

CAST Highlight

产品使用手册

道普云（山东）智能科技有限公司

技术支持：18266417701

客服微信：daopuyun

目录

1. 账户注册.....	3
2. 管理项目组合.....	5
3. 下载扫描代理软件和代码扫描.....	11
4. 问卷回答和结果上传.....	17
5. 结果查看和分析.....	20

1. 账户注册

- 您会从 CAST 收到注册邮件，在邮件中点击红色连接

Greetings s.li ,

You've requested a CAST Highlight account.

Our industry-leading analytics platform allows you to gain insight into the technical risk within your application portfolio.

For more information on how Highlight can help your organization uncover technical risk, visit our page [here](#)

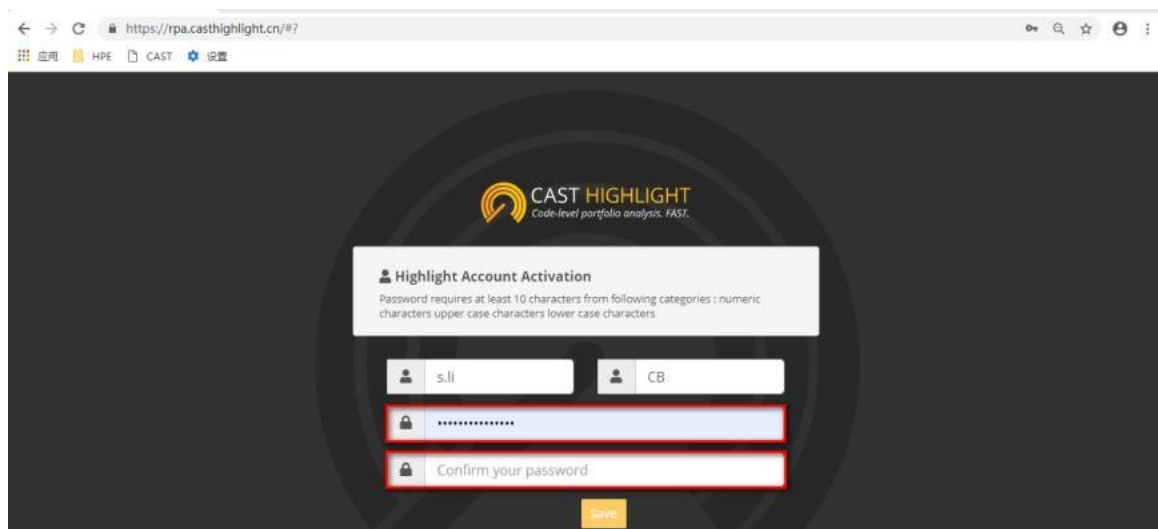
To activate your account, please click the confirmation link below:

<https://rpa.casthighlight.cn/#/?registration=702e7f16-a696-4468-a9cc-d202cd7ee3a4>

(If the link is not working, copy and paste the hyperlink into your browser)

This link will remain valid for 2 days.

- 修改注册密码，点击保存。密码一般为 10 位以上，需要大小写字母和数字组合



CAST HIGHLIGHT
Code-level portfolio analysis. FAST.

Highlight Account Activation
Password requires at least 10 characters from following categories : numeric characters upper case characters lower case characters

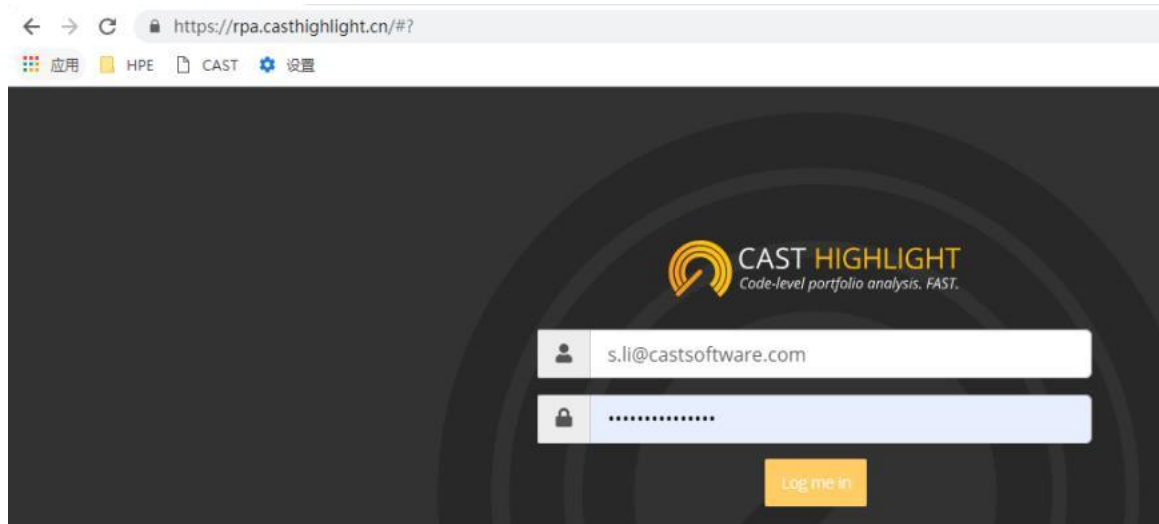
Username: s.li Email: CB

Password: [Redacted]

Confirm your password: [Redacted]

[Save](#)

