有因素，即使你并非每次选择漏洞赏金计划时都会想到这些因素。如果你认为还可能记得更多因素，请继续回想。

  请将每个因素分别另起一行。
  [自由文本回答]

- 有哪些问题会让你停止参与某个特定的漏洞赏金计划？这些问题可能与你和计划组织者之间的关系、你正在调查的系统，或其他外部因素有关。如果你认为还有更多可能记得的问题，请继续回想。

  请将每个问题分别另起一行。
  [自由文本回答]

- 参与漏洞赏金项目对你有哪些益处？请列出你参与漏洞赏金计划的所有原因。如果你觉得还能想起更多原因，请继续回想并列出来。

[7] https://bughunters.google.com/

请将每个原因另起一行。

[自由文本回答]

• 你在参与漏洞赏金计划时面临哪些挑战？哪些因素会让参与漏洞赏金计划变得困难？这些因素可能与计划的组织方式、你正在调查的系统本身或其他因素有关。如果你觉得还想得起更多挑战，请继续回忆。你会如何克服这些挑战?

请将每项挑战另起一行。

[自由文本回答]

• 你使用的漏洞赏金平台有哪些最实用的功能？如果你觉得还想得起更多功能，请继续回忆。

请将每项功能放在单独一行

[自由文本回答]

• 您希望平台和项目实施哪些改变?

[自由文本回答]

[人口统计信息和经验。]

• 请用 1 到 5 分评估您发现漏洞的技能水平（1 分表示初学者，5 分表示专家）。

[介于 1 至 5 之间的整数滑块。]

• 请选择最符合您已发现的软件漏洞数量的范围。

– 0-3–
4-6–
7-10–
11-25–
26-50–
51-100–
101-500–
> 500

• 您在漏洞发现方面有多少年经验?

[自由文本回答]

• 请选择最符合您每周通常花在执行软件漏洞发现任务上的时间的范围。

– < 5小时
– 5-10 小时–
10-20 小时 –
20-30 小时 –
30-40 小时 –
> 40 小时

• 请选择最符合您每周通常花在漏洞发现以外的技术任务上的时间范围（例如软件或硬件编程、系统管理、网络分析等）。

– < 5 小时–
5-10 小时 –
10-20 小时–
20-30 小时 –
30-40 小时 –
> 40 小时

• 请选择最符合您认同性别的选项。

– 男性– 女性– 其他–
不愿回答

• 请注明您的年龄。

–
18-29 岁–
30-39 岁 –
40-49 岁 –
50-59 岁 –
60-69 岁 –
> 70

• 请注明您的族裔

– White
– Hispanic or Latino
– Black or African American
– American Indian or Alaska Native
– Asian, Native Hawaiian, or Pacific Islander
– Other

• 请注明您居住的国家/州/省。[自由文本回答]

• 请注明您已完成的最高学历或教育阶段

– 上过一些高中课程，但未获得文凭或同等学历– 高中毕业，获得文凭或同等学历（例如：普通教育发展证书）– 修过一些大学课程，但未获得学位– 贸易／技术／职业培训– 副学士学位– 学士学位– 硕士学位– 专业学位– 博士学位

• 如果您目前是在读学生或已获得大学学位，请注明您的学习领域（例如生物学、计算机科学等）。

[自由文本回答]

• 请选择最能描述您当前就业状况的选项。

– 受雇并获得报酬或盈利– 失业– 照顾家庭– 学生– 退休– 因永久性疾病或残疾而无法工作– 其他 [自由文本回答]

• 如果您目前有偿工作，请注明您当前的职位名称。

[自由文本回答]

• 请选择最符合您 2018 年税前家庭总收入的范围。

– < $29,999
– $30,000 - $49,999
– $50,000 - $74,999
– $75,000 - $99,999
– $100,000 - $124,999
– $125,000 - $149,999
– $150,000 - $199,999
– > $200,000

• 请选择最符合您 2018 年通过漏洞发现和软件测试获得的税前家庭总收入的范围。

– <$29,999
– 30,000 美元 - 49,999 美元
– 50,000 美元 - 74,999 美元
– 75,000 美元 - 99,999 美元
– 100,000 至 124,999 美元
– 125,000 至 149,999 美元
– 150,000 美元 - 199,999 美元
– >20万美元

