安全小课堂五十七期【白帽子漏洞挖掘指导】

京东安全应急响应中心 2017-05-12

点击上方蓝字关注我们！！！

FOLLOW US

白帽子在挖掘漏洞中有很多疑问，什么样的漏洞价值高？挖洞需要掌握哪些方面的能力？白帽子在挖洞过程中最关心哪些问题？JSRC **安全小课堂第五十七期**，我们来聊一聊白帽子挖洞中的一些问题，本期小课堂邀请到了**小旭、土夫子**师傅进行分享。感谢JSRC白帽子们的精彩讨论。

从审核的角度出发，两位师傅觉得什么样的漏洞算是严重级别漏洞？

京安小妹

肯定是对业务影响比较大、范围比较广的，如果纯粹是技术难度比较大但对实际业务影响较小，从审核角度来看，一般是不会被定为严重级别的。

比如发现了一处比较隐蔽的SQL注入，但最终确认该数据库是测试数据库，那可能对业务影响相对较小。

讲师： 小旭、土夫子

那挖掘严重级别漏洞需要具备什么样的能力呢?

京安小妹

基本的漏洞发现能力是要有的，再者是脑洞要大思路要广，还有就是多关注核心业务，因为核心业务一有漏洞一般影响会比较大些。当然还有Blood_Zer0师傅说的运气。

讲师：王柯、Chu

白帽子提问：蹭wifi进内网算啥级别?

这个得看他们内网安全域的划分。

白帽子提问：对企业邮箱弱口令这块怎么看?

弱口令这一块的应对，不怕神对手，就怕猪队友，安全意识培训、强制密码策略、使用外部公开的社工库进行匹配，一个不能少。弱安全策略下有弱口令，强安全策略下也有强的弱口令。

白帽子观点：感觉这个问题 好像目前没有哪个企业可以完全杜绝，弱密码这个没辙，特别是企业越大越没辙 。

强的弱口令，就要看我讲的社工库匹配了。好像没有好办法完全杜绝，只能是尽量吧，再加上惩罚措施，让员工对此产生敬畏之心。

能否从案例中分享一下挖掘严重漏洞的过程与思路?

京安小妹

我分享一个之前提交到某SRC的业务逻辑漏洞的案例：这个漏洞是一定概率下的批量用户密码重置漏洞，虽然不是100%能重置用户密码，但是由于其用户量非常之巨大，所以影响的用户量还是非常可观的。当时该厂商正在当天的大新闻的风尖浪口上，大家都在热议的问题，他们已经快速应急处理完毕。这时我对他们的重置密码功能进行进一步研究，发现"通过回答安全保护问题"这种方式，可以非常轻松地在非常用设备上把我朋友的帐号进行密码重置，登录上去截个图发给他看，他被震惊到了（嗯，他也是做安全的），毕竟这是涉及钱的业务，发给他的截图就显示了余额呢。

当时提交的时候，写了3个批量验证思路（提交晚了，可能就是因为写这个花了太多时间 /(ㄒoㄒ)/~~）

思路1：针对只设置一个问题的用户，针对出生地这个问题，以深圳为例，将三大运营商深圳的号码段查出来，到该业务的网站上重置密码，遇到安全保护问题为出生地的账号，就填深圳。其它城市同样可以这样来操作。肯定有一定几率是正确并可重置密码的。当然可能还需要配合使用代理IP等方式来绕过单IP多次尝试等风控机制。

思路2：针对只设置一个问题的用户，针对出生地这个问题，找带地址的社工库（快递等带地址信息的泄露数据），取手机号码，对应的地址（主要是城市名，当然区名，街道名，镇名，村名也都

息的泄露数据），取手机号码、对应的地址（主要是城市名，当然区名、街道名、镇名、村名也都是可以的），进行重置密码，几率会比上一个思路高了不少。

思路3：针对出生地、家庭成员姓名、生日这些问题，找带户籍信息的社工库，基本就包含了家庭成员的各种基本信息，比如有的群里，就有人收费查户籍信息的。

以上这些思路都是需要有相关资源储备（比如代理IP、社工库等）才能进行验证利用的（然而我并没有相关资源，毕竟这些都是违法的玩意儿），所以提交的时候也只是提交了验证思路。
可惜的是，我提交的时候，对方回复已有白帽提交，被捷足先登了，但是当时他们并没有很快就把漏洞修复了，过了相当长一段时间才修复，在我看来，应该把该重置密码的方式直接从代码中注释掉就OK了，这样的漏洞其实应该从需求分析阶段就把它扼杀在摇篮里了，毕竟注册该帐号都是需要绑定手机号码的，重置密码通过手机短信验证码的方式会比前面这种方式安全得多（尽管短信验证码也并非无招可破）。

讲师： 小旭、土夫子

大家对对JSRC的漏洞判断标准有什么建议?

京安小妹

对于严重级别的漏洞，可考虑增加额外现金奖励比如AFSRC、ASRC、TSRC、VSRC等都有额外现金奖励。
判断标准目前是V4.0对吧，我觉得挺详细的、挺好的了。

讲师： 小旭、土夫子

白帽子观点：可以来点啥sql xss waf挑战赛之类的。一方面提升白帽子积极性，二方面测试自身waf产品规则的缺陷。

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