安全小课堂第四十七期【网站安全检测常用工具简介】

京东安全应急响应中心 2017-03-10

亲，戳上面的**蓝字**关注我们哦！

网站安全检测常用工具简介

古语有云：工欲善其事，必先利其器。作为一个白帽子，除了一个好用的电脑以外，一些趁手的渗透工具也是必不可少。作为有着多年的网络安全经验的资深白帽子平时做渗透测试时会使用哪些工具呢？JSRC 安全小课堂第**四十八期**，我们邀请到了知名网络安全团队河图安全的大漠、Vern、苏黎世师傅为简单介绍一下他们常用的工具。感谢**大漠**、**Vern**、**苏黎世**师傅的分享，以及 JSRC 白帽子苦逼司马，DragonEgg，沦沦、Ant、iDer、PX1624的讨论。

讲师简介

河图安全：知名网络安全团队，团队成员包含了十名具有多年网络安全经验的白帽子，曾获得JSRC 2016年度最佳白帽子团队称号。
参与本期分享的大漠、Vern、苏黎世都是JSRC核心成员、知名白帽子。

对网站进行安全检测是否一定需要使用工具呢？

京安小妹

这个问题的答案是肯定的哈，实际上电脑是工具，浏览器也是工具，所有用到的安全测试相关的都是工具哈，都能帮助进行安全测试。

对工具肯定是需要的，就跟coding需要ide环境一样。有些基本工具是渗透必须要的。

讲师：河图安全

使用工具有什么利弊呢?

京安小妹

使用工具的好处：

工具能大大提升挖洞效率，来弥补手速的不足。

使用工具的弊端：

第一是不可控，比如使用综合扫描工具对目标进行扫描时，线程太大、发出的包都是攻击包，容易导致目标异常。

比如高并发容易造成服务器负载升高，对可用性有一定影响，还有就是一些错误的

测试方法会造成插入一些垃圾数据，还有就是触发安全设备告警等。

第二个是容易被发现，大漠也提到了触发安全设备告警。

还有一点就是就是工具的覆盖面也并没有那么广，流行的主动扫描工具 并不能完全覆盖所有业务的功能点。

来路不明的工具可能会存在后门，所有要小心啊。并且自动化的扫描工具也不容易发现业务逻辑类型的漏洞。

白帽子观点：大批量发包还容易被拉黑。

讲师：河图安全

对网站进行安全检测的常用/必备工具有哪些呢?

京安小妹

这个太广了我分下类型哈信息收集类型、漏洞检测类、漏洞利用类型。

信息收集类也有很多：比如子域名收集的，还有各种搜索引擎，Google，shodan ， censys等。

常用的话，一般就是burp，sqlmap ， python写的一些脚本，还有一双勤劳的双手。。。

其中burp（全称burpsuite）是代理抓包工具，并且提供api接口调用，支持

python和java插件开发。理论上讲，只要开发插件的能力够强，只需要burpsuite即可以检测所有的漏洞。

Sqlmap是sql注入自动化检测工具，支持的数据库类型包括MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, HSQLDB and Informix。

并且sqlmap和burpsuite还可以结合使用。

burp只是一个辅助渗透测试的利器 关键还得靠使用者的分析。

白帽子观点：还是burp+手法比较靠谱，现在不少网站都有防护，使用sqlmap会直接被禁IP。

讲师：河图安全

白帽子提问

除了wvs、appscan、nesuss还有什么免费的一键自动化扫描器么？

综合扫描器有很多的，比如 arachni、awvs free、Netsparker Community Edition、ZAP。arachni也是免费版综合扫描器中排名第一的，可以试试。

白帽子观点：跟awvs类似，arachni是自动化的扫描神器，有命令行，也有web形式的。起一个服务器端，N多个人可以使用进行扫描各自的任务。

讲师：河图安全

有什么办法避免使用工具带来的弊端么?

京安小妹

根据具体情况选择合适的测试方法，使用无毒无害的工具。
1，加入自己的一些思考，优化工具的测试方式。2，在正确的时间使用正确的工具。

白帽子观点1：自动化的工具，尽量在线下环境中使用，线上环境使用的话要慎重考虑服务器承载能力、系统功能等等。

白帽子观点2：自己写，打造一款最适合自己的渗透组件工具。

白帽子观点3：分布式扫描可以尽可能的不触发一些防御规则，弊端是工程太大。

讲师：河图安全

白帽子提问

某个系统上线之前，如何能最大化的挖掘到系统存在的问题。除了黑盒测试，白盒代码审计之外?

1.测试人员从系统设计阶段接入、了解开发过程，熟悉业务流程，只有掌握了足够多的

信息，才能发现更多的问题。

2.支持agent的扫描器，在目标系统上部署扫描器agent，可以和扫描器进行联动，比如测试只支持delete的sql注入，就能够被这种模式发现。

非常赞同第一点，对系统设计文档进行评审经常能发现问题，这也是SDL中一个环节。把线上流量拉过来，收集整理去重、归纳出业务接口，然后一个个排除。

白帽子观点1：通过镜像流量来挖洞.

白帽子观点2：这个方案小公司估计有点麻烦，得考虑很多成本问题。

白帽子观点3：其实给开发人员开发安全插件或者给QA开发浏览器插件，其实都可以啊。

讲师：河图安全

还有什么补充吗?

京安小妹

最后提醒初学者，安全工具是双刃剑，既能发现问题也能搞破坏，不要随意使用安全测试工具在非授权的情况下对目标进行测试，不要越过法律红线。

讲师：河图安全

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文