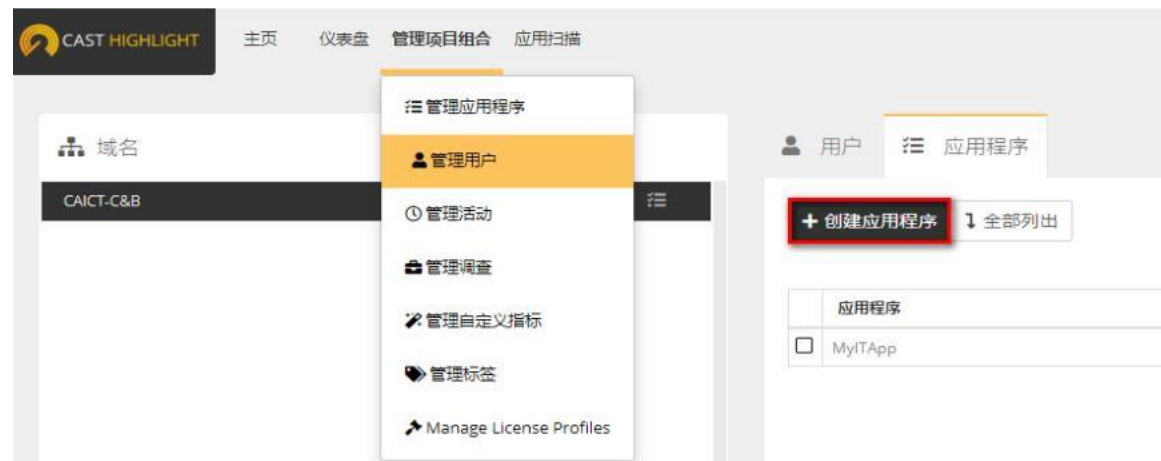
- 修改成功后，您会收到修改成功的邮件，并自动转到登录界面。使用注册的账户和密码，点击“log me in”登录系统



- 以后每次登录，访问 <https://rpa.casthighlight.cn> 登录即可

2. 管理项目组合

- 添加用户，点击“管理项目组合”-“管理用户”-“应用程序”-“创建应用程序”



- 输入应用的名称，如“MyITApp”，点击“保存”

创建应用程序

名称

参与者

- 点击“用户”，点击“邀请用户”



- 选择新建用户的角色，目前系统提供四种角色

应用程序参与者	应用扫描结果的上传和查看
域的贡献者	域的贡献者
结果观察员	最小权限，只有结果查看功能
项目组合经理	最大权限，包括创建用户和应用、创建活动、结果上传和查看

输入用户的邮件地址，点击“邀请用户”，系统会自动发邮件给用户，提醒注册。

 **邀请用户**

请选择域内用户的角色 “CAICT-C&B”

应用程序参与者

域的贡献者

结果观察员

项目组合经理

输入新用户的电子邮件

× abc@castsoftware.com +

×

取消

邀请用户

- 点击用户名，设置用户有权限参与的应用

 用户
  应用程序

+ 邀请用户

↓ 全部列出

Search:

用户	角色	状态
CB s.li	项目组合经理	活跃

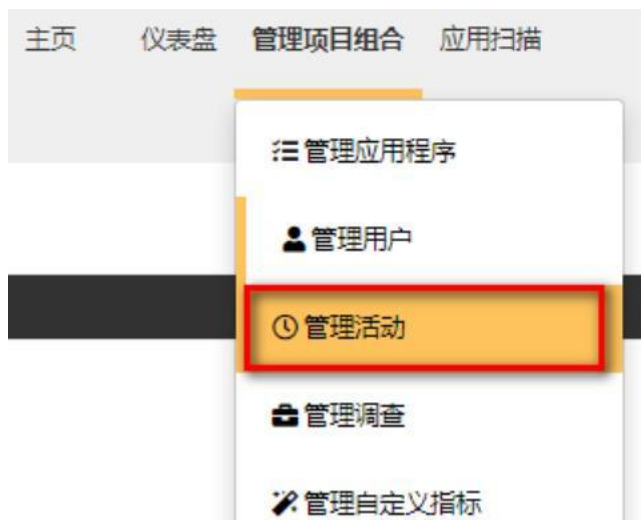
- 选择应用名称，如“MyITApp”，点击保存

编辑用户 s.li+caict CB

电子邮件	s.li+caict_CB@castsoftware.com
状态	活跃
名字	s.li+caict
姓氏	CB
贡献	No application
角	<div> <div>/ CAICT-C&B</div> <div>MyITApp</div> </div>
Portfolio Manager	CAICT-C&B

取消 保存

- 创建活动。点击“管理项目组合”-“管理活动”



- 点击“创建活动项目”，输入活动名称，如“项目活动”，点击“下一步”



创建活动项目

活动项目配置 配置 应用范围 通知

① 活动项目名称

项目活动

截止日期

04/26/2019

取消 下一步

- 保持两个设置为 ON 状态，并选取一个或多个调查问卷，如“业务影响力”，点击“下一步”



创建活动项目

活动项目配置 配置 应用范围 通知

包括资源扫描 ON

包括调查答案 ON

软件维护评估
本节中的问题用于计算给定应用所需维护量（FTE）。本节中的所有问题对于计算软件维护量都是必须的。

业务影响力
业务影响问题用于生成可在结果中查看的每个应用程序的价值概要。如果调查问卷中包含业务价值相关问题，则必须回答所有问题才能计算应用的价值信息。

应用属性
应用信息调查

- 选择域和应用，点击下一步

 创建的活动项目 ✕

活动项目配置

配置

应用范围

通知

 从域中选择

所选域中的所有应用程序将被添加到范围内。域选择将递归到子域。
允许应用范围的手动更改，一旦域列表被更新，应用范围则会被相应重置。

  C&B

 应用范围

所选择的应用程序将添加到此活动项目中

  MyITApp

取消

◀ 后退

下一步 ▶

- 点击“完成”

🕒 创建的活动项目

✕

活动项目配置

配置

应用范围

通知

✉ 启动消息

ON

A new campaign 项目活动 was recently created by your Highlight administrator. You can now start analyzing your applications, which will allow you to identify vulnerabilities and cost drivers through important analytical data.

