m3corp

VERACODE

SCA

Guia de implementação via linha de commando

(Agent-Based Scan)

m3corp

Considerações iniciais

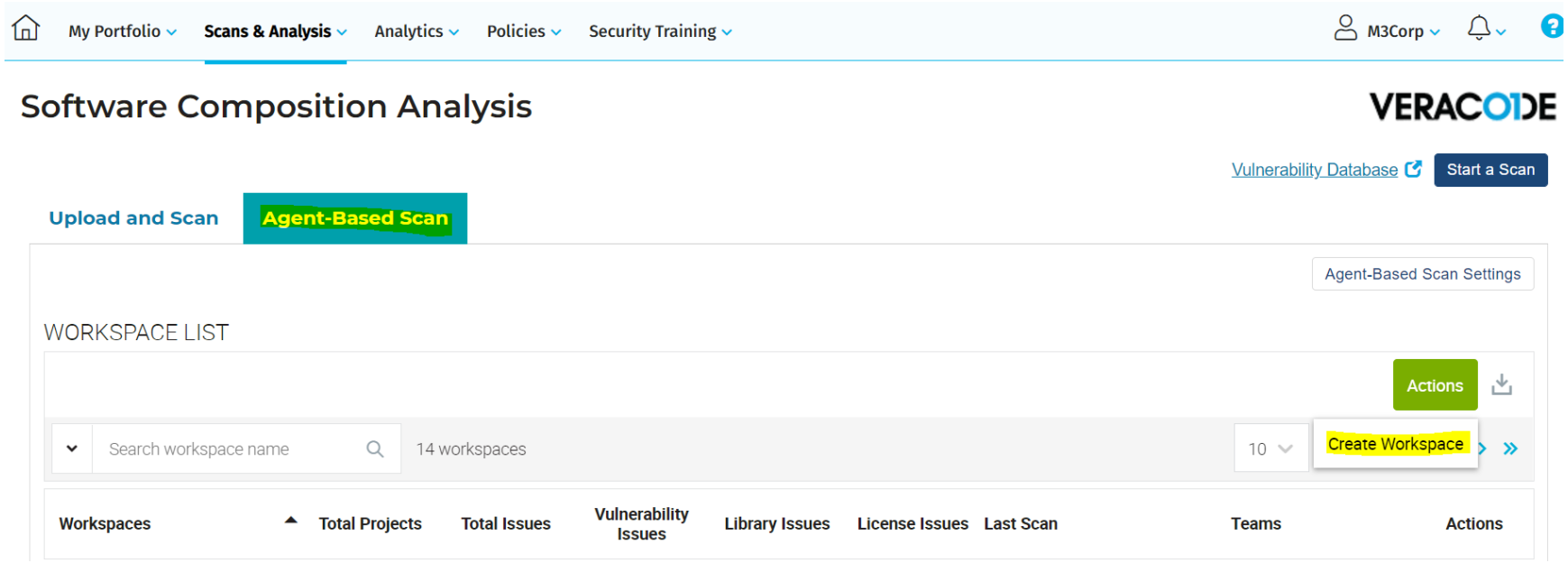
- Para sistemas Mac e Linux, a implementação é a mesma devido ao processo ser feito utilizando Shell script
- Para Windows temos disponível também um script já pronto
- Esse processo pode ser feito em qualquer ferramenta de CI/CD que permita rodar comandos Shell ou Powershell
- Para mais detalhes sobre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

VERACODE

m3corp

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:

