OWASP secureCodeBox

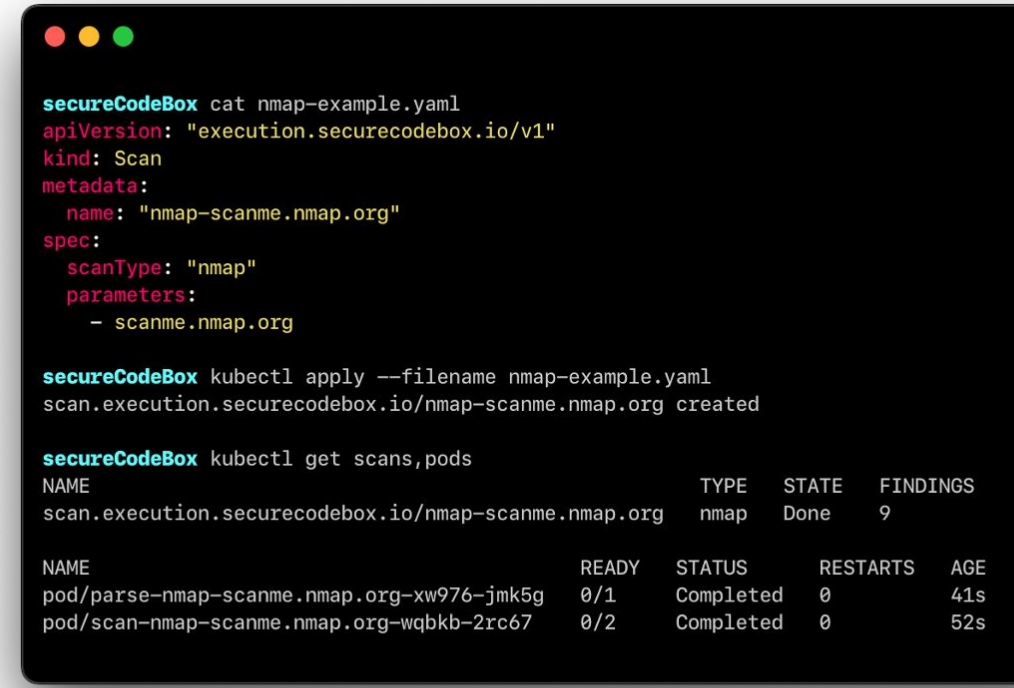
OWASP Hamburg Stammtisch April.2025

- Jannik Hollenbach
- Software Engineer w/ security focus
- Living in Hamburg
- Working at iteratec since 2017
- Project Lead @ OWASP secureCodeBox
- Project Lead @ OWASP Juice Shop

What is the OWASP secureCodeBox?

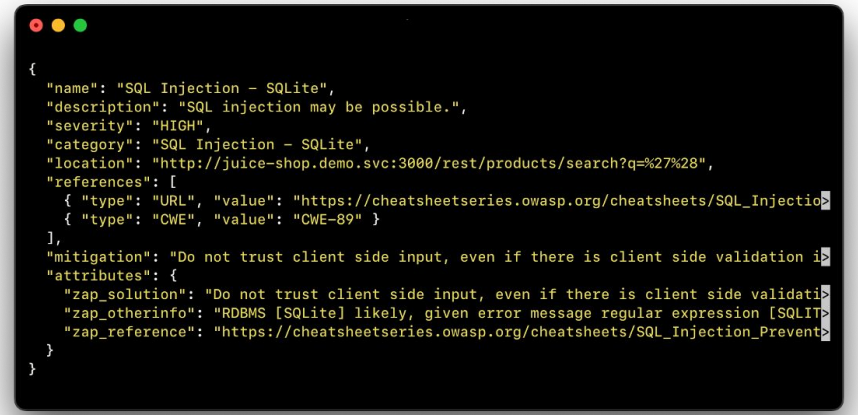
Orchestration

- **Kubernetes Operator** to manage security scanning tools via Custom Resource inside of Kubernetes
- **Scan** CRD to run Scans on the Cluster
- Scans are using a **ScanType** CRD which describes how to turn the scan into a job
- 20+ scanner integrations are maintained by the secureCodeBox team, installable via helm



What is the OWASP secureCodeBox?