此消息将发送给您的活动项目中每个应用的主要参与者。

取消

◀ 后退

完成

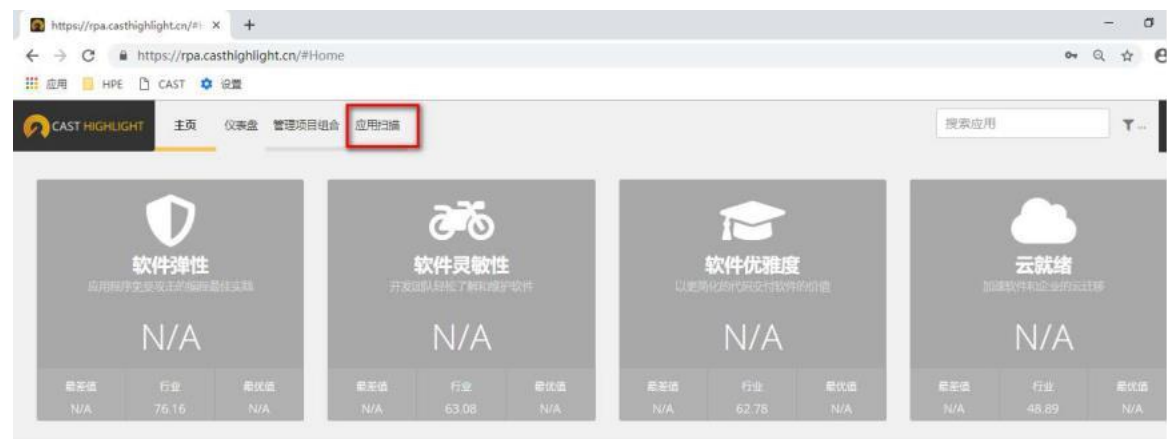
- 点击“开始活动”按钮



至此，项目配置步骤完成。

3. 下载扫描代理软件和代码扫描

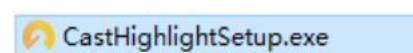
- 登录进入 highlight 站点，点击“应用扫描”链接



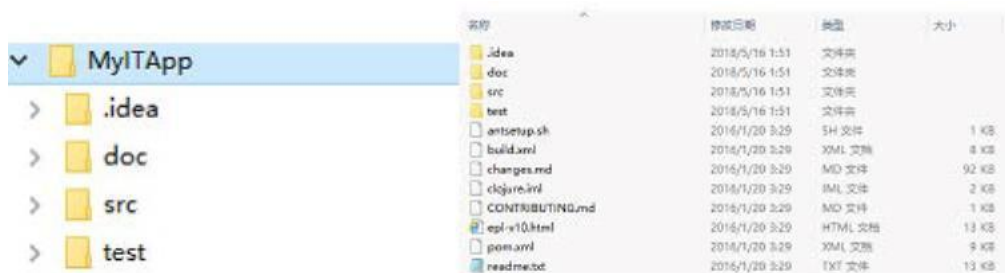
- 点击“下载代理程序”



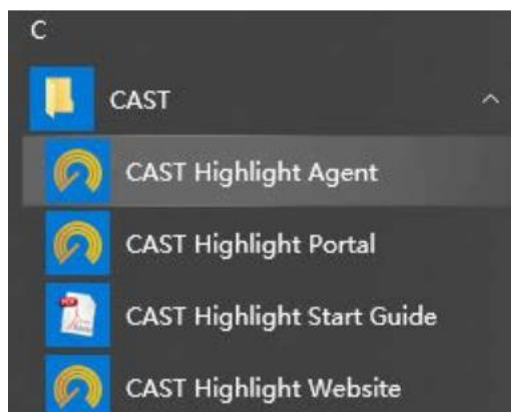
下载 CastHighlightSetup.exe,并双击完成安装。安装过程只需要点击“下一步”即可完成安装。



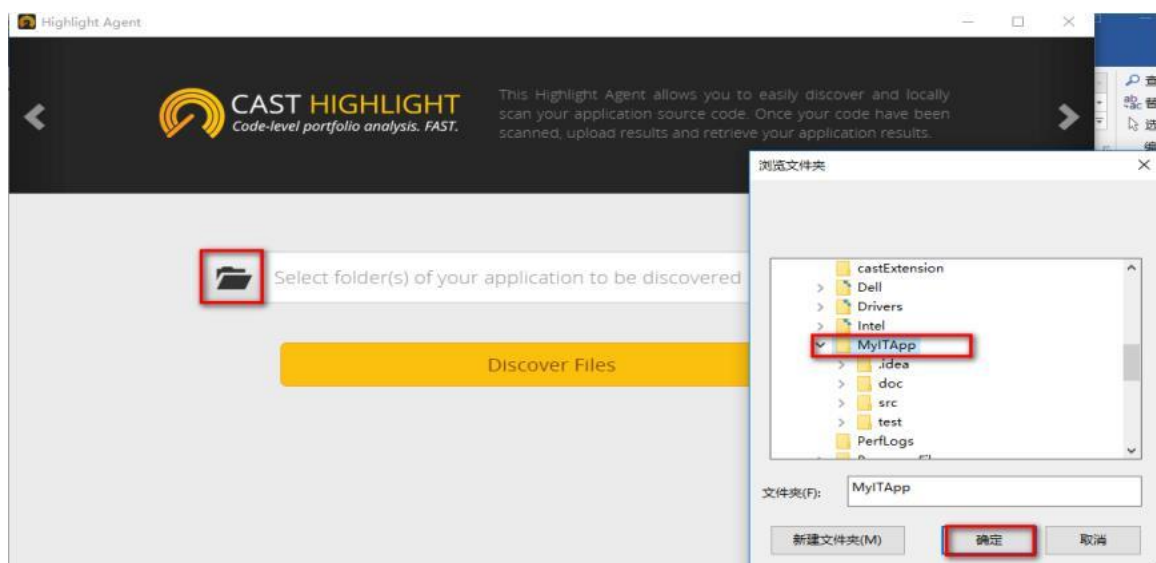
- 将被扫描应用的源代码，放置到文件目录下。注意:文件目录名为英文



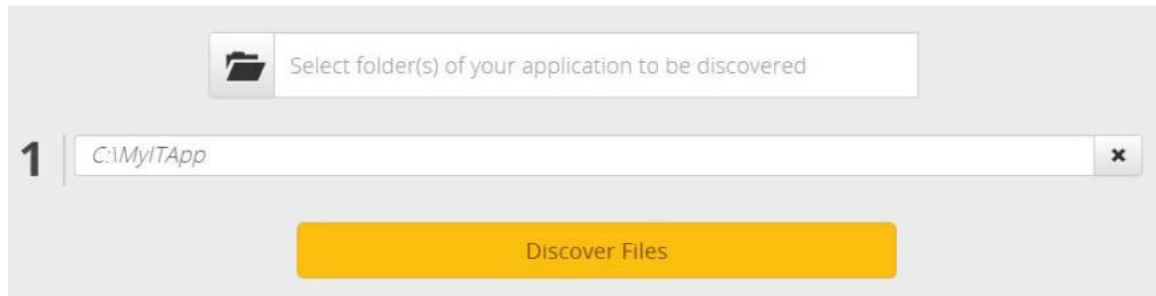
- 从 Windows 启动菜单，启动 Cast Highlight Agent,如下图



