**VIETNAM CYBERSPACE SECURITY TECHNOLOGY**

**JSC**

**🙜🙞🕮🙜🙞**



**TÀI LIỆU**

**CÀI ĐẶT VÀ SỬ DỤNG CHECKMARX**

Người thực hiện: Mai Thành Thắng

HÀ NỘI-10/2019

Mục Lục

[1. Thông tin tổng quan. 3](#_Toc22288709)

[2. Trình bày về CxSAST( Static Application Security Testing) 10](#_Toc22288710)

[a, Tổng quan về CxSAST 10](#_Toc22288711)

[b, Chuẩn bị trước khi cài đặt: 11](#_Toc22288712)

[c, Cài đặt CxSAST 12](#_Toc22288713)

[d, Sửa đổi CxSAST 20](#_Toc22288714)

[e. Sửa chữa CxSAST 21](#_Toc22288715)

[f, Gỡ CxSAST 22](#_Toc22288716)

[g, Sao lưu CxSAST 24](#_Toc22288717)

[h, Tạo và quản lý một dự án CxSAST 24](#_Toc22288718)

[i, Cấu hình Source Control 28](#_Toc22288719)

[k, Bật SSL hỗ trợ cho CxManager 32](#_Toc22288720)

[3. Trình bày CxOSA 43](#_Toc22288721)

[a, Cài đặt CxOSA 44](#_Toc22288722)

[b, Gỡ cài đặt 44](#_Toc22288723)

[c, Tạo và quản lý dự án CxOSA 45](#_Toc22288724)

[d, Bắt đầu quét một CxOSA 46](#_Toc22288725)

[e, Hiển thị kết quả quét 46](#_Toc22288726)

[4. Sử dụng Checkmarx 50](#_Toc22288727)

# Thông tin tổng quan.

**Checkmarx** là hãng phần mềm của Israel, cung cấp nền tảng bảo mật ứng dụng toàn diện để tìm kiếm và sửa chữa các tầng ứng dụng dễ bị xâm nhập trong quá trình phát triển phần mềm cũng như ngăn chặn các cuộc tấn công theo thời gian thực. Nổi bật nhất là giải pháp kiểm thử bảo mật ứng dụng Tĩnh (**CxSAST**), một sản phẩm cho phép các nhà phát triển và kiểm toán dễ dàng rà soát các tập tin không được mã hóa trong tất cả các ngôn ngữ lập trình phổ biến và phát hiện các lỗ hổng bảo mật.

Giải pháp dò quét, phân tích bảo mật định danh các vị trí/dòng code gây ra các lỗ hổng bảo mật và cung cấp các thông tin hỗ trợ sửa chữa, khắc phục tương ứng.

**Lợi ích:**

* Công cụ đánh giá an ninh mã nguồn mạnh nhất.
* Tích hợp chặt với SDLC(chu trình phát triển phần mềm).
* Rà quét nhanh, mức độ chính xác cao.
* Cung cấp mô hình dò quét và phân tích bảo mật ứng dụng tổng thể.
* Đánh giá bảo mật theo chuẩn và tùy biến security script.
* Hỗ trợ nhiều nhất các ngôn ngữ lập trình bao gồm cả Mobile.
* Dễ dàng triển khai, cài đặt và sử dụng Checkmarx

**CxSAST(Kiểm tra bảo mật ứng dụng tĩnh)**

|  |
| --- |
|  |
| **Môi trường** | **Ngôn ngữ Chính** | **Ngôn ngữ thứ 2** | **Nền tảng** | **Tập tin mở rộng** |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/java-logo.png?version=2&modificationDate=1559737043736&cacheVersion=1&api=v2&width=100&height=135** | * Java * J2SE * J2EE | * JSP * JavaScript * VBScript * PL\SQL * HTML5 | * Struts * Spring MVC * Spring Dependency Injection * iBatis\* * GWT * Hibernate * OWASP ESAPI * JSTL FMT Taglib * ATG DSP Taglib * Java Server Faces (JSF) * JSP * Google Guice * PrimeFaces | * .javasln * .project * .java * .jsp * .jspf * .tag * .tld * .hbs |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/csharp1.png?version=1&modificationDate=1556437896229&cacheVersion=1&api=v2&width=100&height=35** | * C# * VB.NET | * ASP.NET * JavaScript * VBScript * PL\SQL * HTML5 | * Enterprise Libraries * Telerik * ComponentArt * Infragistics * iBatis\* * Hibernate.Net [\*] * Entity framework * ASP.Net MVC framework * ASP.Net CORE Razor * ASP.NET Core | * .sln * .csproj * .cs * .cshtml * .xaml * .vb |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/classic-asp.png?version=1&modificationDate=1556437892743&cacheVersion=1&api=v2&width=100&height=100** | ASP | * JavaScript [\*\*] * VBScript * PL\SQL * HTML5 | ASP.Net MVC framework | * .asp |
| **https://checkmarx.atlassian.net/wiki/download/attachments/1269825578/vb6.png?version=1&modificationDate=1556437895994&cacheVersion=1&api=v2** | VB6 |  |  | * .bas * .vbp * .frm * .cls * .dsr * .ctl * .vb |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/cplusplus.png?version=1&modificationDate=1556437893654&cacheVersion=1&api=v2&width=100&height=66** | C/C++ |  | * MISRA * Informix ESQL/C * MySQL | * .cpp * .c++ * .cxx * .hpp * .hh * .h++ * .hxx * .c * .cc * .h |
|  | PHP | JavaScript | * Zend * Kohana * CakePHP * Symfony * Smarty * bWapp * OWASP ESAPI | * .php * .php3 * .php4 * .php5 * .php5.6 * .phtm * .phtml * .tpl * .ctp * .twig |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/apexx.png?version=1&modificationDate=1556437896971&cacheVersion=1&api=v2&width=130&height=54** | Apex | VisualForce | Lightning | * .apex * .apexp * .page * .component * .cls * .trigger * .tgr * .object * .report * .workflow |
| **http://boxchronicles.com/wp-content/uploads/2015/01/ruby.png** | Ruby |  | Ruby on Rails | * .rb * .rhtml * .rxml * .rjs * .erb |
| **http://3.bp.blogspot.com/-PTty3CfTGnA/TpZOEjTQ_WI/AAAAAAAAAeo/KeKt_D5X2xo/s1600/js.jpg** | JavaScript ES5 ES6 |  | * JQuery * Node.js * Ajax * Knockout * AngularJS * ExpressJS * Pug (Jade) * Backbone * Handlebars * Cordova / PhoneGap * Hapi.JS * XS (SAP) * Kony Visualizer * ReactJS\* * SAPUI5 | * .js * .htm * .html * .json |
| Related image | Typescript\*\* |  | Angular | * .ts * .html |
| **http://9v.lt/blog/materiolas/featured_images/vbscript-mini-logo.png** |  |  |  | * .vbs |
| **http://taste-of-it.de/wp-content/uploads/2013/10/perl-logo.jpg** | Perl |  |  | * .pl * .pm * .plx * .psgi |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/android.png?version=1&modificationDate=1556437894992&cacheVersion=1&api=v2 | Android (Java) |  | * Volley (Android) | * .java * .kt |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/apple%20IOS.png?version=1&modificationDate=1556437894093&cacheVersion=1&api=v2&width=130&height=63 | Objective C Swift |  |  | * .m * .h * .swift * .xib |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/html5.png?version=1&modificationDate=1556437894771&cacheVersion=1&api=v2** |  |  |  | * .html * .htm |
| **https://checkmarx.atlassian.net/wiki/download/attachments/1269825578/plsql.png?version=1&modificationDate=1556437892971&cacheVersion=1&api=v2** |  |  |  | * .pls * .sql * .pkh * .pks * .pkb * .pck |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/python.png?version=1&modificationDate=1556437894551&cacheVersion=1&api=v2** | Python | 1. JavaScript 2. VB script 3. PL\SQL | Django | * .py |
| **https://upload.wikimedia.org/wikipedia/commons/thumb/3/36/Groovy-logo.svg/614px-Groovy-logo.svg.png** | Groovy | * JavaScript * VB script * PL\SQL |  | * .groovy * .gsh * .gvy * .gy |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/scala-logo.png?version=1&modificationDate=1556437893875&cacheVersion=1&api=v2&width=130&height=38 | Scala |  | Akka | * .scala * .sc |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/GO.jpg?version=1&modificationDate=1556437898137&cacheVersion=1&api=v2&width=120&height=58 | GO Language |  | Protobuf | * .go |
| Image result for kotlin logo | Kotlin for Android |  |  | * .kt * .kts |
|  |  |  |  | Other extensions:   * .aspx * .ascx * .config * .xml * .cgi * .inc |

**[\*]** YÊU CẦU ĐIỀU CHỈNH NHỎ

**[\*\*]**PHÍA KHÁCH HÀNG

**Open Source Analysis (CxOSA) (Phân tich nguồn mở)**

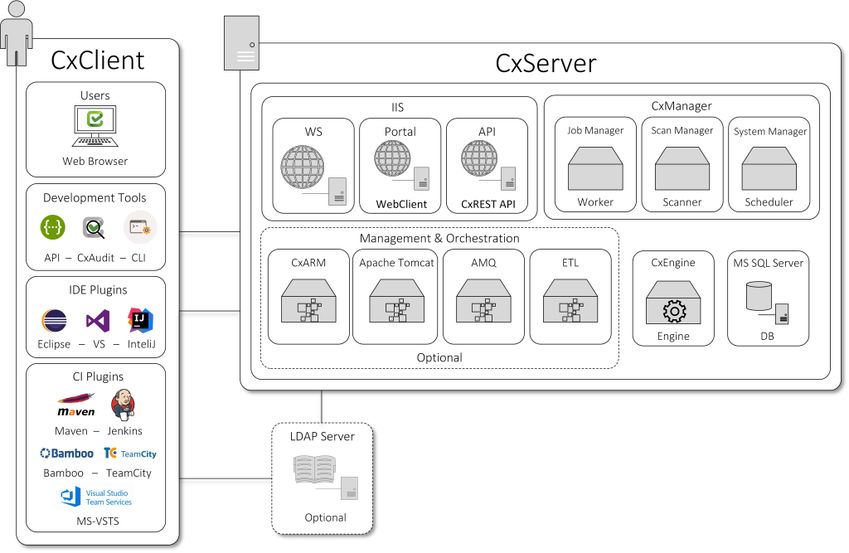
| **Môi trường** | **Tập tin mở rộng** |  | **Môi trường** | **Tập tin mở rộng** |
| --- | --- | --- | --- | --- |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/java-logo.png?version=2&modificationDate=1559737043736&cacheVersion=1&api=v2&width=75&height=101**  **Java** | .Jar |  | https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/dotnet.png?version=2&modificationDate=1559737727238&cacheVersion=1&api=v2&width=150&height=74  **.Net** | .DLL |
| **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/js-logo.png?version=1&modificationDate=1559736877655&cacheVersion=1&api=v2&width=85&height=85**  **JavaScript** | .js |  | https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/TypeScript%20logo.png?version=1&modificationDate=1559736971334&cacheVersion=1&api=v2&width=200&height=56  **TypeScript** |  |
| Image result for React logo  **React** |  |  | https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/nodejs-logo.png?version=1&modificationDate=1559736819501&cacheVersion=1&api=v2&width=85&height=92  **NodeJS** |  |
| Related image  **Angular** |  |  | https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/wcf-logo.png?version=1&modificationDate=1559736764099&cacheVersion=1&api=v2&width=100&height=74  **WCF** |  |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/WPF.png?version=1&modificationDate=1559736695351&cacheVersion=1&api=v2&width=85&height=85  **WPF** |  |  | **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/Fsharp-logo.png?version=1&modificationDate=1559737132405&cacheVersion=1&api=v2&width=85&height=85**  **F#** |  |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/C%23.jpg?version=2&modificationDate=1559734102516&cacheVersion=1&api=v2&width=100&height=100  **C#** | .DLL |  | **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/.net.jpg?version=1&modificationDate=1559734165598&cacheVersion=1&api=v2&width=100&height=100**  **.NET** |  |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/476349238/python.png?version=1&modificationDate=1525096185557&cacheVersion=1&api=v2  **Python** |  |  | Related image  **Groovy** |  |
|  |  |  |  |  |
| **Gói quản lý** |  |  | **Gói quản lý** |  |
| https://checkmarx.atlassian.net/wiki/download/attachments/1269825578/image2019-4-16_10-53-42.png?version=1&modificationDate=1556437892280&cacheVersion=1&api=v2  **Gradle** |  |  | **https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/Apache%20Maven.png?version=1&modificationDate=1559736631597&cacheVersion=1&api=v2&width=150&height=52**  **Maven** |  |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/npm.png?version=1&modificationDate=1559734307550&cacheVersion=1&api=v2&width=100&height=66  **NPM** |  |  | Image result for yarn logo  **Yarn** |  |
| https://checkmarx.atlassian.net/wiki/download/thumbnails/1269825578/nuget.png?version=1&modificationDate=1559734224946&cacheVersion=1&api=v2&width=150&height=45  **NuGet** | .nupkg |  |  |  |

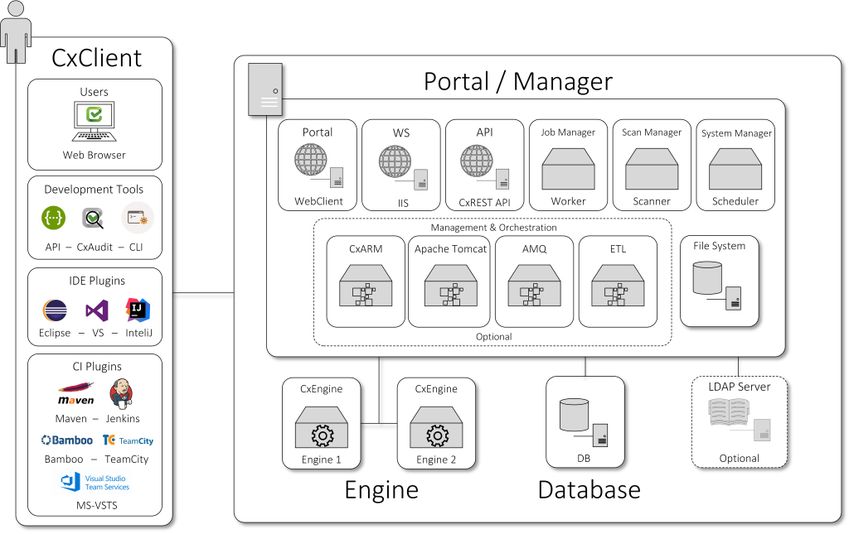
# CxSAST( Static Application Security Testing) và CxOSA

