

🦄 ASPM

story about unicorns,
sneaky business and
unexpected decisions

Ivan Elkin - AppSec TL
exness



In the middle of nowhere

You are an AppSec

What is your daily routine

- Repositories
- Domains
- Libraries
- Vulnerabilities
- Developers
- Scanners:
 - SAST
 - DAST
 - SCA
 - Secrets

Simply you are Running Scanners and Validating Vuls

You are an AppSec

What is your daily routine

- Repositories - **8000**
- Domains - **1000**
- Libraries - **10000**
- Vulnerabilities - **10000**
- Developers - **300**
- Scanners Findings
 - SAST - **3000**
 - DAST - **2000**
 - SCA - **2000**
 - Secrets - **1000**



Take your shovel,
pitchfork and go for a
work

Let's put it everything together
into one system

Initially we developed it ourselves v.1

Scan Center Domains Projects Hosts

+ ADD NEW DOMAIN REMOVE ALL DOMAINS

Filter... sovest

Missing Headers External IP

sovest-test.sovest.com - 195.189.100.20, 195.189.101.20
api-test.sovest.ru - 195.189.101.22, 195.189.100.22
api-partner-test.sovest.ru - 195.189.100.32, 195.189.101.32
api-test.sovest.com - 195.189.101.22, 195.189.100.22
sovest.ru - 195.189.101.16, 195.189.100.16
oauth-test.sovest.com - 195.189.100.21, 195.189.101.21

Scan Center Domains Projects Hosts

Projects

Secure Medium High

afapi_java - java 2018-02-24 0
ssh://afapi_java

Scan Center Domains Projects Hosts

Hosts

Wallarm Monitoring Wallarm Block Internal IP External IP

afapi.qiwi.com - s3499.qiwi.com - 10.11.43.115
Wallarm: default:monitoring custom:no
External IP: 10.250.32.113

afapi.qiwi.com - s3498.qiwi.com - 10.8.43.127
Wallarm: default:monitoring custom:no
External IP: 10.250.32.113



OWASP
Moscow
2018

Initially we developed it ourselves v.2

SCAN CENTER

Dashboard

Scans Today 12

Domains 1001

Repositories 1337

Hosts 2674

Last 24 Hours

Tracked from Github and Gerrit

Just Updated

CheckMarx scans

Updated 4 minutes ago

GIXY - Nginx vulnerabilities

Vulnerabilities count 4

Possible HTTP-Splitting vulnerability.

HIGH

Using variables that can contain “\n” or “\r” may lead to http injection.

http_splitting

Possible SSRF (Server Side Request Forgery) vulnerability.

HIGH

The configuration may allow attacker to create arbitrary requests from the vulnerable server.

ssrf

Last DAST Scans

Scans count 5

Finished	Repository	Severity	Notify Status
2018-11-11T12:14:47.063Z	sovest.com	⚠️	✓
2018-11-11T12:14:47.027Z	sovest.ru	⚠️	✓
2018-11-11T12:14:46.970Z	online.contact-sys.com	⚠️	✓
2018-11-11T12:14:46.863Z	online.contact-sys.com	⚠️	✓
2018-11-11T12:14:46.668Z	fundl.qiwi.com	⚠️	✓

Last SAST Scans

Scans count 30

Finished	Repository	Severity	Notify Status
2018-11-14 11:45:10	AQW/main	✓	✓

The main problem - you need to have
programming skills
to support the code, finding bugs, fixing it

... so yet another Job

Finding a better live in open source



What kind of VM tools do you know?

- DefectDojo - github.com/DefectDojo/django-DefectDojo
- Faraday - github.com/infobyte/faraday
- Vulnwhisper - github.com/HASecuritySolutions/VulnWhisperer?tab=readme-ov-file
- Archery - github.com/archerysec/archerysec
- OWASP VM Center - owasp.org/www-project-vulnerability-management-center/

