- **京东篇**

8.1.0 一般 sql 注入怎么发现触点的，从源码阐述 sqlmap 如何测试注入点的。
8.1.1 masscan 扫描端口时靠什么检测，为什么这么快？请详述.
8.1.2 你写过哪些小工具，你为你使用过的工具做过什么修改.
8.1.3 如何提高采用 python 编写的扫描速度，谈谈对 GIL 锁的了解.
8.1.4 你觉得你发现的那个漏洞影响比较大.
8.1.5 常见的 web 漏洞有哪些.
8.1.6 有没有玩过硬件安全，研究程度如何.
8.1.7 反爬虫，如果是你如何进行反爬虫，如何绕过反爬措施。使用无头浏览器被检测到了，如何绕过
8.1.8 nmap 扫描如何进行扫描。发包与协议，握手和不握手，哪些协议握手，哪些不握手. 如何不直接接触目标服务器探测对方端口是否开放
8.1.9 有没有自己编写过 yara 扫描模块，如果要解决扫描{k1:v1, k2:v2, k3:v3} ，保证同时在 k1 中的 v1 里出现特定值，k2 中出现 v2 特定值，以及 k3,v3。怎么实现
8.2.0 xss 什么原理，如何自己实现一个 beef 类似的 xss 平台. 既然这样实现，面临的跨域如何解决?
8.2.1 ip 频率限制, ip 信誉度模型？
8.2.2 SCTP 协议是什么？如何使用 SCTP 优化网络？