漏洞跟踪

0x00 背景

银联的系统庞大，使用的应用、操作系统、网关以及主机极为复杂，运维人员在对系统进行日常维护难免会出现疏漏之处，无法对整个银联系统的漏洞做到面面俱到的关注。

于此同时，当今世界各款产品的漏洞正在不断被挖掘，许多也被公开披露到一些漏洞发布平台，如wooyun以及补天等。为了保障银联交易系统的稳定运行以及维护持卡人和商户的利益，我们需要一种实时获取多方漏洞信息的手段，这种手段即为**漏洞跟踪**。

0x01 目的

通过使用网络爬虫获取漏洞发布平台对于各产品的漏洞公开信息，将其信息分门别类地存储于数据库内，并通过合理的手段对其进行挖掘，总结出漏洞种类的比例，漏洞随日期的发现情况，不同种类公司或者产品所发现的漏洞比例，漏洞的详情数据，不同公司漏洞的修复情况，得出我们需要重点关注的漏洞信息，为安全室日后的室内培训以及系统安全加固提供方向。

0x02 现状

现已通过Scrapy抓取wooyun公开的漏洞信息，并将其各项信息存储进mysql数据库中存储。现在已爬取所有2015年wooyun中已公开的各漏洞详情。

0x03 后续工作

1. 利用d3.js等数据展示工具将我们需要的数据分布信息以图表形式展现出来。
2. 根据漏洞的具体分类以及分布情况来确定未来我们进行app以及web漏洞扫描的重点。
3. 获知哪些常用软件近期出现漏洞较为频繁，来确定我们运维时需优先升级打上补丁的软件。