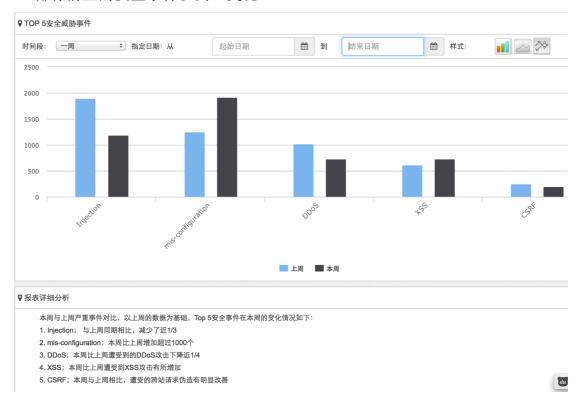
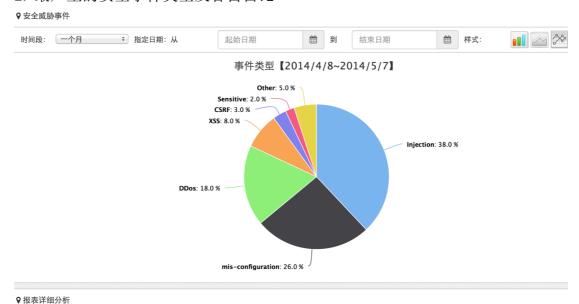
2014.04 网银安全事件评估报告

在过去的4月份,从以下几个方面综合分析网银遭受的安全事件。

1. 排行前五的安全事件以同比变化:



2. 最严重的安全事件类型及各自占比



从4月8日开始,到5月7日,从受控的日志内发现严重的安全事件按数量的占比排列如下:

- 1. Injection异常;系统检测到占总安全事件比例达38%的威胁来自SQL Injection或Script Injection的攻击
- 2. mis-configuration;通过对访问状态码分析,发现有26%的威胁来自于黑客对服务器特殊文件(如index.php.bak, admin, index.rar, etc)或服务器错误配置导致访问到不存在的页面
- 3. DDoS;以客户访问的源始IP结合访问日志分析,找到了18%的访问属于DDoS攻击
- 4. XSS; Cross-Site Scripting, 跨站脚本攻击占比达8%
- 5. CSRF;跨站请求伪造占比达3%
- 6. Sensitive Data;来自于对敏感信息获取的请求异常占2%

3. 各种安全事件在每个 Web 节点上的分布状况