Integration

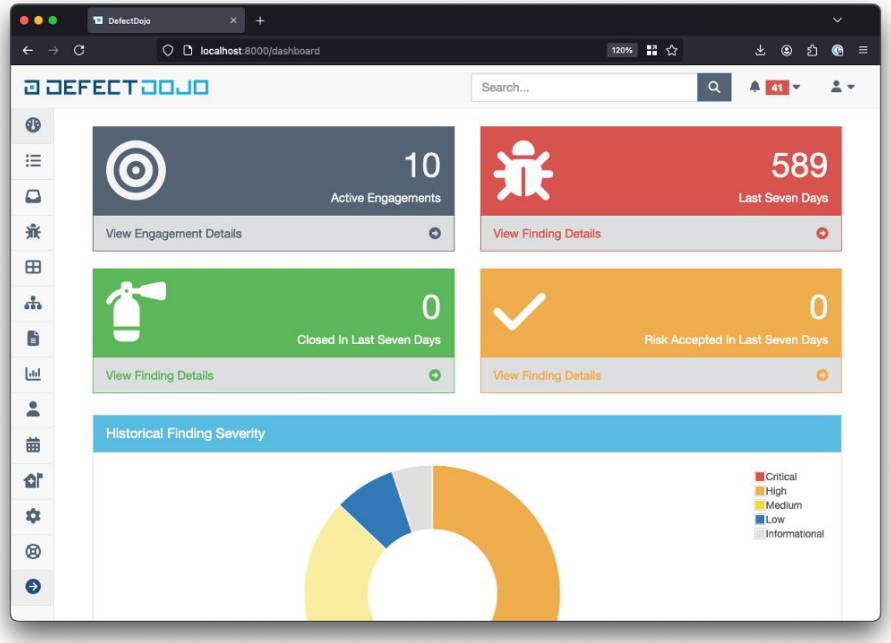


```
{
  "name": "SQL Injection - SQLite",
  "description": "SQL injection may be possible.",
  "severity": "HIGH",
  "category": "SQL Injection - SQLite",
  "location": "http://juice-shop.demo.svc:3000/rest/products/search?q=%27%28",
  "references": [
    { "type": "URL", "value": "https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injectio
    { "type": "CWE", "value": "CWE-89" }
  ],
  "mitigation": "Do not trust client side input, even if there is client side validation i
  "attributes": {
    "zap_solution": "Do not trust client side input, even if there is client side validati
    "zap_otherinfo": "RDBMS [SQLite] likely, given error message regular expression [SQLIT
    "zap_reference": "https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevent
  }
}
```

- Findings from all scanners are translated into a **uniform json** format
- Each finding has a name, location, category, severity which are set for every scanner
- This allows **uniform handling** of findings. E.g. sending a Slack message for all high severity findings

What is the OWASP secureCodeBox?

Modularity & Extendability



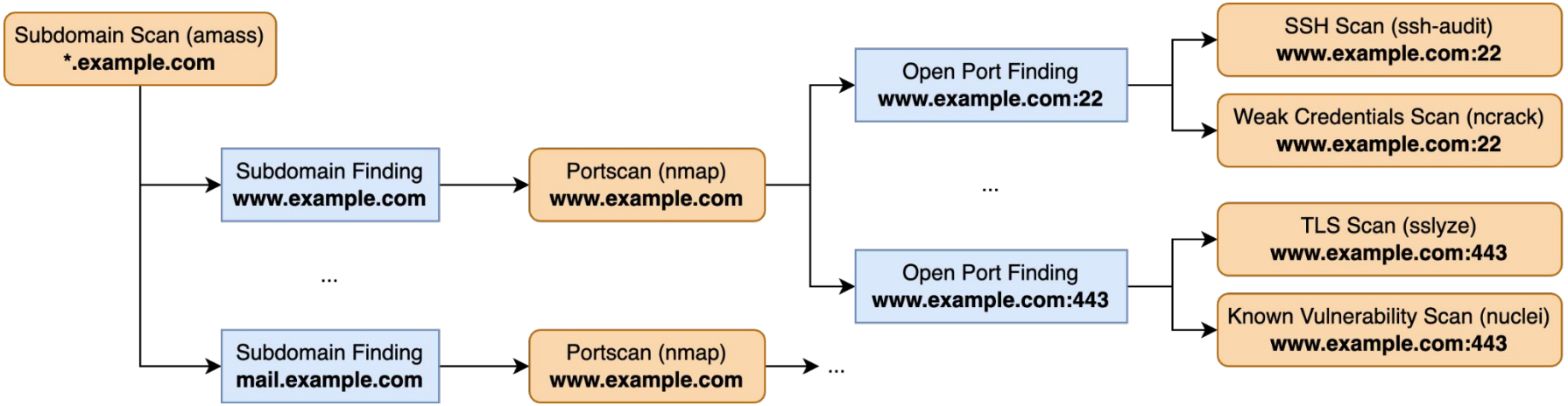
- Hooks allow to handle findings e.g. sending them to external systems
- Official Hooks for sending
  - **Findings** to:
    - OWASP DefectDojo
    - Elastic Stack
  - **SBOMs** to:
    - OWASP DependencyTrack
  - **Notifications** to:
    - Slack
    - MS Teams
    - Email

What is the OWASP secureCodeBox?

