安全小课堂第七十二期【GitHub信息泄露】

京东安全应急响应中心 2017-09-08

GitHub平台对大部分程序员来说已经再熟悉不过，很多开发人员通过GitHub提交代码进行研究、学习已经养成了习惯。企业内开发人员众多，很多程序员存在安全意识不足的问题，将公司源代码提交到GitHub上,GitHub在给开发者带来方便的同时，一个小小的疏忽也带来了一系列安全隐患。JSRC **安全小课堂第七十二期**，本期小课堂邀请到了爱上平顶山、Cliver老师进行分享。同时感谢JSRC白帽子们的精彩讨论。

GitHub的作用是什么?

京安小妹

GitHub 的用处很多，通常我们可以用来做以下的事情：
(1).代码托管：方便随时随地同步代码，再也不用带着U盘到处跑了。
(2).学习优秀的开源项目：减少重复造轮子的时间，学习其他人的优秀设计思想、实现方式。
(3).多人协作：同一个项目多人协作开发，发挥每个人擅长的部分。
(4).搭建博客、个人网站或者公司官网：可以为项目建立静态主页，也可以建立命名特殊的 Repository 来建立个人静态网站，不用忍受各大博客网站的约束与各式各样的广告。
(5).个人简历：如果你在Github上很活跃，维护有自己的开源项目，那么你找工作将是一个非常大的优势，现在程序员的招聘很多公司都很看中你 GitHub 账号，某种意义上 GitHub 就可以算是你的简历了。
(6).其他：GitHub 能做的远不止这些，比如用来做数据存储、预览3D渲染文件、社交平台等，主要是看你想如何去使用它。

①GitHub是一个免费的远程仓库，可以把代码放到GitHub存储。
②GitHub还是一个开源协作社区，通过GitHub，既可以让别人参与你的开源项目，也可以参与别人的开源项目。简单点就是把代码托管到网上。
③同时也能star喜欢的项目，fork并pull为他人项目打补丁、还能配合hexo做个人博客等等。

讲师： 爱上平顶山、Cliver

GitHub给开发者来方便的同时还会存在哪些安全隐患问题?

京安小妹

①账号密码泄露(公司邮箱、联系人通讯录、办公vpn等)
②核心算法泄露(系统、软件被破解)
③API_KEY泄露(利用接口进行攻击等)
④服务器key、配置泄露(危害服务器安全)
⑤源码泄露(代码被审计,可能被人搞0day)

GitHub 的私有仓库是需要花钱才能使用，大部分程序员使用的公共仓库，这就意味着任何人都能查看到你上传的文件，如果文件里包含敏感信息，那么将会造成以下安全隐患：
(1).如果是公司各种应用服务的登陆凭证，黑客可以轻而易举的进入内部人员访问区域，并获取到内部才能获得的信息。
(2).如果是公司的 web 项目代码，黑客可以通过代码审计，更容易的挖掘出漏洞来攻击公司网络。
(3).如果是公司的核心技术代码，可能会被商业竞争对手盗去，对公司造成经济上的损失。
还有就是有些公司直接使用开源项目的代码进行部署，没有对项目代码进行安全审核，如果该开源项目中包含了攻击者的恶意代码，也将会对公司造成安全隐患。

：

讲师： 爱上平顶山、Cliver

站在企业数据安全的角度如何防止GitHub信息泄露?

京安小妹

①开发人员安全培训，代码上传GitHub前做脱敏处理。
②企业建立自动化扫描机制，使用脚本或平台。
③管理制度进行完善，制定源代码安全管理制度，从制度上约束。

GitHub 信息泄露的根本原因是由于程序员的安全意识不足造成的,所以我们可以采取以下几点来预防:
(1).制定《源代码安全管理条例》，在没有经过公司允许脱敏的情况下，对私自上传敏感信息的员工，可以进行相应的处罚与安全教育，并强制员工删除 GitHub 上泄露的信息。
(2).定期对员工进行安全培训,公司的安全部门可以通过出版安全刊、安全培训视频以及线下安全课堂来进行员工的安全教育，提高程序员的安全意识。
(3).部署自动化 GitHub 扫描工具,安全意识再高也会存在疏忽的情况，所以我们还需要进行自动化工具来巡检 GitHub 信息，防止遗漏。

：

讲师： 爱上平顶山、Cliver

是否有检测GitHub信息泄露或者脚本推荐?

京安小妹

①https://github.com/lianfeng30/githubscan
②携程的github监控GithubScan
③https://github.com/sea-god/gitscan (需要改下源码,加上登录)
④https://github.com/metac0rtex/GitHarvester
等等..
建议最好做成定时任务自动化执行。

(1).gitrob
Ruby 开发，该工具将遍历所有公共组织和成员存储库，并匹配出包含敏感或危险信息的文件与文件名。
https://github.com/michenriksen/gitrob
(2).weakfilescan
Python 开发，基于爬虫，动态收集扫描目标相关信息后进行二次整理形成字典规则，利用动态规则的多线程敏感信息泄露检测工具，支持多种个性化定制选项。
https://github.com/ring04h/weakfilescan
(3).GitPrey
Python 开发，根据企业关键词进行项目检索以及相应敏感文件和敏感文件内容扫描的工具。
https://github.com/repoog/GitPrey

讲师： 爱上平顶山、Cliver

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