b.

25 TOOLS & EXTRA TACTICS FOR APP SECURITY

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

b.

table
of contents

app security **OWASP** **tools**

reconnaissance **monitoring**

chapter 1

why should
I **bother**?

Since you already opened this ebook, we assume **you do bother**. No one wants to be woken up in the middle of the night with the message "We've been hacked".

If you are **a software developer** working on a web or mobile app, this ebook will help you **check step by step, if your product is secured**.

If you are **an app owner**, this ebook is full of insights into **what skills and security tactics you should expect** from your software security team.

Let your app live long and securely! ✋

chapter 2

how should
I start?

Time to kick off the **Secure Software Development Lifecycle** in your organization. Beginnings don't have to be hard! Let's start with **the easiest security tactics** that you can implement almost right away.

Secure Software Development Lifecycle (SDLC)

A framework that maps the whole development process, incorporating security in all stages of the lifecycle. Makes security one of the most important phases of SDLC. Related also to DevSecOps.

b.

LOW-HANGING
SECURITY FRUITS

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

Verify login credentials

Ensure that **all admin accounts don't have default login credentials** or **easy-to-break credentials** such as login: admin, password: admin.

Avoid this mistake 👇

FINANCE

Equifax used the word 'admin' for the login and password of a database

PUBLISHED THU, SEP 14 2017·2:47 PM EDT | UPDATED THU, SEP 14 2017·4:59 PM EDT

Thomas Franck
@TOMWFRANCK

SHARE

Source: cnbc.com

Delete sensitive data from code

Check out if **test credentials or sensitive data arent's hard coded** in the frontend code comments.

Avoid this mistake 👇

A newspaper informed Missouri about a website flaw. The governor accused it of 'hacking.'

Analysis by Philip Bump
National columnist

October 14, 2021 at 3:15 p.m. EDT

Source: washingtonpost.com

Check CI/CD credentials

If you use **CI/CD providers and other external tools or dashboards**, ensure that any default accounts **don't have easy-breaking credentials**.

Avoid this mistake 👇

Hackers regularly gaining access to businesses' servers with the same regular – often default – passwords

Story by
James Cook

🕐 May 3, 2022

CYBER SECURITY MONTH · **REPORTS** · **TECHNOLOGY**

Source: businessleader.co.uk

Remove secrets from repo

Verify if **any secrets** e.g. AWS keys, passwords, etc. **aren't checked-in in repositories**.

Avoid this mistake 👇

NEWS

Popular mobile apps leaking AWS keys, exposing user data

Security researchers at CloudSek discovered approximately 40 popular mobile apps contained hardcoded API secret keys, putting both user information and corporate data at risk.

By Shaun Nichols

Published: **06 May 2021**

The Subpostmasters
vs
The Post Office

Source: techtarget.com

Ensure ports aren't exposed

Make sure that the services you use **don't have any unwanted exposed ports**.

Avoid this mistake 👇

Source: vice.com

Don't go with keys from tutorials

When you use crypto, **don't take keys from any tutorials**.

Avoid this mistake 👇

Software developer cracks Hyundai car security with Google search

Top tip: Your RSA private key should not be copied from a public code tutorial

Thomas Claburn   Wed 17 Aug 2022 // 20:19 UTC

Source: theregister.com

Withdraw access

Remember to **regularly withdraw access to any tools**, from ex-employees or people who simply don't need them, to reduce the attack surface. Consider **using a Single Sign-On** for all your services.

Avoid this mistake 👇

1 in 4 Ex-Employees Still Has Access to Company Data

Stephen Taylor
CEO of LeadingIT, a cybersecurity and IT support firm helping companies protect their data (and their bank accounts).

24 lutego 2022

Single Sign-On

Authentication method using one set of credentials to authenticate within multiple services (ex. Google Sign-in) securely.

Source: <u>linkedin.com</u>

chapter 3

introduction to OWASP

Luckily, resources about the app security aren't some secret knowledge. It's the opposite – there are **lots of materials online**. What's more important – **there are trusted sources to follow**. We encourage you to take a comprehensive look at the materials published by OWASP and the community built around it.

OWASP (The Open Web Application Security Project)

OWASP is a non-profit organization whose aim is to improve the security of software. It is the number one security source for software developers and innovators. OWASP shares knowledge through countless open-source projects, docs, and educational events.

b.

TOP OWASP OPEN-SOURCE RESOURCES TO FOLLOW

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

by bright inventions

2023

OWASP TOP 10

10 most popular dependencies to be discovered in web apps. If you want to start from the security basics, this is the place to go. Here you will find the first 10 things you need to do to ensure your app is secure.

check more

OWASP ASVS

ASVS stands for Applications Security Verification Standards.

OWASP ASVS is a standard checklist by OWASP. It touches on different aspects of web app software development. Follow the list and step-by-step check if your app meets dozens of security standards described by OWASP.

check more

OWASP MASVS

OWASP MASVS stands for Mobile Application Security Verification Standard.

This is another OWASP standard checklist made exclusively for mobile application security. If you work with mobile, that's another document to read for you.

check more

A Tip for App Owners

Include in your contract with the development team **a requirement to follow security standards levels listed in OWASP ASVS or/and OWASP MASVS.** There are three security levels stated in the document. You can choose the level you want the software agency to meet.

That's a great way to **ensure, at the very beginning, that your software team will prioritize security**. Remember to keep up with updates on these documents because they are being refactored.

OWASP Cheat Sheet

Top security standards and processes in a nutshell. If you have to fill in some blanks after reading OWASP ASVS and OWASP MASVS, the cheat sheet will come in handy.

