

如何成为一名漏洞赏金猎人

安啦鹿233 FreeBuf 前天

恭喜你！当你决定当一个安全研究员并且准备学习一些新的技能时候，是非常令人激动。我们将在下面收集一些资源来帮助你开始你的安全之旅。请跟着我的脚步往下读。

一、开始阅读

买一些渗透测试和漏洞挖掘的基础入门书。因为给赏金的漏洞通常会包括一些web目标，我们将集中精力先成为一个搞web的黑客，然后再探索其他的领域。

注意：

把兴趣集中在一个领域对于一个黑客是非常重要的。不要想着成为一个全能的黑客而去学习所有的知识，要把精力集中到某一个领域并且持续持续学习。在bugcrowds中最厉害的黑客都有自己专长的领域，但是他们不能黑掉所有的东西。

学习黑客知识是需要很长时间的

下面是俩本入门书：

（1）《The Web Application Hacker's Handbook》

这本书是必读的书并且这本书被web狗们奉为圣经一样。这本书从起点开始，一步步教你安装kali Linux，之后教你如何使用工具和寻找exp

（2）《OWASP Testing Guide v4》

Bugcrowd的Jason Haddix力荐这本书

下面是一些进阶书：

《Penetration Testing》

《The Hacker Playbook 2: Practical Guide to Penetration Testing》

《The Tangled Web: A Guide to Securing Web Applications》

下面是一些给做移动安全的小伙伴的书籍：

《The Mobile Application Hacker's Handbook》

《iOS Application Security》

二、多去练习！

你要确保理解和留住你所学到的东西，这点是非常重要的。有一种非常好的方式就是在模拟的漏洞环境中练习自己的技能。通过模拟方式可以解决现实中遇到的问题。下面是用来练习的网站：

Hacksplaining

<https://www.hacksplaining.com/lessons>

在这个网站里面可以学习到各种web黑客的技能，并且知道他们是怎么样做到的。这其实更像一个真实的演练。非常有用

Penetration Testing Practice Labs

<https://www.amanhardikar.com/mindmaps/Practice.html>

这个网站包含了大量可以被用来练习的应用和系统。在这个网站中可以找到很多练手的系统，这些系统也可以提高你的技能。

三、要经常去读别人的write-ups、poc和YouTube上的视频教程

现在你已经基本明白怎样去发现和利用安全漏洞了，是时候去开始了解更多黑客在各自领域工作的成果了。很幸运的是，安全研究社区通常会乐意分享知识，并且我们也会收集wp和视频的列表。下面是一些网站：

