零基础如何挖漏洞—安全小课堂第三十三期

京东安全应急响应中心 2016-11-11

点击上方**蓝字**关注

安全小课堂第三十三期

由漏洞反查知识，或是先学基础再找漏洞都是可行的办法，最终选择哪一个，因人而异。掌握最基础的知识之后，拿到工具就可以先进行一个自动化的扫描。验证漏洞的过程很有趣，可以让你如痴如醉。这时你会主动的去查资料，将基础知识一点点学起来。

本期我们邀请到
JSRC白帽子
Sven、王松
大家欢呼
ヽ(*°▽°*)ノ

/ 01 /

豌豆妹

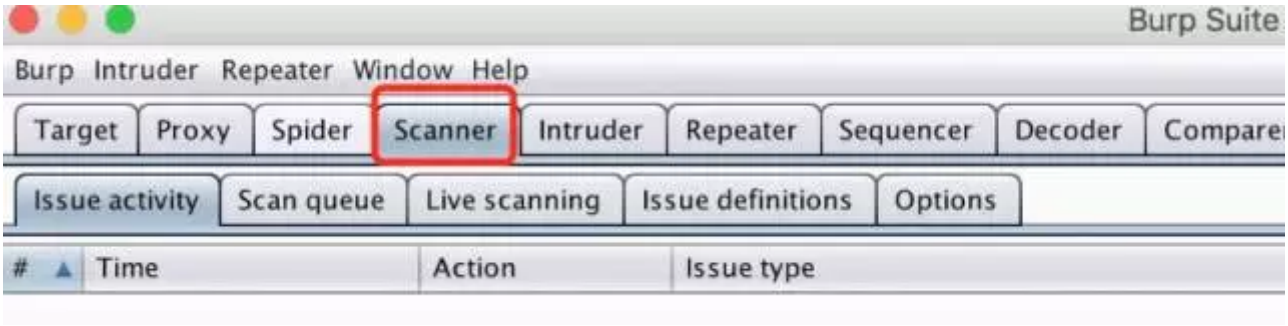
(。·∀·)ﾉﾞ嗨~小伙伴们又见面啦。
请问，挖掘漏洞的需要必备技能有哪些呢？

小新

我们先提一个假设：有网络基础知识or无安全基础，这个还是很有必要的。我个人的

专长在 web 方面，所以就从web 开始咯~我们首先要了解基础知识，只是可以先不用理解太深。

个人一开始学安全是兴趣驱动的 。由漏洞反查知识，或是先学基础再找漏洞都是可行的办法，最终选择哪一个，因人而异。掌握最基础的知识之后，拿到工具就可以先进行一个自动化的扫描。我们就直接从burp 的自动扫描开始吧，http://www.freebuf.com/sectool/21446.html，burpsuite_pro_v1.5.20破解版下载。burp 中有scanner ，功能最适合小白。设置代理，那些有网络基础的人，肯定是ok的。



打开代理之后，在scanner 中开启自动扫描，就可以坐收漏洞了。当然最终的结果还是需要验证一下才能提交的。验证漏洞的过程很有趣，可以让你如痴如醉。这个时候，你会主动的去查资料，将基础知识一点点学起来。

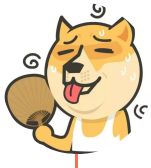
哆啦A梦

个人觉得burp的漏洞扫描插件，真心不咋样，不过如果你能改下它的插件就秒变神器，这时你需要去学习java基础，然后就能自己写插件了。工具只是人的能力进行的复制，但没有人的智能与灵活性。