[未来研究联系同意]

• 请说明您是否愿意让我们就未来研究与您联系。

– 我同意就未来研究与我联系– 我不同意就未来研究与我联系

感谢您抽出时间填写这份调查问卷。您的回答已记录。

如果您想进一步了解我们的研究，请访问我们的网站： [redacted]。研究结束后，我们会在网站上提供已发表研究结果的链接。

C 因素评分研究调查问卷

[参与者将收到招募材料，其中说明了本研究。]显示同意书。]如果未获得同意，请勿继续。]

这份调查问卷分为三个部分：

1. 关于漏洞赏金狩猎相关因素及您对此的看法的问题 2. 关于您参与漏洞赏金狩猎经验的问题 3. 人口统计问题。

在下一部分中，您需要对与漏洞赏金计划相关的若干因素的重要性进行排序。本部分共有 4 个问题。

• 以下因素对您选择参与哪些漏洞赏金计划有多重要？[以李克特矩阵列出所有"选择计划"因素及其定义，格式参照附录 D，顺序随机排列。]量表：极其重要 - 非常重要 - 中等重要 - 一般 - 不太重要 - 重要性较低 - 完全不重要]

• 对您而言，在漏洞赏金计划中工作所面临的以下挑战有多大？[以李克特矩阵列出所有“漏洞挖掘挑战”及其定义，格式参照附录 D，顺序随机排列。]量表：极具挑战 - 非常有挑战 - 中等程度的挑战 - 一般 - 不太有挑战 - 挑战较低 - 完全没有挑战]

• 对你来说，参与漏洞赏金计划的以下益处有多重要？[按照随机顺序，在李克特矩阵中列出“漏洞挖掘的益处”及其定义，如附录 D 所示。]量表：极其重要 - 非常重要 - 中等重要 - 一般 - 稍微重要 - 不太重要 - 完全不重要]

• 对你来说，漏洞赏金平台（例如 HackerOne、Bugcrowd）的以下功能有多大用处？[按照随机顺序，在李克特矩阵中列出“实用的平台功能”及其定义，如附录 D 所示。]量表：极其有用 - 中等有用 - 稍微有用 - 既无用也无益 - 稍微无用 - 中等无用 - 极其无用]技能与经验]下一部分将询问你有关漏洞赏金挖掘经验的问题。

• 您最初是如何参与漏洞赏金计划的？[自由文本回答]

• 按照以下量表，您如何评估自己作为漏洞赏金猎人的技能水平？– 1 - 基础认知（基本知识）– 2 - 新手（经验有限）– 3 - 中级（实际应用）– 4 - 高级（应用理论）– 5 - 专家（公认的权威）

• 您发现过多少个软件漏洞，并因此获得漏洞赏金奖励（包括非货币奖励）？[自由文本数字回答]

• 您参与漏洞赏金计划有多少年经验？[自由文本数字回复]

• 您曾在哪些漏洞赏金平台（即那些承载许多漏洞赏金计划的公司）工作过on?

[自由文本回答]

• 您最近参与过哪些漏洞赏金计划？近来?

[自由文本回答]

• 以下哪个时间范围最符合您通常每周花在漏洞赏金计划上的时间?

– < 5 小时–
5-10 小时 –
10-20 小时–
20-30 小时 –
30-40 小时 –
> 40 小时

• 以下哪个范围最符合你通常每周花在与漏洞赏金无关的技术任务（软件或硬件编程、系统管理等）上的时间?

– < 5 小时–
5-10 小时 –
10-20 小时–
20-30 小时 –
30-40 小时 –
> 40 小时

[人口统计问题]

在下一部分中，你将回答一些人口统计问题。

• 你最认同哪种性别?

– 男性– 女性– 其他 [自由填写]– 不愿回答

• 你多大了?

– 18-29
– 30-39
– 40-49
– 50-59
– 60-69
– > 70

– 不愿回答

• 你目前居住在哪个国家?

– 美国– 印度– 俄罗斯– 德国– 加拿大– 英国– 瑞典– 荷兰– 中国– 澳大利亚– 其他 [自由文本]– 不愿回答

• 您已完成的最高学历或教育程度是什么?