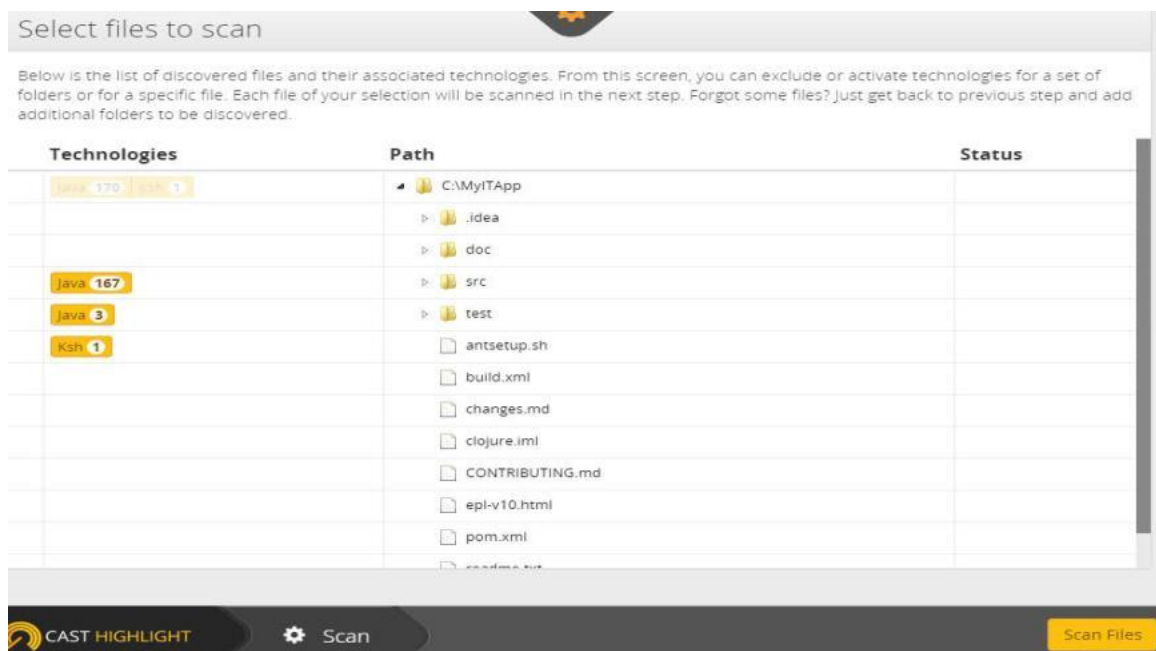
- 点击红色按钮，选择被扫描软件的目录，点击确定



- 点击“discover files”按钮，系统自动发现文件



- 点击“scan files”按钮，执行扫描



- 点击“confirm results”

Scan Results

Below is the list of discovered files and their associated technologies. From this screen, you can exclude or activate technologies for a set of folders or for a specific file. Each file of your selection will be scanned in the next step. Forgot some files? just get back to previous step and add additional folders to be discovered.

Technology	Count	File/Folder	Count
Java	170	C:\MyITApp	171
		└─ .idea	
		└─ doc	
Java	167	└─ src	167
Java	3	└─ test	3
Kotlin	1	└─ antsetup.sh	1
		└─ build.xml	
		└─ changes.md	
		└─ clojure.iml	
		└─ CONTRIBUTING.md	
		└─ epi-v10.html	
		└─ pom.xml	
		└─ readme.txt	

CAST HIGHLIGHT Scan Scan Files Confirm Results

- 点击“confirm frameworks”

Discovered Frameworks

Please confirm the frameworks listed below which have been discovered during the code scan. Only frameworks information you'll select will be sent to the portal.

1 Frameworks referenced by CAST Highlight

Validation	Technology	Framework	Version(s)	Functional type	License
no framework					

2 Possible other frameworks

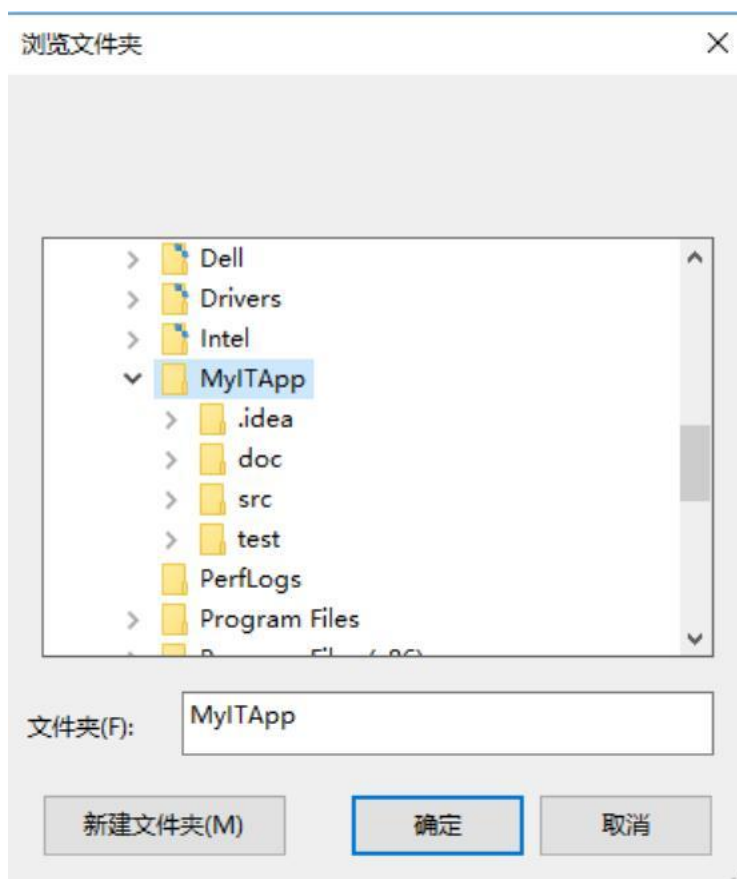
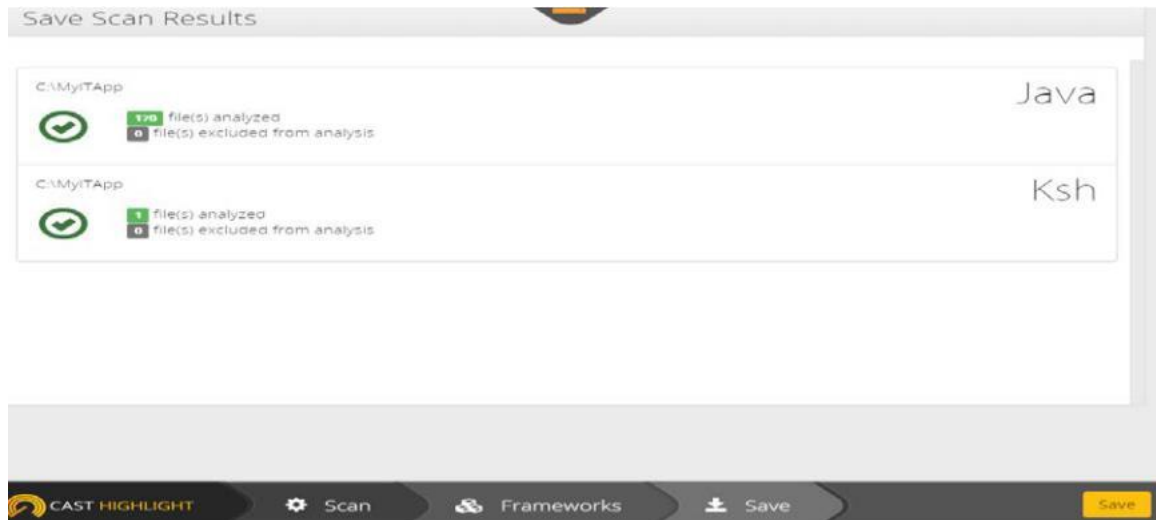
Validation	Technology	Framework	Version(s)	Functional type	License
<input checked="" type="checkbox"/>	Java	org.codehaus.jsr166-mirror	1.7.0		
<input checked="" type="checkbox"/>	Java	org.clojure	0.5.2		EPL

