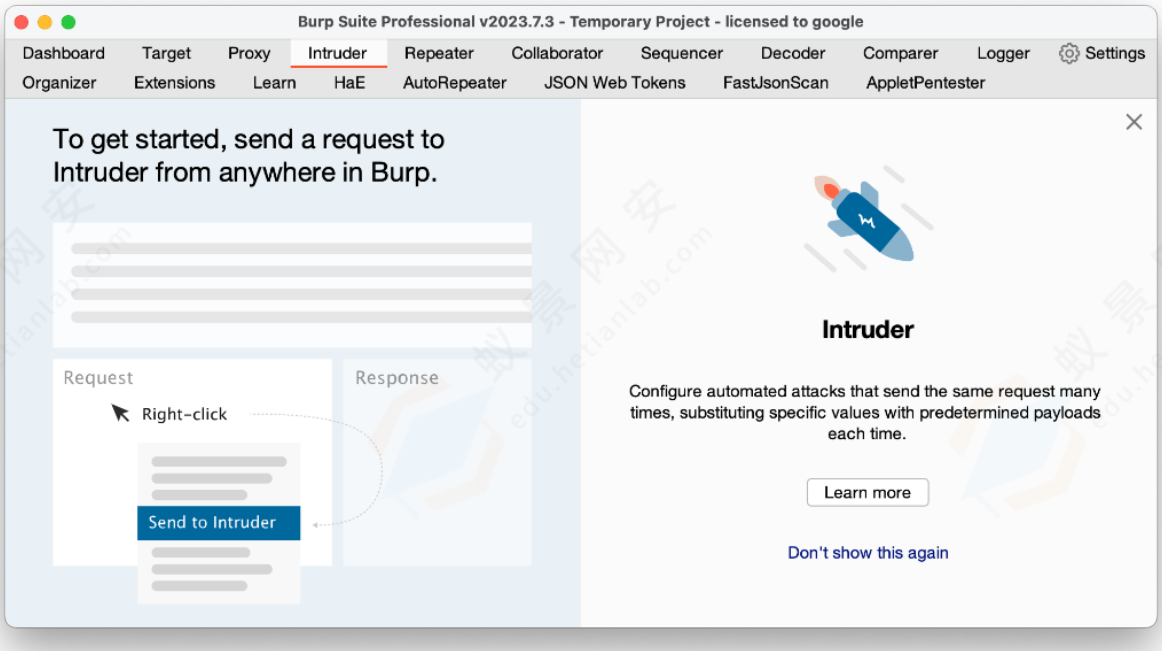
一、弱口令排查

需要注意：弱口令不仅仅会存在于网站中，服务与设备均会出现弱口令，如frp、ssh、smb、rdp等

- 常见爆破工具
  - 网站弱口令爆破
  - burpsuite - intruder



  -
  - 服务弱口令爆破
  - hydra https://www.jianshu.com/p/4da49f179cee
  - yakit https://yaklang.io/products/intro/

- 弱口令分类
  - 通用弱口令
  - 常用密码
    - 123456 admin123 admin 88888888
    - https://nordpass.com/most-common-passwords-list/
    - 其他的一些字典：
    - https://github.com/TheKingOfDuck/fuzzDicts
  - 默认密码
    - https://forum.ywhack.com/password.php
  - 空密码
    - 无需验证或任意密码即可登录，如ftp匿名登录
  - 条件弱口令
  - 信息的组合（姓名+生日 、 身份证后六位）
    - https://shentoushi.top/tools/dict/index.php
    - https://github.com/LandGrey/pydictor
- 如何避免弱口令？
  - 在服务器上对用户输入的密码做复杂度验证

```php
<?php
function checkPasswordComplexity($password) {
    // 定义复杂度要求
    $minLength = 8;  // 密码的最小长度
    $uppercaseRequired = true;  // 是否需要大写字母
    $lowercaseRequired = true;  // 是否需要小写字母
    $numberRequired = true;  // 是否需要数字
    $specialCharRequired = true;  // 是否需要特殊字符

    // 检查最小长度要求
    if (strlen($password) < $minLength) {
        return false;
```

```
    }

    // 检查是否需要大写字母且密码中是否存在
    if ($uppercaseRequired && !preg_match('/[A-Z]/', $password)) {
        return false;
    }

    // 检查是否需要小写字母且密码中是否存在
    if ($lowercaseRequired && !preg_match('/[a-z]/', $password)) {
        return false;
    }

    // 检查是否需要数字且密码中是否存在
    if ($numberRequired && !preg_match('/\d/', $password)) {
        return false;
    }

    // 检查是否需要特殊字符且密码中是否存在
    if ($specialCharRequired && !preg_match('/[^a-zA-Z0-9]/', $password)) {
        return false;
    }

    // 密码符合所有复杂度要求
    return true;
}

// 示例用法:
$userPassword = $_POST['password'];  // 假设密码通过POST方式提交

if (checkPasswordComplexity($userPassword)) {
    echo "密码符合复杂度要求。";
} else {
    echo "密码不符合复杂度要求。";
}
?>
```