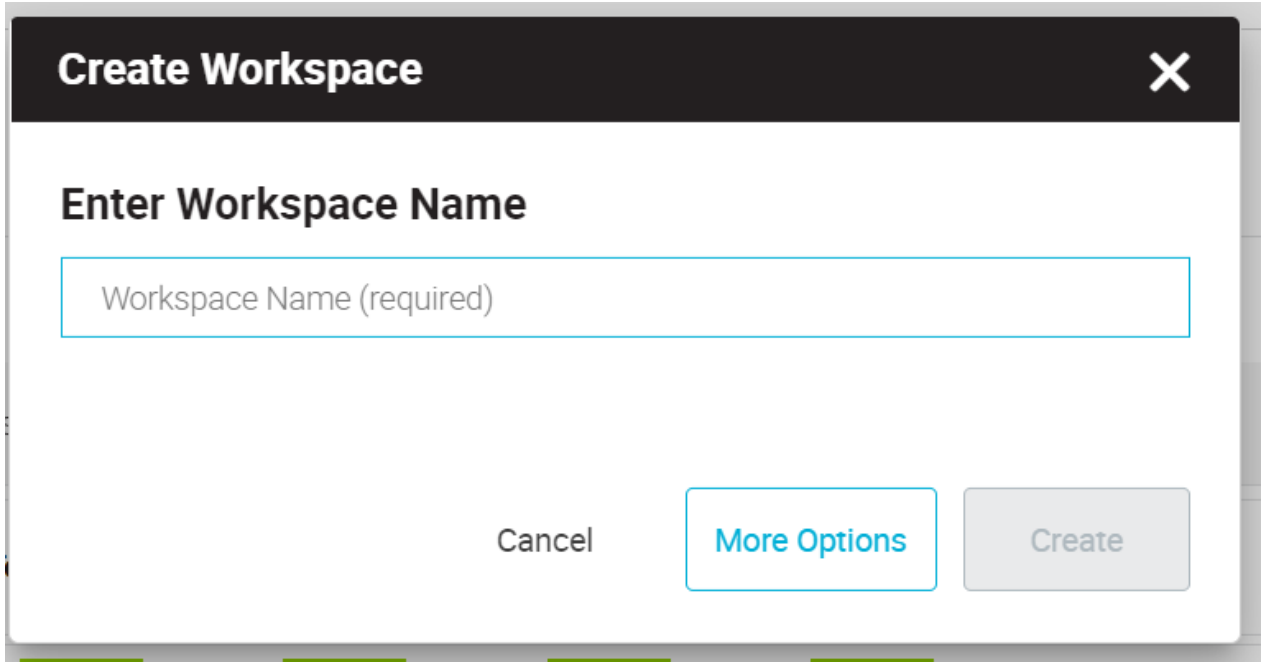


VERACODE

m3corp

Credenciais

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

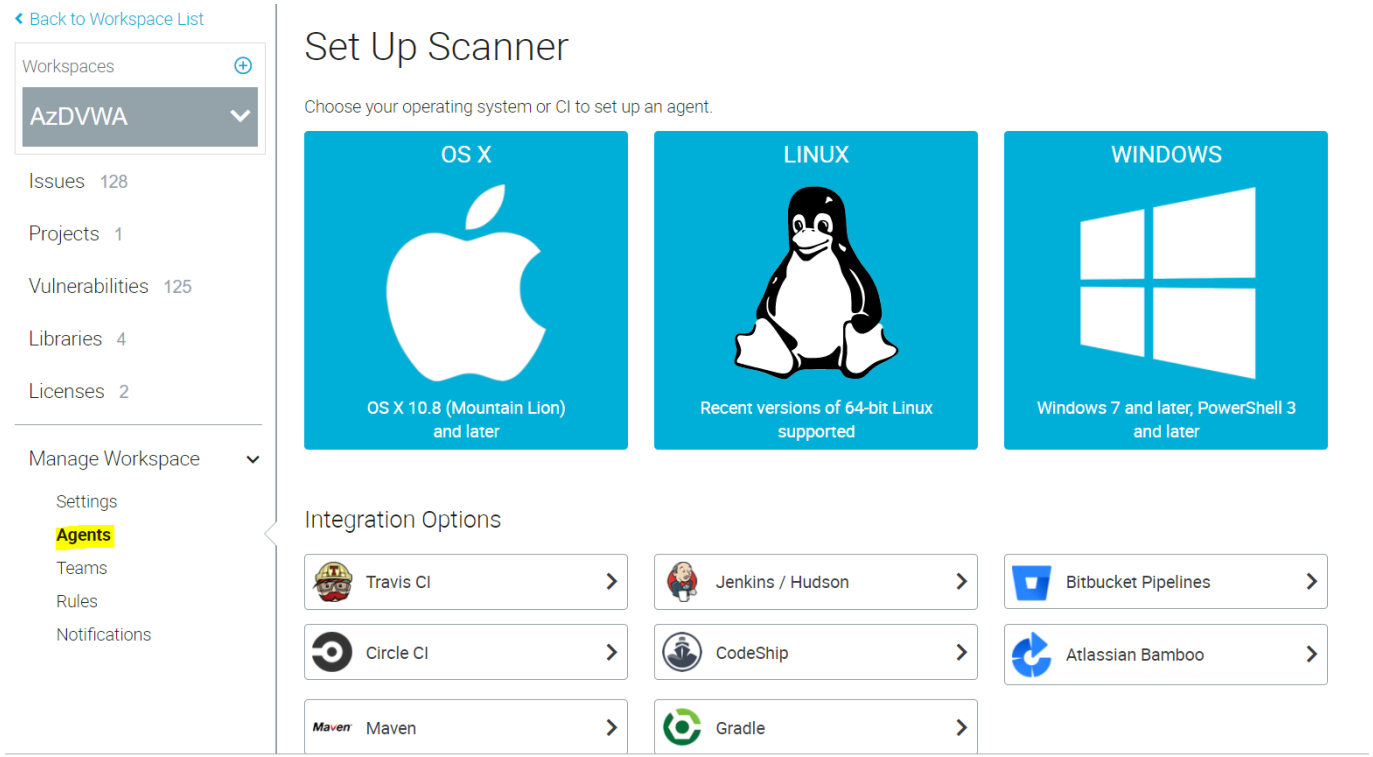


VERACODE

m3corp

Credenciais

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



VERACODE

m3corp

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

VERACODE

m3corp

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="Disponivel no portal da Veracode"
```

- Windows:

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

- Em ferramentas de CI/CD, você tem um campo especifico 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”

VERACODE

m3corp

SCA - Implementação simples

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

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

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

VERACODE

m3corp

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

VERACODE

m3corp

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%

VERACODE

m3corp

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)
```