3 Your framework is not listed above ? Reference a new framework

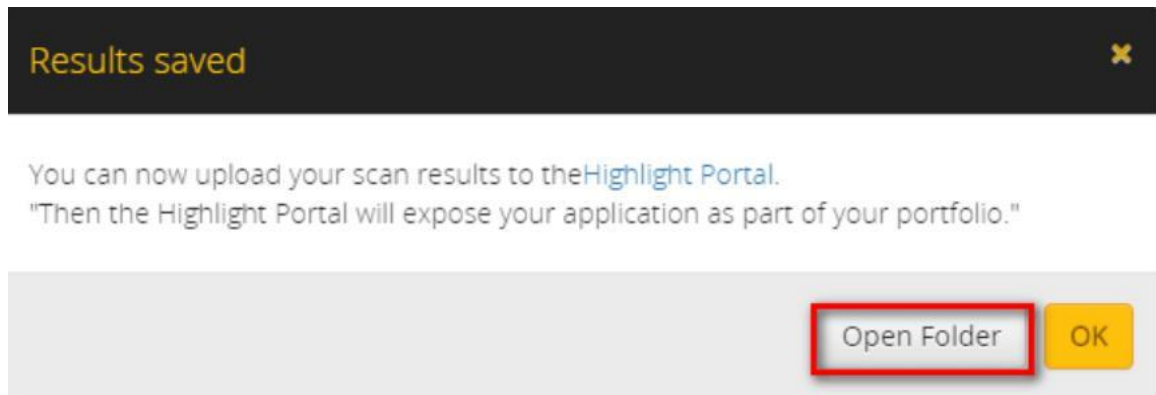
Validation	Technology	Framework	Version(s)	Functional type	License
<input type="checkbox"/>	< techn >	< name >	[version]	[type]	[license]

CAST HIGHLIGHT Scan Frameworks Confirm frameworks

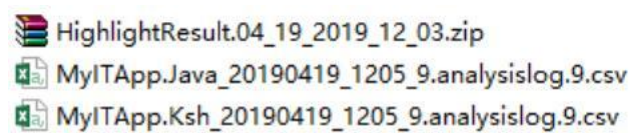
- 点击“save”，选择文件夹，保存扫描结果



- 点击“open folder”,查看扫描的输出结果



扫描结果存储在三个文件中，如下图所示



- 退出 highlight agent，至此就完成了代码的本地扫描工作

4. 问卷回答和结果上传

- 点击“应用扫描”连接，点击“调查”



- 填写调查问卷内容，点击“保存”。

Surveys for MyITApp 项目活动_MyITApp

最终用户的大致数量是多少？

此应用程序的失败会导致中断吗？请定义影响级别。

此应用程序的失败会导致收入或业务机会的损失吗？请定义影响级别。

此应用程序的失败是否会损害公司的公众形象？请定义影响级别。

此应用程序失败会导致客户信心流失吗？请定义影响级别。

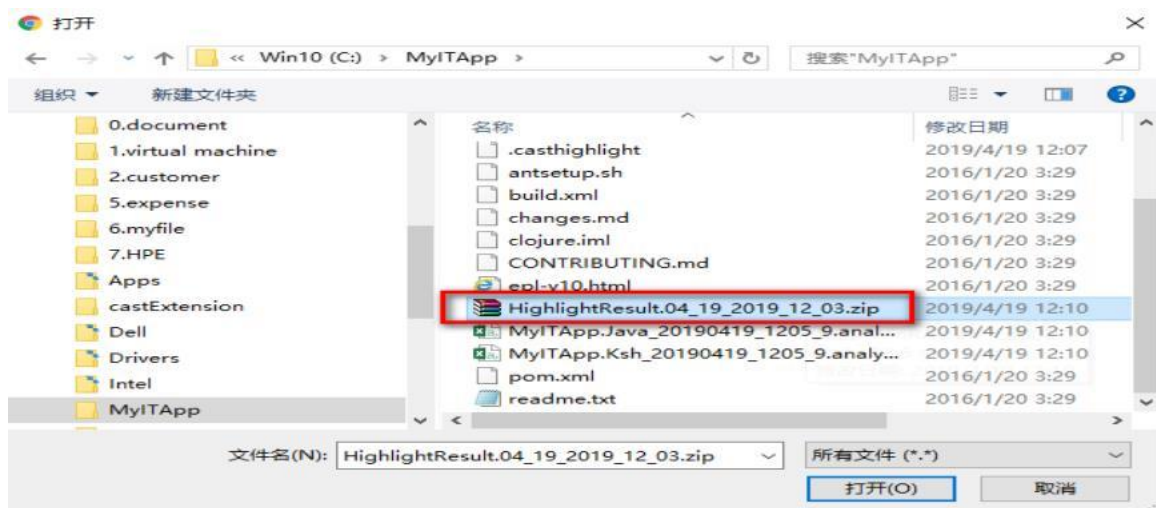
- 点击“上传结果”



