27 世界那么大，我想去看看 - Web安全简介

更新时间：2019-10-16 16:38:37

> 合理安排时间，就等于节约时间。——培根

这一次，跟大家聊一点敏感词：安全。其实这个词于我自己是有挺多感触的，从 10 年开始，我可能算是最早在网络上进行安全测试公开课分享的那批人，也是很多安全测试的视频让我最早被很多测试人包括一些大佬们所认识，更是作为 “普通白帽子” 亲历了 “袁炜事件”、“乌云事件”，算是某种程度上见证了 “白帽子圈” 的兴衰，所以其实有很多话想说，但是又不知从何说起。

可以说，由于国内互联网的迅速发展，性能测试、自动化测试的技术实力已经提升到了一流与二流之间，那么安全测试毫无疑问可以算是测试领域内的软肋。不管是所谓的测试架构也好、总监也罢，除了一线互联网以外，其他的公司几乎完全没有系统完善的安全测试，最多就是基于工具扫一扫而已。

曾经很多公司还依赖于 “乌云模式” 帮助自己进行一些安全方面的众测，但是随着 16 年的 “乌云

妄议，这是不是安全的倒退，但是，至少在现在，安全已经不再让大家陌生和忽视，就像乌云的联合创始人说过的：

> 之前很长时间，我都以为是乌云创造了历史。但现在我知道，是历史选择了乌云。那个时代互联网爆炸式发展，而网络安全没人重视。网络犯罪行为越来越多，但没人告诉大众，他们究竟是如何被侵害的。面对那个坠落的世界，需要有人站出来 —— 这个喊出皇帝新衣的小孩，恰好是我们。人们总在争论乌云的模式是否极端、披露漏洞是否要授权，但在那个时代里，我们别无选择。

额，似乎说的有一点跑题，也确实是这个主题给了我自己不少的感触，我们书归正传，先来聊聊什么是 Web 安全。

官方一点来说，Web 安全测试，是有关验证 Web 应用的安全服务和识别潜在安全性缺陷的过程。当然，我们可以更简单一点去理解，安全的本质是信任。这就好像说，我们新买了一套房子，因为不信任开发商，我们换了个防盗门，认为屋子里很安全，这是基于我们对防盗门厂商的信任，可是如果我们觉得防盗门厂商可能会留一把我们的钥匙，那就不安全了。

所以几乎所有 Web 安全的产生都是源于我们的系统信任和研发所有客户的输入内容，但是实际上总有一些不怀好意的 “黑帽子们” 是不按常理出牌的。于是便有了如家等酒店开房信息泄露、360 出现任意用户修改密码漏洞、携程网数据泄露、12306 用户数据泄露等等一系列由于安全问题爆出的影响。

似乎看起来比较遥不可及，说个我自己经历过的。大概几年前，我帮某新兴电商网站进行众测，结果非常轻松的用绕过的方式拿 0.01 元买到了价值上万的商品。所以相比较起功能测试来说，生产上有遗留的功能问题，最多就是体验不好，业务失败，损失一些用户，本质上问题还不是非常大；如果有安全漏洞，那往小了说，可能会造成资金的损失，大一点可能服务直接瘫痪，再大一些可能会导致服务器资源被黑客利用，被敲诈勒索，甚至是客户数据的丢失和泄露，很可能直接导致业务完全无法运作，带来巨大的损失。

哪怕 “警惕如我”，都在手上漏掉过通过三方鉴权的安全漏洞，直接被黑客刷走了若干奖品。

生活中与安全息息相关的操作，现在更是层出不穷，比如：

- 为什么我们登录的时候经常要求我们输入一个验证码？

- 为什么支付宝之类的支付接口都是 https?
- 为什么银行转账之类的操作都是两步确认?

那么，在 Web 层面都有哪些典型的安全漏洞呢?

我们简单给安全漏洞分一下类，其中最常见的漏洞，就是命令执行类的安全漏洞，这里包含 SQL 注入、XPATH 注入、OS 命令执行、缓冲区溢出等等，再有就是客户端攻击的漏洞，我们前边说过的绕过、大家比较耳熟的 XSS 攻击（跨站脚本攻击），CSRF 攻击等等。这是大家稍微熟悉一点的，另外，有一部分就是大家不太熟悉的，认证授权类的漏洞，这里边覆盖了验证机制和加密授权等各方面的漏洞，这部分虽然出现的漏洞较少，但是比较零散，而且漏洞也会比较严重。还会有一些其他的漏洞，例如设计缺陷、逻辑漏洞等等，都需要我们综合考虑。

可能有些同学对于安全有一些认识和了解，包括很多同事、同行和学员都会有这样一个疑问：既然有一些现成的扫描工具可以用，那我们还需要学习手工安全测试么？直接拿过来结果砸过去不就好了?

实际上，在正式的安全测试过程中，基本上都是自动化审计与人工测试相结合的。一方面，自动化审计的工作也需要安全测试人员利用自己的专业知识，对扫描的结果进行分析和判断，并不是所有扫描结果中的漏洞都是真的安全漏洞，知名如 Appscan、Webinspect 都会有各种错报的现象；另一方面，需要根据安全测试人员的经验，找出一些扫描工具没有办法发现的安全问题，例如，前边提到的认证授权类漏洞、设计缺陷等等。

然后呢，我们往俗气一点说，安全测试是目前互联网行业非常缺少的一项技术能力，虽然在实际工作中，很少需要测试人员全职进行安全测试，但是一旦拥有安全测试的技能，在薪水和级别上都会有一个不错的提升。

最后，我这里需要给大家提个醒，安全测试可以学习，也可以去做，但是不要 “踩过线”。要进行安全测试的实际操作，要不然，用自己搭建一些开源的或是可以用于安全测试练习的系统（WebGoat 等），或者就用自己工作上正在测试的项目，万万不要直接在互联网上觉得哪个网站不错，就任意的去施展自己的攻击才华。

举个可能不太恰当的例子：比如你看到别人家房门没有关，于是你就跑进去了，拿走别人的钱包和手机，并且照个照片，然后在他门上贴个字条告诉对方，你家门没有关啊，你看这个照片就是证明，顺便还评论下别人的钱包现金也太少了，你觉得要让人家情何以堪？所以，纵然安全测试很重要，仍然要约束自己的行为，做一个**合格且合法**的安全测试工程师。

精选留言 1

欢迎在这里发表留言，作者筛选后可公开显示

土豆稀饭

终于等到web安全篇了，顶顶顶

2 回复 2019-10-16

千学不如一看，千看不如一练