

Codebuddy Security

快速入门



腾讯云

【 版权声明 】

©2013–2026 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

快速入门

最近更新时间：2026-07-17 10:36:30

本文为您介绍如何快速购买并使用 Codebuddy Security。

准备工作

- 注册账号：[注册腾讯云账号](#) 并完成 [实名认证](#)。
- 权限配置：确保账号拥有操作目标资源的 [访问策略权限](#)。

❗ 权限说明：

- 当前操作的腾讯云账号需要具有 **AdministratorAccess** 或 **QcloudCBSECFullAccess** 访问策略权限才能完成下单。
- QcloudCBSECFullAccess** 权限：Codebuddy Security 全读写访问权限。
- QcloudCBSECReadOnlyAccess** 权限：Codebuddy Security 只读访问权限。

操作流程

请根据以下操作流程从0开始下单购买到第一次执行源码安全扫描等步骤。

操作步骤	说明
步骤一：下单购买	进入 Codebuddy Security 购买页 ，下单购买 SaaS 企业版，详情参考 购买指南 。如已购买，可跳过该步骤。
步骤二：获取登录信息	进入 Codebuddy Security 控制台 ，单击获取 Codebuddy Security 官网平台的账号、密码，详情请参见 控制台指南 。
步骤三：登录平台	进入 Codebuddy Security 官网平台 ，完成登录。
步骤四：开始使用	配置相关信息，开始第一次执行源码安全扫描。

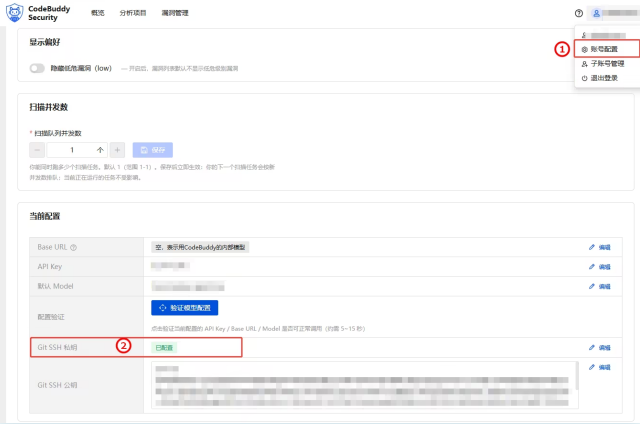
开始使用

前序步骤请参考上述操作流程，在登录到 [Codebuddy Security 官网平台](#) 后即可配置相关信息，开始第一次执行源码安全扫描。

- 在顶部导航栏单击[分析项目](#)，进入分析项目列表页面，然后单击右上角的[创建分析项目](#)。



2. 选择代码来源（Tab 切换，支持 Git 仓库、源码包），配置来源信息。

代码来源	说明
Git 仓库（推荐）	支持 SSH 和 HTTPS 两种格式。 - SSH 格式示例：git@github.com:your-org/your-repo.git。 - HTTPS 格式示例：https://github.com/your-org/your-repo.git。 ⚠ 注意： - 需要前置配置 SSH Key，平台通过 SSH 协议拉取 Git 仓库代码。  - 输入 HTTPS 格式的地址会自动转为 SSH 格式，认证仍然走 SSH Key。
上传压缩包	将代码打包为 <code>.tgz</code>、<code>.tar.gz</code> 或 <code>.zip</code> 上传扫描，SaaS 场景最大可上传 200MB，适用于无法直接通过网络访问仓库的场景。

3. 在扫描配置中，配置相关参数。

 CodeBuddy Security

概览

分析项目

漏洞管理

分析项目列表 > 创建分析项目

创建分析项目

</> 代码来源

Git 仓库

上传压缩包

* Git 仓库地址

git@github.com:org/repo.git 或 https://github.com/org/repo.git

* 分支 / Commit

main

* 项目名称

根据仓库地址和分支名自动生成

扫描配置

从模板填充配置

基础配置 (Token / PoC) PoC 关闭

Token 额度 (M)

0 = 不限制

PoC 动态验证

扫描过滤配置

未配置, 扫描全部文件

多阶段模型配置

全部使用默认模型 (hy3-preview)

创建项目并开始扫描

字段	说明
基础配置	用于配置 Token 额度、PoC 动态验证等。 - Token 额度：分析项目内使用 Token 上限，超限自动熔断。 - PoC 动态验证：开启后会在扫描流程中对发现的漏洞执行 PoC 沙箱验证。
扫描过滤配置	指定扫描范围（只扫/过滤路径），默认不配置表示全量扫描。
多阶段模型配置	指定不同扫描阶段使用什么样的模型。

4. 单击**创建项目并开始扫描**，系统会自动触发首次扫描。创建成功后跳转到项目详情页，可实时查看扫描进度。

❗ 说明：

首次扫描时间取决于仓库大小和代码量。

CodeBuddy Security

概览分析项目漏洞管理

分析项目列表 > | 详情

基本信息

仓库地址
分支/commitmain
创建时间2026-06-11 15:48
创建者
扫描次数5
漏洞总数48
累计 Token135.44M
缓存命中107.27M
Token 额度
扫描配置已配置
按阶段配置模型
PoC 验证已关闭

扫描执行历史 共 5 次

最近一次扫描完成Commit: 7533e9712026-06-22 17:38查看日志

初始化成功威胁建模成功漏洞发现成功对抗审查成功静态验证成功PoC 验证跳过补丁生成成功

漏洞列表 共 19 个

Q 搜索漏洞标题 / 文件路径

严重 × +1

未审核

已发现 × +3

漏洞标题	严重程度	状态	置信度	文件	发现时间
NoOpPasswordEncoder: 明文密码存储	高危	未审核 (已生成补丁)	68%	src	06-17 19:58
WebWolf删除邮件端点未做用户过滤导致...	高危	未审核 (已生成补丁)	92%	src	06-17 19:58
PUT /IDOR/profile/{userId} 存在逻辑漏洞	高危	未审核 (AI 确认可信)	95%	src	06-17 19:58
GET /access-control/users 存在逻辑漏洞	高危	未审核 (已生成补丁)	88%	src	06-17 19:58
Broken Access Control	高危	未审核 (已生成补丁)	82%	src	06-17 19:58
SQL注入类型风险触发, 由入参'statemen...	高危	未审核 (已生成补丁)	92%	src	06-17 19:58
SQL注入类型风险触发, 由入参'query'导...	严重	未审核 (已生成补丁)	82%	src	06-17 19:58
SQL注入类型风险触发, 由入参'query'导...	严重	未审核 (已生成补丁)	95%	src	06-17 19:58
SQL注入类型风险触发, 由入参'checkUs...	高危	未审核 (已生成补丁)	95%	src	06-17 19:58

5. 扫描完成后，可以在任务详情漏洞列表查看漏洞，也可前往漏洞管理查看发现的漏洞并进行审核。