- 点击红色空白处，选择



- 选择步骤 3 中生成的结果 zip 文件（只需要上传.zip 文件）



- 上传完成后，点击“关闭”

🕒 上传代理扫描项目活动_MyITApp

结果将上传到正在进行的活动中项目活动_MyITApp

列表显示了活动项目的所有已上传的结果文件。您可以删除或添加此应用程序的新文件。上传的结果将仅涉及当前的活动项目。对于已关闭的活动，删除或添加新的分析将重新打开该活动，以便于您再次提交该活动。

📄 文档	🏷️ 类型	👤 参与者	📊 状态	🗑️	📥
BinaryLibraries.csv	Shafire	s.li+caict CB	Complete	🗑️	📥
framework.validated.csv	Framework	s.li+caict CB	Complete	🗑️	📥
MyITApp.java_20190419_1205_9.CloudReady.csv	Cloudready	s.li+caict CB	Complete	🗑️	📥
MyITApp.java_20190419_1205_9.csv	Scan	s.li+caict CB	Complete	🗑️	📥
MyITApp.Ksh_20190419_1205_9.csv	Scan	s.li+caict CB	Complete	🗑️	📥

在此处调用CSV或ZIP文件或点击浏览文件

📄

关闭

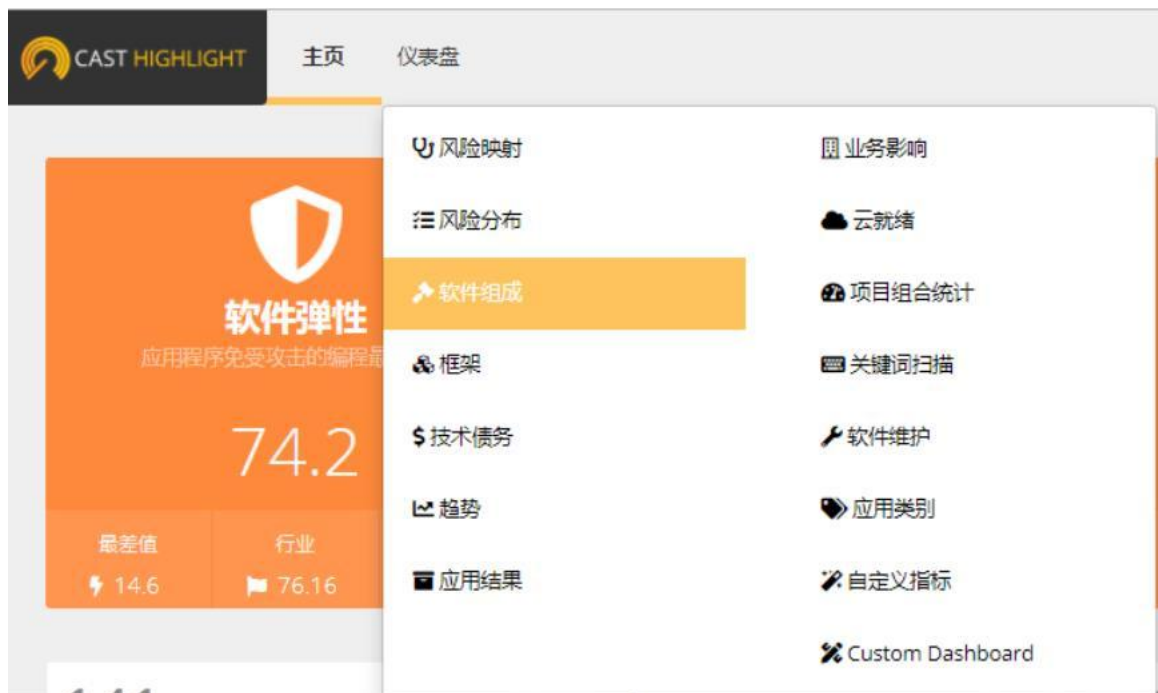
- 然后点击“提交”按钮，完成代码上传

📁 应用程序 🕒 活动 📊 状态 📅 截止日期

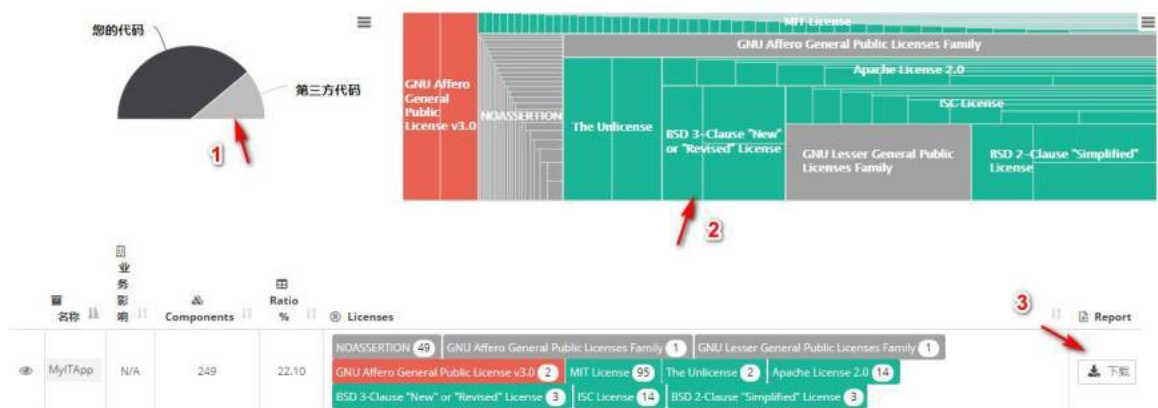
MyITApp	项目活动	持续进行	2019/4/26	📥 上传结果 2 📊 调查 1/1 📄 提交 🗑️
---------	------	------	-----------	--