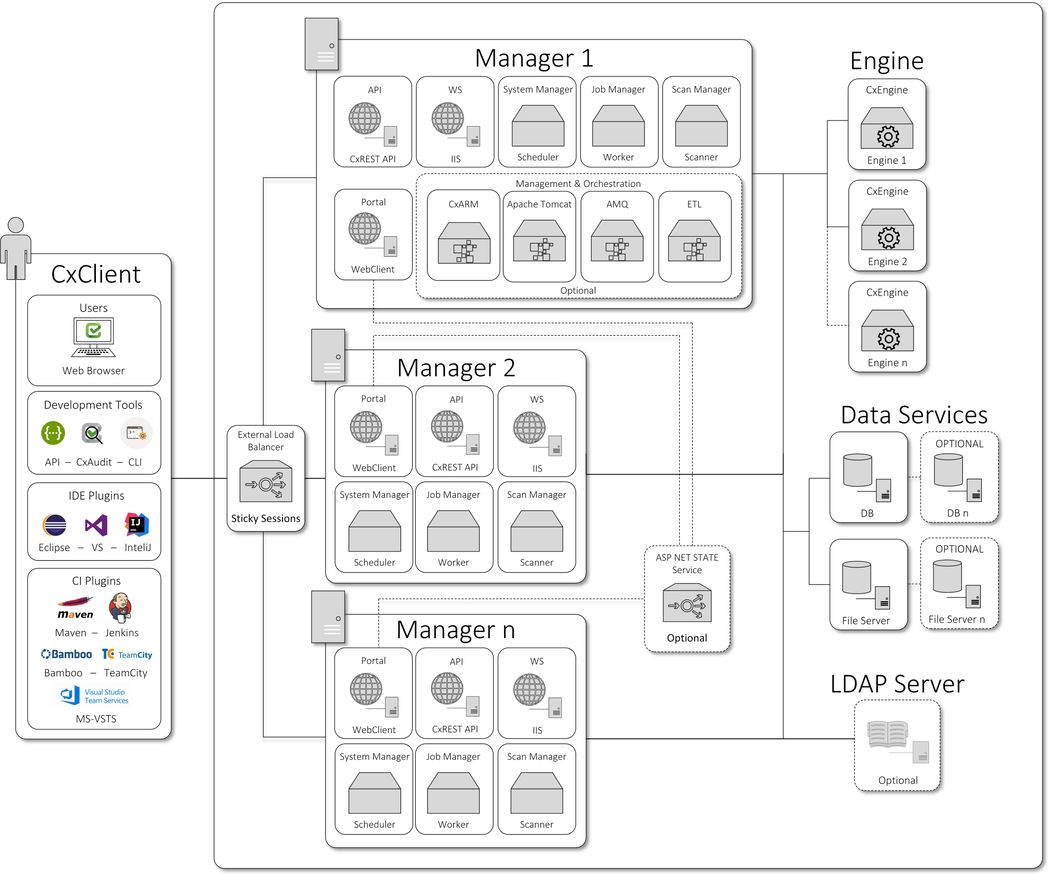
## CxSAST

### a, Tổng quan về CxSAST

CxSAST hỗ trợ kiến ​​trúc tập trung, trong đó tất cả các thành phần máy chủ được cài đặt trên cùng một máy chủ.

  
CxSAST hỗ trợ kiến ​​trúc phân tán, trong đó bất kỳ hoặc tất cả các thành phần máy chủ được cài đặt trên các máy chủ chuyên dụng.



CxSAST hỗ trợ kiến ​​trúc khả dụng cao, trong đó hai hoặc nhiều máy chủ CxManager (ở chế độ hoạt động tích cực) được cài đặt và có thể truy cập cùng một cơ sở dữ liệu. Điều này đảm bảo rằng trong trường hợp một CxManager bị lỗi, hệ thống sẽ tiếp tục hoạt động. 

### b, Chuẩn bị trước khi cài đặt:

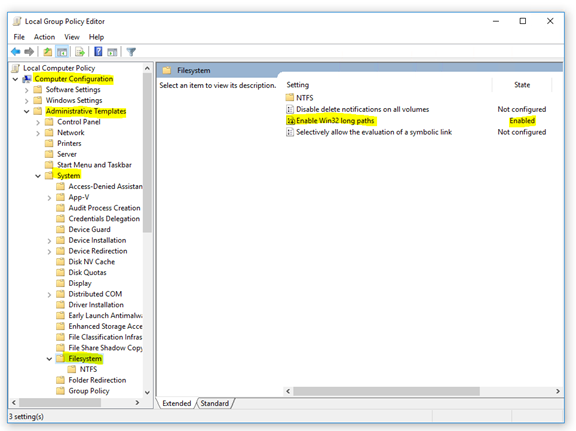
**Yêu cầu về hệ thống server khi cài đặt:**

<https://checkmarx.atlassian.net/wiki/spaces/KC/pages/1157955744/Server+Host+Requirements+v8.9.0>

**Môi trường hỗ trợ:** <https://checkmarx.atlassian.net/wiki/spaces/KC/pages/1274773513/Supported+Environments+v8.9.0>

* Đảm bảo  [Centralized](https://checkmarx.atlassian.net/wiki/spaces/KC/pages/79921191) hoặc [CxManager](https://checkmarx.atlassian.net/wiki/spaces/KC/pages/79921219) hostname không chứa ký tự đặc biệt.
* Đảm bảo hệ thống tường lửa của hệ thống cho phép chạy cổng 80, 1434, 1433
* Nếu sử dụng SQL cho CxSAST đảm bảo rằng: Sql server và Sql server browser luôn chạy
* Nếu sử dụng CxARM: SQL Server Browser luôn bật và chạy  SQL Server  cho CxARM
* Không cho phần mềm quét virut quét các thư mục: **CxSrc, ExtSrc, CxReports.** Thư mục cài checkmarx **C:\Program Files\Checkmarx\**
* **Phải cài đặt và cấu hình IIS.**
* **Lưu ý: Kích hoạt hỗ trợ đường dẫn dài trong Windows 10 và Server 2016:**

**Windows+R: gõ gpedit.msc và cấu hình như ảnh:**



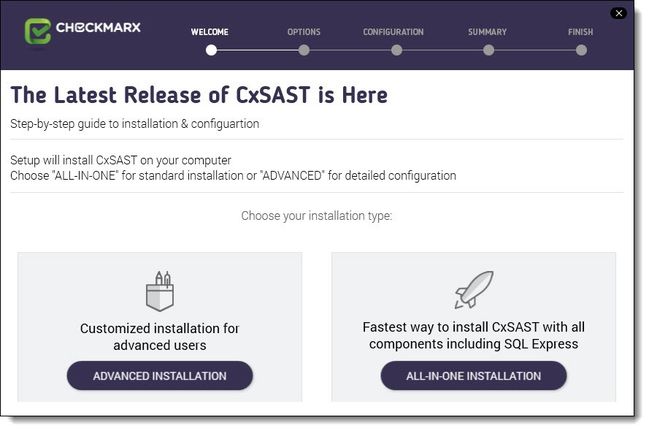
### c, Cài đặt CxSAST

Bước 1: chuẩn bị trước cài đặt

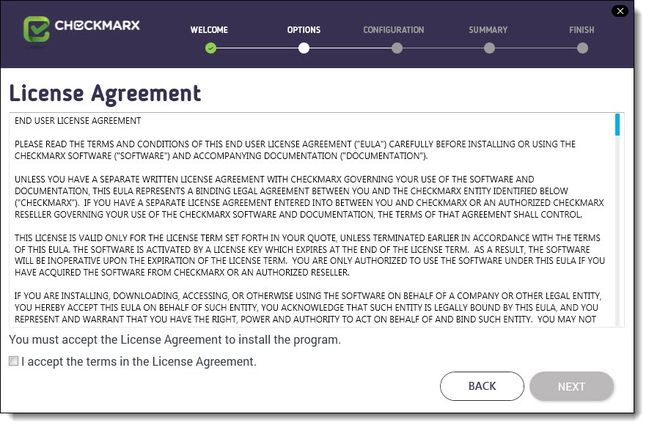
* Cài SQL server cho  **CxSAST( thường dùng SQL express)**
* Cài IIS trên window server.
* Cài đặt gói phần mềm lên như bình thường và xác định các dịch vụ Cx luôn được bật.

Đi cùng với phiên bản cài đặt là ứng với các phiên bản hotfix tải kèm theo. Có 7 phiên bản hotfix khác nhau. Mỗi phiên bản sẽ giải quyết lỗi nhanh khác nhau tùy theo từng phiên bản checkmarx bạn đang sử dụng và language bạn đang chạy thông tin cụ thể xem: <https://checkmarx.atlassian.net/wiki/spaces/KC/pages/1305051169/8.9.0+Hotfix+1-7>

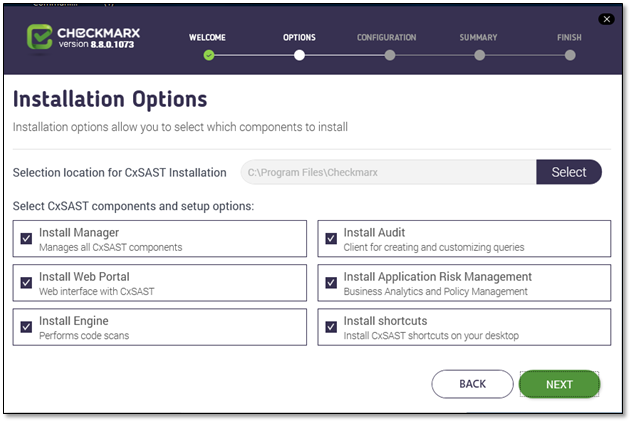
Bước 2: Run file **CxSetup.exe**:



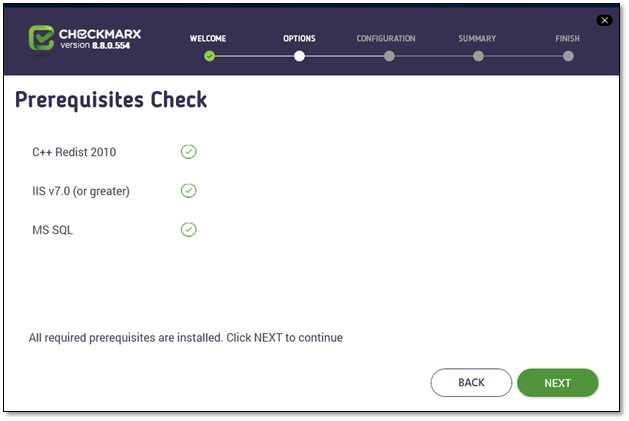
Chọn **Advanced installation.**  Tiếp theo bấm tích **I accept…**  và next



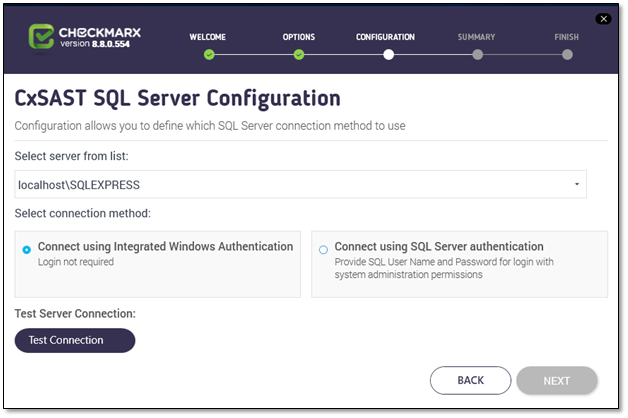
Tích cài đủ dịch vụ như hình.



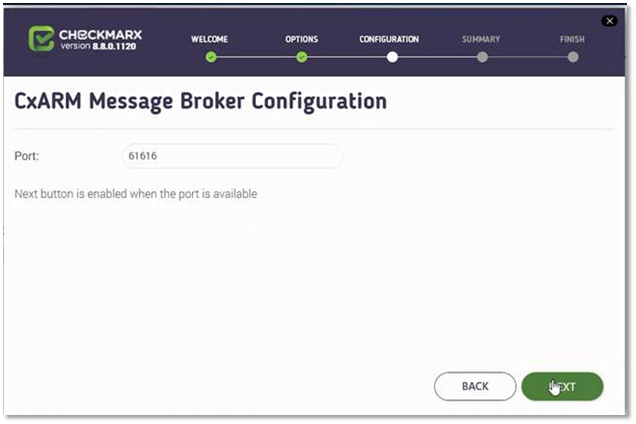
Bấm **Next.** Hệ thống kiểm tra.