VERACODE

m3corp

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

VERACODE

m3corp

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/3O0u0
```

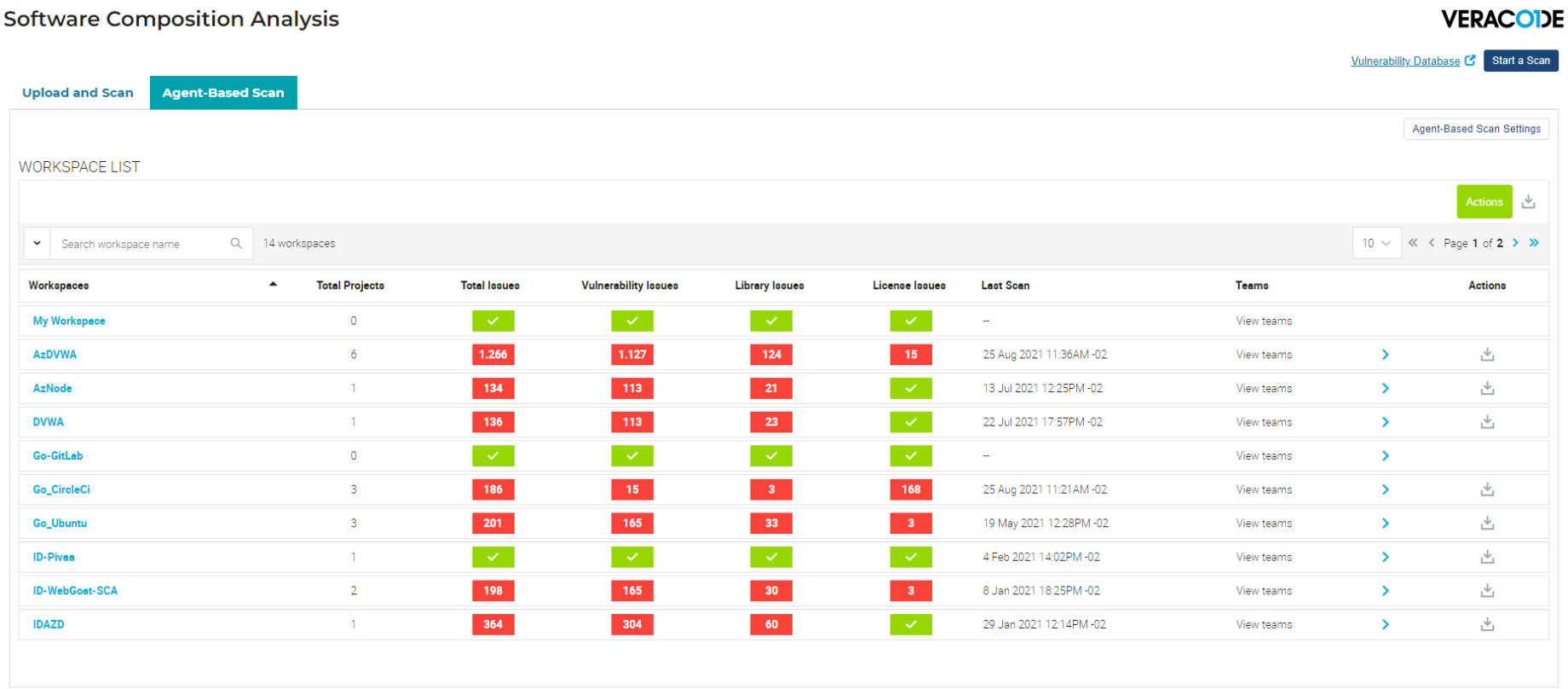
- Todas as informações também ficam disponíveis para serem consultadas no portal da Veracode

VERACODE

m3corp

SCA - Relatorio no Portal

- Dentro do portal temos uma seção especificas para as analises utilizando o agente



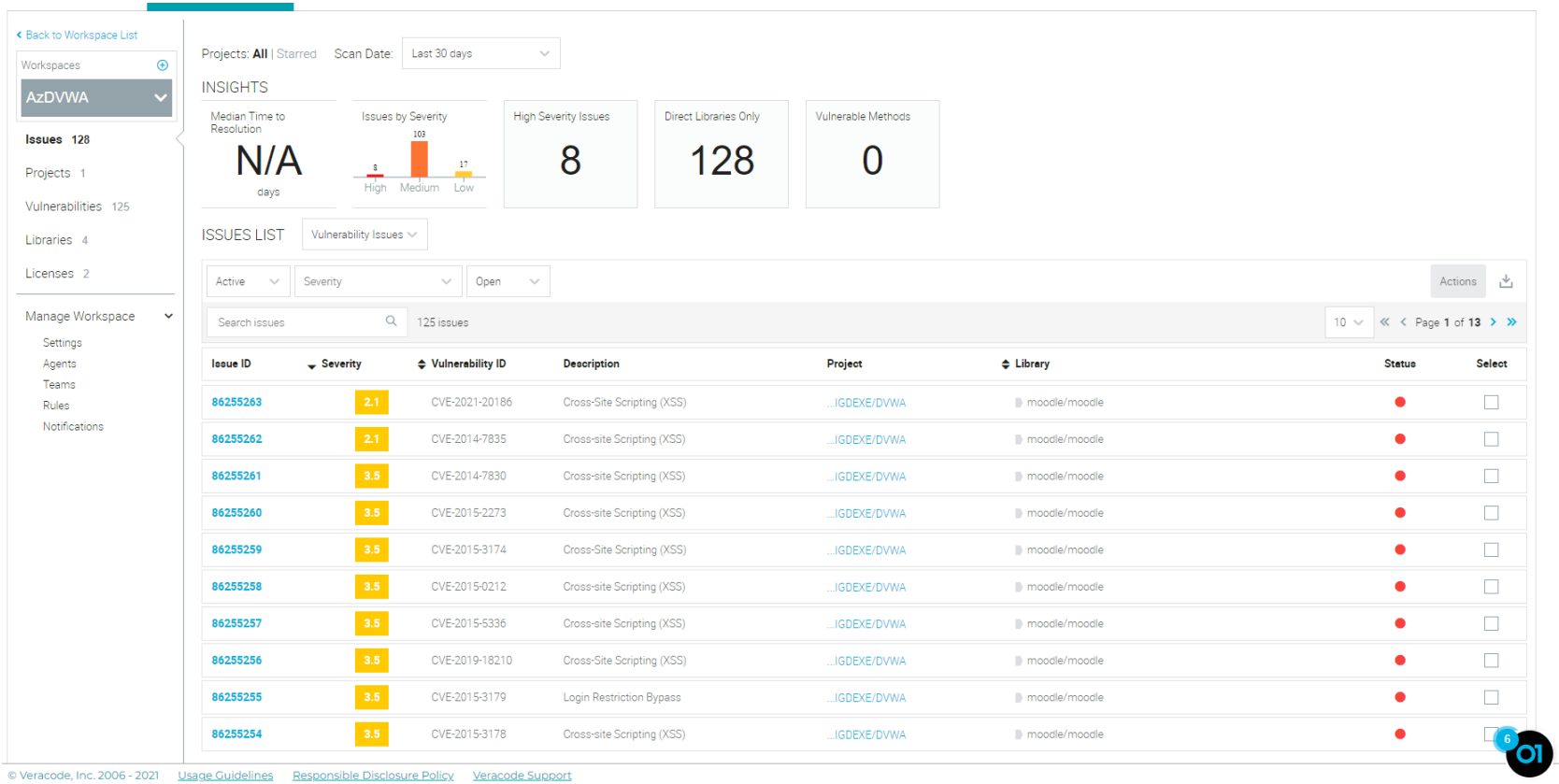
