Web安全研究人员是如何炼成的？

mss**** / 2018-05-28 23:47:29 / 浏览数 26209 技术文章 技术文章 顶(2) 踩(2)

先知原创作者翻译：原文链接

您是否有志于推动Web安全技术的发展，并与信息安全社区分享相关知识呢？在这篇文章中，我将为读者分享与Web安全研究有关的各种建议，当然，这些建议一方面是来

以“黑”为生

大部分研究都是在现有的技术的基础之上，百尺竿头更进一步的，所以，研究工作的第一步就是熟悉当前的技术水平。为了实现这一目标，最快的方法是找一份相关的工作，

我建议有兴趣的读者采用以实践为中心的研究方法，首先从OWASP Broken Web应用程序开始下手，继而转向更具实战性的安全挑战活动，比如hackxor.net，这样的话，就可以通过HackerOne和BugCrowd上难度和回报相对较低的挑战来练手，待

当然，网络上面也有大量免费的在线资源，包括我们站点提供的The Burp Methodology系列文章，HackerOne站点的Hacker101系列文章，以及OWASP测试指南。至于书籍，我推荐读者阅读《WebApp Hacker's Handbook》和《The Tangled Web》。

不要止步不前

一旦开始全职黑客工作，自然能学到很多东西，但一段时间之后，您的专业技能就会停滞不前，除非努力的劲头一直保持不减。

要知新，更要温故

为了不被小伙伴甩在后面，所有业内人士都会密切关注行业专家、新闻聚合和安全会议来跟踪行业的最新动向。然而，如果一门心思追逐最新技术的话，往往会遗忘和忽视大

每当读到优质博客文章时，请细心通读整篇文章。这样做的话，往往能够找到一些宝贵的、被遗忘的信息花絮。例如，这里有一篇关于DNS重绑定的文章，是RSnake于200

此外，仔细阅读文档还可以帮助您避免浪费时间来重复其他人已经完成的工作，例如十年后重新发明CSS攻击。换句话说，一些研究文献真的很难找到，所以偶尔的“重蹈覆辙

力求多样性

要想把各种线索串起来并找出别人错过的机会的话，收集不同来源的信息是至关重要的。首先，不要只阅读安全方面的内容——您很快就会发现，文档手册也可以作为漏洞利

除此之外，还要努力使自己的经历多样化。

在进行安全咨询黑盒测试的过程中，可以接触到各种各样的外部和内部Web应用程序，而这些应用程序则是在漏洞奖励计划中很难遇到的。但是，由于时间限制的缘故，你很

没有任何想法是愚蠢的

最糟糕的陷阱之一，就是仅仅认为某想法行不通就不去尝试，例如，觉得某些想法“别人肯定早就想到了”或“这想法太蠢了，肯定不行”。实际上，我就曾经为此付出过沉重的

迭代，发现，分享

迭代

最简单的入门方法是找一些有前途的研究成果，通过混合其他技术构建新方法，然后将其用于某些实际目标，看看是否有什么有趣的事情发生。

例如，这篇关于CORS配置错误的文章指出了一种有趣的行为，并且表示这种行为很普遍，但并没有探讨它对个人网站的影响情况。

于是，我把这个概念应用到了漏洞赏金网站，因为我可以在这些网站上合法地探索它的影响，并且设法绕过各种可能的缓解措施。在此过程中，我以常见的开放重定向漏洞技
‘null’ origin technique），并探索了缓存中毒的可能性。

在这个过程中，根本无需借助于遥不可及的顿悟或卓尔不凡的技术知识，然而，由此产生的演示文稿和博客文章仍然很容易被大家所接受——毕竟，我付出的努力是大家有目

发现

虽然对他人的工作进行迭代不失为一个好方法，但现实是，好像任何一个角落都可能发掘出相应的研究宝藏，无论是相对路径覆盖还是Web缓存欺骗。我的观点是，个人经验

例如，2011年，我试图破解addons.mozilla.org使用的CSRF保护机制。尽管我可以绕过令牌检查，但这显然是不够的——他们采用的安全机制还会验证Referer头部中的主
Host头部来确定当前网站的主机的，而这个头部恰好可以通过X-Forwarded-Host头部来覆盖掉。换句话说，将其与Flash头部注入漏洞相结合的话，就有可能绕过CSRF检查

之后，通过阅读Piwik的密码重置函数的源代码，发现了如下所示的一行代码：

```
$passwordResetLink = getCurrentUrlWithoutQueryString() + $secretToken
```

我们可以看出，Piwik使用的是PHP语言，众所周知，该语言的路径处理方式是非常搞笑的：如果通过http://piwik.com/reset.php/foo;http://evil.com
请求重置密码，就会生成一个包含两个链接的电子邮件，并且秘密令牌将被发送到evil.com。这个想法果然是有效的，为此，我不仅获得了一笔赏金，并且还为后来的发现奠

第三个也是最后一个“面包屑”就是Piwik修补这个漏洞的方式——他们用getCurrentUrlWithoutFileName()替换了getCurrentUrlWithoutQueryString()函数。这意味着，我
Host头部，也就是说，我可以轻松生成恶意的密码重置电子邮件。事实证明，这项技术同样适用于addons.mozilla.org、Gallery、Symfony、Drupal以及其他一些网站，
Host头部发动有效的攻击。

我之所以啰里啰嗦地阐述上面的发现过程，是希望能够帮助读者揭开安全研究的神秘面纱：许多研究成果，并非从天而降，凭空产生的。从这个角度来看，核心技能（超越

分享

最后，与社区分享您的研究也是至关重要的。这将有助于提高您的知名度，并可能说服雇主为自己分配更多的研究时间。除此之外，它还能帮助您避免浪费时间，并促进进一

请不要仅仅因为没有突破性的发现、两个徽标和一个演示文稿就认为一个技术或想法不值得分享——不要太过苛求，有啥就发布啥好了（当然，理想情况下是发表到博客上

在共享研究时，至少应展示一个应用于实际应用程序的技术示例。否则的话，一方面不利于人们的理解，另一方面，容易让人怀疑它是否具有实际价值。

最后，演讲对于吸引更多观众来说非常有用，不过需要注意的是，不要把太多的时间花在重复过去的演讲上面。

结束语

关于安全研究，我自己还有很多东西要学，所以，我希望能在几年后重新回顾这个话题，并提供更多的线索。另外，我希望其他研究人员提供不同的观点，并期待从他们的

最后，对于正在寻找安全研究的入门读物的读者，我已经准备好了一份博客清单——多年来，我一直从中汲取营养。祝您好运，玩得开心!

上一篇：VPNFilter分析 下一篇：DnsLogSqlinj Tool...

1. 2 条回复


雨苁 2018-05-29 21:17:25

这个不必多说,把这些书吃透你就是神
http://www.ddosi.com/2017/10/26/book-online/

0 回复Ta


风之传说 2018-05-31 17:19:11

可以的。就是要多点S操作。

0 回复Ta

目录