- 从防止爆破入手
  - 添加验证码
    - 短信验证码

- 邮箱验证码

- 安全图形验证码

请在下图依次点击：

确认

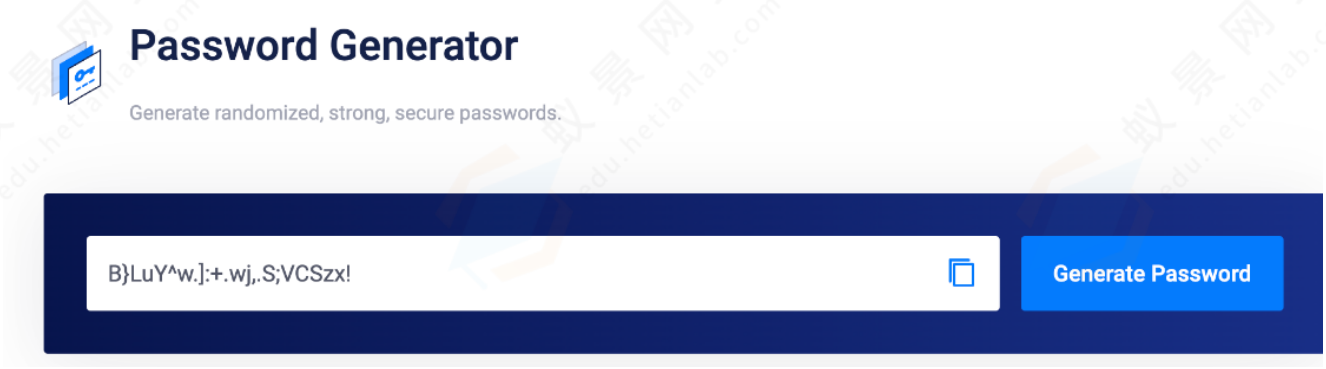
- [google reCAPTCHA]
- TOTP动态口令 Time-based One-time Password 基于时间的一次性密码

- 
Steam 令牌
2YP7G
成功！此设备现在是您的 Steam 令牌手机验证器了。
在删除此应用或还原您的设备之前，记得将此验证器从您的帐户中移除。
- 
320574
NETEASE

- 生物指纹
  - 
腾讯健康系统
腾讯游戏人脸识别验证
帮助
尊敬的用户：
为保证你的游戏健康，请在进入游戏前完成人脸识别，否则你的游戏时长将受到限制。
暂不验证
开始验证