Workspaces	Total Projects	Total Issues	Vulnerability Issues	Library Issues	License Issues	Last Scan	Teams	Actions
My Workspace	0	✓	✓	✓	✓	--	View teams	
AzDVWA	6	1.266	1.127	124	15	25 Aug 2021 11:36AM -02	View teams	
AzNode	1	134	113	21	✓	13 Jul 2021 12:25PM -02	View teams	
DVWA	1	136	113	23	✓	22 Jul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

VERACODE

m3corp

SCA – Relatorio no Portal

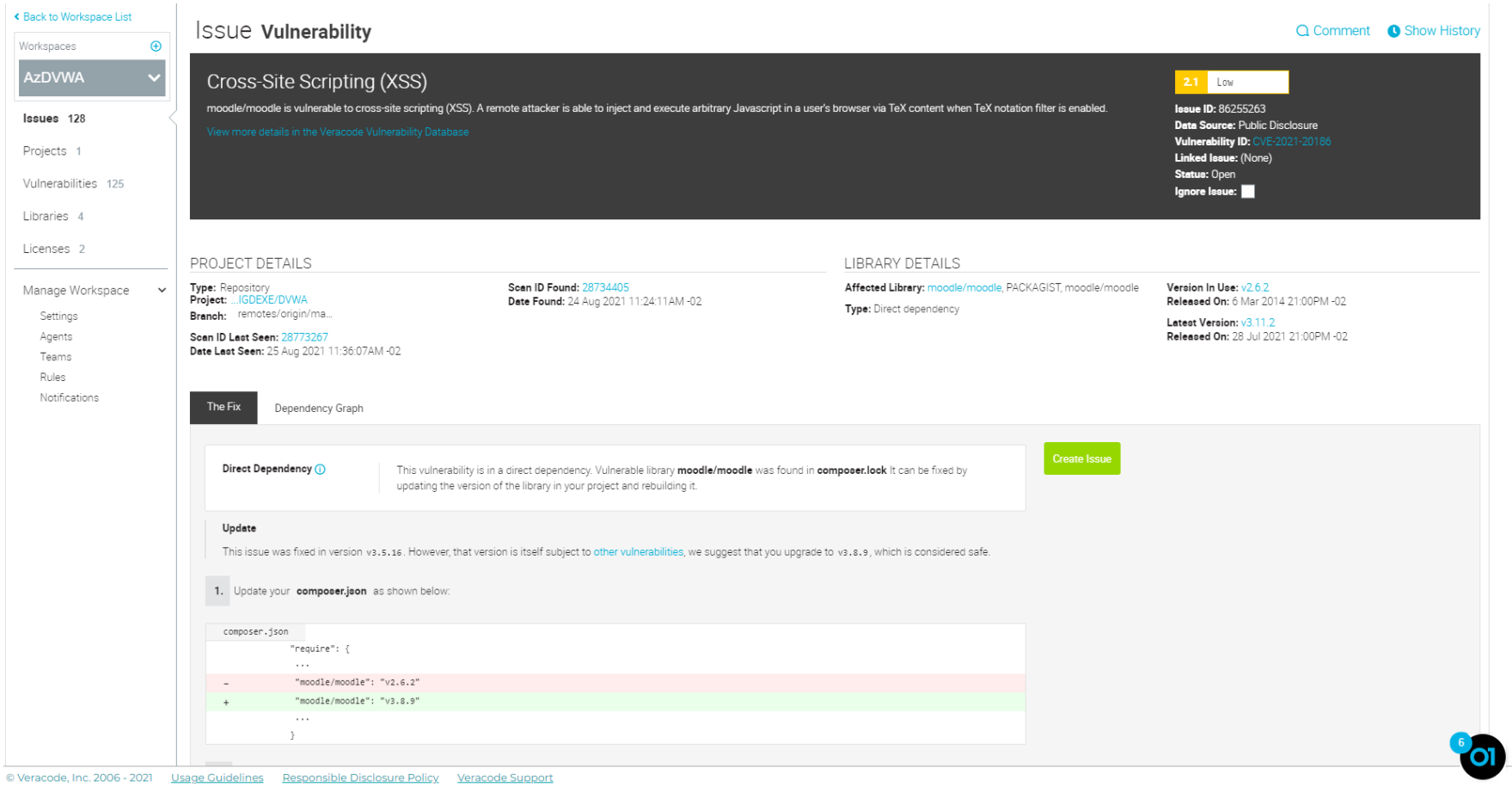
- Em cada Workspace, temos as informações detalhadas do que foi encontrado



VERACODE

SCA - Relatorio no Portal

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



m3corp

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 analise 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

VERACODE


m3corp
Entre em contato com a nossa equipe para mais detalhes:
vendas@m3corp.com.br
SECURING THE SOFTWARE
THAT POWERS YOUR WORLD
VERACODE