SRC漏洞挖掘思路浅析

2016-09-12 魔方安全科技Sven 京东安全应急响应中心

0x01 背景

笔者关于漏洞挖掘方面的积累，说多不多说少不少。观点正如前几日的一篇文章《分享的多少影响人生的高度》，主要目的是抛砖引玉，希望能形成一个积极分享的学习环境，促进大家一起共同进步，同时为社会安全贡献出一份自己的力量。关于因诈骗而死的大学生事件，实话说笔者看到文章时几乎无法控制自己的情绪，因为毁掉的不是一个人，是一家人（笔者生于农村家庭，那种感觉是所有的希望破灭，一家人生无可恋）。每一个人都是社会的一分子，每一个人都可能会遇到欺诈。真正的理解我为人人，人人为我。

0x02 思路

思路本身是指对能力的利用方式，尽可能的发挥能力形成最大输出。对于“思路与能力谁更重要”的辩论从来没有停过，此次笔者也不想引发这种争论。个人观点是能力与思路并重。根据不同的背景进行微调，如学习初期以能力为重，技巧为辅，后期反之！

思路在能力想当的情况下非常重要。反之，比拼思路没有任何的意义。笔者在挖掘过程中总结出三个要素，第一广度，第二深度，第三认知。三者相辅相成才能输出最大的成果。

0x03 三要素

第一 广度

广度是指漏洞挖掘的范围，如果有漏洞的系统不在你的挖掘范围之内，找不到漏洞也是很正常的情况。最明显的案例是之前发现的一个小系统，这属于比较重要的数据库管理系统，在公网开放给用户使用。这个系统没有做任何的防护，常规漏洞、逻辑漏洞、业务漏洞全部都有，仅此一个系统在当月就贡献了近5000元的奖金。可见在信息收集阶段和跟进阶段的重要性，如何最大范围的发现系统，就成了找到更多漏洞的基础。

第二 深度

深度是指发现无法直接使用、看到的功能上出现的漏洞。此类漏洞是在已知的广度范围之内，需要特殊操作之后才能发现。有两个案例，第一个是之前发现的一个批量遍历退货的严重漏洞，漏洞隐藏的并不算深，特点是需要买家真正的付款，卖家发货之后才能操作。第二个是一个接口，需要在第一步验证手机号，然后才能对相应的信息进行操作。关于此类型的漏洞还有很多，还有类似于只有商家才能进入的系统等等。案例中的第一个漏洞在当月提供了4000元奖金，第二个漏洞在当月提供了6000元的奖金。可见深度的重要性，是在有限的范围之内发现更多的问题。

第三 认知

认知是对于漏洞本质的认识与理解。前几日刚写过一篇关于这方面的文章，有兴趣者可以到我

微信（geeksven）中查看《找不到漏洞？其实它在你心里！》。

核心点是SRC关注的是能造成业务损失的问题，这里不用漏洞两个字的原因是很多人对于漏洞的认识已经固化，只有别人告诉他们这是个漏洞，他们才会意识到。如果没有人说这是个漏洞，就算问题在他眼前，他也找不到。这是一个思想上的鸿沟，创造者与拾人牙慧者之间的本质区别！

总结一句话，一切能给SRC业务造成损失或安全威胁的问题，都可以称之为漏洞。而定义的等级是对业务影响的能力，不是漏洞本身的等级。用这种思维方式去找问题，你可能创造出自己的漏洞类型。

0x04 其它

有很多人可能都经历过，自己认为很严重的问题却不被SRC重视。笔者曾经在SRC提交过一个SQL注入漏洞，奖金200元。经过深入的思考后发现，SRC之所以有这种反应，是因为当前的漏洞对业务本身造成的影响很小。对业务影响的大小才是风险的真正等级。这也是一个SQL注入200元最本质的原因。

笔者希望白帽子兄弟们也能明白，大家都是安全圈内的技术人员，更多的是应该惺惺相惜，互帮互助，为自己、公司、社会、国家更安全而努力。