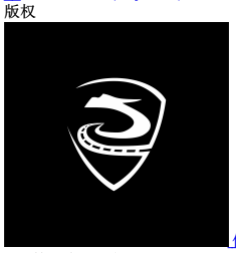
某个小伙伴的信安之路

转载

myh0st@信安之路 于 2022-03-30 09:06:50 发布 12 收藏
分类专栏： 信安之路 文章标签： web安全
原文链接：https://mp.weixin.qq.com/s?__biz=MzI5MDQ2NjExOQ==&mid=2247485900&idx=2&sn=4e6553f19acecf048fd62502c176660a&chksm=ec1e39e4db69b0f2b168343406fd4375685d59b21171fa579c64776a46ba534ff322a8c45f01&token=511550348&lang
版权



Web安全篇

write in my dormitory at 9:47:05 Friday, April 7, 2017 by giantbranch（一个当初想横跨web跟二进制的菜鸡）

————致即将毕业的自己。

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 php 3 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=ECID9d6c0ca797abec20160921161156000001

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

二进制与逆向篇

因为参加比赛，搞论文，就没什么时间写了，今天刚好答完辩，终于有时间开始写我的安全之路下篇了。虽然是5月20日写的，感觉写得太差，主要是技术也不厉害，就没发出来。既然写了，就发出来吧，现在看看有什么完善的再现在发出来吧，确实这个内容比web安全的经历难写，一个是文章题目的原因，另一个是自己接触也不长，经历不足，技术差。

为什么去搞逆向和二进制了

在上一篇中我说过，我参加了一些比赛，由于比赛的题目除了 web，misc 还有逆向和 pwn 等，其中逆向和 pwn 的分值的占比都是比较高的，尤其在高端的比赛中，逆向和 pwn 的占比也是很高，在国外更是如此。

艰难入门之路

一开始就只是自己的孤军奋战，那基本就只能借助与搜索引擎：如何学习逆向，学习逆向的网站有哪些等。

那么你看到的基本都是首先肯定要有 C，C++ 的编程能力，基本的都要理解透彻。（后来你回发现，当你逆向程序，在汇编层面去理解 C++ 的时候，你会理解得更为透彻。）

之后就是汇编语言， 先从 x86 汇编学比较好吧，好书就是王爽的《汇编语言》，当时学校的《汇编语言程序设计》的课我也没选（因为我的那个群的学分已经满了，难得浪费分去选了，自学还可以挑战自我嘛），就看这本书，其实当时学得也并不是很好，用汇编编程的量不足（可以说几乎没编过汇编的感觉，感觉就编了几个 helloworld），选了的话可以强制性地逼你去编。

再之后就自己编程序，查看其汇编代码进行理解。来到这一步，就可以尝试去做一些 crackme 了，或者破解一些简单的软件，这样就差不多入门了。

入门之后还是迷茫啊

发现自己进步得非常慢，几乎没啥大的进步，应该是量还不够，而且由于各种原因，不能完全将时间只投入到逆向的学习与提高上面（这个点是个非常值得注意的点，这是使我有点后悔的一个点，做事一定要专注！【其实当时好像也迫不得已】）。实习的时候是搞渗透的，只能空闲的时间学习逆向，还有就是去参加比赛，但是我还是去当了一个 web 选手，线下比赛很容易就浪费了很多时间。

可以算入了逆向的门，之后一直想玩 pwn，但确实难以入门啊，你要懂得汇编，调试，栈，堆等基本知识，你还要安装工具，你才能够理解和实践。重要的是当时的 pwn 的资料很少，我也没有大牛指导啊，搜索引擎搜到的资料也不多，可能当时没用谷歌吧，所以用好的搜索引擎也很重要，看英文资料也很重要，其实当时国外有个博客有个很好的系列文章，很多国内文章的原型来源于它

> https://sploitfun.wordpress.com/

直到有一次，实习的时候刚好遇上公司的对外培训，我也去水了一下，跟安全研究员交流了一番，才拿到了一些资料，就更加激励我走上这一条路。

实习完就想转岗做安全研究员，当时面试的时候还没分析过什么漏洞，就学过蒸米的那个教程，面试官就叫我尝试去分析二进制漏洞，当时就搞了

ftp 的缓冲区溢出漏洞

> https://www.52pojie.cn/thread-557521-1-1.html

IE 漏洞 (CVE-2012-1889) 分析与利用

> https://www.52pojie.cn/thread-596064-1-1.html

IE 漏洞 CVE-2014-0282 漏洞分析（这个是分析完 ftp 后分析的，收获良多，报告没发出来，踩了挺多坑的），也算了入了 windows 的漏洞分析的门了。

之后就是参加一些 web 偏多的比赛，还有准备毕业设计，还有这段时间一直在颓废了，不禁想问自己：为什么能够颓废这么久呢？

未来之路

现在已经选择了安全研究员之路了，虽然苦逼了一点，但是既然选择就热爱吧。

为什么想去当安全研究员呢，因为自从来到这个信息安全专业，我就基本确定走信息安全的道路了，后来也了解到tk教主就是安全研究员做起的，虽然并不是每个人都能成为 tk，但是有机会还是可以试一下嘛。

逆向的资源就看那个逆向开放实验的指导书吧（这个是为学校写的指导书，也不方便开放）

关于 pwn 的一些好的博客，资源等（其实有些我收集了还没怎么看呢）

【更多等待大家补充了】

> http://angelboy.logdown.com/

> https://wizardforcel.gitbooks.io/sploitfun-linux-x86-exp-tut/content/

> https://github.com/scwuaptx/HITCON-Training

> https://github.com/Kung-Pao-Chicken/ctf

https://github.com/shellphish/how2heap

https://pwnable.tw/

http://pwnable.kr/

https://etenal.me/archives/972#B1

https://heap-exploitation.dhavalkapil.com/