

谈一谈github泄露—安全小课堂第十五期

京东安全应急响应中心 2016-06-24

安全小课堂第十五期

安全领域有一种无坚不摧叫做github在手，俺啥都不会照样轻松搞穿你的内网...本期我们来聊一聊github泄露。

本期邀请到了来自唯品会安全专家先知晓狼、前百度和赶集网安全专家xsjswt'。今儿还有京东安全的小伙伴一起参与讨论哟~

1



豌豆妹

git泄露漏洞是如何被引起的呢？



葫芦娃

据我了解，主要从两方面可引起git泄露漏洞：

- 1) git工具以或相关git项目托管平台自身缺陷问题，存在漏洞，可被恶意利用。例如之前github被曝由于一个coder对Rails的mass-assignment（批量赋值）使用不当造成可以被轻易的篡夺任何代码库的权限。但这种情况比较少，首先利用成本较高，其次相关平台已相对成熟，可利用的漏洞较少。
- 2) 企业内部开发、运维人员安全意识不足，将公司源代码提交到git项目托管平台上，而且没有进行敏感字过滤，其中包含的大部分账号密码都以明文形式直接提交，这是主要原因。这里就不多说了。



哆啦A梦

现在使用git来管理代码、项目是一种趋势。git可以深度的结合到开发流程的各个环节中。各个公司基本也都有在自己内部搭建有gitlab来管理。其实对企业内部员工的安全培训，安全意识的要求，一直都是我们甲方安全工作开展过程中很头疼的一点，就算我们在公司内部纯粹暴力使用技术手段封禁github本身，还有其他的项目共享、托管平台。可以说，git只是这类企业内部信息泄露的一个集中体现点，信息泄露并不仅仅局限在github上。

2



豌豆妹

能说说git信息泄露的分类么？



小新

由于git本身主要用于项目、代码的管理。所以基本上在github上泄露出来的大多数属于：1. 项目源码与配置；2. 项目说明；3. 公司内部技术资料。



小丸子

在我看来，git信息泄露可以从两个方面来分类：

- 1) 数据类型不同区分：产品代码、密码密钥、基础设施信息、客户信息公司业务数据、公司内部信息；
- 2) 涉及系统类型：业务生产系统、业务测试系统、内部IT系统、内部知识管理系统等。

3



豌豆妹

快来说说git信息泄露的危害~

哆啦A梦



危害嘛，那自然最直接的就是可能暴露数据库。其次，看到了项目源码，对于有心的人来说，无论是黑猫还是花猫，都可以通过分析源码，来提高对目标站点的业务流程的了解，降低挖洞/入侵的难度，搜集公司的内部信息等。再次，会向广大IT技术群体暴露自己公司开发人员的智商下限。

小新



对，尤其是内部系统。如果是暴露那些对外开放服务的系统源码、文档，起码公司内部、安全团队，都是重点会解决外部服务的安全性。而对内系统的安全性，很多时候是缺乏保障的，内网应用的安全评估标准比外网低一些。

葫芦娃



git 信息泄露的危害程度视泄露的信息敏感性以及数据类型、可利用难度来判断。危害程度可能小至无关痛痒，大的话可直接从源码获取敏感配置信息，通过进一步审计代码，挖掘文件上传、SQL注入等安全漏洞。更有甚者通过内网漫游，获取核心竞争力代码、敏感业务数据，导致不可估量的影响。

4



豌豆妹

那如何防御git信息泄露呢？

哆啦A梦



就像我就曾经在github上弄到过某公司的域控管理维护脚本和域控数据备份，这个问题其实说难也难，说不难也不难。员工把内部信息上传到外网，这个过程中，关键点是员工是否意识到了自己在做什么，所以归根到底是对员工的管理、员工培训的问题。泄露事件一旦发生，事后是很难甚至无法补救的。

小新



对，如果要通过技术手段实现禁止访问、上传共享其实并不难，但对于互联网企业的我们是不会做这方面完全禁止的管控。你能封掉github，他可以自己搭个svn之类的，技术手段只能解决特例问题，就算有办法封禁所有的代码项目托管站，主要还是从安全意识，制度管控。一方面我们需要通过互联网获取最新的代码填补技术人员自身的不足，同时git确实是一个协同开发，提升效率的好东西。因此我们通过内部自建git项目平台给所有开发者使用，加入权限控制。

5



豌豆妹

那如何应对git信息泄露呢？



小丸子

git信息泄露目前我们已形成处理流程，主要是直接利用github搜索关键字进行分析的。



豌豆妹

合并查找效率高吗？

小丸子



还可以，合并与单独查效率是一样的。

这里细说下应对处理流程中的一些环节：取证、处置。要处理泄密人，必须有明确的证据，处理过程中会往往遇到抵赖的。取证除了利用技术工具定位泄密途径，有时候还需要社工定位，心理学引诱认罪，到后期的法律途径要弄清楚泄密仓库（已离职人员）。



豌豆妹

hhha~感谢大牛为我们分享本期话题，下期再见哟~




安全小课堂往期回顾：

- 1、论安全响应中心的初衷；
- 2、安全应急响应中心之威胁情报探索；
- 3、论安全漏洞响应机制扩展；
- 4、企业级未授权访问漏洞防御实践；
- 5、浅谈企业SQL注入漏洞的危害与防御；
- 6、信息泄露之配置不当；
- 7、XSS之攻击与防御；
- 8、电商和O2O行业诈骗那些事儿（上）；
- 9、电商和O2O行业诈骗那些事儿（下）；
- 10、CSRF的攻击与防御；
- 11、账户体系安全管理探讨；
- 12、远程代码执行漏洞的探讨；
- 13、服务器安全管控的探讨；
- 14、畅谈端口安全配置。



 jsrc_team

 京东安全应急响应中心

动动手指~关注下撒~