Web Hacking 101 中文版 二十、漏洞报告

转载

weixin_34245169 于 2017-03-29 21:15:18 发布 36 收藏
文章标签： 操作系统 运维
原文链接：https://yq.aliyun.com/articles/595493

二十、漏洞报告

作者：Peter Yaworski

译者：飞龙

所以这一天终于来了，你发现了你的第一个漏洞。 首先，恭喜你！ 认真来讲，发现漏洞并不容易，但是有一些不爽的事情。

我的第一条建议是放松，不要过度兴奋。 我知道在提交报告时的极度兴奋感，以及当你被告知它不是漏洞，公司关闭了漏洞报告，损害了你在漏洞平台上的声望，被拒绝的沮丧感。我想帮你避免它们。所以，第一件事是首先：

阅读披露准则

在 HackerOne 和 Bugcrowd 上，每个参与公司都列出了范围内外的程序。希望你先阅读它们，以免你浪费时间。 但是如果没有，请现在阅读。 确保你发现的是未发现的，而不在他们的程序之外。

这是我以前的一个痛苦的例子 - 我在 Shopify 发现的第一个漏洞，如果你在文本编辑器中提交格式不正确的 HTML，其解析器就会对其进行更正并存储 XSS。 我非常兴奋，因为我的挖掘是有回报的。 我无法足够快地提交报告。

太好了，我点击提交，等待我的 500 美元的奖金。 相反，他们礼貌地告诉我，这是一个已知的漏洞，他们要求研究人员不要提交。 然后这个工单被关闭了，我失去了 5 分。 我想钻进洞里。这是一个惨痛的教训。

从我的错误中学习，要阅读准则。

包含细节。之后包含更多东西

如果你希望认真对待报告，请提供详细的报告，其中至少包括：

- 用于查找漏洞的 URL 和任何受影响的参数
- 浏览器，操作系统（如适用）和/或应用程序版本的说明
- 对感知影响的描述。 这个 bug 可能如何被利用？
- 重现错误的步骤

这些标准对于 Hackerone 的主要公司来说都很常见，包括雅虎，Twitter，Dropbox 等。如果你想更进一步，我建议你添加屏幕截图或视频验证（POC）。 两者都对公司有很大帮助，并将帮助他们了解漏洞。

在这个阶段，你还需要考虑该网站的影响。 例如，由于用户和交互数量众多，Twitter 上存储的 XSS 可能是一个非常严重的问题。 相比之下，一个交互有限的站点可能不会将这个漏洞视为严重。不同的是，敏感的网站，如 PornHub 的隐私泄露可能比在 Twitter 上更重要，后者大多数用户信息已经是公开的（而不会尴尬？）。

确认漏洞

你已阅读准则，你已经起草了你的报告，你已经添加了截图。等一下，并确保你的报告实际上是一个漏洞。

例如，如果你要报告公司在其标题中没有使用 CSRF 令牌，那么你是否看到了，要传递的参数是否包含一个像 CSRF 令牌一样的标记，但是标签不一样？

在提交报告之前，我无法鼓励你确保已经验证了此漏洞。 考虑你所发现的重要漏洞，只是让你意识到你在测试时弄错了一些东西，这非常令人失望。

在你提交该漏洞之前，请自行决定是否需要额外的时间并确认该漏洞。

尊重厂商

根据 HackerOne 公司创建的测试流程（是的，你可以作为研究人员进行测试），当公司启动新的漏洞奖励计划时，它们可能会收到大量报告。 提交之后，让公司有机会审查你的报告并回复你。

一些公司在他们的奖励准则上发布时间表，而其他公司则没有。 平衡你的兴奋与他们的工作量。 根据我与 HackerOne 支持者的对话，如果你在至少两周内没有收到公司的消息，他们将帮助你进行跟进。