DEFECTDOJO



Problems we faced

Very specific and not customizable

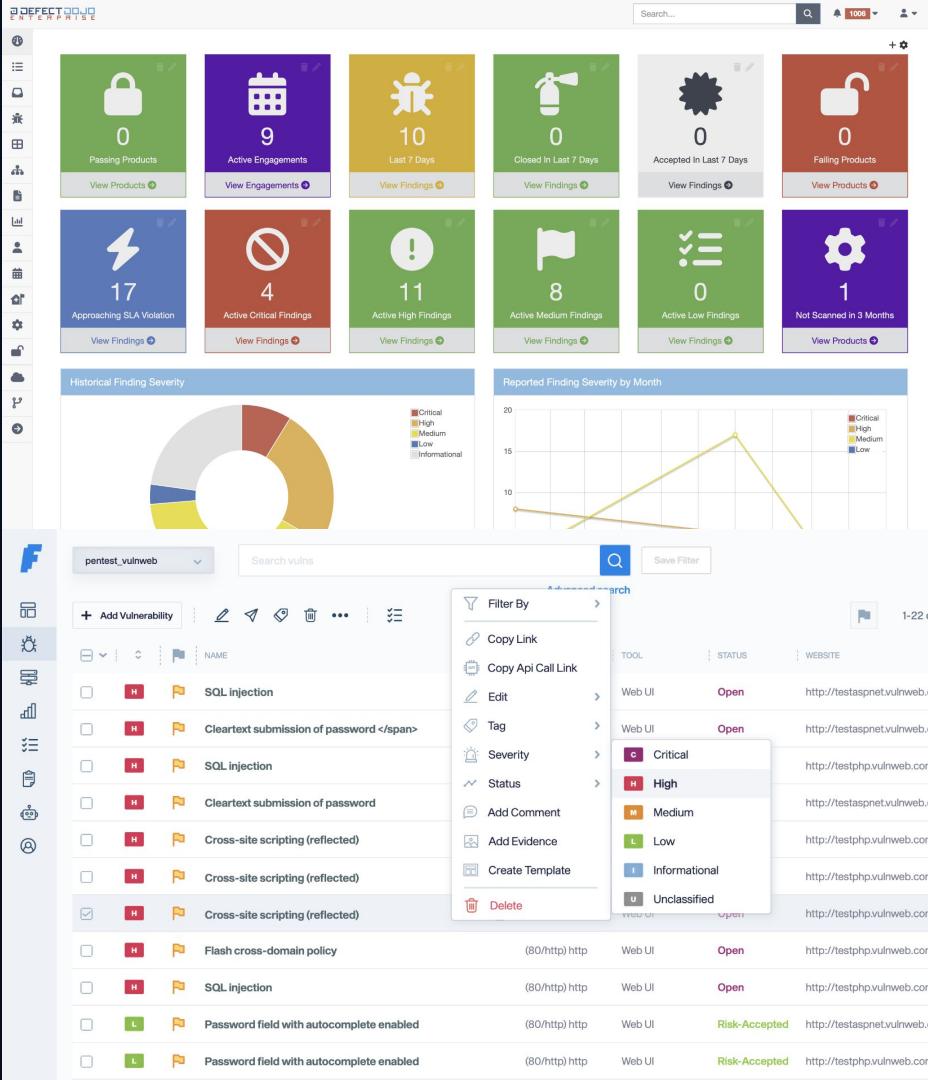
- We need own kind of entities
- We need own metrics and dashboards
- We need custom integrations (scanners)
- Writing integrations is a pain

UX is not so useful

- From Engineers to Engineers
- You have to click 5 times just to mark one vulnerability as a False Positive

Some of them is not highload

- Horizontal scaling not working



One day we found a
Unicorn



And it's name ASPM

The screenshot displays the ASPM (Application Security Performance Management) platform interface, which integrates multiple security tools and provides a central dashboard for monitoring and managing application security.

Top Navigation: The top navigation bar includes links for DAST, DNS, SAST, SCA, SCM, Bug Bounty, CI/CD, Logging, and Workflow. A search bar and a "Explore more connectors" link are also present.

Connectors: A list of connected security tools:

- AppSpider DAST (Connected)
- Checkmark (Connected)
- Dep Scan SCA (Connected)
- Snyk SCA (Connected)
- Qualys DAST (Connected)
- Trivy IaC
- ZAPI

Dashboard: The main dashboard shows the following metrics:

- Score: 1.29 (4% today)
- Assets Management: 1,212 items
- Defects Management: 142 open defects
- Coverage Overview: Champion Leader Board (Julie Serensen, 1070 risk impact)
- Control Coverage: Radar chart showing coverage for OWASP ZAP, Semgrep, Checkmarx, Qualys, and Snyk.
- Defects Trend: Line chart showing defect values over time (2 Jan, 9 Jan, 16 Jan).

SAST weekly scheduled scan: A workflow diagram for a scheduled scan:

```
graph LR; Start(( )) --> Filter1[Filter]; Filter1 --> RunScan1[Run Scan]; RunScan1 --> OR((OR)); Filter2[Filter] --> OR; OR --> Slack[Send Slack Message]
```

Team SLA: A table showing SLA violations and average SLA for different teams:

Team	In SLA	SLA Violation	Average SLA
commerce	100%	0	411
arch	98%	2	330
science	95%	5	329
city	92%	12	340
framework	90%	9	325
front-end	88%	9	346

Bottom Left: A sidebar for managing connectors, showing the last sync date (Jan 22, 2023 4:11 PM) and creation date (May 12, 2020 0:31 PM). It includes buttons for Add, Edit, and Delete.