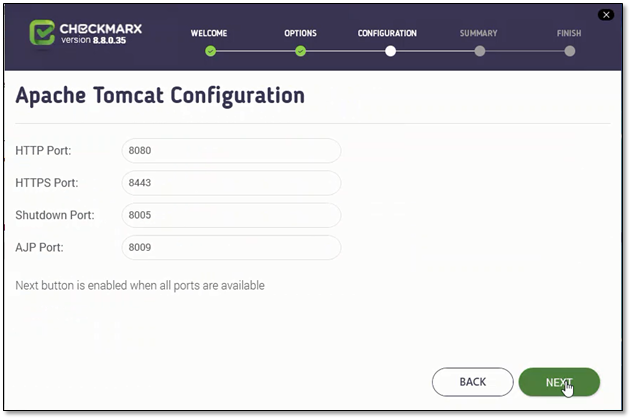
Chọn **Select server from list**( đây là instance SQL đang dùng)



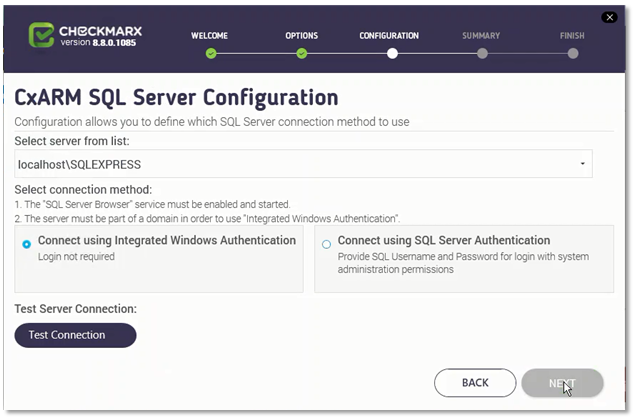
Sau khi cấu hình nên **test connection**

Nếu cấu hình **CxARM. Nó hiển thị**

Nên để thiết lập cổng tin nhắn thông báo mặc định rồi bấm **Next**  Cấu hình Apache tomcat

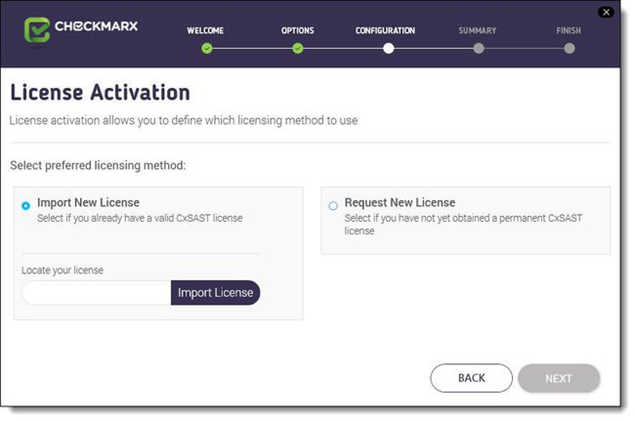


Tiếp theo cấu hình **CxARM SQL Server**

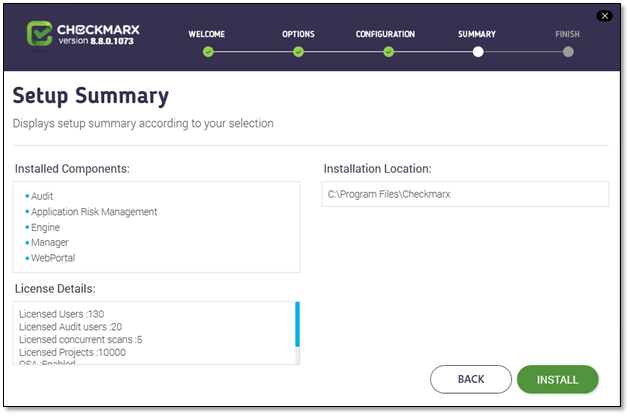


Tương tự như cấu hình SQL ở trên.

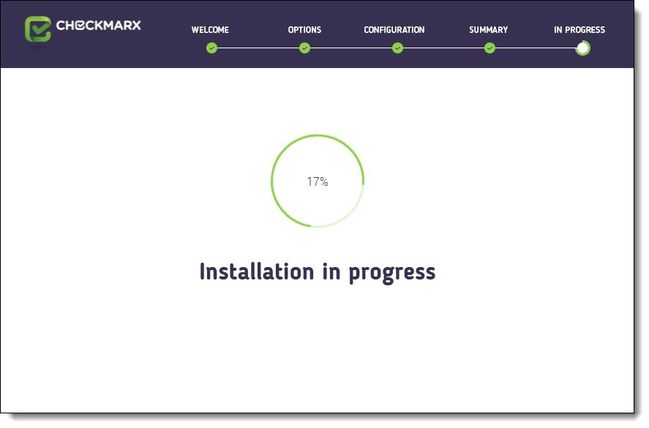
Import License



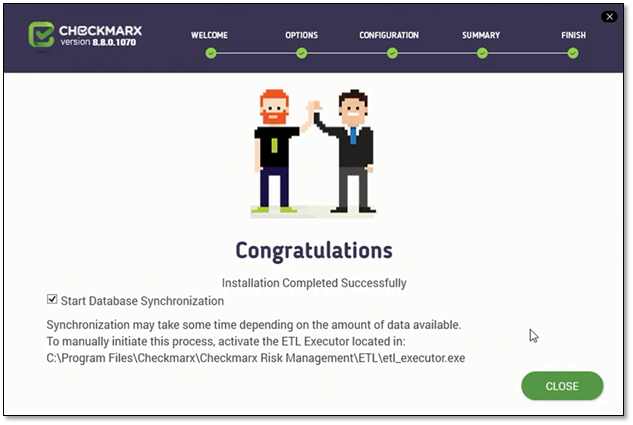
**Next** bước tiếp:



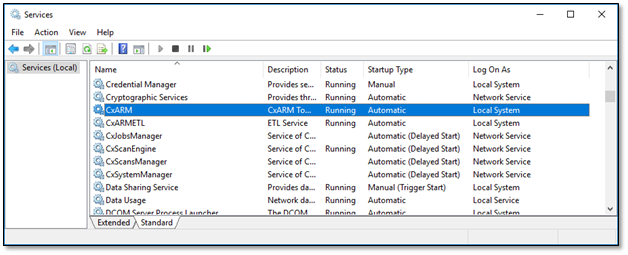
Đây là thông tin phầm sẽ được cài đặt thành phần nào, thông tin license, Đường dẫn lưu file. Bấm **Install** và đợi cài đặt.



Cài đặt thành công.

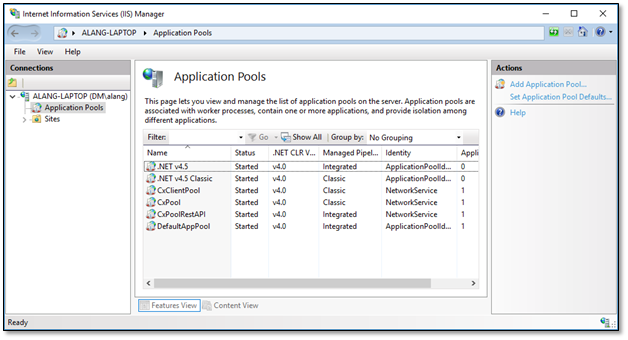


Check xem các dịch vụ của Cx đã start chưa: **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**



Cài đặt kiểm tra **Application Pool** của IIS

**Start** > **Control Panel** > **All Control Panel Items** > **Administrative Tools** > **Internet Information Services (IIS) Manager**



Sau khi kiểm tra ok, vào web brother, trên Url gõ: [**http://localhost/CxWebClient/ login.aspx**](http://localhost/CxWebClient/%20login.aspx) **or http://<ip\_internal\_server> /** **CxWebClient/login.aspx**

**Cấu hình user admin**

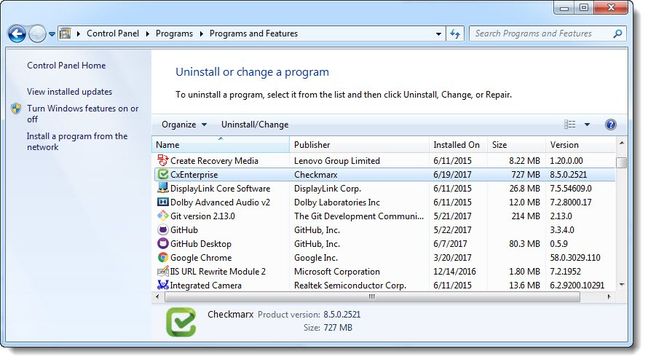


Lưu ý đặt mật khẩu theo đúng yêu cầu.

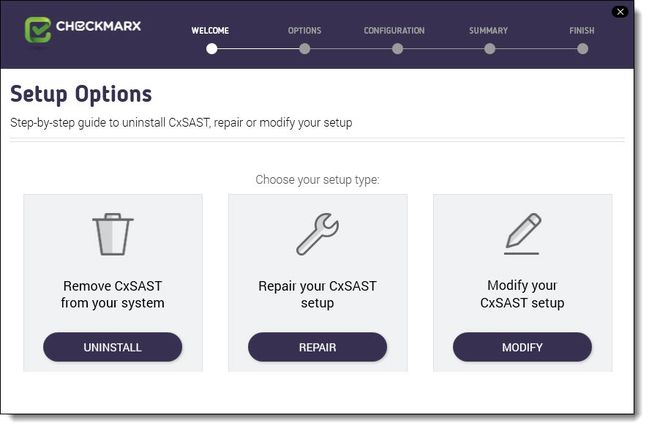
### d, Sửa đổi CxSAST

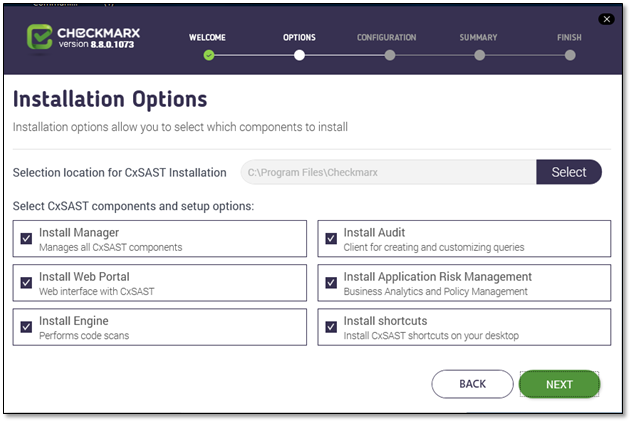
* **Cần tắt hết các dịch vụ của Cx**
* Sau đó vào: **Start > Control Panel > Programs > Programs and Features.**

Click đúp vào **CxEnterprise** chọn **Uninstall/Change**

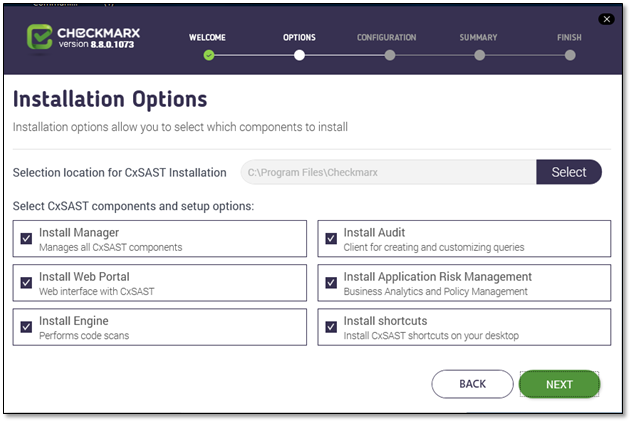


Tại cửa sổ **Setup Options chọn MODIFY click Ok**





Bấm **next.** Tại cửa sổ  **Installation Options** . Chỉnh sửa lại thành phần và cài đặt CxSAST



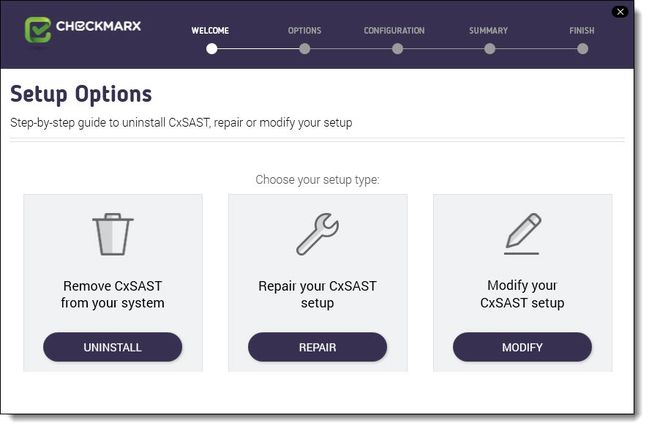
Bấm next chuyển sang cửa sổ tiếp theo. Các bước tiếp theo làm giống **phần cài đặt checkmarx.**

### e. Sửa chữa CxSAST

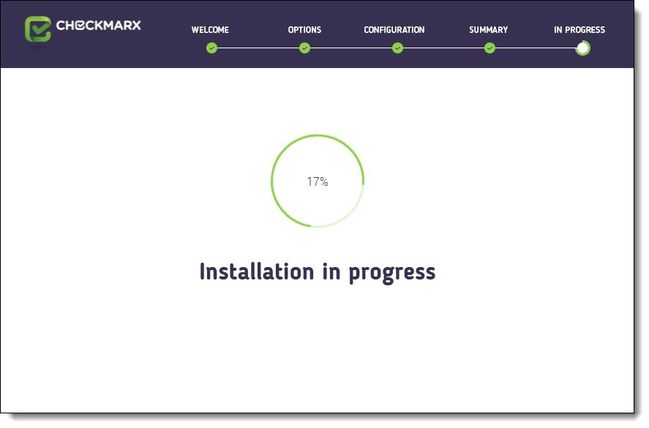
* **Cần tắt hết các dịch vụ của Cx**
* Sau đó vào: **Start > Control Panel > Programs > Programs and Features.**

Click đúp vào **CxEnterprise** chọn **Uninstall/Change**

* Tại cửa sổ **Setup Options chọn REPAIR click Ok**



* Quá trình sửa lỗi sẽ bắt đầu

-

- Thành công

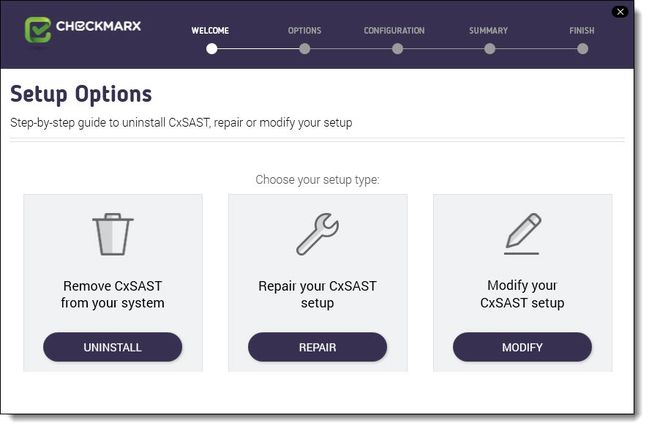


### f, Gỡ cài đặt bằng bộ cài CxSAST

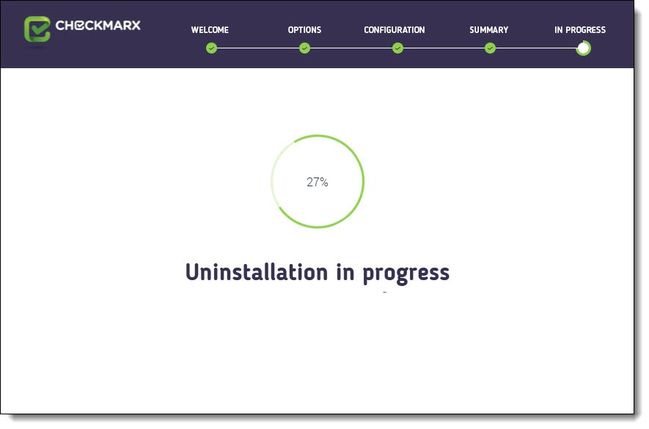
* **Cần tắt hết các dịch vụ của Cx**
* Sau đó vào: **Start > Control Panel > Programs > Programs and Features.**