- 禁用密码

- 随机强密码



  - 很多云服务器厂商就是这样做的

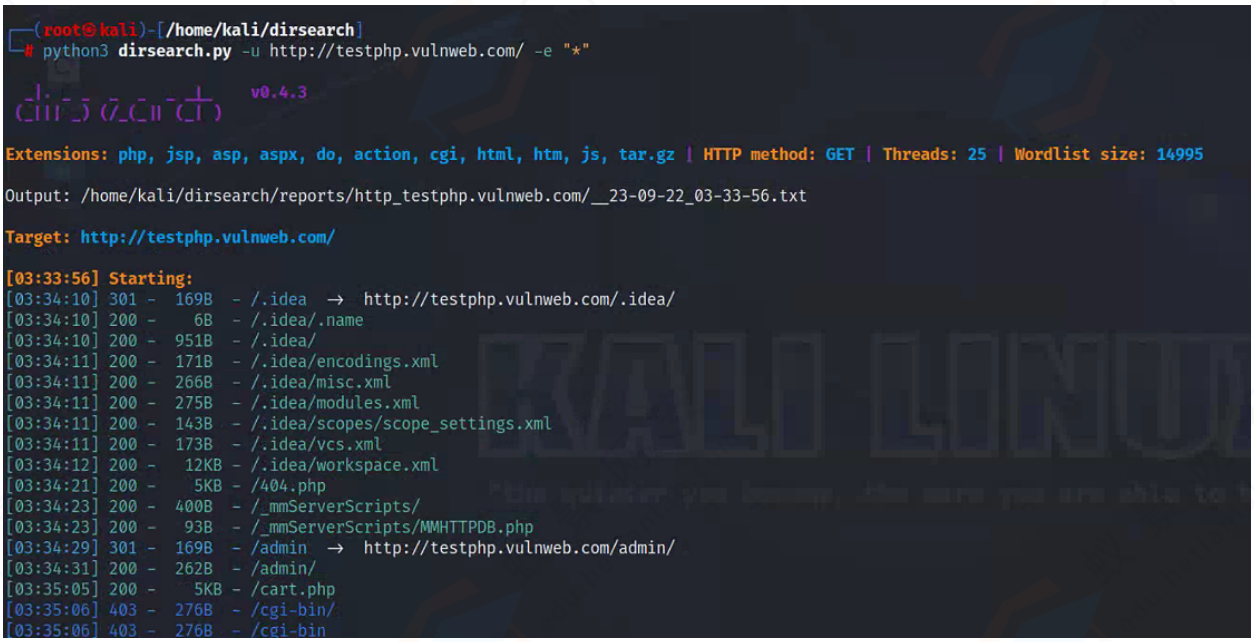
1. 常见接口、未授权访问排查

- 常见未授权访问漏洞
  - https://xz.aliyun.com/t/12582#toc-0
- 接口未授权
  - 一些开发在接口处未做严格的权限验证，或权限验证可以被绕过，产生接口未授权访问漏洞。