Bottom Right: A footer with the text "OWASP Limassol" and the date "31/05/2024".

Inventory of any kind of Assets

Web Assets

Search Filters Columns

Asset (2112)	Open Tasks	Defects	Tags	Controls	Risk	Class	Assignee
> https://jaeger-collector.enso.am 23 items	798	12 43 8 4	XSS +2		2,545	A	
> https://4cce49f60cb4c235 12 items	647	3 102	Dev Prod +2		5,421	B	
> /enso-emails/static_file 67 items	154	56 43 8	Prod		103	C	
> https://oapi.enso.io 102 items	357	102	API Member +1		23	D	
> /sfx/track/number/electronic 3 items	177	82 4 4	Dev Prod +3		2,112	D	
> https://desk1.enso.io 11 items	556	10 8 4	Account API +3		106	A	
> Enso.TTD 23 items	24	12 8	Dev Prod +2		24	C	
> ALTerraform 55 items	540	42 8	Dev Seller +1		504	C	
> https://studio.enso-records.io 21 items	583	12 4	Dev Product +3		1,011	A	
> https://account.sample-client12.com 900 items	142	12 43 8 4	Dev Product +3		88,888	A	
> https://oapi.enso.io 102 items	357	102	Dev Product +3		23	D	

Values

Observe whole system

Tagging assets by criticality

See total risks

Vulns for each kind of asset

The screenshot shows the Enso web application interface. On the left is a vertical sidebar with a purple header containing the 'enso' logo. Below the header are icons for Dashboard, Inventory, Defects, Tasks, Policy, and Connectors. A circular badge at the bottom right of the sidebar indicates 'DE'.

The main area is titled 'Web Assets' and displays a list of assets under the heading 'Asset (2112)'. One asset is expanded, showing its details:

https://jaeger-collector.artlist.m/

Discovered: 02/11/2021 Last scan: 28/11/2021

Score Defects Tasks Events Attributes

Search All This Asset Child Assets Export + Add Defect

Defect	Asset	Source	Status	Ticket	Severity	Created
Generic Secret det...	https://desk.artlist.io	!	IN PROGRESS	+ Add Ticket	HIGH	Dec 30, 2019
Log4j2 RCE through...	https://jaeger-collect...	b	OPEN	TSV-2001	LOW	Dec 30, 2019
Azure takeover de...	https://_4cce49f6079...	!	FIXED	+ Add Ticket	MEDIUM	Dec 4, 2019
Appspec Yml Disc...	https://oapi.artgrid.io	!	DISMISSED	TSV-2112	MEDIUM	Mar 20, 2019
WordPress Core ...	https://em4038.artgr...	✗	IN PROGRESS	TSV-1010	CRITICAL	Feb 2, 2019
Generic API Key de...	https://_4cce49f6079...	!	CLOSED	TSV-1001	MEDIUM	Mar 20, 2019
OAuth token detect...	https://em4038.artgr...	!	DISMISSED	+ Add Ticket	HIGH	Dec 7, 2019
Insecure direct obj...	https://studio.art-list.io	!	OPEN	+ Add Ticket	MEDIUM	Feb 2, 2019

Values

Results of each scan

Details of vulnerabilities

Easy access to any asset

Automate through workflows

Rules

Search

Active First New Rule

Dashboard Inventory Defects Tasks Policy Connectors AT

CI Automation - SCA scans for new PRs on Class A repositories

Last Modified: Apr 24, 2022 2:31 AM
Modified by: james@enso.security

SAST weekly scheduled scan

Last Modified: Apr 24, 2022 2:31 AM
Modified by: james@enso.security

Weekly per-team auto assignment of top impact tasks

Tasks

PT scoping and auto-assignment for a 2-week sprint

Asset

Generate weekly email report on SCA Critical defects with SLA violation

Defect

"New Asset" Slack notification and security review task assignment

Asset

SAST weekly scheduled scan

Last Modified: Apr 24, 2022 2:31 AM
Modified by: james@enso.security

Run Scan

Send Slack Message

OR

Filter

Filter

Filter

Values

No-code automation

- run scans
- change stats

Event triggers

Nice CUSTOM Dashboards!