[**check more**]

The Cheat Sheet is developed by security experts. In theory, everyone can contribute. Naturally, all pull requests are verified by project leaders.

The author of this ebook also <u>contributed to the Cheat Sheet</u>. We encourage you to share your knowledge in the future too!

chapter 4

automated security testing

A huge part of your security activity should be automated security testing. Discover tools that will help you conduct these tests. **Tools that we present are open source or offer a free plan,** so you can test them and decide if they are worth to be used on daily basis.

Automatic security tools are divided into multiple categories such as:

- SAST (Static Application Security Testing) tools.
- DAST (Dynamic Application Security Testing) tools.
- Dependency tracking tools.
- Secret leak detection tools.

We will present a couple of examples of software for every category. It's up to you to decide which tools suit you best. Our **recommendation is to use all of them**.

Before you start

For the purpose of learning, **we will show you the examples of vulnerabilities with <u>OWASP Juice Shop</u>**. It is **an app dedicated to discovering security weak spots**. If you want to learn how to find security holes, this app has been developed especially for this purpose. Feel free to use it. Wherever it is not possible to show some vulnerability via Juice Shop, you can use google.com due to its openness to a bug bounty program (only for presentation/learning purposes).

Always use your own resources to test if you are not sure! Have in mind that **it might be illegal to use any tools mentioned in this ebook to exploit vulnerabilities** found on particular websites. Therefore always look for their security policy or check if they have the bug bounty program open.

STATIC APPLICATION SECURITY TESTING TOOLS

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

SAST tools to consider

SAST tools scan your app's code and notify you about any vulnerabilities such as SQL injections, outdated algorithms, or strings with possible passwords.

Also, even with paid tools author tries to embrace free plans and shows you the usage of them to make security scanning more community popular and make security "shift-left" in SDLC. Presenting 3 different tools with 3 different limitations, so you can choose something for you and your team. The author assumes your code is a close source with a basic plan in Github/Gitlab.

Static Application Security Testing (SAST)

Automatic application scanner, analyzing source code, container images, etc. to find security issues.

Snyk

Snyk is paid SAST tool. The **free version enables ~100 scans a month**. Still, even if you are not considering a paid version (or want to run checks only locally, not on CI/CD server), you should definitely consider it in a format of plugin to your favourite IDE.

check this tool
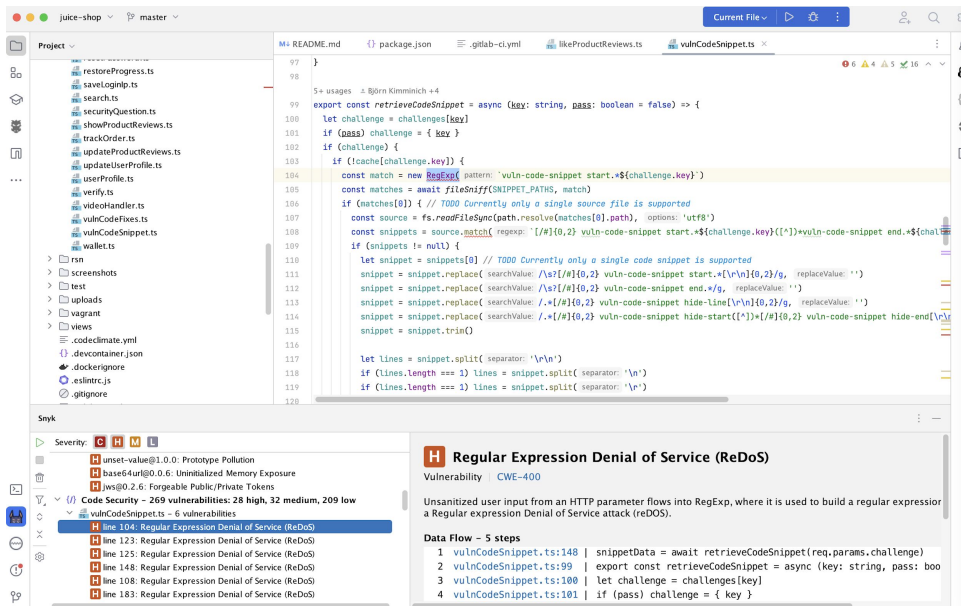
Example of Code Security Scan – ReDos vulnerability found.
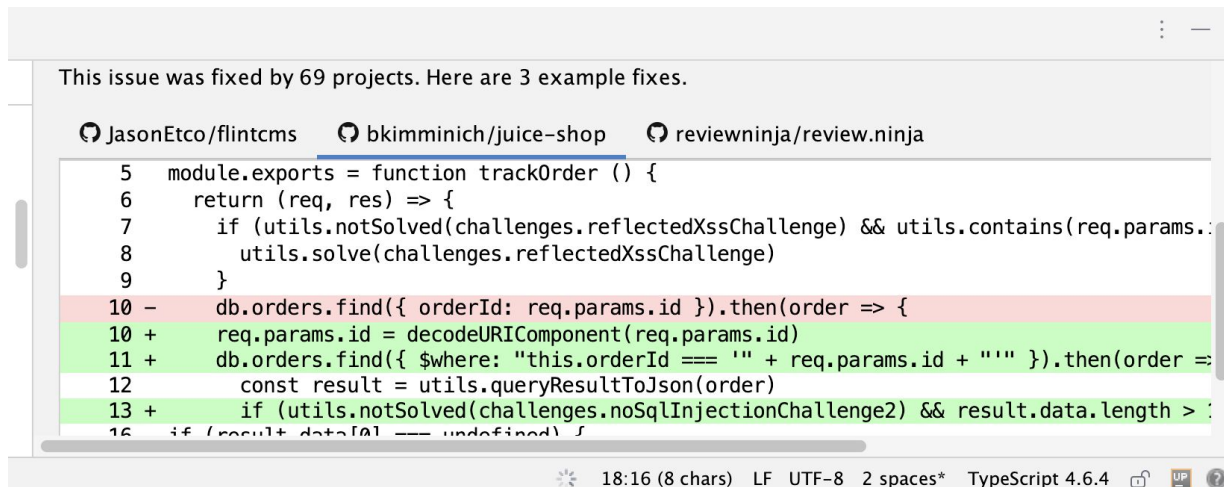
Snyk