Click đúp vào **CxEnterprise** chọn **Uninstall/Change**

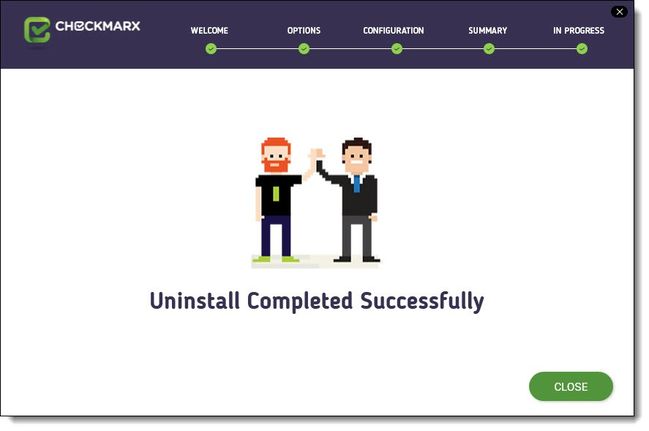
* Tại cửa sổ **Setup Options chọn Unintall click Ok**



* Quá trình gỡ sẽ bắt đầu:



Chú ý nếu có cảnh bảo phải đọc nếu không có gì hiện thị như này là gỡ thành côngs



### g, Sao lưu CxSAST

* Stop dịch vụ Cx
* Stop IIS server



* Sao lưu thư mục Checkmarx bằng cách sao chép nó sang một thư mục khác

Vd: <Checkmarx Installation Path>\Checkmarx -> <Checkmarx Installation Path>\CheckmarxBackup10162019 ( đường dẫn thư mục backup)

* Sao lưu **CxDB, CxActivity và CxARM SQL** bằng **standard Database tools**
* Sao lưu **CxSRC folder** bằng cách copy ra 1 thư mục mới

VD: X:\CxSrc -> X:\CxSrcBackup10162019( tên thư mục backup)

* Sau khi hoàn thành quá trình thì khởi động lại các dịch vụ Cx và IIS server

### h, Tạo và quản lý một dự án CxSAST

* Trên giao diện web chọn **Project & Scans >** **Create New Project**

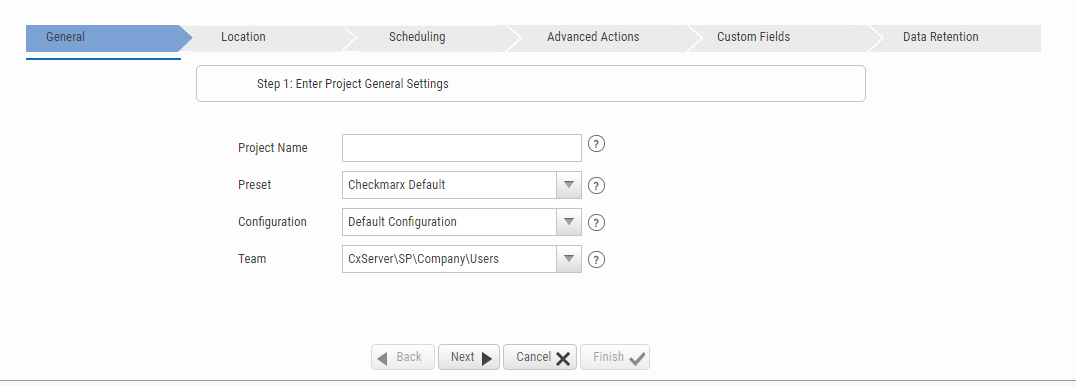
Bước 1: Nhập cài đặt chung của dự án

**Project Name**: Đặt tên cho dự án. ( Tên này phải phù hợp với loại mã nguồn bạn đang thực hiện kiểm tra)

**Preset**: Lựa chọn quy tắc quét cho dự án. Chọn Preset thích hợp từ danh sách.

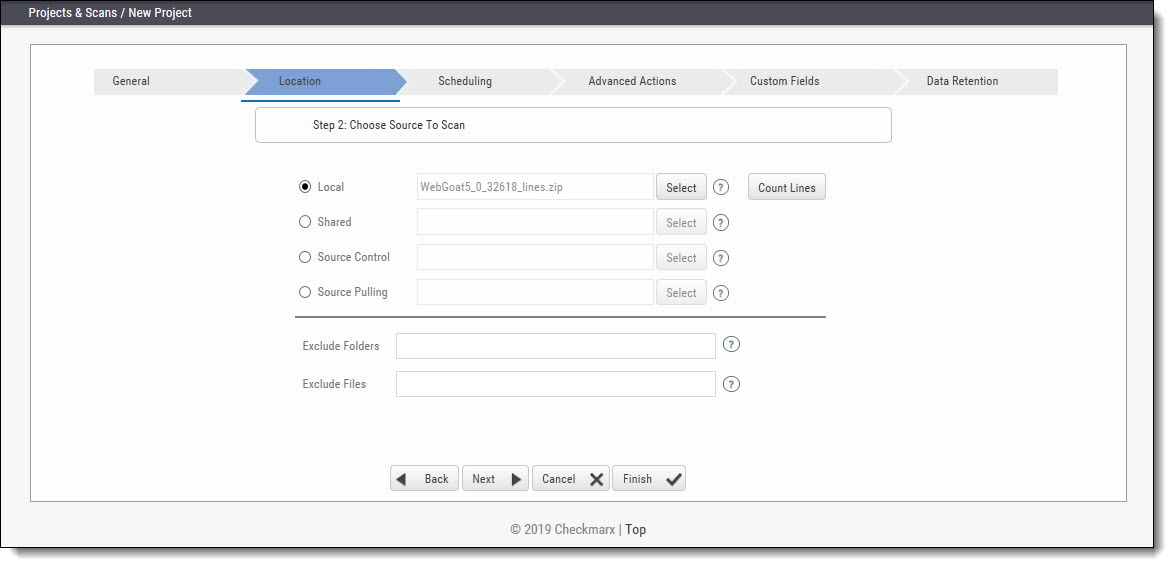
**Configuration**: Chọn cấu hình cho dự án mới. Đối với phiên bản dùng thử, nên thực hiện lựa chọn mặc định.

**Team**: Chọn nhóm cho dự án mới. Đối với phiên bản dùng thử, nên thực hiện lựa chọn mặc định

**Policy:** Chọn một chính sách cho dự án. Đối với phiên bản dùng thử, nên chọn từ lựa chọn mặc định.

* Bấm next.

Bước 2: là bước chọn nguồn để quét .



Phần này cấu hình mã nguồn tải lên theo vị trí( file tải lên .zip):

**Local**: mã nguồn năm tại thư mục nào đó máy chủ bạn muốn quét

**Share**: mã nguồn năm ở một máy chủ chia sẻ mà máy chủ CxSAST có thể truy cập đến

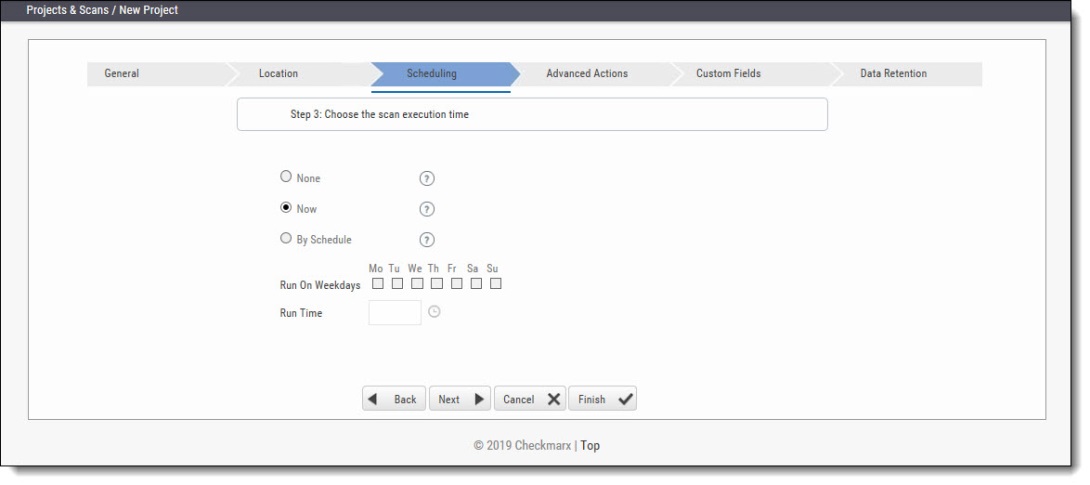
**Source Control**: Mã nguồn nằm trên các máy chủ kiểm soát nguồn nó cũng lưu trữ các nguồn , bao gồm TFS , SVN , GIT

**Source Pulling**: một phần mở rộng cho tùy chọn "Share", "Source Pulling" kích hoạt định cấu hình để kéo mã nguồn từ máy chủ *kiểm soát* nguồn vào vị trí được chia sẻ. Lưu ý: tập lệnh này phải được đặt cấu hình trước đó trong ứng dụng máy khách CxSAST Windows.

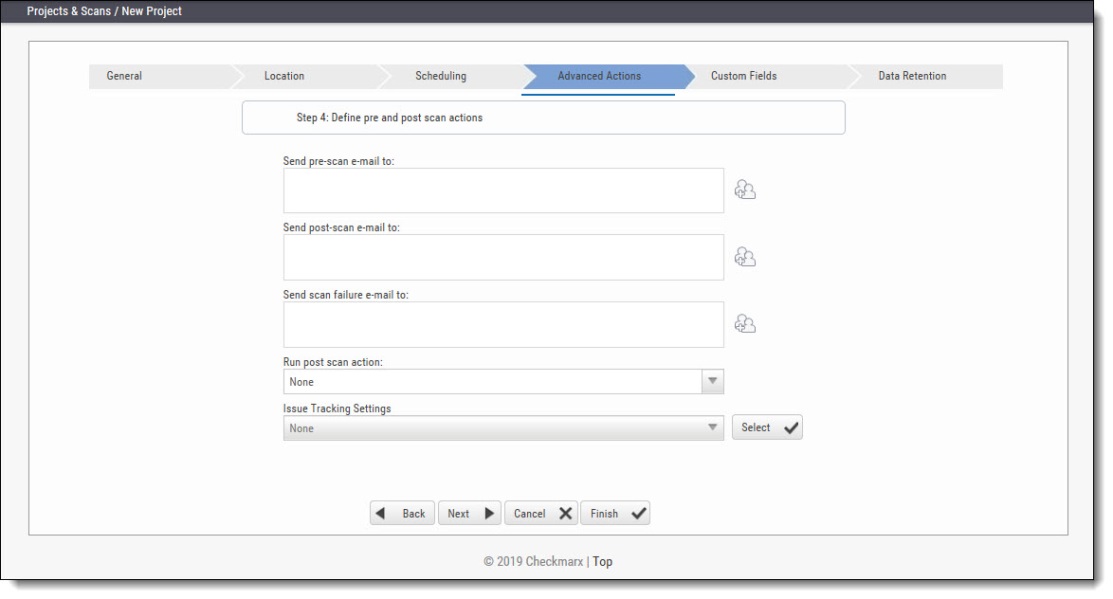
**Lưu ý**: Nếu bạn chọn mã nguồn local bạn phải thực hiện “**Count line**” đếm số dòng code vì mỗi phiên bản Cx chỉ hỗ trợ quét với mã có số lượng dòng code nhỏ hơn hoặc bằng số lượng dòng code của Cx có thể quét.

* Bấm **Next**

Bước 3: Đặt lịch quét (có thể đặt hoặc không )



Bước 4: Có thể cấu hình gửi kết quả quét về cho người dùng ( bước này có thể cấu hình hoặc không cần cấu hình)

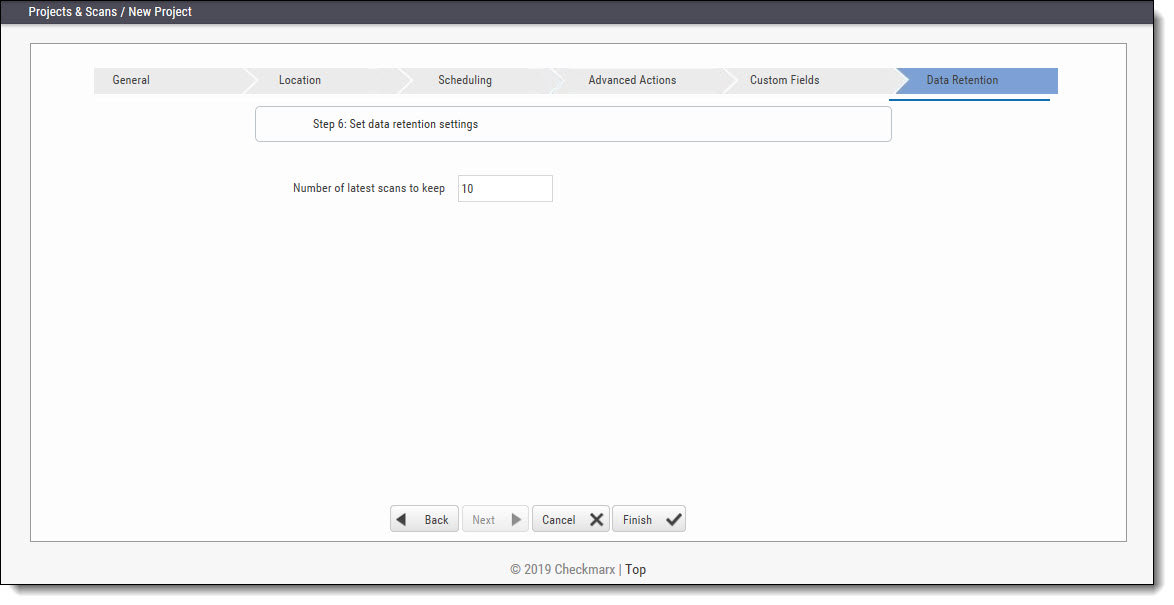


Bấm **Next**.