Dashboard

Asset Breakdown

1,657 Hosts	256 New
145 Endpoints	35 New
1,256 Repositories	498 New
634 Users	27 New

SAST Control Coverage

Amount

Coverage Status	Percentage
Covered	61
Non-Covered	39

SLA Trend

Amount

Month

Month	Yellow Line (High)	Purple Line (Medium)	Green Line (Low)
Jan 21	800	700	600
Jun 21	750	600	450
Dec 21	600	200	100

Top assets with defects

Type

Amount

Type	Critical	High	Medium	Low
A	250	150	100	100
B	100	50	50	50
C	150	100	100	50
D	200	100	100	50

● Critical ● High ● Medium ● Low

Defect Breakdown with Drill-down

Amount

Severity

Severity	Amount
Critical	689
High	400
Medium	450
Low	824

Cancel Save

+

Add Widget

Values

Metrics for

- Coverage
- AppSec team
- Dev teams

Pros, Cons, Kudos

- Made by good engineers and specifically AppSecs for AppSec
- Many new features that it will rise day by day
- Startup with \$16.5M on 2nd round of investments
- PoC Pilot went very good even with Highload (Hybrid installation)
- Fair price as we are one of the first big customers
- Good support (slack, often meetings, quick response)

Security tools Never works out-of-the-box, but it's not a problem

- spend 100+ m/h to resolve some issues
- Created 60+ issues to support

Let me tell a short story...

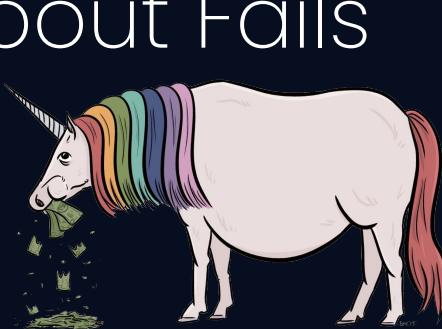
Short fairy tale about Fails

or how to hack yourself

1. Find cyber-unicorn 🦄
2. Spend 100+ hours to integrate unicorn on-prem
3. Create 60+ issues to unicorn-support
4. Believe that in the end unicorn will solve all your problems!
5. Receive news that cyber-wolves ate your unicorn 🐺



enso



So, what happened?

Q1 - We started integrating ASPM

Q3 - Big company bought ASPM startup

Q4 - Big company **discontinued** ASPM



So, I have to say to wolves



Unexpected solution
and follow the



User: I need something to visualize tables in database
change data on a flight
build charts and dashboard
and it should be open source...

... 7 minutes after...

AI: Use Headless-CMS

NO-Code Headless CMS solutions

The image shows two screenshots of a headless CMS platform. The left screenshot displays a list of customers with columns for First Name, Last Name, Visits, and Date Created. The right screenshot shows a welcome page with links to documentation, code examples, tutorials, and a blog.

Customer List (Left Screenshot):

	First Name	Last Name	Visits	Date Created
=	Keri	Guzman	636	just now
=	Heather	Robles	426	
=	Ollie	Padilla	24	
=	Marina	Numbers	87	
=	Enrique	Numbers	7,432	
=	Leonor	Prefix	158	
=	Dorothy	Suffix	254	
=	Han	Link	100	

Welcome Page (Right Screenshot):

Welcome 🌟

We hope you are making good progress on your project! Feel free to read the latest news about Strapi. We are giving our best to improve the product based on your feedback.

Content-type Builder SEE MORE ON THE BLOG

Read the documentation
Discover the concepts, reference, guides and tutorials.

Code example
Learn by testing real project developed by the community

Tutorial
Discover the concepts, reference, guides and tutorials.

Blog
Discover the concepts, reference, guides and tutorials.

Join the community
Discuss with team members, contributors and developers on different channels.

SEE OUR ROAD MAP ROADMAP

Github **Discord**
Reddit **Twitter**
Blog **Forum**

No-code Headless CMS



strapi

Star 31.9k ▾



Budibase

github.com/strapi/strapi



appsmith_

github.com/budibase/budibase

github.com/appsmithorg/appsmith



directus

github.com/directus/directus

ASPM based on Headless CMS

The screenshot displays the Directus application interface, specifically the 'Data Model' settings for the 'repository' collection. The left sidebar contains navigation links such as ASPM, Data Model (selected), Access Control, Flows, Settings, Appearance, Bookmarks, Translations, Marketplace (Beta), Extensions, Report Bug, Request Feature, and Directus 10.11.0. The main area shows the 'repository' collection with fields like id*, url, name_with_namespace, tags, date_created, archived, reviewed, commits, scans, and defects. A modal window titled 'Data Model' is open, showing the 'Fields & Layout' section for the 'repository' collection. The right side of the screen shows the 'Defects (repository)' relational trigger configuration, which includes a 'Sort Field' section and a 'Relational Triggers' section with triggers for 'On Deselect of defect...' and 'On Delete of repository...'. The 'On Deselect of defect...' trigger is set to 'Nullify the repository field', and the 'On Delete of repository...' trigger is also set to 'Nullify the repository field'.