5.结果查看和分析

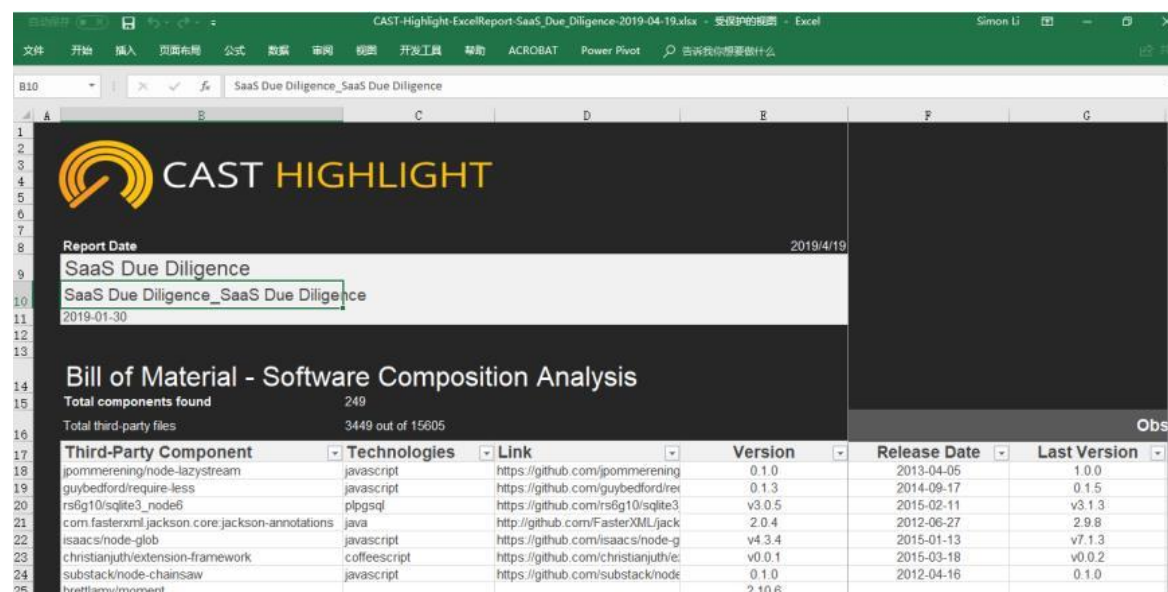
- 点击“仪表盘”-“软件组成”，进入所有应用的总体视图



- 视图展示所有应用的许可证构成。按照下图标识，依次点击：1 处显示第三方代码占比，2 处许可证的子类型，3 处下载应用构成的物料清单(BOM)



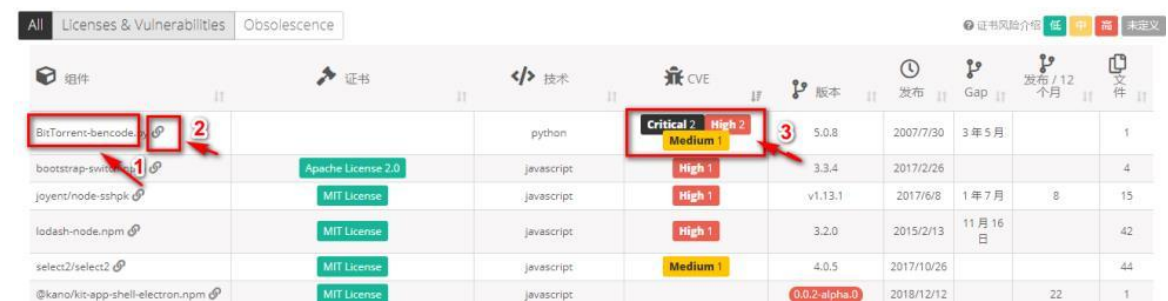
3 处生成的 BOM 清单，详细列出了具体信息。



Third-Party Component	Technologies	Link	Version	Release Date	Last Version
jpmmerening/node-lazystream	javascript	https://github.com/jpmmerening	0.1.0	2013-04-05	1.0.0
guybedford/require-less	javascript	https://github.com/guybedford/require-less	0.1.3	2014-09-17	0.1.5
rs6g10/sqlite3_node6	plpgsql	https://github.com/rs6g10/sqlite3	v3.0.5	2015-02-11	v3.1.3
com.fasterxml.jackson.core.jackson-annotations	java	http://github.com/FasterXML/jackson-annotations	2.0.4	2012-06-27	2.9.8
isaacs/node-glob	javascript	https://github.com/isaacs/node-glob	v4.3.4	2015-01-13	v7.1.3
christianjuth/extension-framework	coffeescript	https://github.com/christianjuth/extension-framework	v0.0.1	2015-03-18	v0.0.2
substack/node-chainsaw	javascript	https://github.com/substack/node-chainsaw	0.1.0	2012-04-16	0.1.0
brettlamy/moment	javascript	https://github.com/brettlamy/moment	2.10.6		

- 点击应用“MyITApp”，进入单个的应用视图

第三方组件



组件	证书	技术	CVE	版本	发布	Gap	发布 / 12 个月	文件
BitTorrent-bencode		python	Critical 2 High 2 Medium 1	5.0.8	2007/7/30	3 年 5 月		1
bootstrap-switch	Apache License 2.0	javascript	High 1	3.3.4	2017/2/26			4
joyent/node-sshpk	MIT License	javascript	High 1	v1.13.1	2017/6/8	1 年 7 月	8	15
lodash-node.npm	MIT License	javascript	High 1	3.2.0	2015/2/13	11 月 16 日		42
select2/select2	MIT License	javascript	Medium 1	4.0.5	2017/10/26			44
@kano/kit-app-shell-electron.npm	MIT License	javascript		0.0.2-alpha.0	2018/12/12		22	1