  Bước 5: Định cấu hình thuộc tính Trường tùy chỉnh theo các trường tùy chỉnh có sẵn của dự án



Bấm  **Next**. Bước 6: cài đặt duy trì dữ liệu:

Cấu hình các thuộc tính lưu giữ dữ liệu

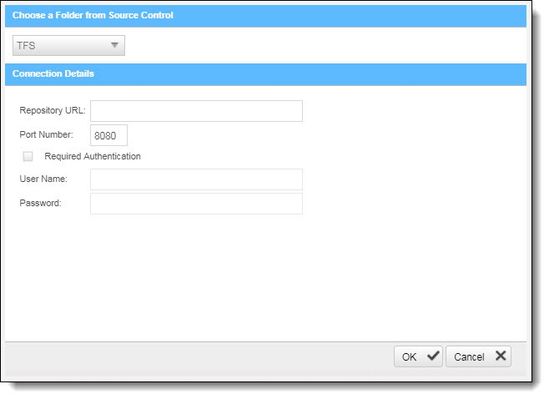
**Chú ý:** Bạn có thể kết thúc bước tạo dự án (project) sau khi hoàn thành bước số 2.

### i, Cấu hình project tích hợp với Source Control

**Cấu hình TFS(Team Foundation Server) cho CxSAST**

Team Foundation Server (TFS) là một chương trình server được sử dụng để quản lý mã nguồn của các lập trình viên trong các dự án chung.

Chọn **TFS**. Mô tả thông số cần cấu hình



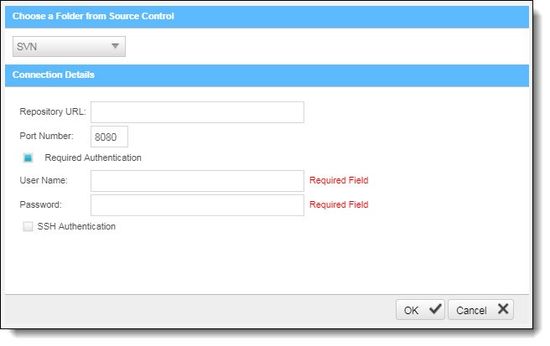
* **Repository URL** – Địa chỉ web lưu trữ nguồn (hỗ trợ HTTP và HTTPS, ví dụ: <protocol>://<site name>:<port>/tfs/<Collection> (Chỏ đến tên kho lưu trữ <Collection>)).
* **Port Number** – Số cổng
* **Required Authentication** – Lựu chọn yêu cầu xác thực hay không
* **User Name** – tên tài khoản
* **Password** – mật khẩu xác thực

Chọn  **OK Khi cấu hình xong**.

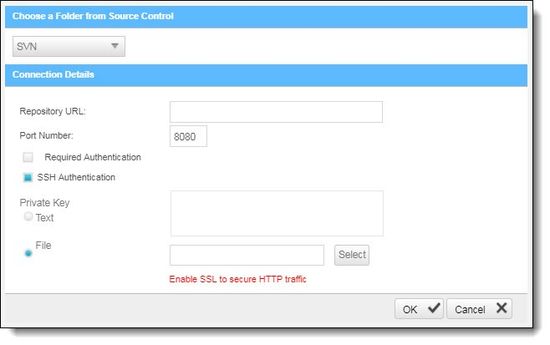
**Cấu hình SVN(Subversion) cho CxSAST**

**SVN** Subversion **là** hệ thống quản lý source code tập trung (Centralized). **SVN** Subversion **là** hệ thống quản lý phiên bản mạnh mẽ, hữu dụng, và linh hoạt. ... **SVN** Subversion giống như một hệ thống file **server** mà các client có thể download và upload file một cách bình thường.

Chọn **SVN** . bạn cần cấu hình những thông số sau:



* **Repository URL** – Địa chỉ web lưu trữ nguồn (hỗ trợ HTTP , HTTPS, và SSH khóa riêng/công khai, ví dụ:  <protocol>://<server\_ip>/<repository\_name>)
* **Port Number** – số cổng
* **Required Authentication** – Lựu chọn yêu cầu xác thực hay không
* **User Name** – tên tài khoản
* **Password** – mật khẩu xác thực
* **SHH Authentication** - chọn sử dụng xác thực an toàn với SSH hay không

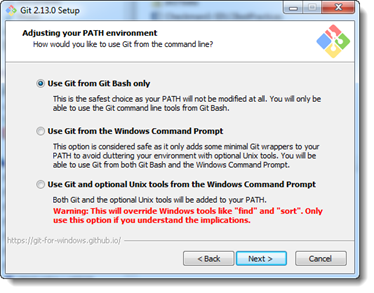


Nếu chọn phải cấu hình đủ thông số

* **Private Key Text** – thêm nội dung khóa riêng
* **Private Key File** – Hoặc lựa chọn tập tin khóa riêng
* **Bấm Ok hoàn thành**

**Cài đặt git cho CxSAST:**

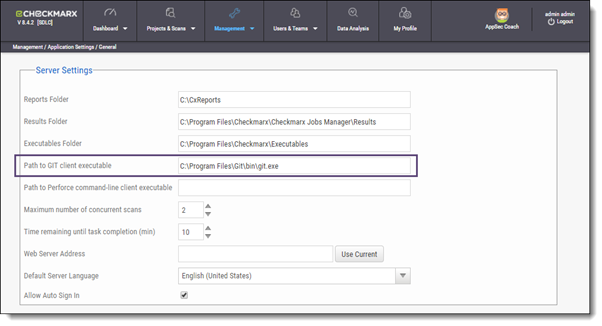
* Tải gói phần mềm cài đặt git: <https://git-scm.com/download>
* Chạy gói tải về để thiết lập mặc định cho đến phần **Path Environment**  chọn như hình



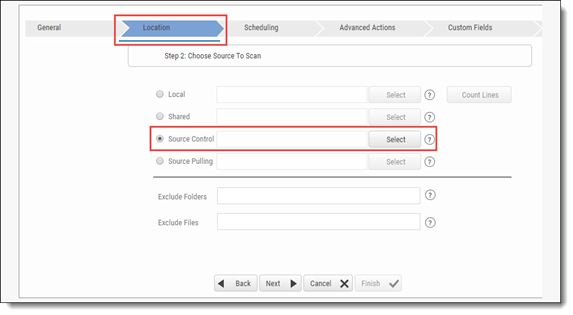
* Bấm next và chọn vị chí lưu file **git.exe**. Mặc định là đường dẫn **C:\Program Files\Git\bin**

**Trên giao diện web chọn Management** > **Application settings** > **General** > **Server Settings**

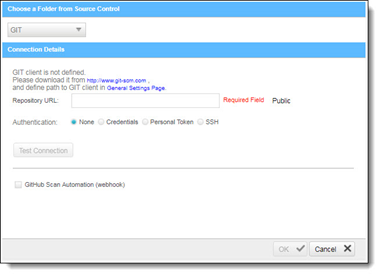
Sửa **Path to GIT client executable** Cài đặt như hình **git.exe**



**Projects & Scans** > **Create New Project** > **Location**):



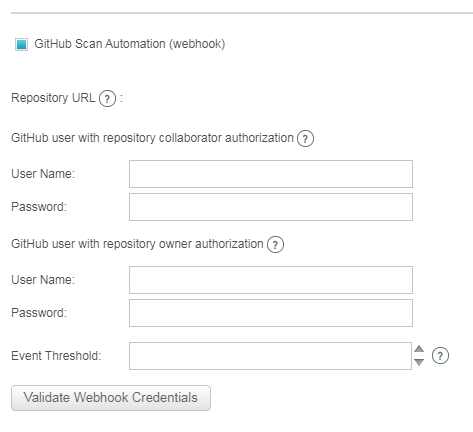
Chọn **Select** và chọn **GIT** từ **Source Control** trên xuống.



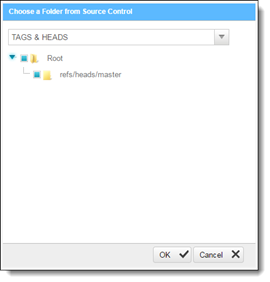
Phần này có thể đặt xác thực hoặc không cần thiết lập xác thực.

Nhấp vào tùy chọn **GitHub Scan Automation ( nếu cần)** Để tự động quét GitHub, ở đây phải chọn phần cấu hình phù hợp:

* Người dùng GitHub với quyền là công tác viên kho lưu trữ
* Người dùng GitHub có quyền chủ sở hữu kho lưu trữ



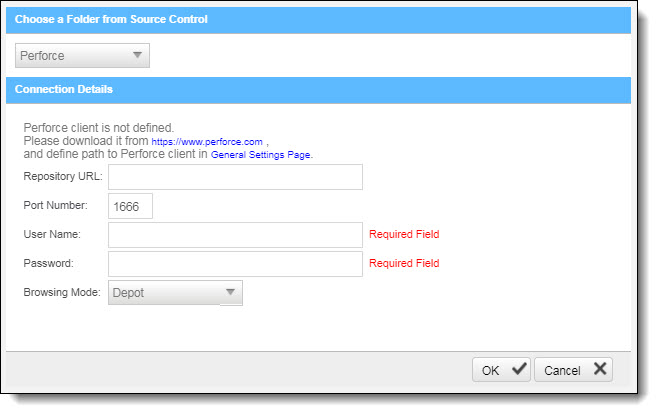
Sau khi cấu hình xong bấm **Ok.** Màn hình Source Control Folder sẽ hiện thị.



Bấm ok để kết thúc tạo dự án và tiến hành thực hiện bước quét mã nguồn

**Lưu ý:** repository URL bạn có thể lấy link public của trên github để quét nếu dùng mã nguồn trên github để xây dựng trang web.

**Cài đặt Perforce cho CxSAST**

Chọn Perforce . Hiển thị thông tin cần cấu hình:

* **Repository URL** – Địa chỉ web lưu trữ nguồn (Vi dụ SSL:<server\_ip> or <server\_ip>)
* **Port Number** – Số cổng
* **User Name** – tên tài khoản
* **Password** – mật khẩu xác thực
* **Browsing Mode(chọn chế độ)** – chọn **Depot** (cho kho lưu trữ tập tin được chia sẻ) hoặc **Workspace** (cho nhóm kho lưu trữ tập tin).

Chọn **OK** Kết thúc

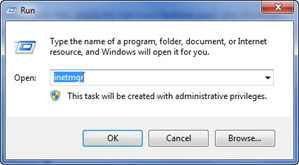
### k, Bật SSL và cài đặt https cho checkmarx

* Chuẩn bị một **Domain Server**
* Chuẩn bị một CA Certificate

+ Cài đặt chứng chỉ SSL free Let’s Crypt

<http://woshub.com/howto-install-free-lets-encrypt-ssl-cert-on-iis/>

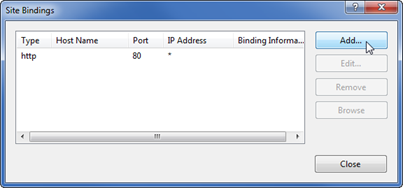
* Mở window+ R nhập: **inetmgr**



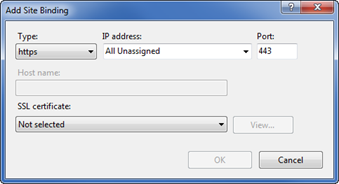
* Hiển thị IIS Manager .



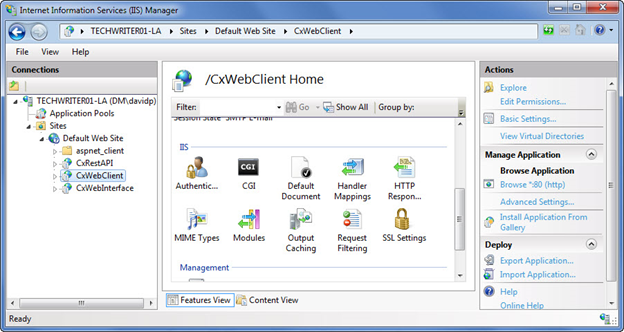
* Chọn **Default Web Site** từ **Sites**
* Chọn **Bindings**...