ASPM

Data Model

Access Control

Flows

Settings

Appearance

Bookmarks

Translations

Marketplace Beta

Extensions

Report Bug

Request Feature

Directus 10.11.0

repository

defect

web_assets

containers

commits

developer

scans

System Collections

ASPM

Data Model

Access Control

Flows

Settings

Appearance

Bookmarks

Translations

Marketplace Beta

Extensions

Report Bug

Request Feature

Directus 10.11.0

repository

url

name_with_namespace

tags

date_created

archived

reviewed

commits

scans

defects

Fields & Layout Saves Auto

Schema

Relationship

Field

Interface

Display

Validation

Conditions

Defects (repository)

This Collection

repository

Related Collection

defect

url

repository

Sort Field

Add Sort Field...

Relational Triggers

On Deselect of defect...

Nullify the repository field

On Delete of repository...

Nullify the repository field

OWASP Limassol

31/05/2024

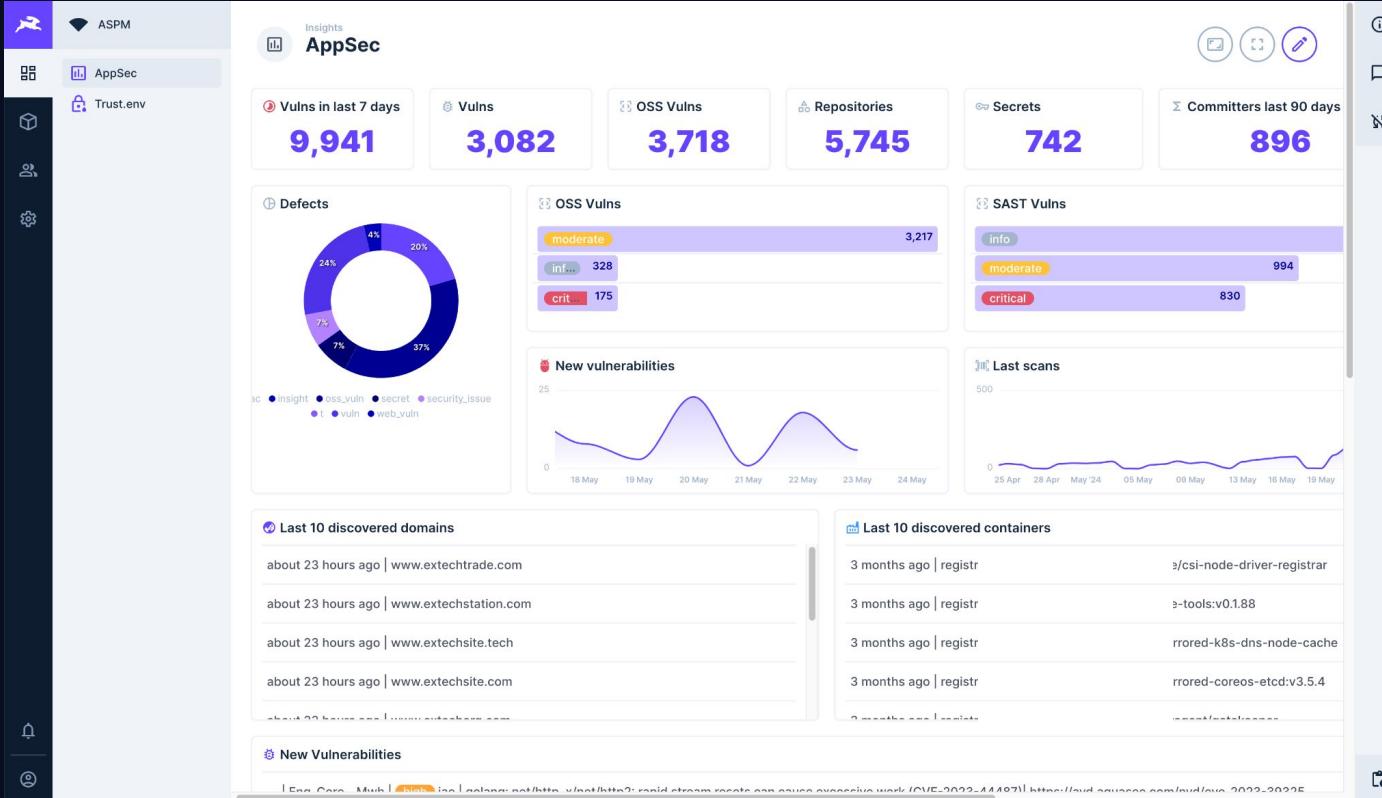
Customizable assets

Views and bookmarks

Filters

Batch update

Dashboards - yes, they are custom!



Drag'n'Drop widgets

Aggregations

Filters

Workflows

The screenshot illustrates the Directus interface for managing workflows. On the left, a sidebar contains various navigation items: ASPM, Data Model, Access Control, Flows (selected), Settings, Appearance, Bookmarks, Translations, Marketplace (Beta), Extensions, Report Bug, Request Feature, and Directus 10.11.0. The main area shows a table of active flows, followed by a detailed view of a specific flow named "Test Webhook".

