



# VERACODE

## SCA

Guia de implementação via linha de comando  
(Agent-Based Scan)



# Considerações iniciais

- Para sistemas Mac e Linux, a implementação é a mesma devido ao processo ser feito utilizando Shell script
- Para Windows temos disponível também um script já pronto
- Esse processo pode ser feito em qualquer ferramenta de CI/CD que permita rodar comandos Shell ou Powershell
- Para mais detalhes sobre a ferramenta, sempre recomendamos a leitura da documentação

# Credenciais



- Para o SCA, precisamos criar um agente e um token para utilizarmos
- No portal, entramos na seção do SCA, clicamos em Agent-Based Scan, Actions e Create:

The screenshot displays the Veracode SCA portal. At the top, the navigation bar includes 'My Portfolio', 'Scans & Analysis' (selected), 'Analytics', 'Policies', and 'Security Training'. The user is logged in as 'M3Corp'. The main heading is 'Software Composition Analysis'. On the right, there's a 'Vulnerability Database' link and a 'Start a Scan' button. Below the heading, there are two tabs: 'Upload and Scan' and 'Agent-Based Scan' (highlighted in yellow). The 'Agent-Based Scan' tab shows 'Agent-Based Scan Settings'. Below this, the 'Workspace List' section features a search bar with the text 'Search workspace name' and a magnifying glass icon, followed by '14 workspaces'. To the right of the search bar is a dropdown menu set to '10' and a 'Create Workspace' button (highlighted in yellow). Below the search bar is a table with the following columns: 'Workspaces', 'Total Projects', 'Total Issues', 'Vulnerability Issues', 'Library Issues', 'License Issues', 'Last Scan', 'Teams', and 'Actions'. The 'Actions' column has a green button labeled 'Actions' with a download icon.

# Credenciais



- Definimos um nome para o nosso Workspace, que é onde vamos armazenar os resultados do Agente

**Create Workspace** [X]

**Enter Workspace Name**

Workspace Name (required)

Cancel More Options Create

# Credenciais



- Na tela de configuração do agente, vamos ter um guia para todas as integrações possíveis, com todas as orientações necessárias

The screenshot shows the 'Set Up Scanner' interface in the Veracode console. On the left is a sidebar with navigation links: 'Workspaces' (with a dropdown menu showing 'AzDVWA'), 'Issues' (128), 'Projects' (1), 'Vulnerabilities' (125), 'Libraries' (4), 'Licenses' (2), 'Manage Workspace', 'Settings', 'Agents' (highlighted in yellow), 'Teams', 'Rules', and 'Notifications'. The main content area is titled 'Set Up Scanner' and includes the instruction 'Choose your operating system or CI to set up an agent.' Below this are three large blue buttons for 'OS X' (with an Apple logo and text 'OS X 10.8 (Mountain Lion) and later'), 'LINUX' (with a Tux penguin logo and text 'Recent versions of 64-bit Linux supported'), and 'WINDOWS' (with a Windows logo and text 'Windows 7 and later, PowerShell 3 and later'). Underneath these is an 'Integration Options' section containing a grid of buttons for various CI/CD systems: Travis CI, Jenkins / Hudson, Bitbucket Pipelines, Circle CI, CodeShip, Atlassian Bamboo, Maven, and Gradle. Each button has a right-pointing arrow.

# SCA - Analise de código de terceiros



- Conseguimos com o SCA analisar não só os componentes de terceiros de um projeto, como também de um repositório em uma ferramenta de GIT e imagens Docker
- Temos o retorno com todas as informações disponíveis no próprio terminal
- Aqui vamos mostrar como fazer a implementação mais simples, mas na [documentação](#) temos detalhes sobre tudo o que pode fazer com ele
- Para a utilização do SCA precisamos apenas do “SRCCLR\_API\_TOKEN” configurado como variável de ambiente



# SCA - Configurando o SRCCLR\_API\_TOKEN

- Uma vez com o valor, precisamos apenas coloca-lo como uma variável de ambiente
- Linux ou Mac:

```
export SRCCLR_API_TOKEN="Disponível no portal da Veracode"
```

- Windows:

```
$Env:SRCCLR_API_TOKEN = "Disponível no portal da Veracode"
```

- Em ferramentas de CI/CD, você tem um campo específico para fazer isso, mas a ideia é a mesma, basta criar uma variável de ambiente com o valor do token e o nome "SRCCLR\_API\_TOKEN"



# SCA - Implementação simples

- Com apenas essa linha de comando, fazemos a análise completa de todos os componentes de terceiros, suas bibliotecas e histórico de versionamento

```
# SCA Simple  
curl -sSL 'https://download.sourceclear.com/ci.sh' | bash -s - scan
```