Onboarding is quite easy – **create an account in the Snyk cloud portal**. Then, upon downloading the plugin you have to authenticate yourself in the app. When you are done, voila – you can use Snyk on your codebase.
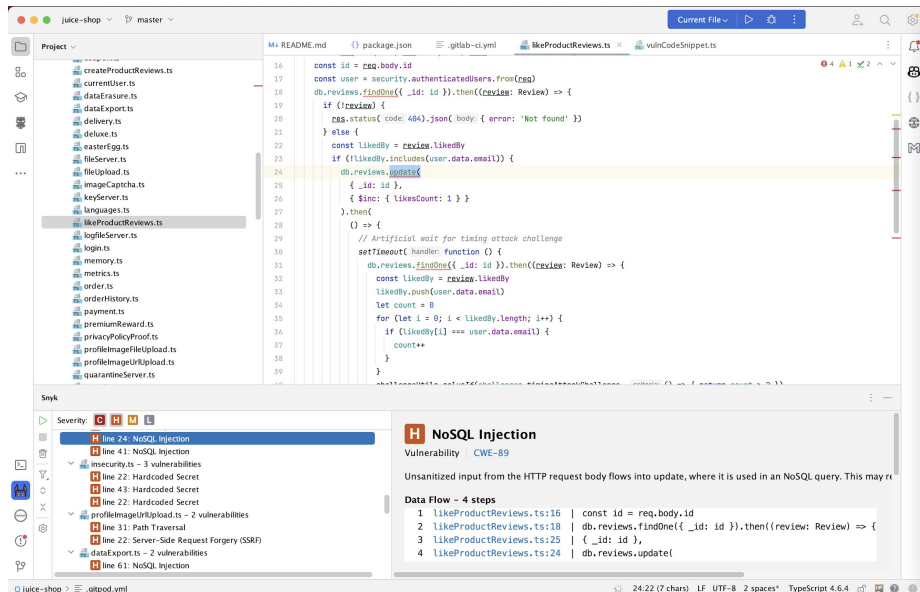
Example of Code Security Scan – NoSQL vulnerability found.

Snyk

When scanning for code security, it gives you the severity of the issue, what is the issue exactly, and how to fix those.


```
This issue was fixed by 69 projects. Here are 3 example fixes.

  JasonEtco/flintcms      bkimminich/juice-shop        reviewninja/review.ninja

    5    module.exports = function trackOrder () {
    6      return (req, res) => {
    7        if (utils.notSolved(challenges.reflectedXssChallenge) && utils.contains(req.params.
    8          utils.solve(challenges.reflectedXssChallenge)
    9        }
   10  -      db.orders.find({ orderId: req.params.id }).then(order => {
   10  +      req.params.id = decodeURIComponent(req.params.id)
   11  +      db.orders.find({ $where: "this.orderId === '" + req.params.id + "'" }).then(order =>
   12          const result = utils.queryResultToJson(order)
   13  +        if (utils.notSolved(challenges.noSqlInjectionChallenge2) && result.data.length > 
   16        if (result.data[0] === undefined) {

                              18:16 (8 chars)   LF   UTF-8   2 spaces*   TypeScript 4.6.4
```

Example of Snyk "How to fix" functionality.

Snyk

It also scans your dependencies and gives you an advisor score of the package taking into consideration security issues, maintenance, etc.
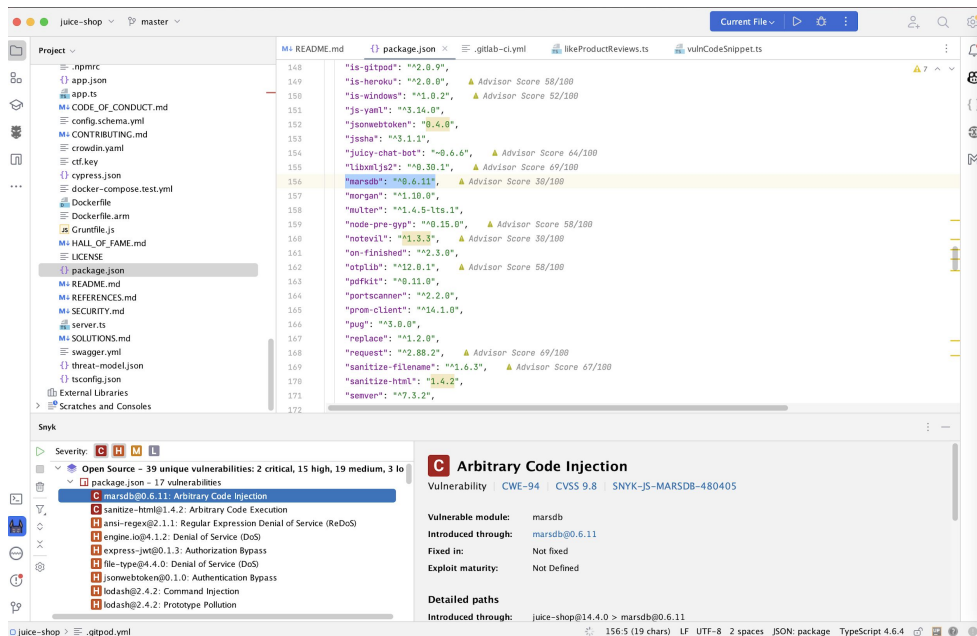
Example of Dependency scan – code execution in package marsdb.