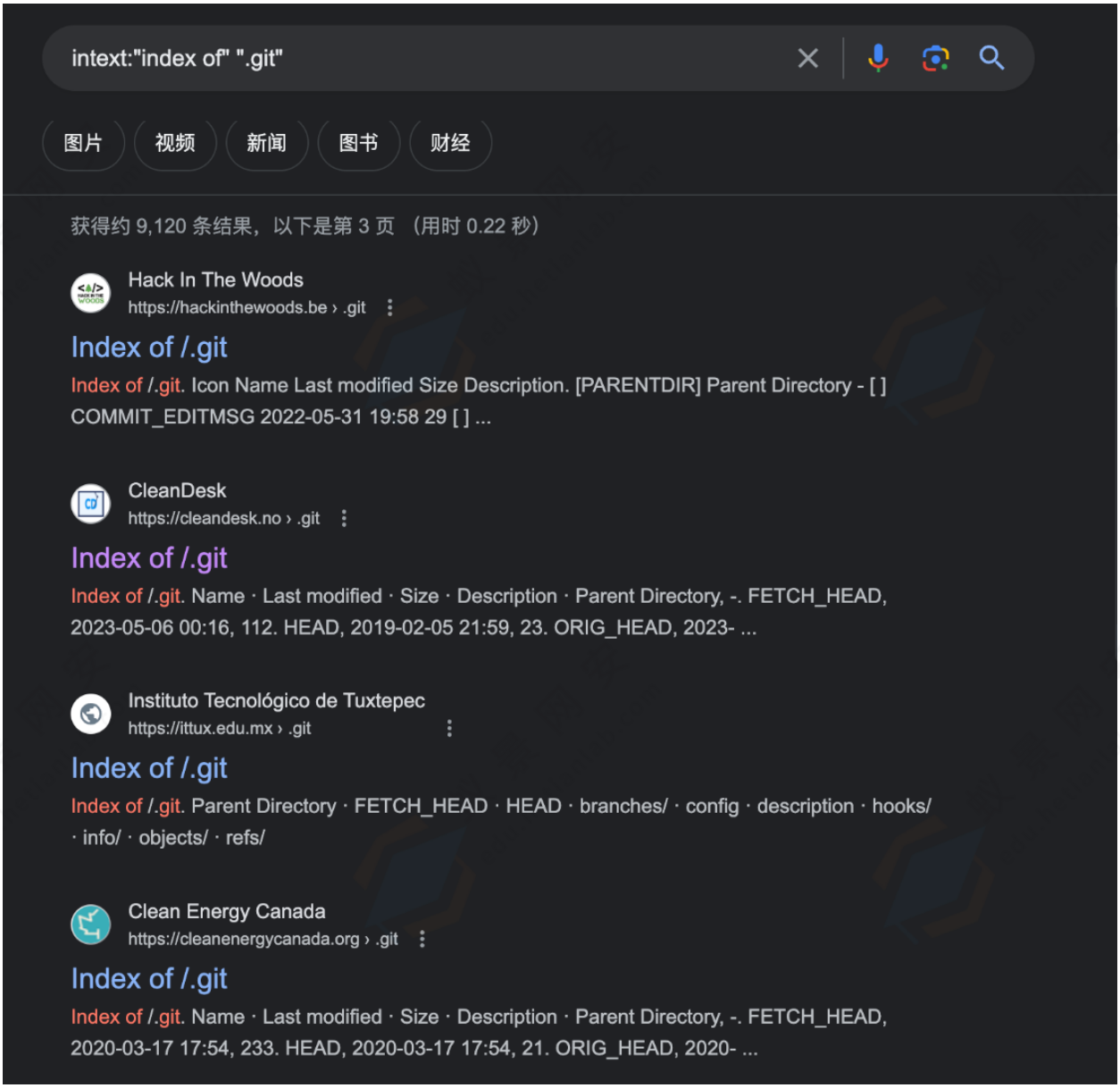
2. 敏感文件排查

> 如何开展排查
> - 白盒角度：浏览文件
> - 黑客角度：扫描网站信息
>   - dirsearch
>   - 安装与使用：（以kali系统为例，实现下面操作必须保证kali能联网）
>   - sudo su 切换至root用户

- git clone https://ghproxy.com/https://github.com/maurosoria/dirsearch.git
- 上面这个命令需要联网下载（无需科学上网）
- cd dirsearch
- pip3 install -r requirements.txt -i https://mirrors.aliyun.com/pypi/simple
- 上面这个命令需要联网下载（无需科学上网）
- 使用方法：python dirsearch.py -u "目标网站URL地址" -e "*"
- 如python3 dirsearch.py -u http://testphp.vulnweb.com/ -e "*"



  - 谷歌黑客语法：
  - inurl: 指定url
  - site: 指定网站域名
  - intext：指定网站内容
  - https://www.exploit-db.com/google-hacking-database



-

- 备份文件
  - .git源码泄漏
  - 漏洞成因：在运行git init初始化代码库的时候，会在当前目录下面产生一个.git的隐藏文件，用来记录代码的变更记录等等。在发布代码的时候，把.git这个目录没有删除，直接发布了。使用这个文件，可以用来恢复源代码。
  - 漏洞利用：工具： https://github.com/lijiejie/GitHack
  - 不是看到 .git 就能获取到所有的源码，.git 泄漏不是单纯的源码泄漏
  - .DS_Store文件泄漏
  - 漏洞成因:在发布代码时未删除文件夹中隐藏的.DS_store，被发现后，获取了敏感的文件名等信息。
  - 漏洞利用: https://github.com/lijiejie/ds_store_exp

> 我们的教学平台 Linux 小课 ppt 就存在 .DS_Store泄漏，不过没啥危害

- SVN导致文件泄露
  - 漏洞成因：Subversion，简称SVN，是一个开放源代码的版本控制系统，相对于的RCS、CVS，采用了分支管理系统，它的设计目标就是取代CVS。互联网上越来越多的控制服务从CVS转移到

Subversion。Subversion使用服务端–客户端的结构，当然服务端与客户端可以都运行在同一台服务器上。在服务端是存放着所有受控制数据的Subversion仓库，另一端是Subversion的客户端程序，管理着受控数据的一部分在本地的映射（称为“工作副本”）。在这两端之间，是通过各种仓库存取层（Repository Access，简称RA）的多条通道进行访问的。这些通道中，可以通过不同的网络协议，例如HTTP、SSH等，或本地文件的方式来对仓库进行操作。