在你选择这条路线之前，在报告上发布礼貌的消息，询问是否有更新。 大多数时候，公司会回应并让你了解情况。 如果他们并没有留出太多时间，在问题升级之前再试一次。 另一方面，如果公司已经确认了这个漏洞，一旦完成，与他们一起确认修复。

在写这本书的时候，我很幸运地和 Adam Bacchus 聊天，他是截至 2016 年 5 月的 HackerOne 团队的新成员，任首席奖励官，我们的对话真的让我开阔了眼界。 在他的背景中，Adam 拥有 Snap Chat 和 Google 的工作经验。在 Snap Chat 时，他衔接了安全团队，和其他软件工程团队。在 Google 时，他在漏洞管理团队工作，并帮助执行 Google 漏洞奖励计划。

亚当帮助我理解了，运行奖励计划时，有一些分析者会遇到的问题，包括：

噪音：不幸的是，漏洞奖励计划会收到大量无效的报告，HackerOne 和 BugCrowd 都已经写过这个。 我知道我绝对有贡献，希望这本书可以帮助你避免这个问题，因为提交无效报告会为你和奖励计划浪费时间和金钱。

优先级：漏洞计划必须找一些方法来为漏洞修复排序。 当你有多个具有类似影响的漏洞，但报告持续不断进入时，这非常困难，奖励计划面临严峻的挑战。

验证：在分析报告时，必须验证漏洞。 这就是为什么我们的黑客必须提供明确的指示，并解释我们发现的内容，如何重现它以及为什么它是重要的。 只是提供一个视频并不能切中它。

资源：并不是每个公司都能雇得起全职工作人员来运行奖励计划。 有些计划很幸运，有专门的人对报告做出回应，而其他计划则由工作人员兼任。 因此，公司可能会有轮流的时间表，人们轮流回应报告。提供必要信息中的任何信息差距或延误都会产生严重影响。

编写修复：编码需要时间，特别是如果有完整的开发生命周期的时候，包括调试，编写回归测试，分期部署，最后推送到生产环境。如果开发人员甚至不知道漏洞的根本原因怎么办？这一切都需要时间，而我们黑客不耐烦，想要奖励。这就是沟通交流的重点，每个人都需要相互尊重。

关系管理：黑客奖励计划希望黑客能够回来。 HackerOne 已经在文章中写到，在黑客向单个程序提交更多漏洞的同时，漏洞的影响如何增长。 因此，奖励方案需要找到一种方法来平衡发展这些关系。

媒体关系：漏洞可能会错过，花费太长时间才能解决，或者被认为奖励太低，总是有黑客会在 Twitter 或媒体上曝光的压力。还有，这会对分析者造成影响，并影响他们与黑客发展关系和协作的方式。

看完所有这一切，我的目标是真正有助于使这个过程人性化。我有两方面的经验，好的和坏的。 然而最后，黑客和程序员将一起工作，了解每一个面临的挑战，这有助于改善各方面的成果。

奖金

如果你向支付奖金的公司提交了一个漏洞，请尊重他们对奖金金额的决定。

根据 Joaro Abma（HackerOne 联合创始人） Quora 上 的回答：我如何成为一个成功的漏洞赏金猎人？：

> 如果你不同意收到的金额，请讨论你为什么相信它值得更高的奖励。在没有详细说明你为什么相信的情况下，不要索要另一份奖金。作为回报，一家公司应该表示尊重你的时间和价值。

不要在穿越池塘之前喊“你好”

在 2016 年 3 月 17 日，Mathias Karlsson 撰写了一篇很牛并且很棒的博客文章，关于寻找可能的同源策略（SOP）绕过（同源策略是一个安全特性，它定义了 Web 浏览器如何允许脚本从网站访问内容），我在这里包含一些内容。 除此之外，Mathias 在 HackerOne 上有很好的成绩 - 截至 2016 年 3 月 28 日，他发现了 109 个漏洞，在 Signal 上为第 97 个百分比，在 Impact 上是第 95 个，公司包括 HackerOne，Uber，Yahoo，CloudFlare 等。