Snyk

You should definitely **consider at least a free version** to check up on your project for issues that you might not be aware of! You can also easily **scan your CI/CD**, **add new team members** to your project but you have to **bear the limits in mind**.

Example Snyk Advisory Score for package marsdb.

Semgrep

Semgrep is the next paid SAST tool, but is **available as SaaS for free for teams of up to 20 persons** (based on developers who made commits in the last 30 days).

check this tool

Semgrep Cloud platform - vulnerabilities.

Semgrep

Onboarding is also quite easy – you have to **create an account on Semgrep Cloud**. Then, register your scanner locally and scan the code. You also have the possibility to use the scanner with CI/CD pipeline and use the Web dashboard.

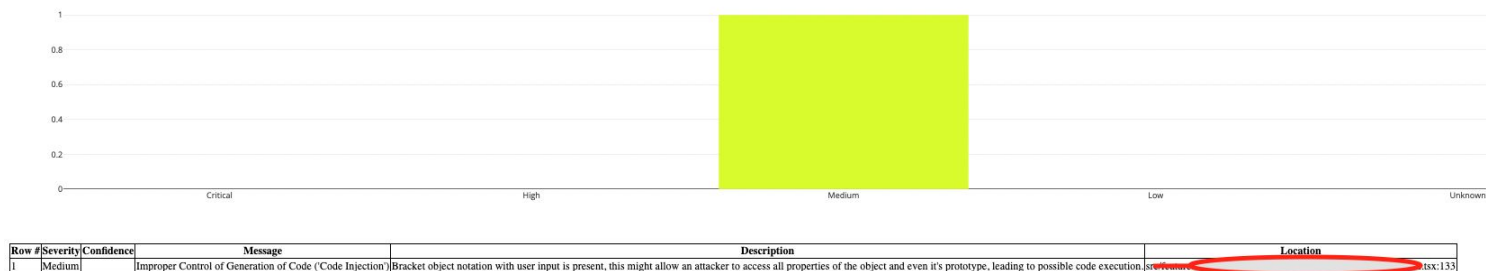*Semgrep vulnerability details – secret detection.*

Semgrep

Another option to use Semgrep as Open Source tool (without the limits) is for example built-in **GitLab Security Scanner**, which produces scanning report after job.

Semgrep open source built in Gitlab pipeline.
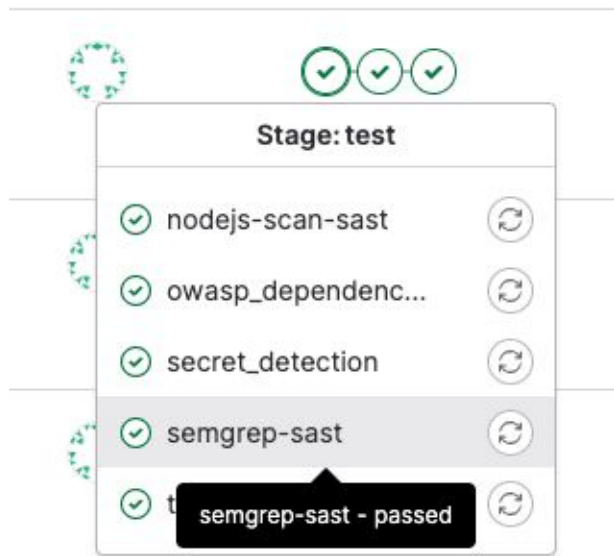
Semgrep

For using it in free mode you have to **parse the report JSON file** by yourself to create an HTML report.

For built-in Security UI, you will need a Gitlab Ultimate subscription.

Vulnerability Report

| Row #	Severity	Confidence	Message	Description	Location
1	Medium		Improper Control of Generation of Code ('Code Injection')	Bracket object notation with user input is present, this might allow an attacker to access all properties of the object and even it's prototype, leading to possible code execution. src/components/... .tsx:133	

Semgrep open source report example

SonarQube

Sonarqube, similarly to Snyk **has a free and paid version**. Sonarlint is a free IDE extension that will analyze your project similar to Snyk.

The problematic thing about it though is that the **rules set is quite limited when you are not using a local SonarQube server or SonarQube cloud.** So out of the box capabilities are in my opinion less powerful than Snyk.