  - 漏洞利用：https://github.com/anantshri/svn-extractor

- WEB-INF/web.xml泄露

WEB-INF是Java的WEB应用的安全目录。如果想在页面中直接访问其中的文件，必须通过web.xml文件对要访问的文件进行相应映射才能访问。

```
  - WEB-INF主要包含一下文件或目录:
      - /WEB-INF/web.xml: Web应用程序配置文件，描述了 servlet 和其他的应用组件配置及命名规则。
      - /WEB-INF/classes/: 含了站点所有用的 class 文件，包括 servlet class 和非servlet class，他们不能包含在 .jar文件中
      - /WEB-INF/lib/: 存放web应用需要的各种JAR文件，放置仅在这个应用中要求使用的jar文件,如数据库驱动jar文件
      - /WEB-INF/src/: 源码目录，按照包名结构放置各个java文件。
      - /WEB-INF/database.properties: 数据库配置文件
```

- 网站备份压缩文件
  - 漏洞成因
  - 该漏洞往往会导致服务器整站源代码或者部分页面的源代码被下载，利用。源代码中所包含的各类敏感信息，如服务器数据库连接信息，服务器配置信息等会因此而泄露，造成巨大的损失。被泄露的源代码还可能会被用于代码审计，进一步利用而对整个系统的安全埋下隐患。
  - 常见备份文件的后缀
  - .rar
  - .zip
  - .7z
  - .tar.gz
  - .bak
  - .swp
  - .txt
  - .html
- 公开文件
  - github / gitee / csdn
  - 一些开发者安全意识薄弱，会把含有敏感信息（短信收发或oss或阿里云控制中心的密钥、密码、身份凭据）的数据上传到github，可以通过一些关键字搜索

THE ULTIMATE GITHUB DORKS LIST V3 (@obheda12)