- Podemos passar como parâmetro um arquivo específico, diretório, site ou imagem Docker
- Nesse caso, fazemos a análise na pasta onde está linha foi executada





# SCA - Com commit de atualização

- Podemos também configurar o SCA para fazer um commit atualizando as versões com problemas e que possuem alguma atualização disponível com a correção

```
# SCA  
curl -sSL 'https://download.sourceclear.com/ci.sh' | bash -s - scan --update-advisor --pull-request
```

- Precisamos apenas informar os parâmetros de Update Advisor e Pull Request, junto com as credenciais para acesso ao Git
- Para saber em detalhes como configurar o acesso em sua ferramenta de gerenciamento de código [acesse essa documentação](#)

# SCA - Retorno no terminal

- No terminal temos um relatório geral do que foi analisado

```
Summary Report
Scan ID                a1dcaeff-3085-42ed-88ab-e747cba646c8
Scan Date & Time       Jul 05 2021 03:11PM UTC
Account type           ENTERPRISE
Scan engine             3.7.40 (latest 3.7.40)
Analysis time          20 seconds
User                   vsts
Project                 /home/vsts/work/1/s
Package Manager(s)     Composer

Open-Source Libraries
Total Libraries         4
Direct Libraries        2
Transitive Libraries    2
Vulnerable Libraries    2
Third Party Code        97.6%
```

# SCA - Retorno no terminal



- As vulnerabilidades são separadas em dois grupos, as que são de conhecimento publico (Public Data) e as que a Veracode identificou mas que ainda não foram divulgadas pelo fabricante do componente (Premium Data)

Vulnerabilities - Public Data		
CVE-2019-3809	High Risk	Server-side Request Forgery (SSRF)
CVE-2015-5358	High Risk	Cross-Site Request Forgery(CSRF)
CVE-2018-10891	High Risk	Cross-Site Scripting (XSS)
CVE-2015-5332	High Risk	Denial Of Service (DoS) Through Disk
CVE-2017-2641	High Risk	SQL Injection
CVE-2014-7845	High Risk	Insecure Random Password Generation
CVE-2014-3541	High Risk	PHP Object Injection
CVE-2019-3850	Medium Risk	Information Disclosure
CVE-2014-0213	Medium Risk	Multiple Cross-Site Request Forgery (
CVE-2014-0216	Medium Risk	Information Disclosure
CVE-2014-3617	Medium Risk	Information Disclosure
CVE-2019-14881	Medium Risk	Cross-Site Scripting (XSS)
CVE-2018-1134	Medium Risk	Unauthorised Downloads
CVE-2021-20185	Medium Risk	Denial Of Service (DoS)
CVE-2018-1135	Medium Risk	Unauthorised Arbitrary File Downloads
CVE-2019-14884	Medium Risk	Cross-site Scripting (XSS)
CVE-2018-1136	Medium Risk	Unauthorised Editing To Web Pages
CVE-2019-3847	Medium Risk	Cross-Site Scripting (XSS)

# SCA - Retorno no terminal

- Os problemas são catalogados conforme CWEs e severidades

Issues			
Issue ID	Issue Type	Severity	Description
80175234	Vulnerability	6.4	NO-CVE: Cross-site Scripting (XSS)
80176685	Vulnerability	7.5	CVE-2017-2641: SQL Injection
80176686	Vulnerability	7.5	CVE-2014-3541: PHP Object Injection
80176687	Vulnerability	7.5	CVE-2018-10891: Cross-Site Scripting (XSS)
80176688	Vulnerability	7.5	CVE-2014-7845: Insecure Random Password Generation
80176689	Vulnerability	7.5	CVE-2019-3809: Server-side Request Forgery (SSRF)
80176690	Vulnerability	7.1	CVE-2015-5332: Denial Of Service (DoS) Through Disk Cor
80176691	Vulnerability	7.1	CVE-2015-5358: Cross-Site Request Forgery(CSRF)
80176692	Vulnerability	6.8	CVE-2019-10186: Cross-site Scripting (XSS)
80176693	Vulnerability	6.8	CVE-2015-1493: Directory Traversal
80176694	Vulnerability	6.8	CVE-2015-0213: Cross-Site Request Forgery (CSRF)
80176695	Vulnerability	6.8	CVE-2015-0218: Denial Of Service (DoS) Through Cross-si
80176696	Vulnerability	6.8	CVE-2015-2268: Regular Expression Denial Of Service (Re
80176697	Vulnerability	6.8	CVE-2014-7838: Cross-site Request Forgery (CSRF)
80176698	Vulnerability	6.8	CVE-2018-16854: Cross-site Request Forgery (CSRF)
80176699	Vulnerability	6.8	CVE-2014-7836: Cross-site Request Forgery (CSRF)
80176700	Vulnerability	6.8	CVE-2016-2157: Cross-site Request Forgery (CSRF)
80176701	Vulnerability	6.8	CVE-2014-0214: Session Hijack