check this tool
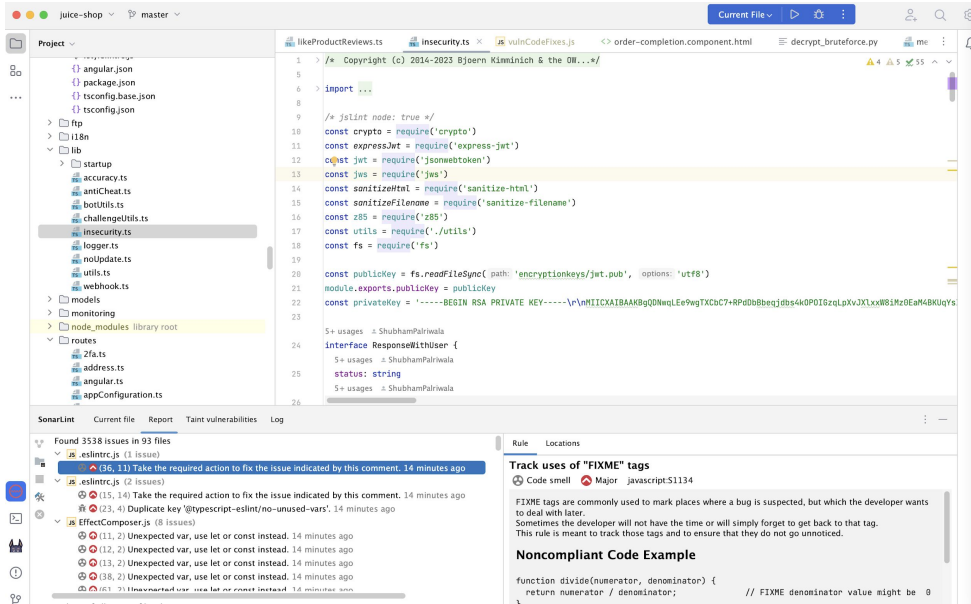

Sonarlint example findings

SonarQube

What you can do though to enjoy free linting with extended rules set is **download the SonarQube Community Edition and run a server locally**. It is more cumbersome to set up than Snyk, but you are not limited to a number of scans.

In my case, it required running the docker image with community edition, logging in with default credentials (then changing them 🙂) and configuring the scanner with the project. As a result, you will have **a nice UI with code quality security issues**:

Self hosted SonarQube instance - vulnerability list.
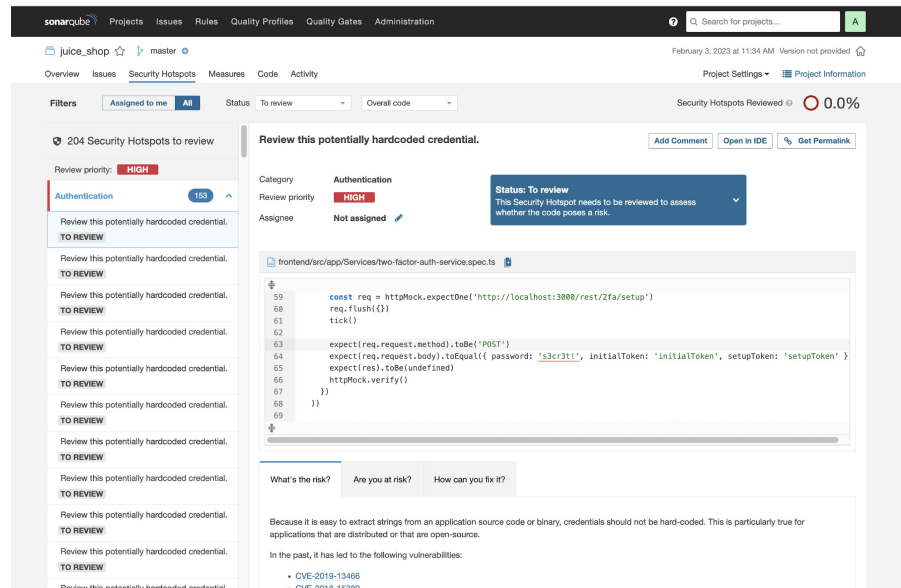
SonarQube

What is nice, you can **configure the server for your team**, expose it to them and start to manage the issues together. Also, you can combine it with your CI/CD, adding one step forward to the complication of setup.
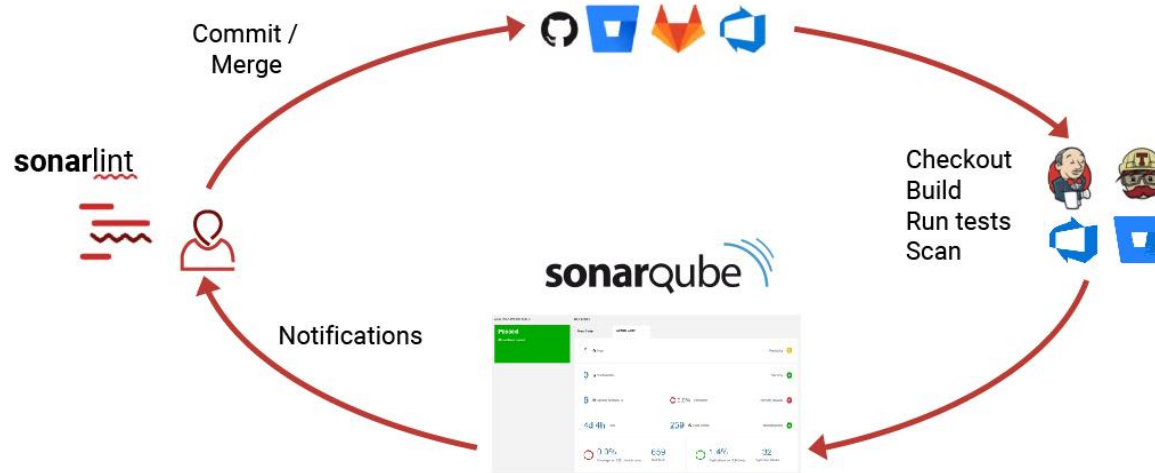
Source: docs.sonarqube.org

SAST tools – final thoughts

SAST tools are great solutions out there **especially if you want to scan your code as a developer** (incorporate it in your development process). Adding more users, working on security as a team, making it interactive for pull requests, etc. costs either more effort or more money. Still, **taking into account that such great tools can be used for free it is a bargain** to do so. For security purposes, I would suggest:

- **Snyk** plugin for l**ocal development** due to its multi-purpose and power.