.mlab.com password	browserstack_access_key	dotfiles	filename:.netrc password	filename:netrc	google_private_key	mailgun	ossrh_password	sandbox_aws_secret_access_key	ssh2_auth_password
WFClient Password extension:ica	bucket_password	droplet_travis_password	filename:.npmrc _auth	filename:npmrc	google_secret	mailgun apikey	pagerduty_apikey	sauce_access_key	sshpass
access_key	bucketeer_aws_access_key_id	dynamoaccesskeyid	filename:.pgpass	filename:pass	google_server_key	mailgun_key	parse_js key	secret	staging
access_token	bucketeer_aws_secret_access_ke	dynamosecretaccesskey	filename:.remote-sync.json	filename:passwd path:etc	gpg_key_name	mailgun_password	pass	secret access key	stg
admin_pass	built_branch_deploy_key	elastica_host	filename:.s3cfg	filename:pgpass	gpg_keyname	mailgun_priv_key	passwd	secret_access_key	storePassword
admin_user	bx_password	elastica_port	filename:.sh_history	filename:prod.exs	gpg_passphrase	mailgun_secret_api_key	password	secret_bearer	stormpath_api_key_id
algolia_admin_key	cache_driver	elasticsearch_password	filename:.tugboat NOT _tugboat	filename:prod.exs NOT prod.secret.exs	HEROKU_API_KEY language:json	manage_key	password_travis	secret_key	stormpath_api_key_secret
algolia_api_key	cache_s3_secret_key	encryption_key	filename:bash	filename:prod.secret.exs	HEROKU_API_KEY language:shell	mandrill_api_key	passwords	secret_key_base	strip_key
alias_pass	cattle_access_key	encryption_password	filename:bash_history	filename:proftpdpasswd	heroku_oauth	mapbox api key	path:sites databases password	secret_token	strip_secret_key
alicloud_access_key	cattle_secret_key	env_heroku_api_key	filename:bash_profile	filename:recentservers.xml	heroku_oauth_secret	master_key	paypal_secret	secret.password	stripe
amazon_secret_access_key	certificate_password	env.sonatype_password	filename:bashrc	filename:recentservers.xml Pass	heroku_oauth_token	mg_api_key	paypal_token	secretaccesskey	stripe_key
amazonaws	ci_deploy_password	eureka.awssecretkey	filename:beanstalkd.yml	filename:robomongo.json	heroku_secret	mg_public_api_key	pem private	secretkey	stripe_secret
ansible_vault_password	client_secret	extension:avastlic support.avast.com	filename:CCCam.cfg	filename:s3cfg	heroku_secret_token	mh_apikey	personal_key	secrets	stripeToken
aos_key	client_zpk_secret_key	extension:bat	filename:composer.json	filename:secrets.yml password	herokuapp	mh_password	playbooks_url	secure	svn_pass
api_key	clojars_password	extension:cfg	filename:config	filename:server.cfg	HOMEBREW_GITHUB_API_TOKEN language:shell	mile_zero_key	plotly_apikey	security_credentials	swagger
api_key_secret	cloud_api_key	extension:dbeaver-data-sources.xml	filename:config_irc_pass	filename:server.cfg rcon password	htaccess_pass	minio_access_key	plugin_password	send_keys	tesco_api_key
api_key_sid	cloud_watch_aws_access_key	extension:env	filename:config.json auths	filename:settings	htaccess_user	minio_secret_key	postgres_env_postgres_password	send.keys	Tester_keys_password
api_secret	cloudant_password	extension:exs	filename:config.php dbpasswd	filename:settings.py SECRET_KEY	incident_channel_name	mix_pusher_app_cluster	postgresql_pass	sendgrid_api_key	testuser
api_googlemaps Aiza	cloudflare_api_key	extension:ini	filename:configuration.php JConfig passwd	filename:sftp-config.json	internal	mix_pusher_app_key	preprod	sendgrid_key	thera_oss_access_key
apidocs	cloudflare_auth_key	extension:json api.forecast.io	filename:connections	filename:sftp.json path:.vscode	irc_pass	msg ntcsserv identify filename:config	private	sendgrid_password	token
apikey	cloudinary_api_secret	tension:json googleusercontent client_secr	filename:connections.xml	filename:shadow	JEKYLL_GITHUB_TOKEN	mydotfiles	private -language:java	sendkeys	trusted_hosts
apiSecret	cloudinary_name	extension:json mongolab.com	filename:constants	filename:shadow path:etc	jsforce extension:js conn.login	mysql	private_key	ses_access_key	twilio_secret
app_debug	codecov_token	extension:pem	filename:credentials	filename:spec	jwt_client_secret_key	mysql password	private_signing_password	ses_secret_key	twilio_account_id
app_id	config	extension:pem private	filename:credentials aws_access_key_id	filename:sshd_config	jwt_lookup_secret_key	mysql_root_password	prod	setdstaccesskey	twilio_account_secret
app_key	conn.login	extension:ppk	filename:cshrc	filename:tugboat	jwt_password	netlify_api_key	prod_password	sidsecretkey	twilio_account_sid
app_log_level	connectionstring	extension:ppk private	filename:database	filename:ventrilo_srv.ini	jwt_secret	nexus password	prod.access.key.id	sf_username	twilio_account_sid