Demo

Scanning entire in-/external Attack Surfaces

Using “Cascading Scans”



https://www.securecodebox.io/docs/how-tos/scanning-networks

Scanning entire in-/external Attack Surfaces

Finding

```
{
  "name": "Open Port: 80 (http)",
  "description": "Port 80 is open using tcp protocol.",
  "category": "Open Port",
  "location": "tcp://scanme.nmap.org:80",
  "severity": "INFORMATIONAL",
  "attributes": {
    "port": 80,
    "state": "open",
    "service": "http",
    "protocol": "tcp",
    "method": "table",
    "hostname": "scanme.nmap.org",
    "ip_addresses": ["45.33.32.156"],
    ...
  },
  ...
}
```

Cascading Rule

```
apiVersion: cascading.securecodebox.io/v1
kind: CascadingRule
metadata:
  name: nuclei-http
spec:
  matches:
    anyOf:
    - attributes:
        service: http*
        state: open
      category: Open Port
  scanSpec:
    scanType: nuclei
    parameters:
    - '-target'
    - '{{$.hostOrIP}}:{{attributes.port}}'
```

https://www.securecodebox.io/docs/how-tos/scanning-networks

Scanning entire in-/external Attack Surfaces

OWASP®

Finding

```
{
  "name": "Open Port: 80 (http)",
  "description": "Port 80 is open using tcp protocol.",
  "category": "Open Port",
  "location": "tcp://scanme.nmap.org:80",
  "severity": "INFORMATIONAL",
  "attributes": {
    "port": 80,
    "state": "open",
    "service": "http",
    "protocol": "tcp",
    "method": "table",
    "hostname": "scanme.nmap.org",
    "ip_addresses": ["45.33.32.156"],
    ...
  },
  ...
}
```

Cascading Rule

```
apiVersion: cascading.securecodebox.io/v1
kind: CascadingRule
metadata:
  name: nuclei-http
spec:
  matches:
    anyOf:
    - attributes:
        service: http*
        state: open
      category: Open Port
  scanSpec:
    scanType: nuclei
    parameters:
    - '-target'
    - '{{$.hostOrIP}}:{{attributes.port}}'
```

https://www.securecodebox.io/docs/how-tos/scanning-networks

Scanning entire in-/exteral Attack Surfaces

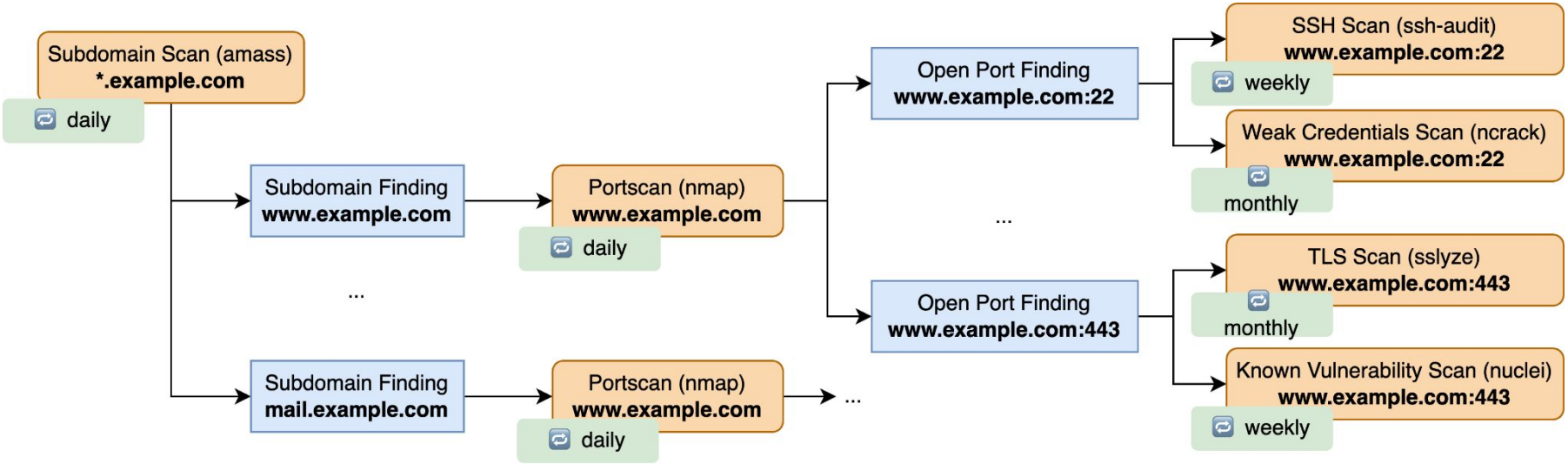
Using “Cascading Scans”

Demo

https://www.securecodebox.io/docs/how-tos/scanning-networks

Optimizing Scan Costs / Overhead

Using scan-deduplicator (experimental)



https://github.com/secureCodeBox/scan-deduplicator

Scanning Software in Kubernetes Clusters

Using “Kubernetes AutoDiscovery”

- The AutoDiscovery is an optional component in the secureCodeBox
- It „watches“ the cluster for „scannable“ resources and then starts scans for them.
- Currently supported:
  - **Pods**: Automatically start container image scans for newly created containers. E.g. for **trivy**
  - **Services**: Automatically start network scans for updated network services. E.g. for **ZAP** or **Nuclei**
- Automatically starts new scans once a service is updated.

https://www.securecodebox.io/docs/how-tos/autodiscovery

OWASP®

Jannik Hollenbach

📧 e-mail jannik.hollenbach@owasp.org

🐘 mastodon @infosec.exchange/@jannik

bluesky @jannik-hollenbach.bsky.social

Demo Repo:

https://github.com/secureCodeBox/scb-cascades-demo