

Probely Process

Below is the step-by-step process we took to install and experiment using Probely with Jenkins.

1. Sign-up for a Probely account.
2. Add a new target for the site/application you would like to check the security of. We chose to do a “Free Target” (unpaid target) for the purpose of experimenting with this plugin.

3. Enter the target details. Your name of your target and the address (URL) of the site/application you would like to scan.

EDIT TARGET

Type Details Options Validate

Enter the target details

ENTER THE NAME AND THE URL OF THE TARGET:

NAME

vulnweb

ADDRESS (URL)

http://

testphp.vulnweb.com

BACK CONTINUE SKIP

4. Install the Probely plugin on Jenkins by searching Probely in the available plugins section found under Manage Jenkins -> Manage Plugins.

Probely Security Scanner Plugin



Scan your web application for security vulnerabilities with [Probely](#).

1.1.0

5. Generate an API key for Jenkins to use in order to communicate with Probely's API. Once logged in, navigate to the Settings package using the menu on the left hand side. Once on the settings page, select the Integrations tab. From here you can enter the name for your API key (we entered "Jenkins") and click generate new key.

SETTINGS

SCANNERS INTEGRATIONS

API Keys

Use our APIs to integrate with your tools (e.g., CI)


Check the documentation [here](#).

NAME

Jenkins

GENERATE NEW KEY CANCEL

- Add the API key to your jenkins credentials store as a secret text. You can navigate to the Credentials page by going to Manage Jenkins -> Manage Credentials. Hovering over the global domain under the “Stores scoped to Jenkins” section will display an arrow and allow you to select “Add credentials”.



Credentials

T	P	Store ↓	Domain	ID	Name
		Jenkins	(global)	9c25c561-6fe2-4749-a477-6290bf842863	kdf131@uregina.ca/*****

Icon: [S](#) [M](#) [L](#)

Stores scoped to Jenkins

P	Store ↓	Domains
	Jenkins	 (global)

- Add a credential of Kind = Secret Text. Copy the API key into the Secret field and enter an ID and Description for the credentials. Click “OK”.

Kind

Secret text

Scope

Global (Jenkins, nodes, items, all child items, etc)

Secret

ID

probely-test-site

Description

API Credentials for Probely

OK

- From here, you can create a new Jenkins project or use the plugin in an existing project. For testing purposes, we created a new freestyle project.
- Leaving all project configurations as default, add the “Probely Security Scanner” build step to the project configuration. You must enter the Target ID provided by Probely for the target created in steps 2 & 3. Then use the Credentials dropdown to select the API credential added in step 6 & 7. A message saying “Credentials verified successfully” should be displayed below the credentials dropdown.

Build

Probely Security Scanner

Target ID

U9LxUMoggyB4

Credentials

API Credentials for Probely

Add

Credentials verified successfully

☐ Wait for the scan to finish

Fail the build if vulnerabilities are found

Medium or above

☒ Stop scanning if the build fails

Add build step

- Save your configurations and “Build now”. This will configure Probely to scan your target every time your Jenkins project builds. For testing purposes, we had a test website as a target but it could be implemented to scan a web application that you are developing. The results of the “Free Target” scan will be emailed to the Probely account email and

are also visible within the Probely dashboard. A coverage CSV file can be downloaded from the scan results.

Email Results:

[Probely] Scan complete [↗](#)



From [Probely](#) on 2021-04-05 18:11

[Details](#) [Plain text](#)



Hello!

Probely finished scanning vulnweb and found the following vulnerabilities.

0
HIGH

0
MEDIUM

4
LOW

[View findings details](#)

If you have any questions about the report, please [contact us](#).

Connect with us on:



This email is a notification from [Probely](#). Please do not reply to this email.

Dashboard results:

Scan Specific Results:

SCAN RESULTS

STARTED: 2021-04-05 · 18:11:05
ENDED: 2021-04-05 · 18:11:18 (00:00:13)
SCAN STATUS: Completed
PROFILE: Lightning
REPORT: Scan completed
COVERAGE: [Download CSV](#)

004



SEARCH

Search vulnerabilities

Q

FILTER

SEVERITY

STATE

ASSIGNED

LABEL

SHOWING ALL VULNERABILITIES (4 entries)

<input type="checkbox"/>	#	Severity	Title	Last Found	State	Label	Action
<input type="checkbox"/>	3	LOW	Referrer policy not defined http://testphpvulnweb.com	Today at 6:11 PM	NOT FIXED		CHOOSE
<input type="checkbox"/>	4	LOW	Missing Content Security Policy header http://testphpvulnweb.com	Today at 6:11 PM	NOT FIXED		CHOOSE
<input type="checkbox"/>	2	LOW	Missing clickjacking protection http://testphpvulnweb.com	Today at 6:11 PM	NOT FIXED		CHOOSE
<input type="checkbox"/>	1	LOW	Browser content sniffing allowed http://testphpvulnweb.com	Today at 6:11 PM	NOT FIXED		CHOOSE