Flows Table:

Status	Name	Description
Active	CRON - Aggregate Develop...	...
Active	CRON - Containers Loader	Loads list of deployed containers through Sp...
Active	CRON - Gitlab Loader	Loads Gitlab repos by cron
Active	CRON - Shiftleft Loader	Loads ShiftLeft scan results
Active	CRON - Webassets	
Active	Manual - Container Loader	
Active	Manual - Gitlab Loader	
Active	Manual - Shiftleft Loader	
Active	Manual - Webassets	
Active	Update - Shiftleft hook	
Active	Webhook - Gitleaks	
Active	Webhook - Nuclei	
Active	Webhook - Trivy	
Active	Webhook - Trufflehog	
Active	Webhook-trufflehog2	

Test Webhook Flow Details:

```
graph LR; Trigger[Trigger] --> Cond[Condition]; Cond --> Log1[Log to Console]; Cond --> Log2[Log to Console]
```

The flow starts with a "Trigger" node (Webhook, Method: POST, URL: <https://directus.prod.e...>) which leads to a "Condition" node (Check Auth Condition Rules). This condition splits into two paths: one leading to a "Log to Console" node (Allowed Message: Allowed) and another leading to a "Log to Console" node (Denied Message: Denied).

CRON and Webhooks

Drag'n'drop flows

Custom JS extensions

Extensions

The screenshot shows the Directus Extensions settings page. On the left, a sidebar menu includes options like ASMP, Data Model, Access Control, Flows, Settings, Appearance, Bookmarks, Translations, Marketplace (Beta), Extensions (selected), Report Bug, Request Feature, and Directus 10.11.0. The main area displays a list of bundles under the heading "Bundles". Each bundle entry shows the bundle name, version, status (Enabled), and a three-dot menu icon. The bundles listed are:

- directus-extension-asmp-bundle 0.0.18 (Enabled)
- web-assets-loader (Enabled)
- table-selector (Enabled)
- display-multiline (Enabled)
- defect-writer (Enabled)
- gitlab-loader (Enabled)
- splunk-loader (Enabled)
- shiftleft-loader (Enabled)
- repository-url-to-name (Enabled)
- repository-display (Enabled)
- ai-release-summary-loader (Enabled)

On the right side of the interface, there is a sidebar with a tree view of files and folders under "src". The tree structure is as follows:

- src
 - ai-release-summary-loader
 - defect-writer
 - display-multiline
 - example-loader-template
 - flow-scripts
 - gitlab-loader
 - api.ts
 - app.ts
 - gitlab-client.ts
 - models.ts
 - nuclei-loader
 - repository-display
 - repository-url-to-name
 - shiftleft-loader
 - splunk-loader
 - table-selector
 - web-assets-loader

Even Custom styles

Using Built-in styles

Custom CSS

```
1 .metric-bar {  
2     min-width: 20%;  
3 }  
4 .v-list-item-content .render-template {  
5     white-space: pre-wrap!important;  
6 }  
7 .links .v-list-item-content {  
8     height: initial!important;  
9 }  
10 .v-list-item-content .datetime {  
11     color: var(--theme--primary);  
12 }
```

Writing custom component

```
<template>  
    <div class="text-multiline" v-html="formattedValue"></div>  
</template>  
  
<script>  
  1+ usages  ± Ivan Elkin *  
  export default {  
  
    props: {  
      value: {  
        type: String,  
        default: null,  
      }  
    },  
    computed: {  
      formattedValue() {  
        return this.value.replace(  
          searchValue: /([A-Z]+-\d+)/g,  
          replaceValue: '<a href="https://jira.exness.io/browse/$1" target="_blank">$1</a>'  
        );  
      }  
    };  
  </script>
```



Profit comparison

	Self developed	Open Source	Vendor	Headless CMS
Time to first start	Very Slow	Fast	Fast / Slow	Medium
Customization	100%	50%	Very Low ?	80%
Customization speed	Slow	Slow	Medium ?	Very Fast
Support	Slow	Very Slow	Very Fast	Fast
Integrations	Any	Any but Limited	Limited	Any

* In my humble opinion

P.S. Hacking the marketing



P.S Hacking the marketing

What is an ASMP?
Just yet another Buzzword that cost like an airplane

 CrowdStrike
<https://www.crowdstrike.com> › cloud-security › applicati... 

What is Application Security Posture Management (ASPM)?

ASPM is the holistic process of evaluating, managing, and enhancing the security stance of an organization's custom applications.

 Gartner
<https://www.gartner.com> › reviews › market › applicati... 

Application Security Posture Management (ASPM) Tools

Application security posture management (ASPM) tools continuously manage application risk through collection, analysis and prioritization of security issues ...

 ArmorCode
<https://www.armorcode.com> › learning-center › what-is... 