# SCA - Retorno no terminal

- Na seção do Update Advisor vemos quais versões são propostas para a correção dos problemas encontrados

```
Update Advisor
Library Name & Version      Safe Version
moodle/moodle v2.6.2        v3.10.4
appserver-io/http 1.1.6     1.1.7

Full Report Details         https://sca.analysiscenter.veracode.com/teams/300u08
```

- Todas as informações também ficam disponíveis para serem consultadas no portal da Veracode

# SCA - Relatório no Portal

- Dentro do portal temos uma seção específicas para as análises utilizando o agente

## Software Composition Analysis

VERACODE

[Vulnerability Database](#) [Start a Scan](#)[Upload and Scan](#) [Agent-Based Scan](#)[Agent-Based Scan Settings](#)

### WORKSPACE LIST

Actions									
14 workspaces									
Workspaces	Total Projects	Total Issues	Vulnerability Issues	Library Issues	License Issues	Last Scan	Teams	Actions	
<a href="#">My Workspace</a>	0	✓	✓	✓	✓	--	<a href="#">View teams</a>		
<a href="#">AzDVWA</a>	6	1.266	1.127	124	15	25 Aug 2021 11:36AM -02	<a href="#">View teams</a>	>	⬇
<a href="#">AzNode</a>	1	134	113	21	✓	13 Jul 2021 12:25PM -02	<a href="#">View teams</a>	>	⬇
<a href="#">DVWA</a>	1	136	113	23	✓	22 Jul 2021 17:57PM -02	<a href="#">View teams</a>	>	⬇
<a href="#">Go-GitLab</a>	0	✓	✓	✓	✓	--	<a href="#">View teams</a>	>	
<a href="#">Go_CircleCi</a>	3	186	15	3	168	25 Aug 2021 11:21AM -02	<a href="#">View teams</a>	>	⬇
<a href="#">Go_Ubuntu</a>	3	201	165	33	3	19 May 2021 12:28PM -02	<a href="#">View teams</a>	>	⬇
<a href="#">ID-Pivae</a>	1	✓	✓	✓	✓	4 Feb 2021 14:02PM -02	<a href="#">View teams</a>	>	⬇
<a href="#">ID-WebGoat-SCA</a>	2	198	165	30	3	8 Jan 2021 18:25PM -02	<a href="#">View teams</a>	>	⬇
<a href="#">IDAZD</a>	1	364	304	60	✓	29 Jan 2021 12:14PM -02	<a href="#">View teams</a>	>	⬇

# SCA - Relatório no Portal

- Em cada Workspace, temos as informações detalhadas do que foi encontrado

The screenshot displays the Veracode SCA portal interface for a workspace named 'AzDVWA'. The left sidebar contains navigation links: 'Back to Workspace List', 'Workspaces' (with a dropdown for 'AzDVWA'), 'Issues 128', 'Projects 1', 'Vulnerabilities 125', 'Libraries 4', 'Licenses 2', and 'Manage Workspace' (with sub-links for Settings, Agents, Teams, Rules, and Notifications). The top navigation bar shows 'Projects: All | Starred' and 'Scan Date: Last 30 days'. The main content area is divided into two sections: 'INSIGHTS' and 'ISSUES LIST'. The 'INSIGHTS' section includes a 'Median Time to Resolution' of 'N/A days', a bar chart for 'Issues by Severity' (High: 8, Medium: 103, Low: 17), and three summary boxes: 'High Severity Issues: 8', 'Direct Libraries Only: 128', and 'Vulnerable Methods: 0'. The 'ISSUES LIST' section features a table with columns: Issue ID, Severity, Vulnerability ID, Description, Project, Library, Status, and Select. The table lists 125 issues, with the first 10 displayed. The footer contains copyright information for Veracode, Inc. (2006-2021) and links to 'Usage Guidelines', 'Responsible Disclosure Policy', and 'Veracode Support'.

Back to Workspace List

Workspaces

AzDVWA

Issues 128

Projects 1

Vulnerabilities 125

Libraries 4

Licenses 2

Manage Workspace

Settings

Agents

Teams

Rules

Notifications

Projects: All | Starred

Scan Date: Last 30 days

INSIGHTS

Median Time to Resolution

N/A days

Issues by Severity

High: 8, Medium: 103, Low: 17

High Severity Issues: 8

Direct Libraries Only: 128

Vulnerable Methods: 0

ISSUES LIST

Vulnerability Issues

Active, Severity, Open

Search issues

125 issues

10, Page 1 of 13

Issue ID	Severity	Vulnerability ID	Description	Project	Library	Status	Select
86255263	2.1	CVE-2021-20186	Cross-Site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255262	2.1	CVE-2014-7835	Cross-site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255261	3.5	CVE-2014-7830	Cross-site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255260	3.5	CVE-2015-2273	Cross-site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255259	3.5	CVE-2015-3174	Cross-Site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255258	3.5	CVE-2015-0212	Cross-site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255257	3.5	CVE-2015-5336	Cross-site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255256	3.5	CVE-2019-18210	Cross-Site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255255	3.5	CVE-2015-3179	Login Restriction Bypass	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>
86255254	3.5	CVE-2015-3178	Cross-site Scripting (XSS)	..IGDEXE/DVWA	moodle/moodle	●	<input type="checkbox"/>