Bug Bounty write-ups and POCs

<https://forum.bugcrowd.com/t/researcher-resources-bounty-bug-write-ups/1137>

从一些成功的赏金猎人手里收集的漏洞报告

Bug Hunting Tutorials

<https://forum.bugcrowd.com/t/researcher-resources-tutorials/370>

我们从Bugcrowd和beyond社区中收集了一些很棒的教程

/r/Netsec on Reddit

<https://www.reddit.com/r/netsec>

Reddit上的Netsec几乎完全是技术文章和其他研究人员的POC，非常棒的资源

JackkTutorials on YouTube

jackk 创建了很多的教学视频，包括csrf, xss, sql注入，目标发现等……

DEFCON Conference videos on YouTube

历年的DEFCON中演讲的视频，非常有用

Hak5 on YouTube

Hak5是典型的硬件黑客，除此之外，他们还有“Metasploit Minute”节目，tips:还有NMAP的教程

四、收集一些常用的攻击工具

工具不能把一枚小白变成黑客，但是这些工具确实非常有用，Bugcrowd推荐了大量工具，大家可以把这些工具尽情的收藏起来

Bugcrowd Researcher Resources - Tools

<https://forum.bugcrowd.com/t/researcher-resources-tools/167>

五、加入到一些社区里面

你需要加入到一个拥有29000个黑客的社区，幸运的是他们中的大多数都非常乐意分享自己当前的研究

在推特上关注白帽子

<https://twitter.com/Bugcrowd/lists/security-researchers/members>

上面一些赏金猎人的推特，大家可以去关注

Join the #Bugcrowd IRC channel

<http://webchat.freenode.net/?channels=#bugcrowd>

这个irc频道里面有超过100位安全研究员

Follow @Bugcrowd on Twitter

<https://twitter.com/bugcrowd>

关注bugcrowd可以看到最新的安全信息

Join the Bugcrowd Forum

<https://forum.bugcrowd.com/>

可以获得更多的资源并且能和更多的安全研究员做交流

六、开始了解更多关于漏洞赏金的事情吧

现在我们几乎到了开始挖掘赏金的时候了，但是首先，我们去了解漏洞赏金猎人是怎么工作的，是如何开始这一切的。这些能保证我们能更加成功。

如何更加接近目标

<https://forum.bugcrowd.com/t/how-do-you-approach-a-target/293>

听取他赏金猎人中的建议，可以帮助你更进一步的接近漏洞赏金

如何写一份超棒的漏洞报告

<https://blog.bugcrowd.com/advice-for-writing-a-great-vulnerability-report/>

他将指导你编写一个很棒的漏洞报告。一份很棒的报告就会有更大的机会获得赏金。

如何写poc

<https://blog.bugcrowd.com/writing-up-a-poc-by-planet-zuda>

poc可以向客户展示漏洞是怎样被利用的和它是如何工作的。这对成功获得奖励至关重要。

如何报告一个漏洞

<https://researcherdocs.bugcrowd.com/docs/reporting-a-bug>

我们建议通过Bugcrowd平台来报告漏洞

漏洞披露政策

<https://researcherdocs.bugcrowd.com/docs/disclosure>

有一些规则必须被遵守。了解赏金计划的摘要和披露政策是非常重要的

了解一位赏金猎人挖漏洞的方法

这展示了@jhaddix 在15年DEFCON的演讲，这个视频里面介绍他是怎样成功挖掘到漏洞的，非常有用。下面是他的github和视频

<https://github.com/jhaddix/tbhm>

https://www.*****.com/watch?v=VtFuAH19Qz0

七、放手去干吧

是时候去放手去干了！当你是个新手的时候，最好不要试图去找特别流行厂商的漏洞，如果初学者试图去找特斯拉，facebook，Pinterest等这些公司的漏洞话，会感受到很大挫折，因为这些流行厂商会非常注重安全并且会收到很多漏洞报告

挖一下只给积分的厂商（原文里面的Kudos似乎是一种积分）

<https://bugcrowd.com/programs/points-only>

集中精力挖一挖那些被其他人忽略厂商。虽然那些厂商不会给你金钱奖励，但是在Bugcrowd会给你积分奖励。这是很好的开端并且也可以向Bugcrowd展示你的能力。当你提交足够多有效的漏洞之后，即使这些漏洞来全部来自于只给积分的厂商，我们也会邀请你去参加私有众测。私有众测是邀请制的，并且会限制参加的人数。私有众测意味着更小的竞争，也会获得更多的漏洞奖励。

八、持续的学习和交流

就像我之前提过那样，掌握黑客技术是一个长期学习过程。这个领域充满激情！这里总是有新的文章和论文去学习，和兴趣相投的人一起参加会议或者多参加一些线下的沙龙，和他们一起寻找新的机会。

挖漏洞是进入信安行业最好的方式，这也可以成为你的职业。挖漏洞也可以为你带来额外收入，也可以提高你的技能，认识更多的人，甚至可以重塑你的职业。

记住，做事要专业，对人要和善。这虽然是一个小众的社区，但是我们也会关注每一个人，你永远不会知道遇到谁

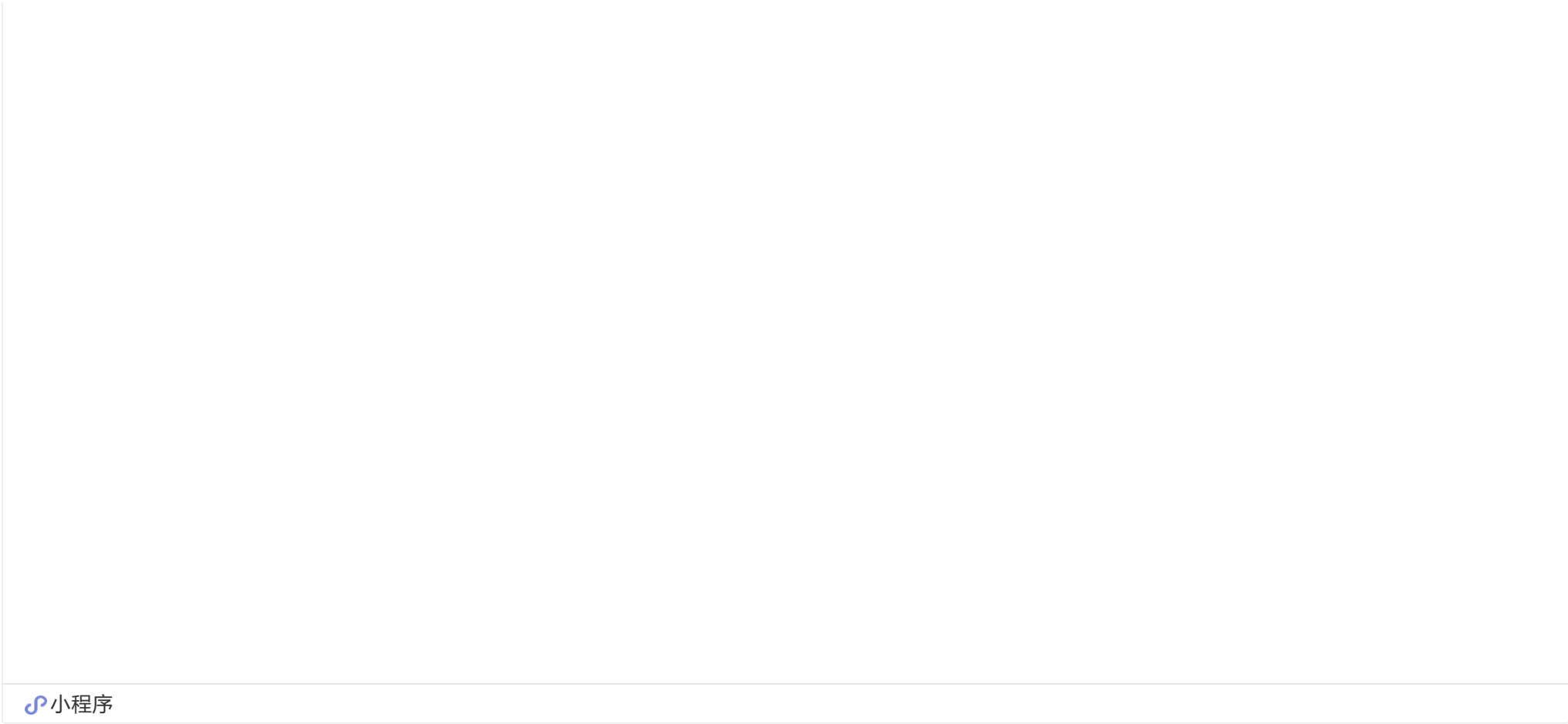
翻译参考来源: Researcher Resources - How to become a Bug Bounty Hunter