- **Semgrep** App for **CI/CD if your development team is small (up to 20 developers)** and you are able to create an organization via SCM (Github, Gitlab). Semgrep for CI/CD as a standalone app if you do not have that possibility or your team extends 20 developers.

- **SonarQube** for **CI/CD scans** as self-hosted Community Edition i**f your team is bigger** (but requires some time to set it up).

b.

DYNAMIC
APPLICATION
SECURITY TESTING
TOOLS

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

by bright inventions

DAST tools to consider

DAST tools are used to **test your application from outside**. Often they have the possibility to **proxy the requests, record them, tamper with them, replay them, inject parameters, build a site map** by crawling, etc.

Dynamic Application Security Testing (DAST)

The process of app scanning to analyze security based on running the app (dynamically).

OWASP ZAP (Zed Attack Proxy)

It is a freeware tool. It gives you the possibility to **run the ZAP proxy with a browser of your choice**. When you start navigating the page, **a site map is created**.

Also, the **automatic scanner for requests is ongoing, so it warns you when a security issue arises** – a security header is missing (for example Strict Transport Security not enforced) or data is exposed.

check this tool
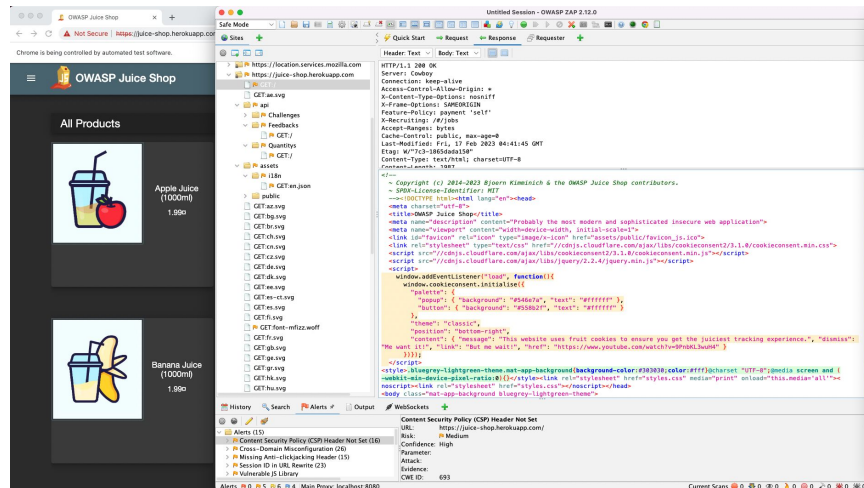
Juice Shop UI - Response, Alerts example.

OWASP ZAP (Zed Attack Proxy)

You can either **do the navigation manually or you can use the ZAP Spider tool to build a site map**. ZAP **keeps a history of requests.** You can send given requests to the request editor and re-try it with a changed payload.


Juice Shop site map.

Burp Suite Community Edition

It is an **alternative to OWASP ZAP**. It has more extensions and better community support. It is also **easier to navigate the app and documentation** (no wonder – this is a paid tool).

However, in Community Edition you are getting support for only some of the features (e.g. Repeater).

To start open a web browser from Burp Community Edition App. Requests should be visible upon HTTP history.

check this tool
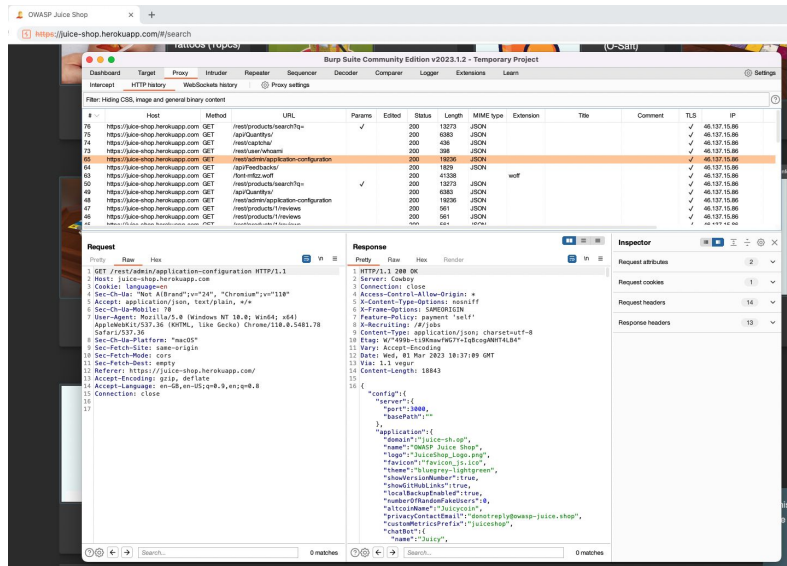
Analyzing HTTP history with Burp Suite.

Burp Suite Community Edition

Same as with ZAP by navigating the page you **build a page map that you use later**. You can later send a request to the o Repeater tool, change it and send it again.