– 上过一些高中课程，但未获得文凭或同等学历– 高中毕业，获得文凭或同等学历（例如：普通教育发展证书）– 修过一些大学课程，但未获得学位– 贸易／技术／职业培训– 副学士学位– 学士学位– 硕士学位– 专业学位– 博士学位– 其他 [自由文本]– 不愿回答

• 如果您目前是学生或已获得大学学位，您的学习领域是什么／曾是什么（例如生物学、计算机科学）？

[自由文本回答]

• 哪项最符合您目前的就业状况?

– 有偿工作或以营利为目的– 失业– 照顾家庭– 学生– 退休– 因永久性疾病或残疾而无法工作– 其他 [自由文本回答]– 不愿回答

• 如果您目前有工作，您的职位名称是？

[自由文本回答]

• 以下哪个范围最符合您家庭在2019年的税前总收入?

– < $29,999
– $30,000 - $49,999
– $50,000 - $74,999
– $75,000 - $99,999
– $100,000 - $124,999
– $125,000 - $149,999
– $150,000 - $199,999
– > $200,000
– Prefer not to answer

• 以下哪个范围最接近您在2019年的漏洞赏金税前总收入?

– < $29,999
– $30,000 - $49,999
– $50,000 - $74,999
– $75,000 - $99,999
– $100,000 - $124,999
– $125,000 - $149,999
– $150,000 - $199,999
– > $200,000
– Prefer not to answer

[未来研究联系同意]