What is Application Security Posture Management (ASPM)?

ASPM unifies testing, ticketing, CI/CD, and other development tools to create holistic visibility into the security posture of applications, prioritize findings ...

 Synopsys
<https://www.synopsys.com> › glossary › what-is-applicati... 

Application Security Posture Management

Application security posture management (ASPM) is a holistic approach to application security (AppSec) that provides a single source of truth to identify, ...

 Check Point Software
<https://www.checkpoint.com> › Secure The Cloud 

What is Application Security Posture Management (ASPM)?

Application security posture management (ASPM) helps to scale and enhance AppSec programs through automation. ASPM solutions automatically identify applications ...

 Cycode
<https://cycode.com> › blog › application-security-posture... 

What Is Application Security Posture Management (ASPM)?

2 Nov 2023 — Application Security Posture Management (ASPM) detects, correlates, prioritizes, and remediates security vulnerabilities across the SDLC.

1. What we achieved in General

1. Asset discovery and inventory

2. Risk assessment

3. Scanners Orchestration

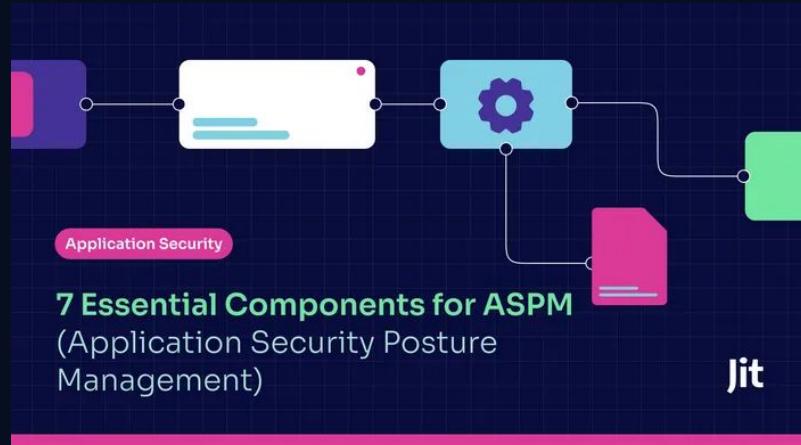
4. Reports and Dashboards

5. Real-time monitoring

6. No-Code Automation

7. Compliance Monitoring

8. It's not just a security tool



Category	ASPM	Traditional AppSec	ASOC	CSPM
Purpose	Manage and scale an AppSec program based on business risk	Secure applications against vulnerabilities	Orchestrate and correlate security activities	Manage and monitor the security of cloud environments
Benefits	Provides holistic visibility into the app environment to enable effective risk management and remediation	Enhances app security against threats	Streamlines security operations and responses	Identifies and mitigates cloud security risks
Integrations	On-premises and cloud-based environments	Embedded in app development lifecycle	Organization-wide deployment	Cloud infrastructure and services

2. De-duplication is not a feature

Project: RiskAssessment Labels: InternetFacing

Vulnerabilities are already de-duplicated so that you can start to triage!

Total: 721

next

Change View:

Quick Filters

Search Vuln Name

Per Page: 15

Actions ↗

Issue	ID	Vulnerability Name	Branch	Status	Scanner	Severity	CVSS	First Seen	Actions
●	eec3e	Blocklisted import crypto/md5: weak cryptographic primitive	master	Recurrent		High	8.0	17 May 2023	
●	778fa	Blocklisted import crypto/md5: weak cryptographic primitive	master	Recurrent		Medium	6.0	17 May 2023	
●	eec3c	Use of weak cryptographic primitive	master	Recurrent		Critical	10.0	17 May 2023	
●	778f8	Blocklisted import crypto/md5: weak cryptographic primitive	master	Recurrent		Medium	6.0	17 May 2023	
●	4203d	Use of weak cryptographic primitive	master	Recurrent		Medium	6.0	17 May 2023	
●	ba664	GHSA-x4jg-mjrx-434g node-forge:0.10.0	master	New		Low	3.0	16 May 2023	
●	ba662	CVE-2022-24771 node-forge:0.10.0	master	New		Critical	10.0	16 May 2023	
●	38393	CVE-2022-24773 node-forge:0.10.0	master	New		Low	3.0	16 May 2023	
●	38391	GHSA-cfm4-qjh2-4765 node-forge:0.10.0	master	New		High	7.5	16 May 2023	

2. De-duplication is not a feature

In most cases de-duplication can be done by
creating unique ID, based on Vulnerability
META-information