app_secret	consumer_key	extension:properties	filename:dbeaver-data-sources.xml	filename:WebServers.xml	jwt_secret_key	nexus_password	prod.secret.key	SF_USERNAME salesforce	twilio_accountsid
appkey	consumer_secret	extension:sh	filename:deploy.rake	filename:wp-config	jwt_token	node_env	PT_TOKEN language:bash	shodan_api_key language:python	twilio_acount_sid NOT env
appkeysecret	credentials	extension:sls	filename:deployment-config.json	filename:wp-config.php	jwt_user	node_pre_gyp_accesskeyid	publish_key	sid_token	twilio_api
application_key	cypress_record_key	extension:sql	filename:dhcpd.conf	filename:zhrc	jwt_web_secert_key	node_pre_gyp_secretaccesskey	pusher_app_id	signing_key_password	twilio_api_auth
appsecret	database_password	extension:sql mysql dump	filename:dockercfg	firebase	jwt_wwp_secert_key	npm_api_key	pwd	signing_key_secret	twilio_api_key
appspot	database_schema_test	extension:sql mysql dump password	filename:env	flickr_api_key	key	npm_password	queue_driver	slack_api	twilio_api_secret
auth_token	datadog_api_key	extension:yaml mongolab.com	filename:environment	fossa_api_key	keyPassword	npm_secret_key	rabbitmq_password	slack_channel	twilio_api_sid
authorizationToken	datadog_app_key	extension:zsh	filename:express.conf	ftp	language:yaml -filename:travis	npmrc _auth	rds.amazonaws.com password	slack_key	twilio_api_token
authsecret	db_password	fabricApiSecret	filename:express.conf path:.openshift	ftp_password	ldap_password	nuget_api_key	redis_password	slack_outgoing_token	twilio_secret
aws_access	db_server	facebook_secret	filename:filezilla.xml	gatsby_wordpress_base_url	ldap_username	nuget_apikey	response_auth_jwt_secret	slack_signing_secret	twilio_secret_token
aws_access_key_id	db_username	fb_secret	filename:filezilla.xml Pass	gatsby_wordpress_client_id	linux_signing_key	nuget_key	rest_api_key	slack_token	twilioapiauth
aws_bucket	dbpasswd	filename:.netrc password	filename:git-credentials	gatsby_wordpress_user	ll_shared_key	oauth_token	rinkeby_private_key	slack_webhook	twina_password
aws_key	dbpassword	filename:.bash_history	filename:gitconfig	gh_api_key	location_protocol	object_storage_password	root_password	slash_developer_space_key	twitter_secret
aws_secret	dbuser	filename:.bash_profile aws	filename:global	gh_token	log_channel	octest_app_password	ropsten_private_key	snowonyp_password	twitterKey
aws_secret_key	deploy_password	filename:.bashrc mailchimp	filename:history	ghost_api_key	login	octest_password	routes3_access_key_id	socrata_password	x-api-key
aws_token	digitalocean_ssh_key_body	filename:.bashrc password	filename:htpasswd	github_api_key	lottie_happo_api_key	okta_key	rtd_key_pass	sonar_organization_key	xoxb
AWSSecretKey	digitalocean_ssh_key_ids	filename:.cshrc	filename:hub oauth_token	github_deploy_hb_doc_pass	lottie_happo_secret_key	omise_key	rtd_store_pass	sonar_project_key	xoxp
b2_app_key	docker_hub_password	filename:.dockercfg auth	filename:id_dsa	github_id	lottie_s3_api_key	onesignal_api_key	s3_access_key	sonatype_password	zen_key
bashrc password	docker_key	filename:.env DB_USERNAME NOT homestead	filename:id_rsa	github_key	lottie_s3_secret_key	onesignal_user_auth_key	s3_access_key_id	sonatype_token_password	zen_tkn
bintray_apikey	docker_pass	filename:.env MAIL_HOST=smtp.gmail.com	filename:id_rsa or filename:id_dsa	github_password	magento password	openwhisk_key	s3_key	soundcloud_password	zen_token
bintray_gpg_password	docker_passwd	filename:.esmtprc password	filename:idea14.key	github_token	mail_password	org_gradle_project_sonatype_nexus_password	s3_key_app_logs	sql_password	zendesk_api_token
bintray_key	docker_password	filename:.ftpconfig	filename:known_hosts	gitlab	mail_port	org_project_gradle_sonatype_nexus_password	s3_key_assets	sqsaccesskey	zendesk_key
bintraykey	dockerhub_password	filename:.git-credentials	filename:logins.json	gmail_password	mailchimp	os_password	s3_secret_key	square_access_token	zendesk_token
bluemix_api_key	dockerhubpassword	filename:.history	filename:makefile	gmail_username	mailchimp_api_key	ossrh_jira_password	salesforce_password	square_token	zendesk_url
bluemix_pass	dot-files	filename:.htpasswd	filename:master.key path:config	google_maps_api_key	mailchimp_key	ossrh_pass	sandbox_aws_access_key_id	squareSecret	zendesk_username

- [redacted]

```
11
12  # esms.vn info from tho@virtualsushi.com
13  sms_api_key=EB41AE0BDF74EBCF2BA36E8D561B37
14  sms_secret_key=20653D9DC735F7E647[redacted]
15
16  server.session.timeout=86400
17
```