- 组件列 显示了应用包含的第三方组件
- 证书列 显示了各个组件使用的许可证类型
- 技术列 显示了组件的编程技术
- CVE 列 显示了此组件版本包含的漏洞个数和严重级别
- 版本列 显示了应用中所使用的组件的版本号
- 发布列 显示了组件版本的发布日期

- Gap 列 显示了所使用的版本和目前最新版本的时间插件
- 发布列 显示了所使用的版本和目前最新版本之间相差多少个版本
- 文件列 显示了此组件包含的文件格式

● 显示组件版本历史

第三方组件

All Licenses & Vulnerabilities Obsolescence		证书风险介绍 低 中 高 未定义						
组件	证书	技术	CVE	版本	发布	Gap	发布 / 12 个月	文件
BitTorrent-bencode.py		python	Critical 2 High 2 Medium 1	5.0.8	2007/7/30	3 年 5 月		1
bootstrap-switch.js	Apache License 2.0	javascript	High 1	3.3.4	2017/2/26			4
joyent/node-sshpk	MIT License	javascript	High 1	v1.13.1	2017/6/8	1 年 7 月	8	15
lodash-node.npm	MIT License	javascript	High 1	3.2.0	2015/2/13	11 月 16 日		42
select2/select2	MIT License	javascript	Medium 1	4.0.5	2017/10/26			44
@kano/kit-app-shell-electron.npm	MIT License	javascript	0.0.2-alpha.0	2018/12/12		22		1

点击上图 1 处，将显示当前的版本以及此组件的版本变化历史，如下图所示



- 显示组件的项目信息

第三方组件

All Licenses & Vulnerabilities Obsolescence		证书风险介绍 低 中 高 未定义						
组件	证书	技术	CVE	版本	发布	Gap	发布 / 12 个月	文件
BitTorrent-bencode.js		python	Critical 2 High 2 Medium 1	5.0.8	2007/7/30	3 年 5 月		1
bootstrap-switch.js	Apache License 2.0	javascript	High 1	3.3.4	2017/2/26			4
joyent/node-sshpk	MIT License	javascript	High 1	v1.13.1	2017/6/8	1 年 7 月	8	15
lodash-node.npm	MIT License	javascript	High 1	3.2.0	2015/2/13	11 月 16 日		42
select2/select2	MIT License	javascript	Medium 1	4.0.5	2017/10/26			44
@kano/kit-app-shell-electron.npm	MIT License	javascript		0.0.2-alpha.0	2018/12/12		22	1

点击上图 2 处，将链接到此组件的项目信息网站

- 显示组件的漏洞信息

第三方组件

All Licenses & Vulnerabilities Obsolescence		证书风险介绍 低 中 高 未定义						
组件	证书	技术	CVE	版本	发布	Gap	发布 / 12 个月	文件
BitTorrent-bencode.js		python	Critical 2 High 2 Medium 1	5.0.8	2007/7/30	3 年 5 月		1
bootstrap-switch.js	Apache License 2.0	javascript	High 1	3.3.4	2017/2/26			4
joyent/node-sshpk	MIT License	javascript	High 1	v1.13.1	2017/6/8	1 年 7 月	8	15
lodash-node.npm	MIT License	javascript	High 1	3.2.0	2015/2/13	11 月 16 日		42
select2/select2	MIT License	javascript	Medium 1	4.0.5	2017/10/26			44
@kano/kit-app-shell-electron.npm	MIT License	javascript		0.0.2-alpha.0	2018/12/12		22	1

点击上图 3 处，将显示此组件包含的漏洞的详细信息，如下图所示

Possible Vulnerabilities (5)

CVE-2015-5474

CRITICAL Score 9.3 CWE-77 Improper Neutralization of Special Elements used in a Command (Command Injection)

Report false positive

BitTorrent and uTorrent allow remote attackers to inject command line parameters and execute arbitrary commands via a crafted URL using the (1) bittorrent or (2) magnet protocol.

References

zerodayexpress.com

CVE-2014-8515

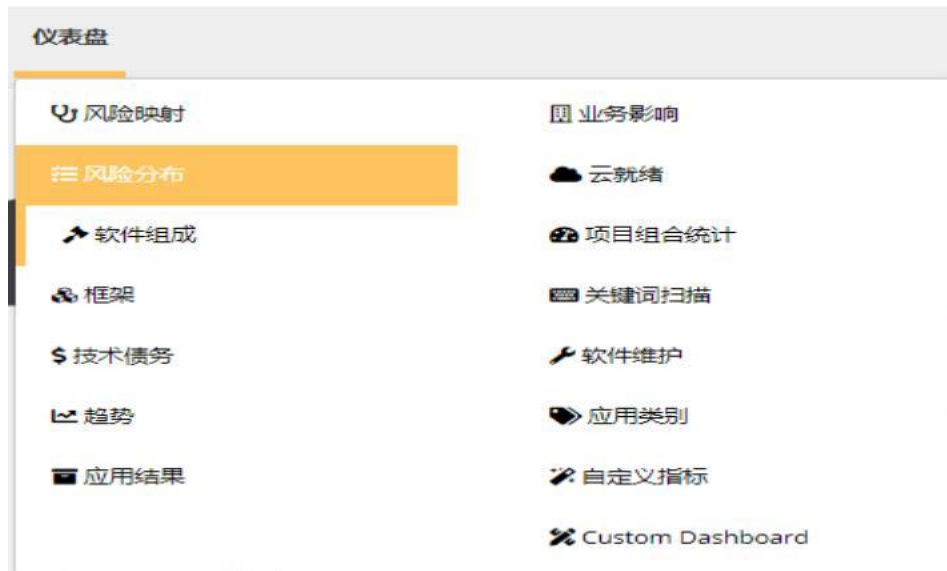
HIGH Score 6.8 CWE-77 Improper Neutralization of Special Elements used in a Command (Command Injection)

Report false positive

The web interface in BitTorrent allows remote attackers to execute arbitrary commands by leveraging knowledge of the pairing values and a crafted request to port 10000.

● Highlight 总体管理视图

分别点击仪表盘上的各项视图，查看 Highlight 的结果分析视图。这些视图，是整个企业的所有扫描应用的总体管理视图。



● 单个应用的管理视图

点击关心的应用，进入单个应用的视图，分别点击视图类型，查看单个应用的信息。