Apart from that, in the community edition you also have an option to **inject various payloads (Intruder), check token randomness (Sequencer), decode the data (Decoder) or compare it (Comparer).**
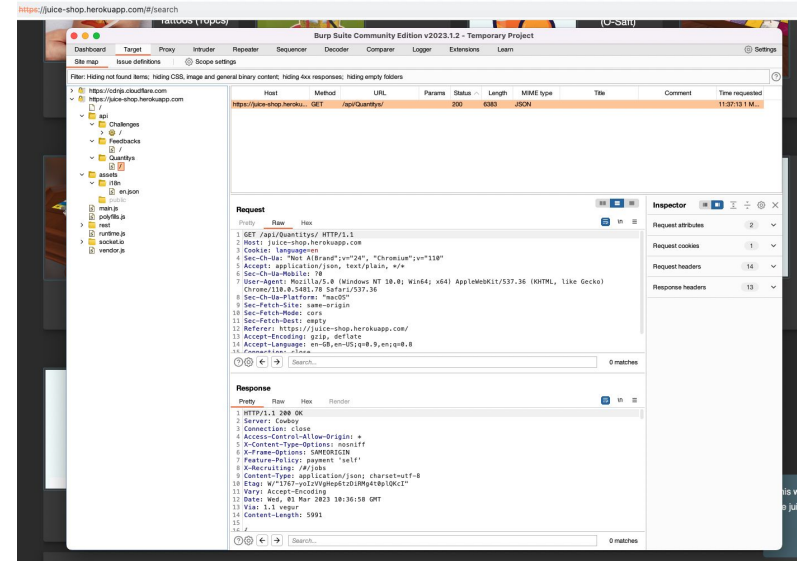
Juice Shop site map.

DAST tools – final thoughts

Which tool you should you choose? My advice is to **play a little bit with OWASP ZAP and Burp Suite and choose one that suits your needs best**. Both of them have support for basic proxing, editing of the requests which might be enough for start.

b.
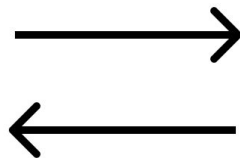
DEPENDENCY
TRACKING TOOLS
TO CONSIDER

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

Dependency tracking tools to consider

These tools will notify you about any vulnerabilities. The best practice is to **merge them into your pipeline**. Dependency tracking tools **ensure that you have security updates**. They can notify you to install them or even do it automatically for you. If you can't merge this tool into your pipeline, then **run it regularly**, for example before a commit with <u>Githooks</u>.
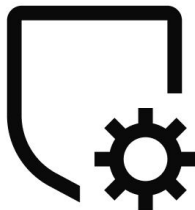
Dependabot

GitHub's tool that sends you **alerts** when your repository uses a vulnerable dependency or malware. Nice thing is that Dependabot is **built in the GitHub repo, available for all repository types**.

Not only do you receive notifications that packages are outdated but dependable can run pull requests. Based on the test results you can decide whether to merge them or not. **Must have for GitHub repos**! It's possible for other providers but you have to do more work to integrate it.

check this tool
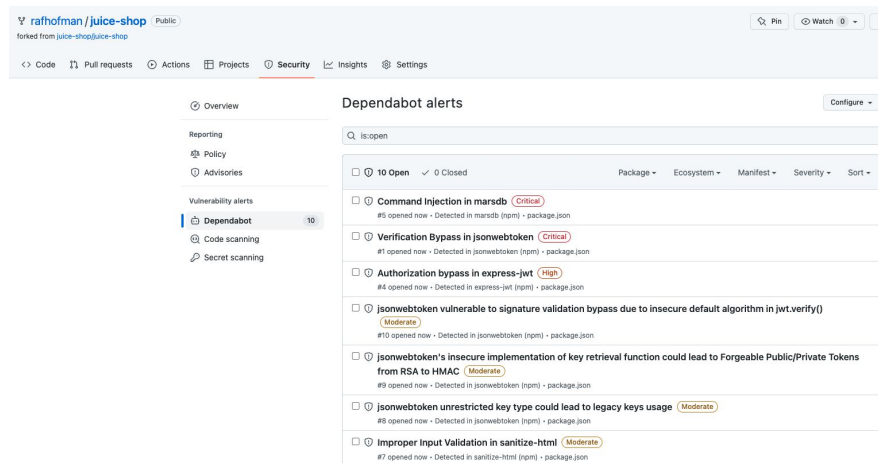
Outdated dependencies list by dependabot.

OWASP Dependency Check

It is an open source and free software, more platform agnostic than Dependabot. You can **easily incorporate it in your CI/CD pipeline** and generate an **HTML report** about dependencies afterward.

It checks and downloads the whole NVD vulnerabilities database, so you have to configure it correctly (otherwise it will be time-consuming work). You can also run it on a local development machine.

check this tool

Outdated dependencies list by OWASP dependency check.

Retire.js

Dependency check tool for client JS code. You can install a <u>Chrome extension</u> to analyze the code of visited websites.

check this tool

Outdated dependencies on example site with Retire.js extension.

Built-in tools

OWASP dependency check is a great tool. Yet, as mentioned, it might be time-consuming to use. **Another option is to use built-in tools in your package manager**. The scan will be targeted on one technology only. However, you don't have to worry about download times. For example, an npm-audit or a yarn audit tool can be used for the JS stack.

critical	Command Injection in marsdb
Package	marsdb
Patched in	No patch available
Dependency of	marsdb
Path	marsdb
More info	https://www.npmjs.com/advisories/1086801

Outdated dependencies list by yarn audit.

SECRET LEAK DETECTION TOOLS

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

Secret leak detection tools to consider

These types of automation tools will help you discover any secret leaks. Types of secrets are:

- Database password,
- JWT key,
- API keys (e.g. AWS Access Key ID & Secret, Google Maps, Twilio Account_sid and Auth Token).

All of presented tools are free or offer a free plan. You will be able to test tool's potential to decide whether you want to upgrade a plan or not. We won't be surprised if you find these tools essential at your work. 🙂

Gitleaks

It can be installed **locally or on CI/CD server**. In all Gitlab plans available **for free as Secret Leaks scanning tool**. You can also configure it as a **pre-commit hook.**

check this tool

```
  o
  |\
  | o
o  ▦
  ▦    gitleaks

2:55PM INF 129 commits scanned.
2:55PM INF scan completed in 7.1s
2:55PM WRN leaks found: 2
```

Secret found on page by Gitleaks.