© Veracode, Inc. 2006 - 2021

[Usage Guidelines](#) [Responsible Disclosure Policy](#) [Veracode Support](#)

# SCA - Relatorio no Portal

- E dentro de cada falha temos as informações sobre ela, incluindo dicas de correção

The screenshot displays the Veracode portal interface for a vulnerability report. On the left, a sidebar shows navigation options like 'Workspaces', 'Issues', 'Projects', 'Vulnerabilities', 'Libraries', 'Licenses', and 'Manage Workspace'. The main content area is titled 'Issue Vulnerability' and features a dark header for the 'Cross-Site Scripting (XSS)' issue. Below this, the 'PROJECT DETAILS' and 'LIBRARY DETAILS' sections provide specific information about the repository, scan ID, and affected library. The 'The Fix' section includes a 'Direct Dependency' warning and an 'Update' section with instructions and a code snippet for updating the composer.json file. A 'Create Issue' button is also visible.

[Back to Workspace List](#)

Workspaces ⊕

AzDVWA ▼

Issues 128

Projects 1

Vulnerabilities 125

Libraries 4

Licenses 2

Manage Workspace ▼

Settings

Agents

Teams

Rules

Notifications

## Issue Vulnerability 🔍 Comment 🕒 Show History

### Cross-Site Scripting (XSS)

moodle/moodle is vulnerable to cross-site scripting (XSS). A remote attacker is able to inject and execute arbitrary Javascript in a user's browser via TeX content when TeX notation filter is enabled.

[View more details in the Veracode Vulnerability Database](#)

Issue ID: 86255263

Data Source: Public Disclosure

Vulnerability ID: CVE-2021-20186

Linked Issue: (None)

Status: Open

Ignore Issue: ☐

#### PROJECT DETAILS

Type: Repository

Project: [...IGDEXE/DVWA](#)

Branch: [remotes/origin/ma...](#)

Scan ID Found: [28734405](#)

Date Found: 24 Aug 2021 11:24:11AM -02

Scan ID Last Seen: [28773267](#)

Date Last Seen: 25 Aug 2021 11:36:07AM -02

#### LIBRARY DETAILS

Affected Library: [moodle/moodle](#), PACKAGIST, moodle/moodle

Type: Direct dependency

Version In Use: [v2.6.2](#)

Released On: 6 Mar 2014 21:00PM -02

Latest Version: [v3.11.2](#)

Released On: 28 Jul 2021 21:00PM -02

#### The Fix

Dependency Graph

**Direct Dependency** 🔗 This vulnerability is in a direct dependency. Vulnerable library [moodle/moodle](#) was found in [composer.lock](#). It can be fixed by updating the version of the library in your project and rebuilding it.

[Create Issue](#)

#### Update

This issue was fixed in version [v3.5.16](#). However, that version is itself subject to [other vulnerabilities](#), we suggest that you upgrade to [v3.8.9](#), which is considered safe.

1. Update your [composer.json](#) as shown below:

```
composer.json
{
  "require": {
    ...
    "moodle/moodle": "v2.6.2"
  }
}
+ "moodle/moodle": "v3.8.9"
```

© Veracode, Inc. 2006 - 2021 [Usage Guidelines](#) [Responsible Disclosure Policy](#) [Veracode Support](#)



# Conclusão



- Como vimos nesse material, mesmo a forma “difícil” de implementar Veracode é muito simples e propicia uma grande liberdade para sua equipe definir como e onde quer trabalhar
- Nossas ferramentas são desenhadas para uma utilização simples, mas sempre pensando em maximizar os resultados.
- Com poucas linhas de código, vai conseguir uma análise completa do seu projeto, com a menor taxa de falsos positivos do mercado e de forma simultânea, sem precisar em se preocupar com infraestrutura, já que todos os scans são feitos em nossa nuvem

Entre em contato com a nossa  
equipe para mais detalhes:  
[vendas@m3corp.com.br](mailto:vendas@m3corp.com.br)

SECURING THE SOFTWARE  
THAT POWERS YOUR WORLD

---

VERACODE