所以，“不要在穿越池塘之前喊‘你好’”是一个瑞典谚语，意思是你在绝对确定前不应该庆祝。 你可能猜到我为什么说这个 - 挖漏洞并不总是充满阳光和彩虹。

根据 Mathias 的说法，他正在使用 Firefox，并注意到浏览器会接受格式错误的主机名（OSX），所以 URL `http://example.com..`会加载`example.com`，但是在主机头中发送`example.com..`。然后他尝试了`http://example.com..evil.com`并得到相同的结果。

他立即知道了，这意味着 SOP 可以被绕过，因为 Flash 会将`http://example.com..evil.com`视为`*.evil.com`域下。他检查了 Alexa 前 10000 名，发现有 7% 的网站可以被利用，包括`Yahoo.com`。

他创建了一个 WriteUp，但决定做一些更多的确认。 他检查了一个同事，他们的虚拟机也证实了这个 bug。他更新了 Firefox，bug还在那里。然后他在 Twitter 暗示了他的发现。对他来说，Bug 已经验证了，对吧？

并不是。它所犯的错误就是它没有将它的操作系统更新到最新版本。这样做之后，Bug 就消失了。很明显，这在 6 个月之前就有人报告了，并且更新到 OSX 10.0.5 会修复这个问题。

我将其包含在这里来展示，即使优秀的黑客也可能弄错，以及在报告之前确认 Bug 的利用十分重要。

非常感谢 Mathias 让我包含这个 - 我推荐关注它的 Twitter 动态`@avlidienbrunn`，以及`labs.detectify.com`，Mathias 在那里的文章中写到了它。

最后的话

希望本章能帮助你，你最好准备撰写一份“杀手”报告。在发送之前，请稍等一下，真正考虑一下报告 - 如果要公开披露和公开阅读，你会感到自豪吗？

无论你提交了什么，你应该为提供支持做好准备，为公司，其他黑客和你自己辩护。我不是说这个来吓到你，而是作为一些建议的话，我希望我最开始也能知道它。我最开始的时候，绝对提交了可疑的报告，因为我只是想上排行榜，并且助人为乐。但是，企业受到了轰炸。找到完全可重复的安全漏洞，并清楚地报告它更有帮助。

你可能会想知道谁真正关心它 - 去问公司，以及在乎其他黑客的想法的人吧。 这很公平。 但至少在 HackerOne 上，你的报告是重要的，你的统计数据将被跟踪，每当你收到有效的报告时，都会根据你的“Signal”记录数据，范围为 -10 到 7，可以平均显示你的报告值：

- 提交灌水，你会得到 -10
- 提交被拒绝，你会得到 -5
- 提交说明式信息，你会得到 0
- 提交可解决的报告，你会得到 7

同样，谁在乎呢？ Signal 现在用于判断谁能够收到私有计划的邀请，以及谁可以将报告提交给公开的计划。私有计划对于黑客来说，通常都是鲜肉 – 这些站点刚刚进入漏洞奖励计划，仅仅向一部分黑客开放他们的站点。这意味着，潜在的漏洞和较少的竞争。

对于报告给其它公司 – 使用我的经验作为一个警告的故事吧：

我被邀请参加一个私有计划，在一天之内，发现了八个漏洞。 但是那天晚上，我向另一个计划提交了一份报告，得到了一个无效。 这使我的 Signal 到了 0.96。 第二天，我再次向私有公司报告，并得到了通知 - 我的 Signal 太低了，我必须等待 30 天来储存点数，并且其他公司要求 Signal 为 1.0。

真是糟糕！ 虽然没有人找到我在那段时间发现的漏洞，但是他们可能会花费我的钱。每一天我都检查了我是否可以再次报告。 从那以后，我发誓要提升我的 Signal ，你也应该这样！

祝挖掘顺利！