我的安全之路——Web安全篇

原创

giantbranch 于 2017-04-08 21:41:34 发布 18052 收藏 26

分类专栏： 有感而发 安全之路 文章标签： 如何学习web安全

本文链接：https://blog.csdn.net/u012763794/article/details/69787883

write in my dormitory at 9:47:05 Friday, April 7, 2017 by giantbranch（其实当初想横跨web跟二进制的）

————致即将毕业的自己。

这是我的安全之路系列第一篇，敬请期待第二篇：**《我的安全之路——二进制与逆向篇》**

总览

大一：基本都在学习学校的课程，C语言，C++，高数啊，不过分数还可以，在大一复习周还在php3小时光速入门呢

大二：web开发，大概在下学期5月份这样子开始web安全

大三：开始去参加比赛,刷题，学习各种ctf需要的知识，后期也接触了逆向

大四：继续学习二进制知识，分析各种漏洞，当然也有搞web，还参加世安杯，蓝盾杯总决赛，铁三数据赛

前情回顾

我并没有像别人那样小学初中或者高中就已经在搞安全，那时候我们都在应试教育，或者沉迷游戏不能自拔吧，初高中我也是沉迷游戏，那时候也中病毒什么的，最多也会搞个360杀杀毒，重装系统什么的，自从有了第一次重装系统，之后一言不合就重装系统，其实当时也想过别人是怎么入侵电脑，入侵网站的，不过可能是环境和机遇的原因没有走上这条路。

后来高考要选专业了，其实当时是一心想考个好分数，也没考虑过选个什么专业，再过几天就要选专业了才去考虑的，选专业当然要自己喜欢的，我左思右想，我小时候不是很喜欢拆解各种小电器吗，也许对硬件会感兴趣，第一志愿报了电子科学与技术（而且后面的有网络工程啥的，就是没有信息安全），最后由于分数没够，没能去到那专业，由于是服从分配，分配到了有点关联的专业——信息安全专业，其实来之前对这个专业基本没多少了解的。

Web开发之路

到了大学也不是一上来就沉迷信息安全学习，不能自拔，因为其实我们一开始跟软工上的课都是一样的，那就老老实实学C语言，高数，什么的。那又是如何接触到Web的呢，那是因为加入了计算机协会，其实在我们这组织并不是很厉害，只不过是当时有个活动是给协会会员讲课，我选择去讲网页开发，当时找了个Dreamweaver开发网页的教程，可以说是可视化的Web开发，非常的简单，从此就走上Web的坑咯。

其实大一还加入了电脑义修队，哈哈，一言不合就重装电脑，在大一快结束的时候被另一义修队员拉到一个校园微信公众号的一个团队去搞微信开发去了，自此走上web开发之路。什么查天气，发定位测距离就是入门的一些小实例，挺好玩的。之后在公众号里面开发了查校园网上网参数，失物招领，基于WeCenter的微信问答系统等。

这公众号凭借着师兄开发的查电费功能迅速“走红”，学校某个部门领导就发现了我们这个技术团队，所以后来就给这个部门开发了3个web，我写后台，当时主要是为了学习，也没用什么框架，确实也是学到了东西。

但是由于没用框架，当时无论是教程还是自己都是没有安全意识，触发了一个重大事件——自己开发的web网站被人报wooyun了。其实就是新手开发网站存在最经典的问题，我的问题存在于新闻详情页存在sql注入，更加坑爹的就是使用root连接的数据库，服务器直接被拿下咯。除此之外，还有明文储存密码。

web开发陆陆续续干了一年，对接下来的web安全之路的作用无疑非常巨大，可以说是web安全之路的“催化剂”。

Web安全之路

由于那次入侵，我就尝试根据WooYun提交的报告，复现了一次报告者的入侵过程，收益良多。

况且由于我的专业是信息安全，由此踏上了Web安全之路。

之后在合天网安实验室“疯狂”做实验（那时候i春秋还没出来呢），还申请当了内测人员（新出的实验免费做，不过要写评价，还有实验中存在的问题等），之后邀请了合天网实验室来了一次见面会(http://www.hetianlab.com/html/news/Geek-jnu.html)，之后还搞了个合粉俱乐部，再之后就向合天投稿了一个实验(http://www.hetianlab.com/expc.do?ec=ECID9d6c0ca797abec2016092116115600001)从而成为了一位实验设计师了。

其实最重要的就是参加比赛，一有机会就报名参加，每次都是我们3个人报名，我们3个随便谁一看到有比赛，就马上相互提醒要报名，不管题目难不难，至少也得看一下，不行就赛后看一下writeup咯。

之后就边比赛，边刷CTF的题，还有安排其他一些知识点的深入学习，比如sql注入，xss等漏洞的学习，也深入python的编程。

还有的话就是我也是买了很多书的，看的web安全的书也是比较多了，看了一些后就没看了，主要是看了之后发现这个知道，直接翻到下一页了，一下就看完了。

其实还有一个就是参加了学习的开放实验，那时是metasploit和XSS，两个实验可以选，都是要自学，跟着做出点成绩来，后来我就设计了个逆向与二进制初探的一个开放实验指导给老师，师弟师妹你们有福了。

其实很难具体讲清楚，看我的博客就知道我大概的学习轨迹了。

但是！！！每个人都不一样，学习资源日新月异，知识也会更新，以上提供的仅作为参考，希望你走出更加牛逼的自己