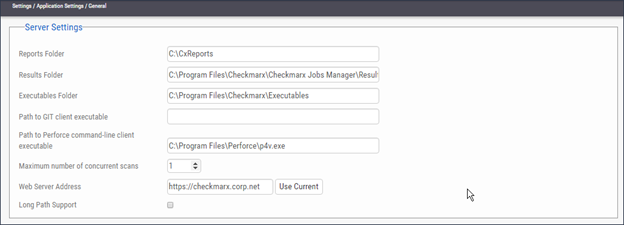
* Bấm **Add** thêm sites mới



* Chọn **Type** và chọn **https**.
* Chọn **SSL Certificate** và chọn chứng chỉ bạn tạo ra cho checkmarx.
* Bấm **OK** rồi bấm **Close**.
* Nếu muốn người dùng Nền tảng tiếp xúc với phần mềm Checkmarx chỉ có thể sử dụng **HTTPS / SSL**, hãy quay lại cửa sổ IIS manager và, đối với mỗi dịch vụ web có liên quan (CxWebClient, CxWebInterface), hãy thực hiện như sau:
* Bấm 2 lần **Default Web Site**



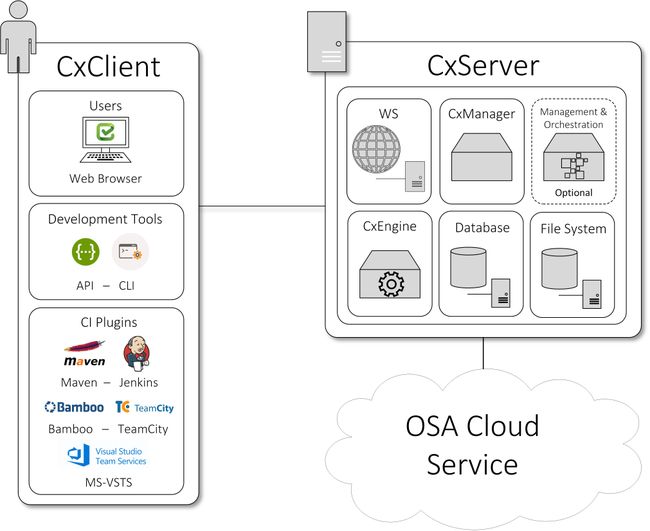
* Chọn **CxWebClient** và bấm 2 lần **SSL Settings**.
* Chọn **Require SSL** và bấm **Apply** .
* Thực hiện tương tự với **CxRestAPI** và **CxWebInterface**.
* Vào thư mục **C:\Program Files (x86)\Checkmarx\CheckmarxWebPortal\Web**, mở file **config** tìm từ khóa sau "**CxWSResolver.CxWSResolver**".
* Chỉnh sửa "**http://**" to "**https://**" và thay thế"**localhost**" (nếu có) với chứng chỉ được cài đặt sẵn của bạn <tên/tiêu đề>.
* Chuột phải Server web bấm stop rồi start lại.
* Trên **Giao diện web nền tảng tiếp xúc với phần mềm Checkmarx,** chọn **Management > Application Settings > General**. Phần **General Settings** như bên dưới.



* Chọn **Edit**.
* Nhập **Server URL** (e.g. https://checkmarx.corp.net) trong **Web Server Address**
* Chọn **Update** lưu thay đổi rồi truy cập lại web hằng https://

## CxOSA

Trinh phân tích mã nguồn mở là một quy trình có cấu trúc để xác định các vấn đề bảo mật và pháp lý được cộng đồng biết đến trong nguồn mở được sử dụng bởi các ứng dụng của khách hàng. Các lỗi chưa được phát hiện trong mã nguồn mở có thể khai thác và xâm nhập.



**Thành phần Client :**

* Web Portal
* API
* CLI
* CI Plugins

**Thành phần Server :**

* WS (IIS Web Service)
* CxManager
* Management & Orchestration (Optional)
* OSA Cloud Service
* Database.

Công cụ phân tích mã nguồn mở sẽ xác định rủi ro bằng các tiêu chí chính sau:

Dủi do bảo mật, rủi do chất lượng code, rủi do pháp luật.

**Tiến trình quét và trả kết quả:**

+ Cxclient tiến hành quét

+ Cx Server gửi figerprint (tệp quản lý gói) và kho lưu trữ đầy đủ (danh sách tất cả các thư viện nguồn mở nghi ngờ có lỗ hổng) đến Dịch vụ đám mây OSA

+ Osa cloud định nghĩa thành phần của mã nguồn và gán metadata (dạng dữ liệu miêu tả về dữ liệu)

+ OSA Cloud Service thực hiện quét và gửi kết quả về CxServer

+ Kết quả CxOSA quét lưu lại trong csdl của CxServer

+ CxServer gửi lại kết quả quét cho CxClient

### a, Cài đặt CxOSA

Tải sửa lỗi nhanh cho v8.9

* EXE: <https://download.checkmarx.com/8.9.0/HF/8.9.0.QF_OSA.zip>
* CLI: <https://download.checkmarx.com/8.9.0/HF/8.9.0.QF_OSA.CLI.zip>

và giải nén xong chạy tệp .exe

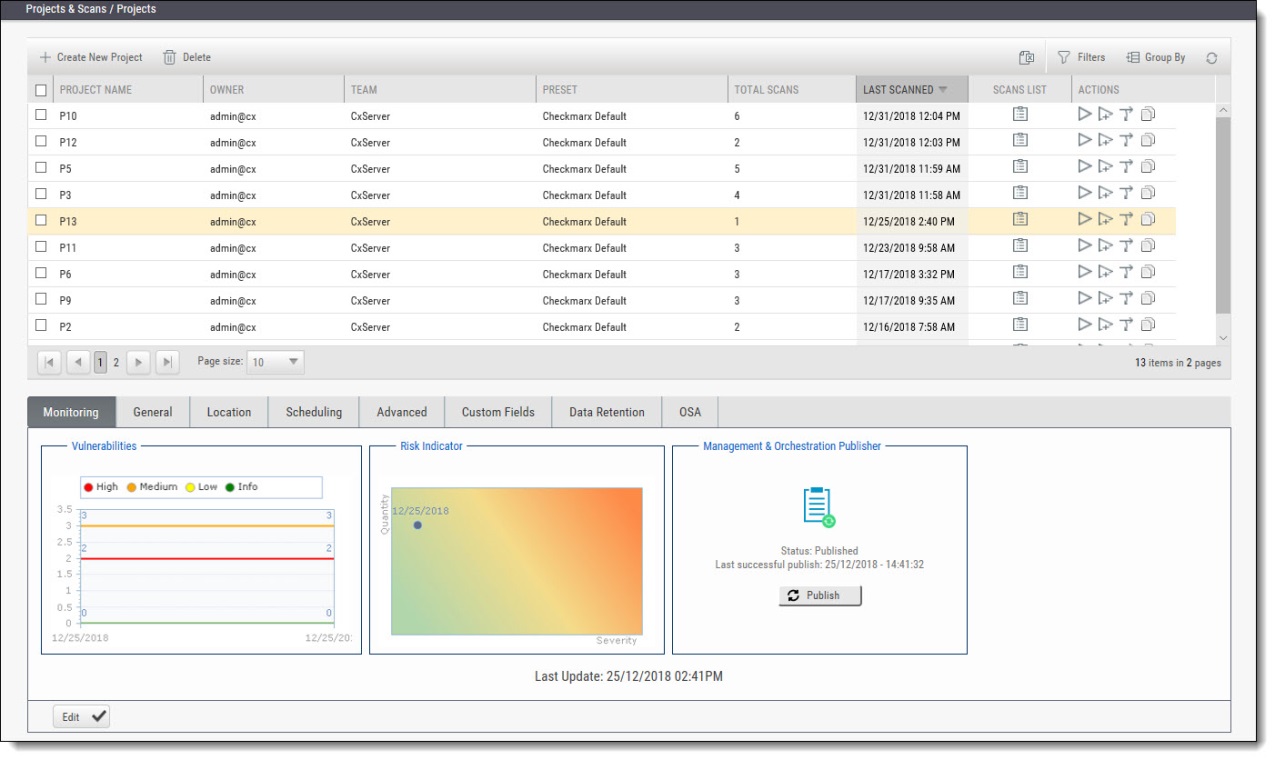
### b, Gỡ cài đặt

Thực hiện bước tương tự gỡ cài đặt trình bày ở CxSAST

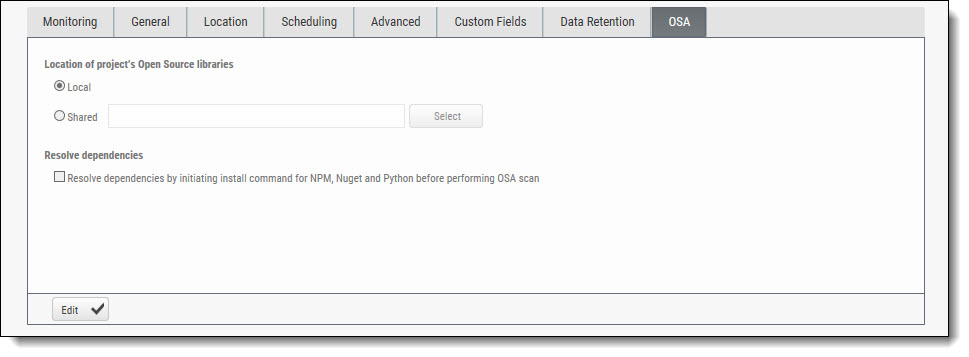
### c, Tạo và quản lý dự án CxOSA

* Tạo dự án CxOSA làm tương tự tạo một dự án CxSAST
* **Cấu hình dự án CxOSA**

**Chọn Projects & Scans -> Projects** hiển thị lên các dự án được tạo. Chọn lấy dự án muốn cấu hình OSA.



Chọn tab OSA



Chọn **edit** để chỉnh sửa:

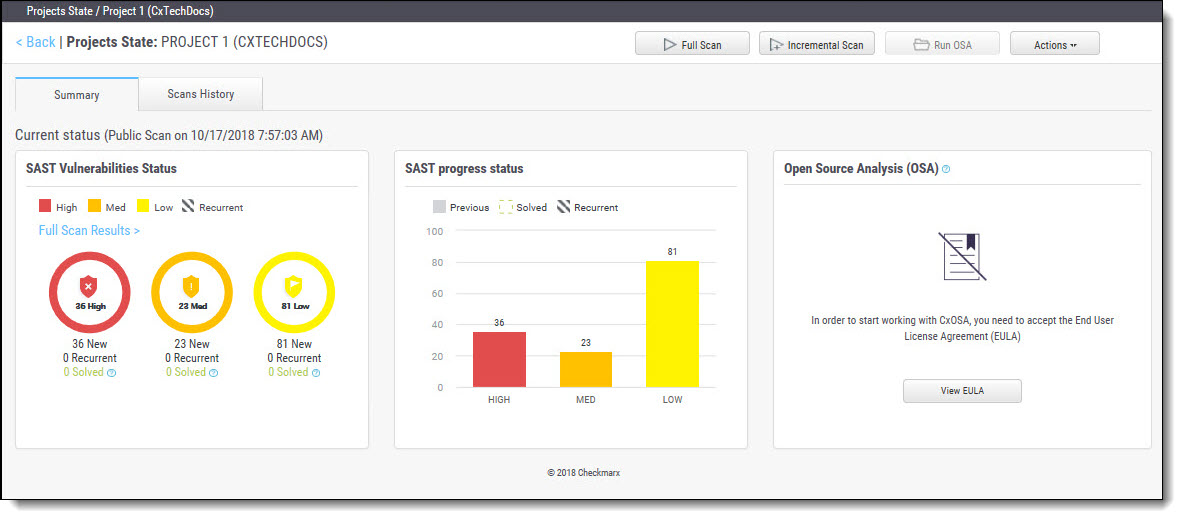
**Local**: thư viện nguồn mở được duy trì cục bộ. Sau khi được xác định, hãy điều hướng đến màn hình Trạng thái dự án hợp nhất để truy cập vào thư mục cục bộ, chọn tệp nén (.zip) có chứa các thư viện mã nguồn mở của dự án và chạy quét CxOSA.

**Shared**: các thư viện mã nguồn mở được duy trì trên một máy chủ mạng có thể truy cập từ Máy chủ CxSAST. Bấm Chọn, cung cấp thông tin xác thực miền Windows của bạn để CxSAST truy cập mạng (định dạng tên người dùng: domain\_name \ tên người dùng) và chọn một hoặc nhiều thư mục mạng chứa thư viện nguồn mở của dự án.

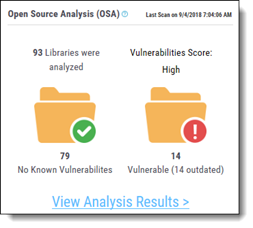
**Resolve dependencies** : Bấm tích để giải quyết các phụ thuộc bằng cách khởi chạy lệnh cài đặt cho NPM và Nuget trước khi thực hiện quét OSA**.**

### d, Bắt đầu quét một CxOSA

* Chọn **Dashboard -> Project State**  và chọn dự án bạn muốn thực hiện quét OSA



* Chọn EULA , đọc chính sách và đồng ý với chính sách
* Chọn Run CxOSA chọn mã nguồn .zip bạn muốn Scan và chọn Upload. Ví dụ hiển thị như hình.



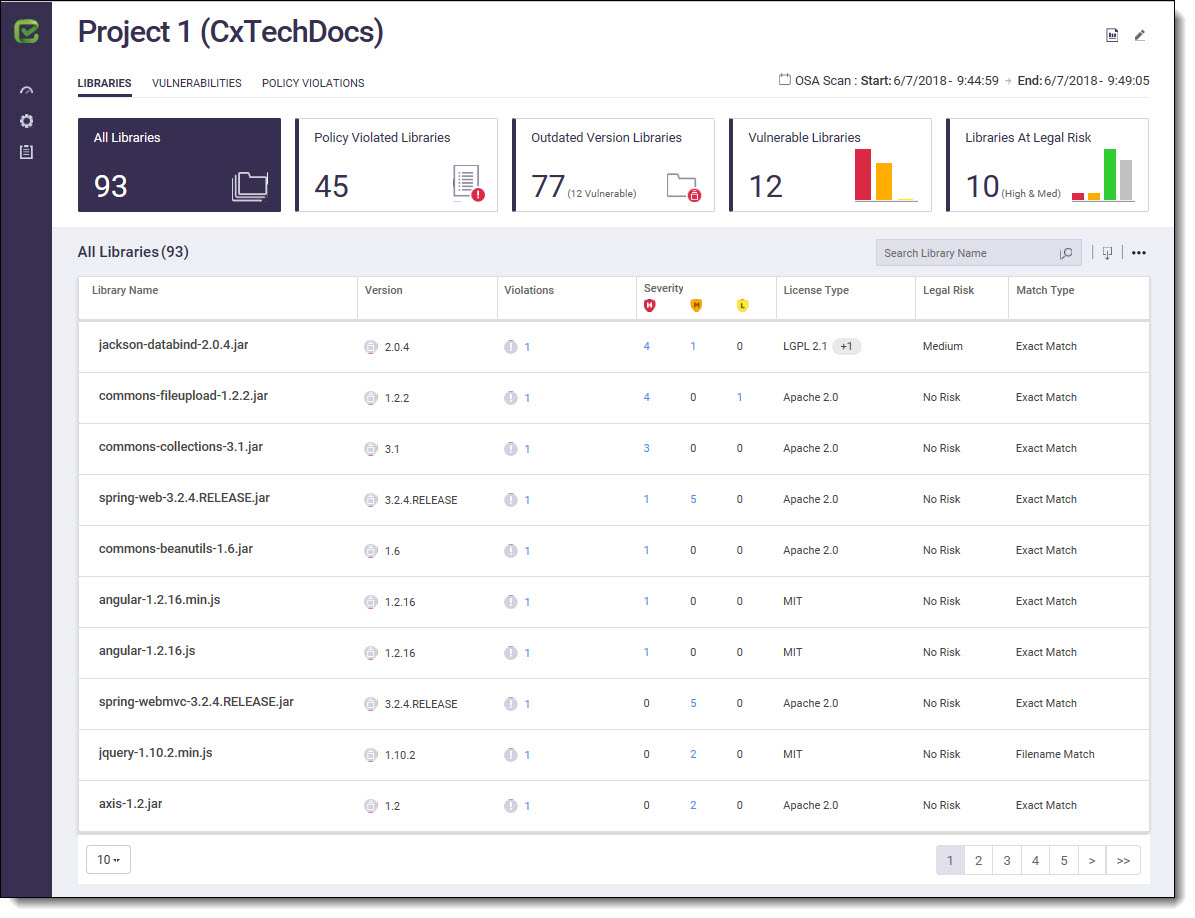
* Bấm View Analysis Results để xem kết quả quét.