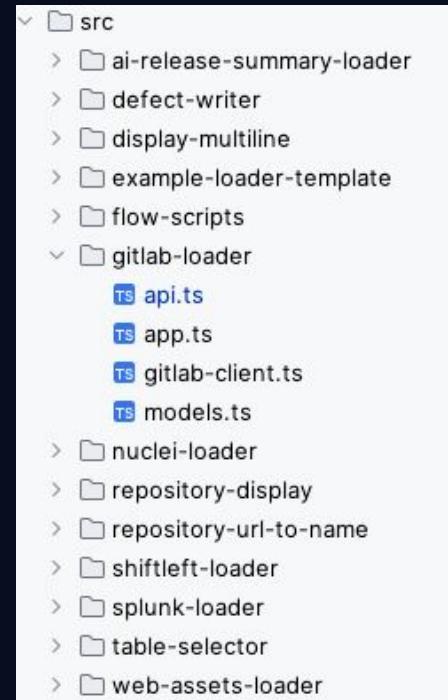
```
sha256(repo + filename + param + vuln_type) [0:31]  
( "tfg_" + sha256(repo + filename + secret)) [0:31]  
( "dast_" + sha256(domain + param + vuln_type)) [0:31]
```

3. Feature requests & Support

Sometimes is easier to help yourself

No need to wait several month until vendor will add a requested feature to product.

You can write a feature by your hands,
even if you are not a professional developer



4. We have AI

Also is a kind of marketing to sell you an AI

Summarizing of
yesterday commits to get
latest news per project

Everyone have own AI :)

Breaking news!

May 28, 2024 4:51PM - [Payments-Platform](#) - [Ethereum](#) - [Ethereum-Approver](#)

1. Devtools (uv + ruff) updated under NOTASK.
2. Pydantic upgraded from version 1 to version 2 for [CRYPTO-4806](#).

May 28, 2024 4:51PM - [Payments-Platform](#) - [Crypto](#) - [Crypto-Addresses](#)

1. Implemented support for different corporate addresses based on countries ([CRYPTO-4656](#)).
2. Upgraded Pydantic from version 1 to 2 ([CRYPTO-4615](#)).
3. Added a new load balancer IP address for the production environment cluster ([RE-2654](#)).
4. Introduced a new bff key for handling GET requests to /assigned-addresses ([CEX-7149](#)).

May 29, 2024 11:00AM - [Payments-Platform](#) - [Crypto](#) - [Crypto-Addresses](#)

1. Added bff key for GET /assigned-addresses in payments-platform/crypto/crypto-addresses.

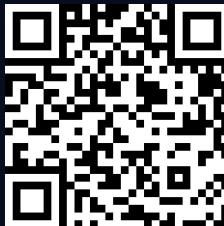
May 28, 2024 4:51PM - [Payments-Platform](#) - [Tron](#) - [Tron-Approver](#)

1. Implemented check and sign functionality for TRX outgoing transfer in payments-platform/tron/tron-approver to address

5. PoC for you

- Linked models (Defects, Repositories...)
- Dashboard
- Workflows and Extensions
 - Github Loader
 - Nuclei
 - SemGrep
 - Trufflehog

github.com/vankyver/directus-aspm-poc



README

Directus-ASPM-PoC

The screenshot shows the Directus application interface. On the left is a sidebar with navigation items: Directus, Repository, Vulnerable, Defect (selected), Critical Issues, Web Assets, Containers, Commits, Developer, Scans, and Releases. The main content area is titled "Content" and "Defect". It displays a table with 494 items, showing columns for Severity (Info, Info, Info, Info, High, High, High, Medium, Medium), Source (nuclei, nuclei, nuclei, semgrep, semgrep), Status (In progress, Fixed, Open, Open), Summary (Wappalyzer Technology Detection, WAF Detection, Silverlight cross-domain policy, Server-Side Request Forgery (SSRF)- Java..., SQL Injection+ spring - security, SQL Injection+ spring - security, SQL Injection+ jdbc - security), Type (http, http, http, OSS, OSS), and URL (https://api.github.com/repos, https://api.github.com/repos, https://api.github.com/repos).

Proof of Concept for building Application Security Posture Management (ASPM) based on [Directus Headless-CMS](#).

🚀 Running

```
docker-compose up
```

use following credentials to login to Directus:

email: admin@example.com
password: d1r3ctu5

The END - Morale

Sec tools won't work out-of-the-box

- All the companies are unique (because of technology stack)

You need ability to develop it by yourself

- You have to adjust security tools to your needs / team / company

Think out of the box

- Don't use only what market gives you

Use new technologies

- No Code
- AI

P.P.S

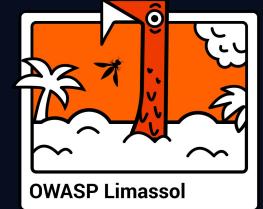


P.P.S Remember!

There are a lot of cool
Open Source tools nowadays

But there is a Big Company
behind the each Big Open Source





Thank you!

ivan.elkin@exness.com

@vankyver