<https://forum.bugcrowd.com/t/researcher-resources-how-to-become-a-bug-bounty-hunter/1102>

*本文作者: 安啦鹿233, 转载请注明来自FreeBuf.COM

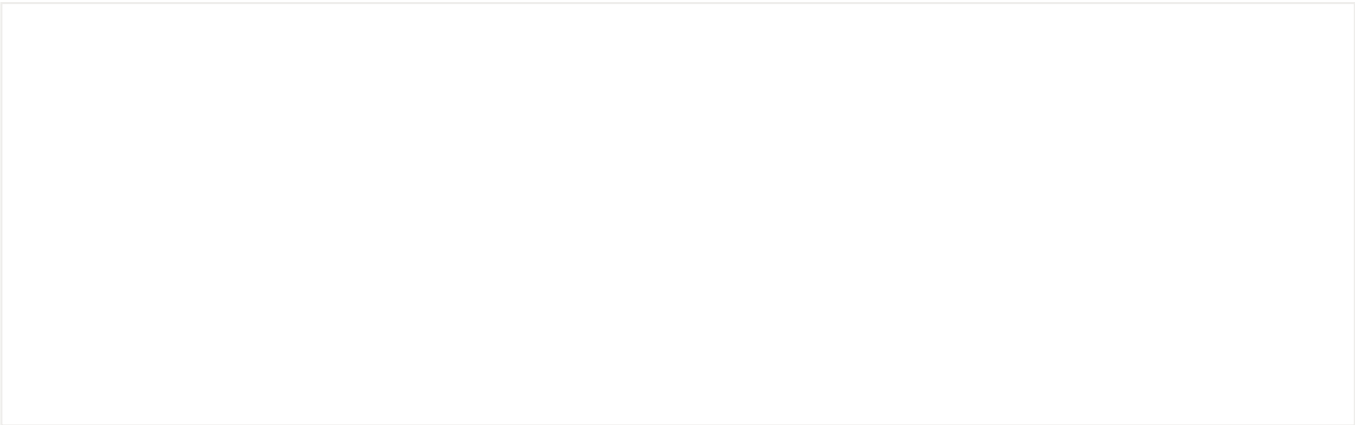
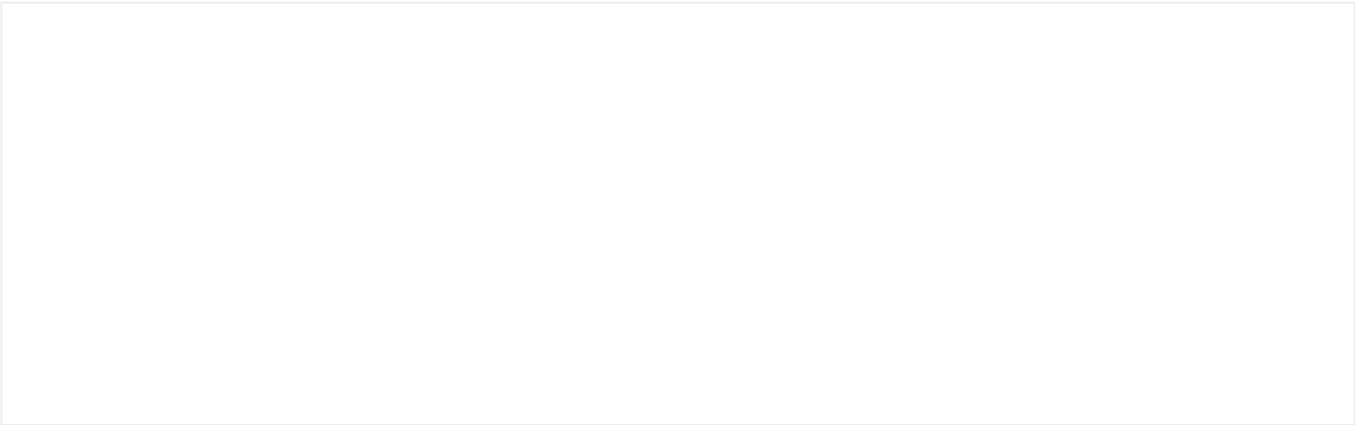
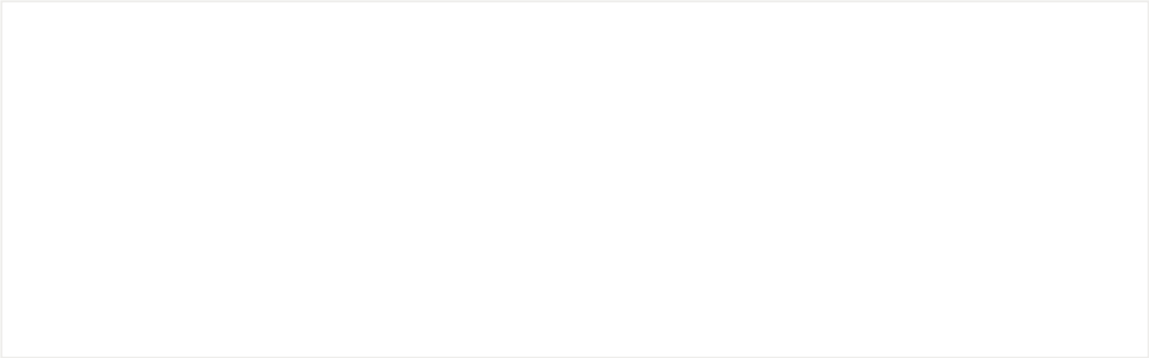