### e, Hiển thị kết quả quét

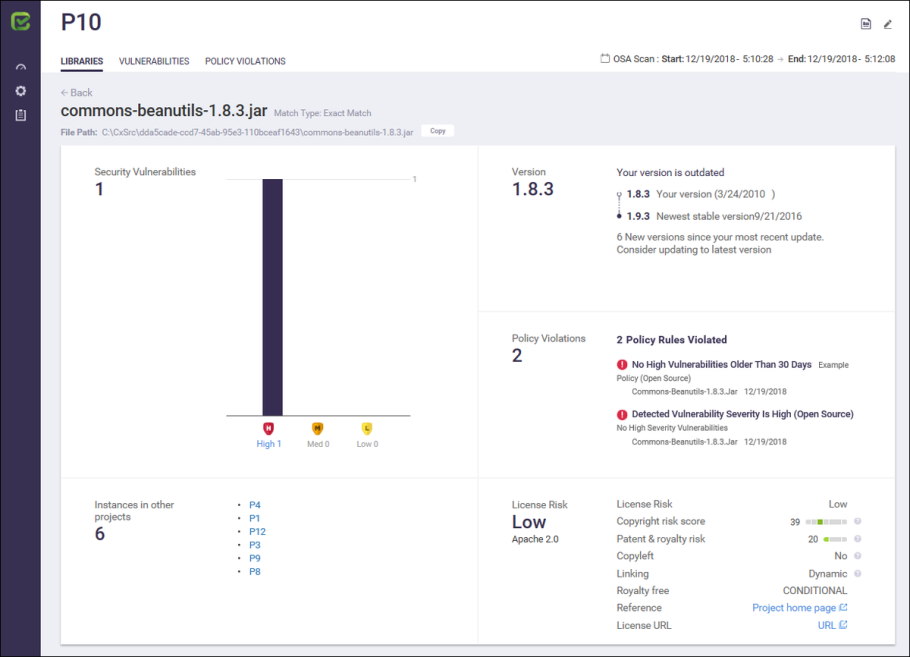
Xem một dự án OSA: Chọn một dự án từ màn hình **Consolidated Project State**, bấm **Actions** và chọn **Open CxOSA Viewer** từ trên xuống.

Ở thanh menu bên trái

|  |  |
| --- | --- |
| https://checkmarx.atlassian.net/wiki/download/attachments/976552191/Project%20State%20Icon.png?version=1&modificationDate=1539093039773&cacheVersion=1&api=v2 | **Project State** – Cung cấp quyền truy cập vào trạng thái dự án |
| https://checkmarx.atlassian.net/wiki/download/attachments/976552191/Application%20Settings%20Icon.png?version=1&modificationDate=1539093040350&cacheVersion=1&api=v2 | **OSA Settings** – Cung cấp quyền truy cập vào cài đặt quét CxOSA |
| https://checkmarx.atlassian.net/wiki/download/attachments/976552191/Policy%20Management%20icon.png?version=1&modificationDate=1539093040795&cacheVersion=1&api=v2 | **Policy Management - Cung cấp quyền truy cập vào quản lý chính sách CxOSA** |



Xem trạng thái thư viện: Chọn thư viện muốn xem, bấm vào sẽ hiển thị kết quả sau:

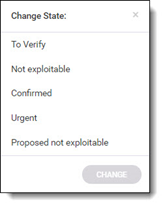


Quản lý lỗ hổng:

* Có thể thêm thông tin bình luận cho lỗ hổng

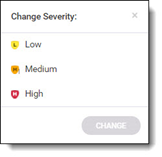


* Thay đổi trạng thái lỗ hổng

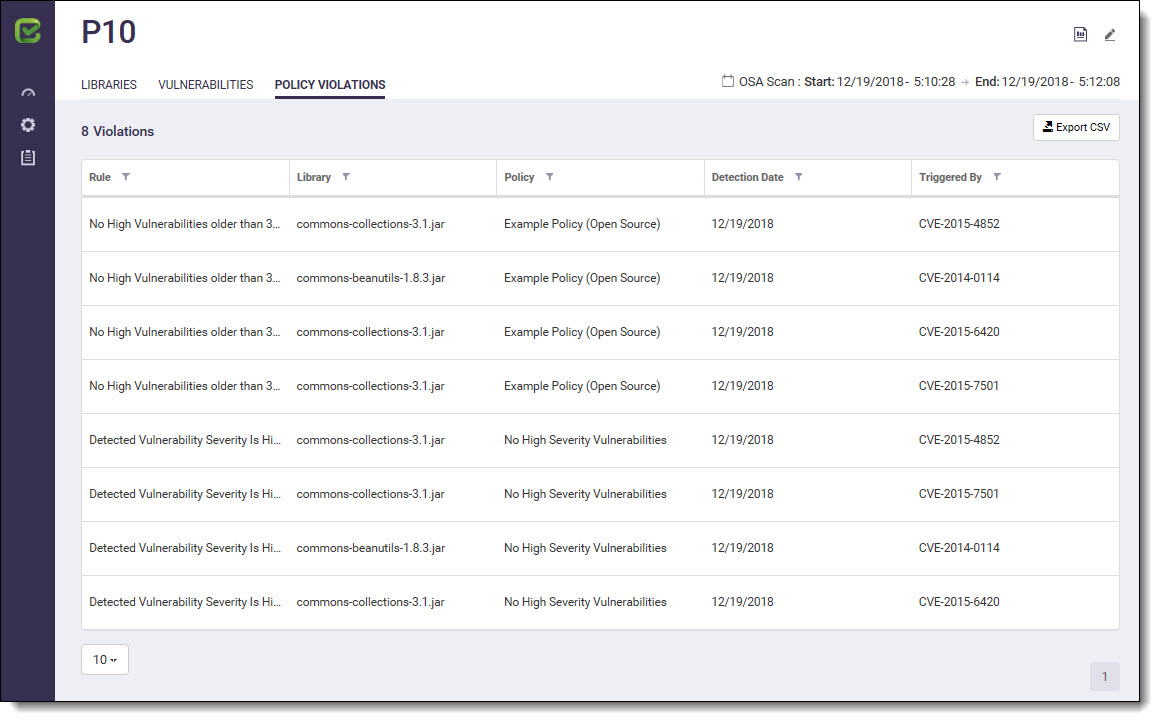


|  |  |
| --- | --- |
| **Loại** | **Mô tả** |
| **To Verify (default)** | Lỗ hổng cần được xác minh |
| **Not Exploitable** | Lỗ hổng được xác nhận không thể khai thác |
| **Confirmed** | Lỗ hổng có thể khai thác và cần xử lý |
| **Urgent** | Lỗ hổng có thể khai thác và cần xử lý gấp |
| **Proposed Not Exploitable** | Các lỗ hổng được xác định với trạng thái này vẫn là một mối đe dọa tiềm tàng cho đến khi trạng thái đó được thay đổi thành 'Xác nhận' hoặc 'Không thể khai thác' |

* Thay đổi mức độ nghiêm trọng của lỗ hổng

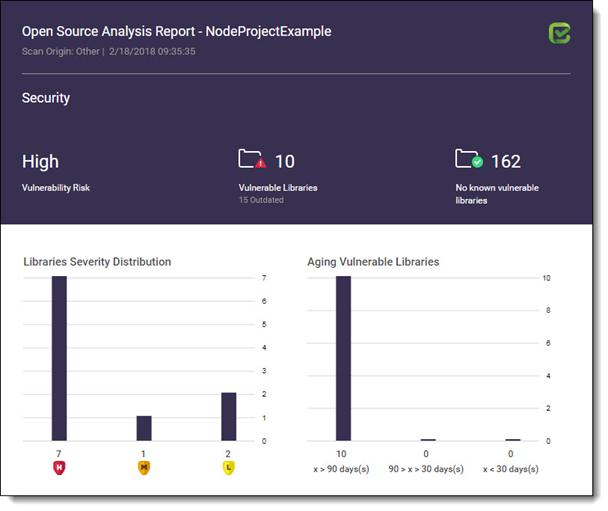


Hiển thị chính xác vi phạm chọn tab Policy Violations



Tạo kết quả báo cáo quá trình quét OSA:

Chọn Open Report icon https://checkmarx.atlassian.net/wiki/download/attachments/968622682/image2018-10-9_17-54-35.png?version=1&modificationDate=1539096877372&cacheVersion=1&api=v2 trên CxOSA Project view trên cùng bên phải

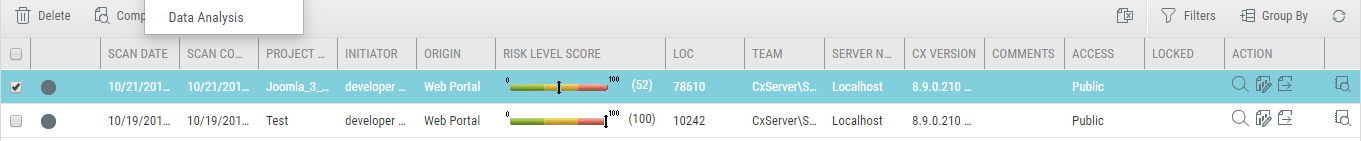


# Sử dụng Checkmarx

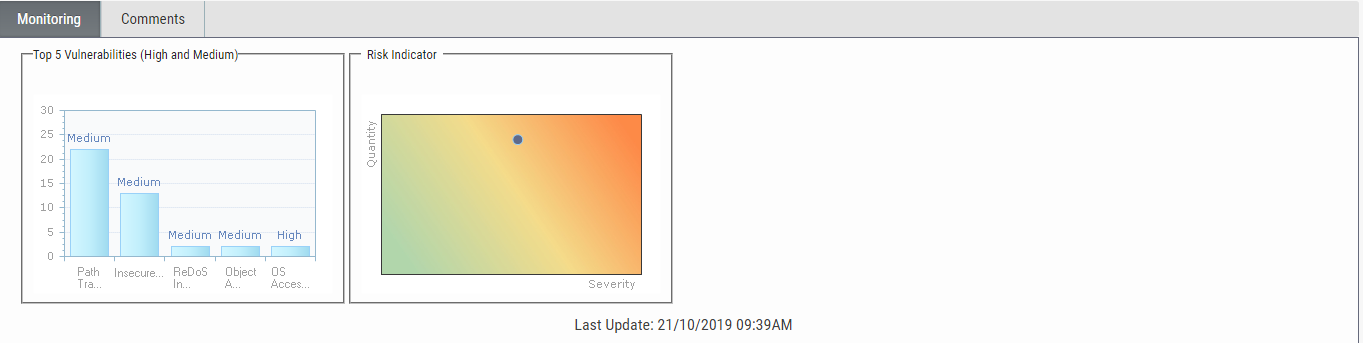
## 1, Sử dụng checkmarx xem kết quả quét

* Trên giao diện web checkmarx chọn **Projects & Scan -> All Scan**

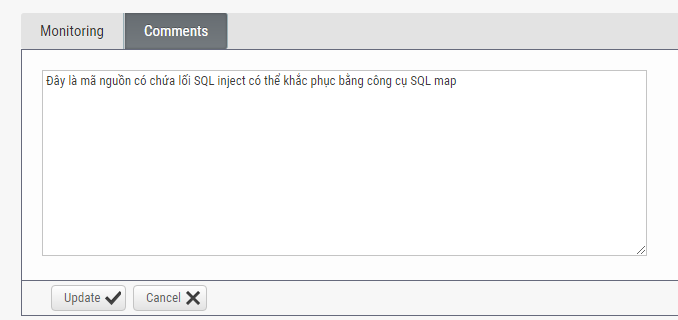
Các dự án tạo sẽ được hiện thị lên như hình, chọn dự án muốn kiểm tra kết quả bằng cách bấm tích vào dự án đó.



