

Netsparker Cloud Scan Plugin

Jenkins plugin for Netsparker Cloud

Description

Allows users to start security scans via Netsparker Cloud and see their reports in Jenkins

Features

Global Settings

Netsparker Cloud plugin needs the admin user to define the API settings only once.

Netsparker Cloud

Netsparker Cloud Server URL

http://localhost:2097/

API Token

.....

Test Connection

Save

Apply

Global Settings Override

As from version 1.1.5, global settings can be overridden in pipeline scripts by giving ncApiToken and/or ncServerURL parameters.

Example Script

```
node{
step([$class: 'NCScanBuilder',
ncApiToken: 'LH5pBO+aVYFp5PVTLKHmlyNbrsT+axzHd/wSqDXajYY=',
ncServerURL: "http://localhost:2097/",
ncScanType: "FullWithPrimaryProfile", ncWebsiteId: "7d7eeb95-5a63-4973-0395-a96c04c157b8"])
}
```

Scan Task

Once you define global API settings, the plugin retrieves available scan settings such as scannable website list and scan profile names. You can easily select relevant settings.

Build

Netsparker Cloud Scan

Scan Settings

Scan Type: Incremental

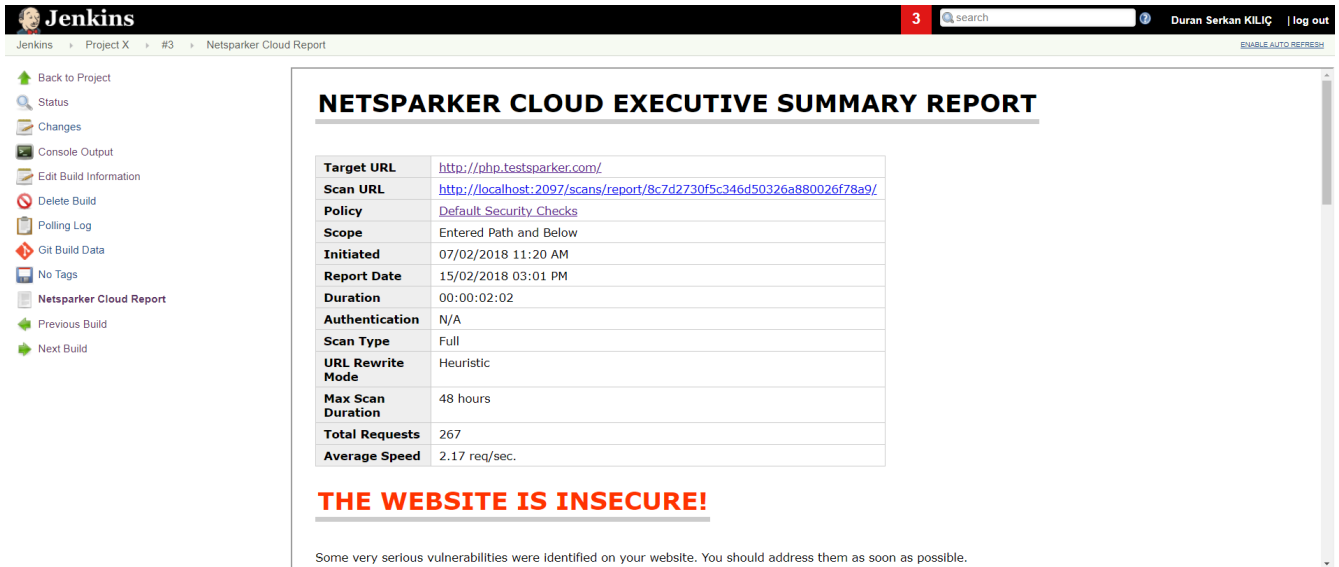
Website Deploy URL: ASP (http://aspnet.testsparker.com/)

Profile Name: asp

Save Apply

Scan Report

Once your initiated scan is completed, you can easily see your executive scan report on the build result window.



Jenkins | Project X | #3 | Netsparker Cloud Report | 3 | search | Duran Serkan KILIÇ | log out | ENABLE AUTO REFRESH

Back to Project | Status | Changes | Console Output | Edit Build Information | Delete Build | Polling Log | Git Build Data | No Tags | Netsparker Cloud Report | Previous Build | Next Build

NETSPARKER CLOUD EXECUTIVE SUMMARY REPORT

Target URL	http://php.testsparker.com/
Scan URL	http://localhost:2097/scans/report/8c7d2730f5c346d50326a880026f78a9/
Policy	Default Security Checks
Scope	Entered Path and Below
Initiated	07/02/2018 11:20 AM
Report Date	15/02/2018 03:01 PM
Duration	00:00:02:02
Authentication	N/A
Scan Type	Full
URL Rewrite Mode	Heuristic
Max Scan Duration	48 hours
Total Requests	267
Average Speed	2.17 req/sec.

THE WEBSITE IS INSECURE!

Some very serious vulnerabilities were identified on your website. You should address them as soon as possible.

Requirements

In order to use the Netsparker Cloud scan plugin, following requirements needs to be satisfied:

- The user must have API token which has permission to start security scan.
- The token belongs to the Netsparker Cloud account must have at least one registered website.

User Guide

Netsparker Cloud Jenkins Plugin documentation is always available at:

<https://www.netsparker.com/blog/docs-and-faqs/how-to-install-configure-netsparker-cloud-scan-jenkins-plugin/>

Netsparker Cloud SDLC documentation is always available at:

<https://www.netsparker.com/blog/docs-and-faqs/integrating-netsparker-software-development-lifecycle-sdlc/>

Checksum

Version

1.1.5

Method	Checksum
SHA-256	47fdccb5e600de9c884b770696cd120d42725e9695bde8ac872c980104aa3afc
SHA-1	db3b4d406ec549de409a3491a4a27575f06b1708
MD5	7e0aebfab565b5662f1799c084b6e90c

1.1.4

N/A

1.1.3

Method	Checksum
SHA-256	f9134f00113bf8b0c818ae88bf2a04175c3fefe6b439d2c3bd75da6fb7df88b

SHA-1	1cf1521962ee78c20732f291488e64005e6f9144
MD5	423ea363a2ddc217395efa3df5714122

1.1.2

Method	Checksum
SHA-256	4f0ec9f7fd8a88244a174d1c09de369db947497cc0f988095de2de1ba52eb0d8
SHA-1	110d7c9b9151abe4cc71bd5ff0a828dfeec64f2
MD5	7f0f9b540e3b98abf03fb7d1d6da054a