

记一次从别样的侦察到未授权访问


Author: CyberSecurity

Blog: <https://1337er.com>

前言

在 Twitter 上看到 Intigriti 推送了一个很精致的 Tip，于是便想着上手试试，康康能不能利用这个 Tip 挖个漏洞，通过后续的结果证明，确实是可行的。

0x01



BUG BOUNTY TIP

Internal Google Groups

Misconfigured Google Groups sometimes expose internal discussions containing endpoints, code snippets, credentials or other valuable info.

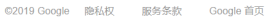
Testing is easy, crawl (internal) domains and go to:

<https://groups.google.com/a/<DOMAIN.COM>/forum>

 @vulnh0lic  @vulnh0lic www.intigriti.com

这是 TIP 的原图，原理讲的就是如果某谷歌群组配置不当，允许非群组成员浏览，便会泄露一些敏感信息，就比如群组内成员的 真实姓名，邮箱地址 一类信息；

说白了，类似于QQ群的设置，是否允许外人通过群组名称发现群组，<DOMAIN.COM> 是一个占位符，举个例子，比如说我要检索币安域名的谷歌群组: <https://groups.google.com/a/binance.com/forum/> 如果出现下图所述的内容，意思就是群组存在，但是不允许外人浏览群组内容



Error 404

Google

搜索群组或帖子

· 🔍

网上论坛

👤 0 ⚙️

我的群组

[首页](#)

我的讨论

加星标主题

收藏夹

点击群组的星标即可收藏它

最近的搜索

隐私权政策 · 服务条款

 我的群组

 浏览所有群组

“一站式”管理所有讨论内容
利用收藏夹和文件夹进行分类整理，可透过电子邮件进行跟踪，并能快速找出来读的帖子。

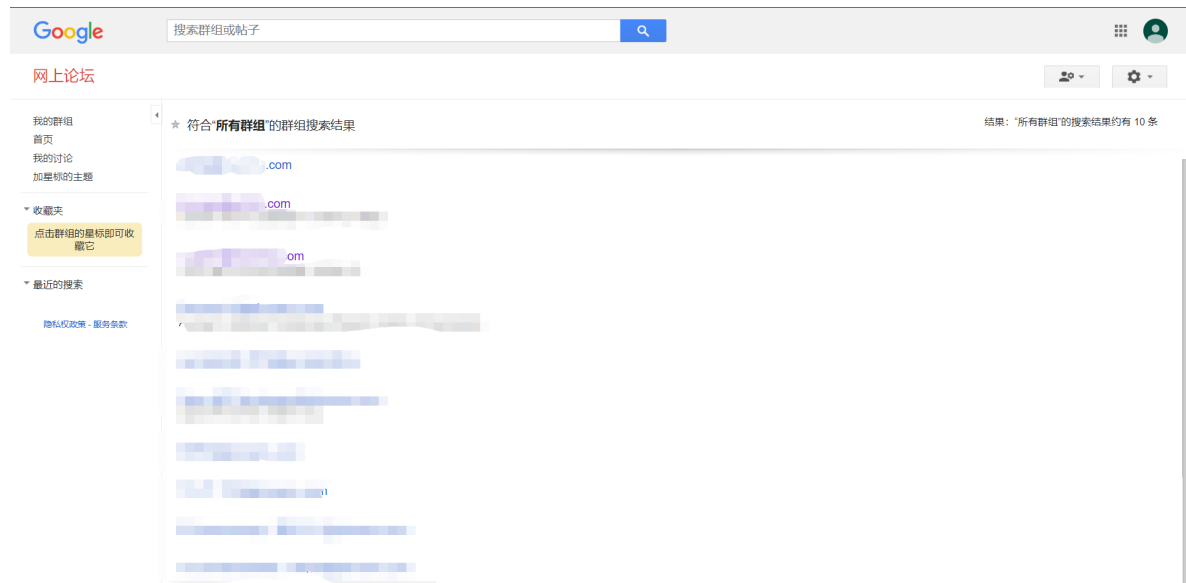
分享您的看法
使用富文本编辑可自定义您帖子的字体、颜色和图片。

讨论动力以人人为本
通过照片、昵称和自动翻译功能与别人分享您的想法。

速度第一
快捷键和流线型设计可让您减少熟悉产品所需花费的时间。按“?”可查看完整的快捷键列表。

移动设备适用
随时随地在移动设备上转至我们经过优化的[网站](#)访问Google网上论坛。

上图便是我的测试目标，通过浏览群组这一功能，发现了一些敏感信息，内容包括用户名，邮箱地址，还有用于简述此用户用于什么用途的黑色字体，目前漏洞未修复，原谅重马



0x02

通过上述所发现的邮箱地址，我发现了几个后缀并不属于目标主域名的邮箱地址，我怀疑是内部域名，专门用于内部员工 `Test`，`Developers`，`Product`，我在此文中将目标域名命名为 `example.com`，对目标域名做了子域名收集之后，找到了一处用于托管 `harbor` 的子域，发现未开放注册用户功能之后，我便放弃通过 CVE-2019-16097 注册管理员账户的想法（其他几个同一时期的漏洞基本都是需要登录之后才能利用的，CVE-2019-3990 可以枚举用户，但是我太懒了，如果找不到其它漏洞的话，我还是会回过头来看它的），而后在思考中发现收集到的域名少了一些什么东西，`harbor` 服务一般都是跟随 `Docker registry` 一同部署的，但是我的 `checklist` 没有发现那个子域，手工拼接一下域名：

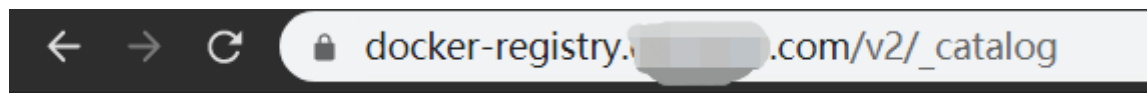
<https://docker-registry.example.com/>



发现存在未授权访问的情况，一般这个服务都是需要鉴权的，俗话就是 401 认证，回手一个 `/v1/ -> 404 page not found`

`/v2/ 试试？`

看一下仓库



```
{"repositories":["", "production"]}
```

看命名规则像是生产环境的线上业务，发现确是 latest 版本



```
{"name": "production", "tags": ["latest"]}
```

自动化脚本，可以直接拖拽 docker 镜像 https://github.com/NotSoSecure/docker_fetch/

后续从镜像发现了一些 ak/sk，连带着报告一起提交给了厂商，截至发文，厂商还未回复。

0x03

有时通过主站或者子域无从下手的时候，利用一个第三方的工具也许就会改变现状，不要放过任何细节，知识面，决定看到的攻击面有多广；知识链，决定发动的杀伤链有多深；