/ 02 /

豌豆妹

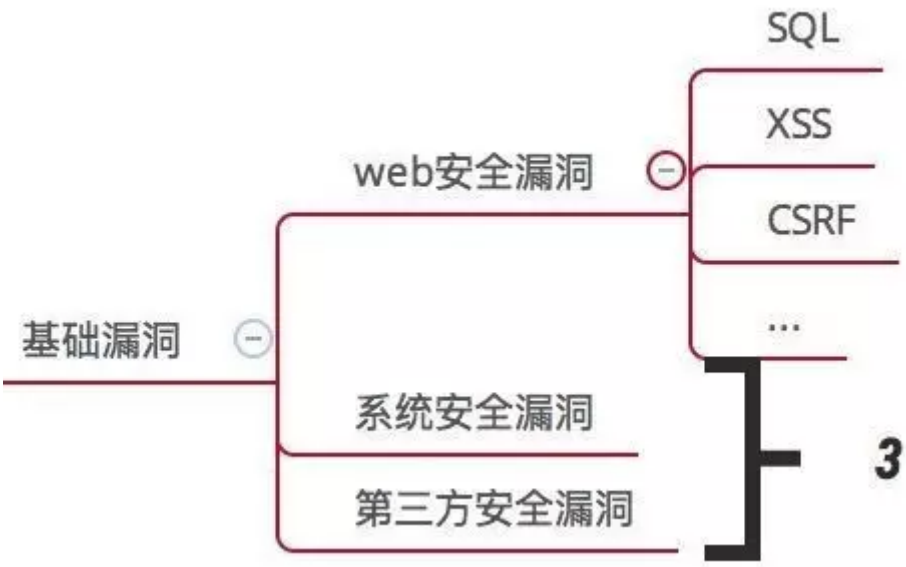
分享下挖掘漏洞必备技能的学习顺序吧。



柴可夫斯基

学习顺序，第一建议是，将web基础搞明白，也就是下图：

第二个，掌握基础漏洞的原理与测试方法。建议将《owasp 渗透测试指南》这本书作为基础来学习。看的时候可以分两遍，第一遍粗略看一下，了解结构，第二遍再细读。根据基础的漏洞类型在各大安全网站中找方法。

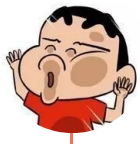


/ 03 /

豌豆妹

挖掘漏洞的基本步骤能介绍下吗？

小新



“工欲善其事，必先利其器”。我们首先是需要找到好工具。http://sectools.org/这个是工具谱，大家可以选择喜欢的工具。web手工测试推荐burp suite，扫描工具AWVS，手工测试类的还有Fiddler可以作为备用，系统安全方面可以使用metasploit、open-vas，扫描类可以使用 nmap、zmap。
在最开始时因为害怕困难而去选择简单的工具，对于后续发展没有好处 。这里可以参考一本书《Kali Linux渗透测试的艺术》，把主要的测试顺序学习一下。重点是学习基础的步骤。

/ 04 /

豌豆妹

挖掘漏洞的思路能分享下么。

葫芦娃

思路方面，针对不同的SRC，其策略也不同 。每个SRC 在安全建设的阶段不同，漏洞的类型也不同 。我这里有一篇在个人公众号上曾经发布的关于技巧总结的文章，可以参考一下：http://t.cn/RfyX2NN。

/ 05 /

豌豆妹

挖掘漏洞时，需要注意哪些误区呢？

小新

误区方面，就需要提到关于漏洞定级的问题。漏洞的定级需要与业务的重要程序相关，这个是比较客观的定级方法。可能有前期刚入门的兄弟不太理解。一个网站如果是花了2000块制作出来的，只是为了展示内容。在上面有sql注入的漏洞，最高只能定个中危， 甚至有可能是低危。简而言之，漏洞的定级 = 是否存在敏感数据+漏洞利用成本+漏洞的危害面积。另外，最重要的是，千万注意停止点，保护自身安全，行业内已经有太多案例，安全是为了让自己更好，让家人更好。

豌豆妹

好哒~谢谢小伙伴的耐心解读哟~这个话题要说起来可是内容太多，咱俩先暂时告一段落呢，下周见！

微信公众号：jsrc_team
新浪官方微博：
京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