Bạn có thể xem tổng quan thông tin sau khi quét mã nguồn của dự án ở phía bên dưới:



Bạn có thế viết bình luận cho dự án này ở tab “ comment”



* Tab menu

Xóa một dự án. Nếu muốn xóa một dự án chọn tích dự án đó và bấm delete

 So sánh 2 dự án, đây là so sánh trực quan giữa 2 dự án cùng loại nguồn để xem dự án mới đã khắc phục được lỗi dự án ban đầu còn tồn tại

 Xuất file .csv. Đây là một file hiển thị thông tin dự án bạn đang có

 Dùng để lọc thông tin ở trường nào đó trong bảng bạn muốn tìm nếu có nhiều dự án

 Gộp một số cột mà muốn xem thông tin vào một nhóm để xem thông tin

 Làm mới trang

* Ở phần mỗi dự án: 

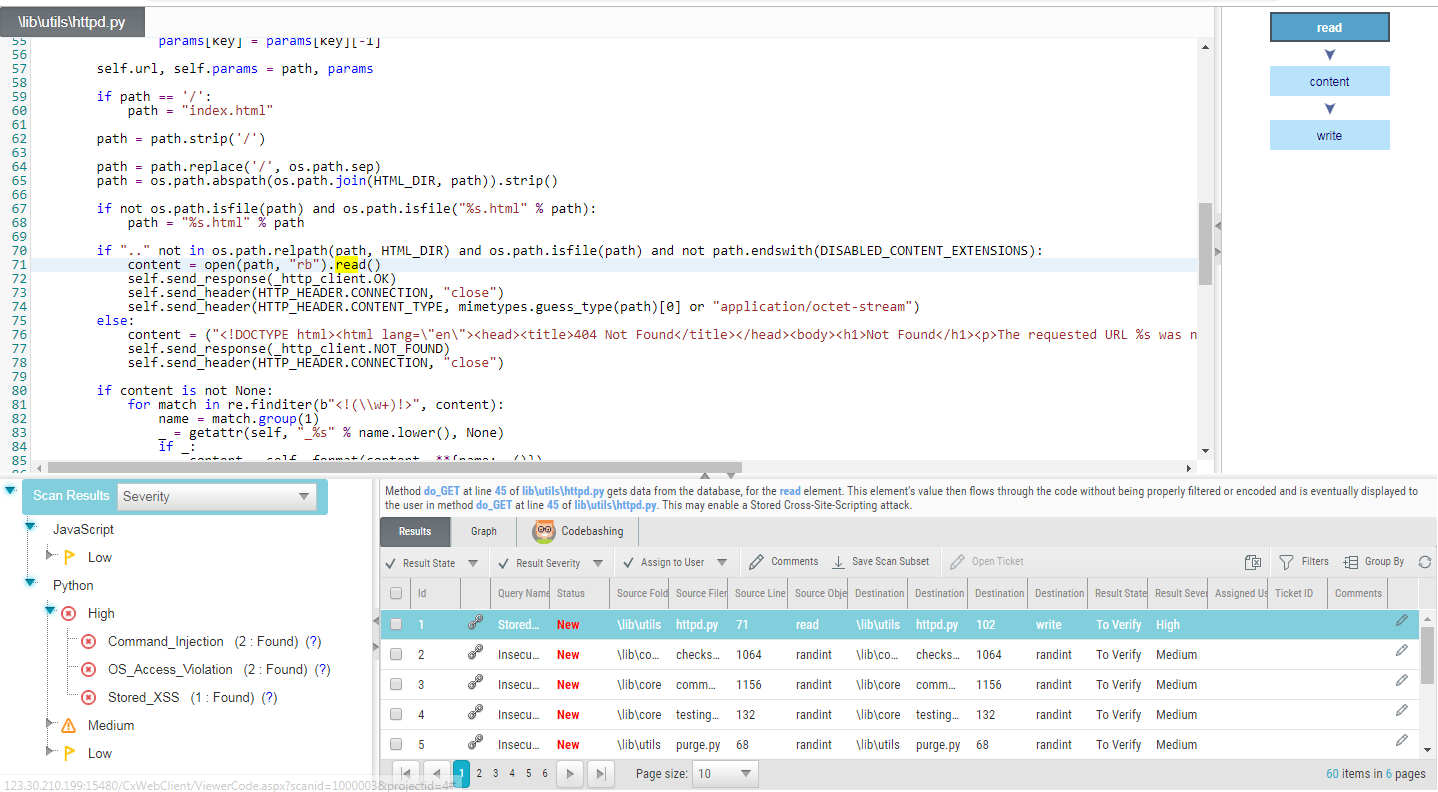
: Hiển thị lên lỗi trong mã nguồn và trạng thái mã nguồn một cách chi tiết nhất

 : Tạo báo cáo cho dự án

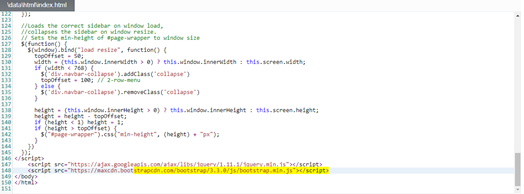
: Hiện thị thông quét tổng thể

: Tải kết quả scan logs

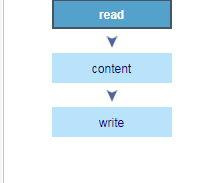
* Khi bấm  ở dự án bạn muốn xem hệ thống trả về trang như hinh



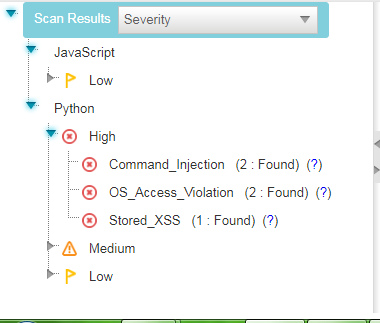
Phần này là phần nội dung code, phần mà có thể thấy được vị trí lỗ hổng đó tồn tại.

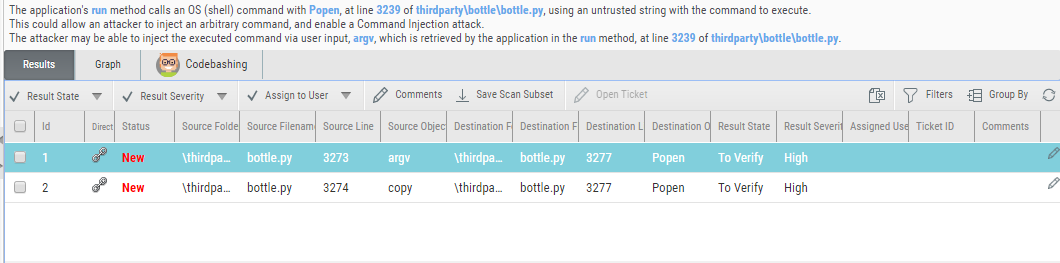


Phần này hiển thị kiến trúc thực hiện công việc “POST” hoặc “GET” trong hệ thống từ đâu đến đâu.



Phần này là kết quả quét nó là những kiểu tấn công có thể thể thực hiện



Phần này chúng ta có thể xem cụ thể vị trí lỗ hổng, đường dẫn mà lỗ hổng có thể thực thi,…  


## Xem dashbash của từng mã nguồn

* Trên giao diện web checkmarx chọn **Dashboard-> Risk** :

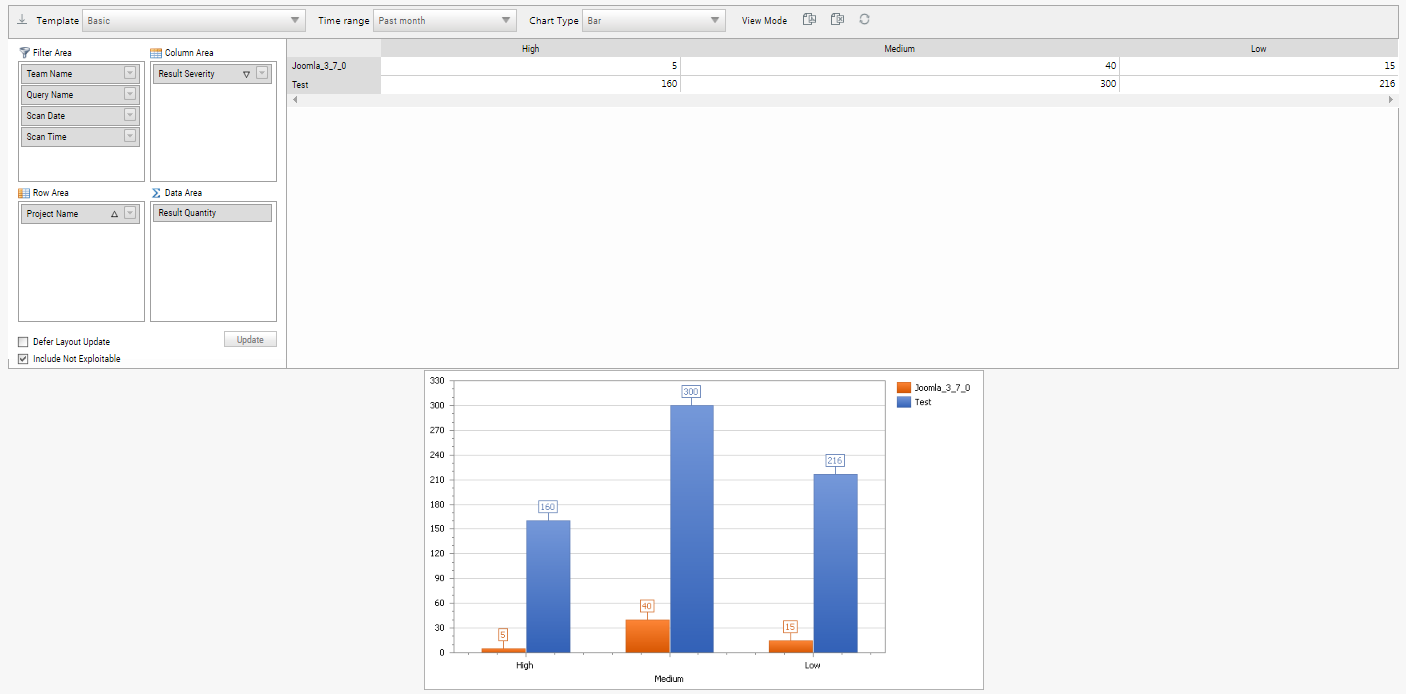
+ Hiện thị bảng thống kê rủi ro lớn nhất hay trong thời gian 7 ngày qua

+ Xu hướng rủi ro



* Nếu trên giao diện web checkmarx chọn **Dashboard-> Data Analysis**

Hiển thị lên giao diện phân tích dữ liệu của các dự án



Thanh menu

 : nút lưu lại bảng dashboard

: chọn trạng thái project khi quét

: Chọn khung thời gian quét

: Loại biểu đồ hiển thị.

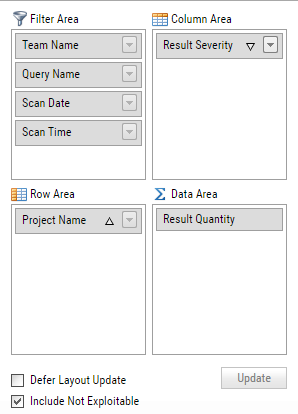
: chế độ hiển thị, có 2 chế độ là full(đầy đủ) và compact(ngắn gọn)

: Xuấ file PDF

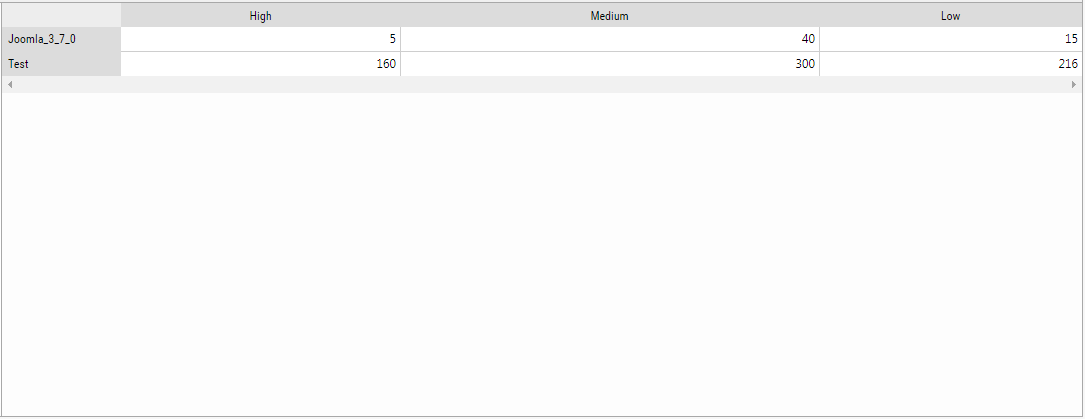
 Xuất file CSV

: Làm mới lại trang

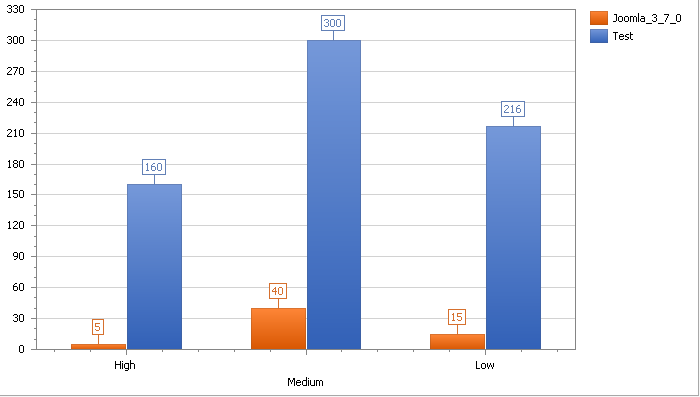
Phần lọc hiển thị thông tin của nguồn bạn muốn xem dashboard



Phần này thống kê bằng bảng số lượng rủi do theo từng mức.



Phần này là hiển thị mức độ rủi ro của các dự án



# Xử lý sự cố

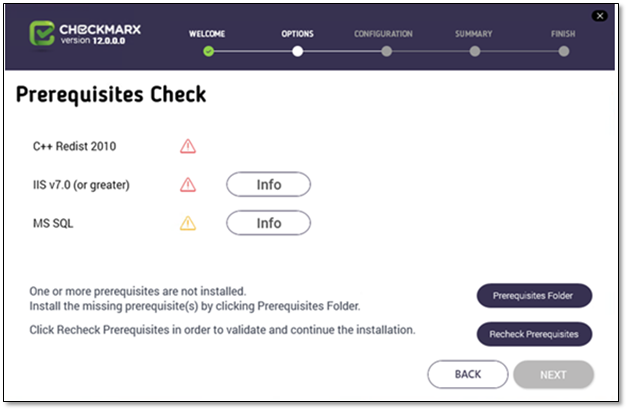
Trường hợp không nhớ pass sql server cần reset, nếu là sql server express:

Mở CMD:

OSQL -L: show các instance

OSQL -S "SERVERNAME or IP ADDRESS\INSTANCE\_NAME" -E -Q "exec sp\_password NULL, 'pass'i, 'sa'"

Nếu chưa cài đặt đủ thành phần bạn bấm vào **Info** xem thông tin cần cài và chọn **Prerequisites Folder**  để cài những thành phần còn thiếu.



Cấu hình SQL. Bạn sẽ **chọn connect using SQL server authentication**

Điền thông tin User và password của SQL server.