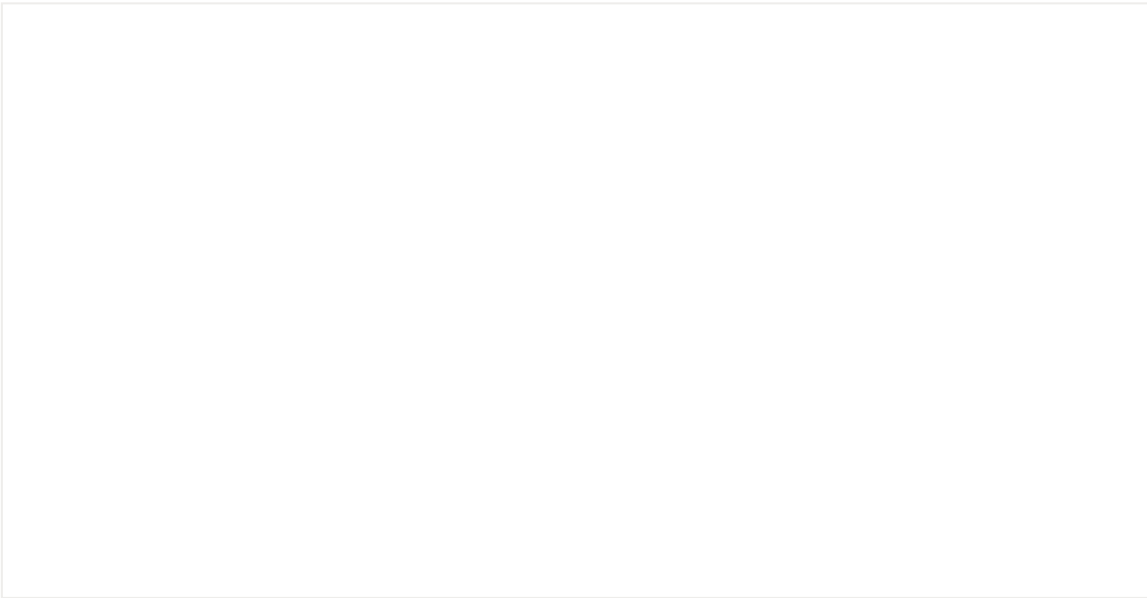
FreeBuf+小程序: 把安全装进口袋



 小程序

精彩推荐





阅读原文