• 您是否愿意我们就未来研究与您联系？– 我同意就未来研究与我联系– 我不同意就未来研究与我联系

感谢您的回复！我们将根据您的回复联系您，邀请您参与本研究的访谈部分。同时，如有任何问题，请参阅我们的网站 [redacted] 。

D 因素完整列表

问题	代码名称	描述	佛罗里达州	μ_r	价值 (π)
Choosing a program	范围：	计划中包含的域名或资产数量。	28	6.10	0.156
	奖励：	预期的货币或非货币奖励（例如周边商品、硬件、订阅）。	36	5.91	0.120
	漏洞赏金表：	管理者设定的奖励规则和范围（例如，严重性较低的漏洞奖励 50 美元，而严重性较高的漏洞奖励 5000 美元）。	16	5.87	0.117
	技术熟悉度：	对资产所用技术的熟悉程度（例如，熟悉 Web 或 iOS 技术）。	22	5.86	0.113
	法律安全港：	计划中的措辞承诺：对于遵循规则和/或明确授权按照规则进行测试。	4	5.71	0.098
	计划声誉：	计划在社区中是否以合作愉快而闻名（即其他黑客对该计划的评价关于该计划）。	15	5.68	0.086
	学习机会：	对资产所用技术不熟悉（例如，有兴趣学习加密技术或 Android）。	1	5.35	0.064
	私有或公开：	私人计划（仅限受邀者访问）与公开计划（任何人均可访问）。	4	5.16	0.048
	对公司的熟悉程度：	项目所属公司广为人知，或者你或你的同行使用该公司的产品或服务（例如，因为喜欢或使用 Uber 的服务而参与其项目）。	15	5.04	0.047
	饱和度：	收到的报告数量，或参与该计划的黑客人数。	8	5.17	0.047
	职业机会：	未来有机会在运营该计划的公司谋求职业发展。	3	4.49	0.027
	公开披露：	问题解决后通常允许公开披露漏洞，且保密协议较为宽松保密协议。	6	4.63	0.027
	Age:	该计划已运行多长时间。	6	4.44	0.023
	业务领域：	该计划背后公司的业务领域（例如，社交媒体、保险、医疗）。	2	4.47	0.021
	国家：	该计划背后的公司位于何处。	1	3.34	0.006
Challenges of bug hunting	响应不佳：	项目管理人员未作响应或响应缓慢。	30	5.39	0.130
	对响应不满：	奖励低于规则承诺的标准（例如，下调严重程度、影响，或对重复漏洞）。	26	5.36	0.120
	范围不明确：	项目范围未明确界定。	3	4.99	0.082
	平台支持不佳	对平台处理问题的方式不满，例如在黑客与项目之间进行调解。	1	5.03	0.079
	重复漏洞：	太多报告被标记为重复漏洞。	4	5.02	0.078
	超出专业范围的资产	资产超出专业领域，缺少某些所需技能。	11	4.87	0.068
	安全资产：	发现漏洞太困难。	5	4.78	0.064
	压力与不确定性：	担心倦怠、工作时社交孤立、收入不稳定等。	5	4.8	0.062
	劳动工作过多：	琐碎任务（例如，验证码、等待超时、代码混淆、设置测试账户）。	12	4.62	0.050
	无聊：	厌倦了参与该计划，或有更有趣的计划启动。	8	4.62	0.050
	缺乏代表性的声誉系统：	黑客的声誉积分无法反映其真实经验，也无法在不同平台之间转移。	1	4.59	0.047
	难以与管理者合作：	漏洞赏金计划管理员难以合作（例如，不尊重人、要求额外工作）。	23	4.48	0.044
	时间不足：	没有足够的时间参与漏洞赏金计划。	2	4.45	0.043
	漏洞披露受限：	限制严格的漏洞披露政策和保密协议可能会阻止你在问题解决或缓解后发布自己的工作成果。问题解决或缓解后。	2	4.49	0.041
	法律威胁：	担心面临法律后果（民事或刑事）的威胁。	2	3.96	0.028
	缺乏沟通或语言技能：	沟通困难，因为你觉得自己缺乏语言技能，并且在沟通时感到焦虑沟通 , etc.	2	3.45	0.014
Benefits of bug hunting	金钱奖励：	金钱补偿。	42	6.31	0.191
	学习：	学习或提升技能。	32	6.18	0.170
	乐趣：	白帽黑客攻击的乐趣或挑战。	20	6.08	0.140
	法律安全港：	只要遵守规则，进行黑客攻击就不会面临法律诉讼威胁。	4	5.96	0.118
	灵活性：	与传统雇佣相比，工作时间安排和地点灵活性更高。	16	5.85	0.095
	职业发展：	与公司建立关系并提升声誉，以获得就业机会和其他工作机会。	11	5.71	0.091
	社区：	漏洞赏金打造了一个黑客社区。	3	5.52	0.071
	利他主义：	为帮助他人而提升网络安全，通过黑客攻击让互联网对所有人都更安全。	5	5.54	0.062
	声誉：	赚取平台声誉积分、积累关注者等。	14	5.36	0.048
	非货币奖励：	非货币补偿（例如周边商品、硬件、订阅）。	4	4.35	0.013
Useful platform features	支付便利性：	以标准化、无烦扰的方式收取付款。	12	6.51	0.156
	报告便利性：	轻松生成、提交和跟踪报告及其状态。	16	6.46	0.142
	查看已披露的漏洞：	平台提供用于查看他人发现的漏洞的界面。	15	6.41	0.137
	私人计划邀请：	访问平台上的私人计划。	5	6.28	0.107
	计划目录：	在一个地方列出许多项目，并提供统计数据、详情等。（能够查看 Uber、PayPal 等项目在同一页面上的统计数据）。	17	6.02	0.068
	标准化规则：	平台正在规范范围、奖励、严重性等的定义方式。	3	5.99	0.063
	社区：	平台努力打造黑客社区。	11	5.77	0.057
	平台奖励：	例如，平台周边礼品、资助差旅。	1	5.89	0.054
	调解：	平台负责解决黑客与项目之间的争议。	13	5.77	0.051
	平台管理的披露：	平台提供的工具/机制，用于公开披露已解决的漏洞。	6	5.86	0.050
	学习资源：	平台提供有关如何进行黑客攻击的免费资源（例如 Bugcrowd University）。	2	5.59	0.047
	声誉系统：	平台为黑客管理的声誉系统。	6	5.70	0.043
	平台分流：	由平台负责分流（例如，由 HackerOne 而非 Uber 对你的报告进行分流）。	5	5.06	0.023
	无：	平台不提供任何实用功能。	4	-	-

表3：因素评分研究中使用的因素，按因素组整理。佛罗里达州：在自由列举研究中列出该因素的参与者人数。价值（π）：因素相对重要性的估计值（详情请参阅 §3.2 ）。列出李克特平均值（μ_r）是为了展示其与基于 LLBT 的分析之间的差异。