TruffleHog

It is another option to consider after Gitleaks. It is slightly more sophisticated but on the other hand, gives you more options to **customize output/view the leak**. For example, there is a possibility to verify with an e.g. AWS provider that those are indeed correct secrets leaked from their site (TruffleHog is calling GetCallerIdentityApi).

What is interesting is **TruffleHog Chrome Extension** which shows secret leaks on websites. It can scan .git and .env leaked files.
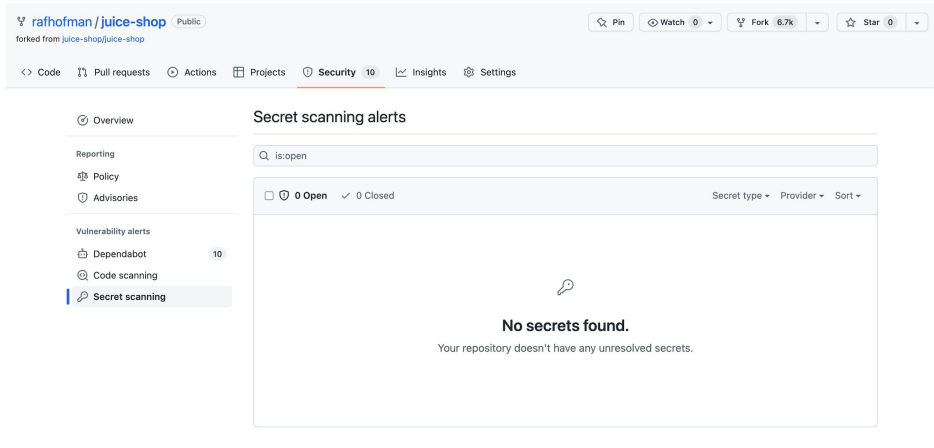
check this tool
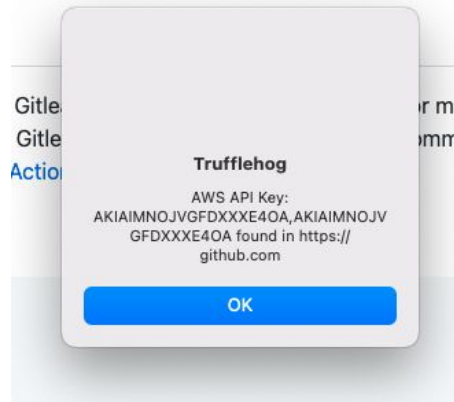
Secrets found by TruffleHog extension – page had printed AWS secrets.

GitHub Secret Scanning

Secret scanning alerts that runs automatically to notify you about secret leads on GitHub.com. Recently available for all repositories.

If you use GitHub, make sure you enabled this feature.

check this tool

Secret scanning alerts.

chapter 5

infrastructure reconnaissance

Applications don't exist in a vacuum. Behind every solution is the infrastructure. Recently software developers are becoming more and more responsible for IT operations. A part of that is securing your infrastructure. We gathered **tools that are useful for infrastructure reconnaissance**.

These are publicly accessible and free tools and **everyone can check your infrastructure with them**. So make sure that they don't show any vulnerabilities of your app **before someone else discovers them**.

INFRASTRUCTURE RECONNAISSANCE TOOLS

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

by bright inventions

crt.sh

A tool for subdomains reconnaissance. Here you can **insert your domain to see all subdomains**. Crt.sh will make you quickly realize that **your staging domains aren't something others cannot find**. Confirm that all your environments and all your tools have **strong credentials or are not accessible without VPN**.

Another thing to note is that depending on your domain naming, one can know what you are working on and with whom. If that is a secret, keep it to yourself.

check this tool

List of possible subdomains registered for google.com.

VirusTotal

It's a subdomain reconnaissance tool too.
Compared to crt.sh it also shows domain IPs.

check this tool

Subdomains (3.22 K) ⓘ		
gmail-smtp-in.google.com	0 / 87	64.233.191.26
google-proxy-66-102-6-114.google.com	0 / 87	66.102.6.114
google-proxy-64-233-172-38.google.com	0 / 87	64.233.172.38
google-proxy-66-102-9-223.google.com	0 / 87	66.102.9.223
google-proxy-66-249-93-222.google.com	0 / 87	66.249.93.222
rate-limited-proxy-74-125-218-23.google.com	0 / 87	74.125.218.23
google-proxy-66-249-82-13.google.com	0 / 87	66.249.82.13
mail-oa1-f80.google.com	0 / 87	209.85.160.80
google-proxy-66-102-6-12.google.com	0 / 87	66.102.6.12
google-proxy-74-125-215-77.google.com	0 / 87	74.125.215.77

List of possible subdomains with IPs registered for google.com.

Censys

It's a search engine that you can use, for example, to **scan any IP address and check open ports, software versions, location of the servers**, etc. It's highly recommended to scan your site to see if you do not have any unnecessary open ports or outdated software versions that do have CVE.

check this tool

Censys result of IP analysis of Juice Shop app example hosting server.

Phonebook.cz

Apart from listing all domains, phonebook.cz also **shows email addresses from the scanned domains**. It's a great way to check what email addresses could be found on your website and remove the ones you don't want to be public.

<div>check this tool</div>

A Tip for App Owners

Find out if any unnecessary emails are listed in phonebook.cz and delete them from your app's code. This might reduce the risk of phishing attacks against your employees.

Phonebook.cz

Logout

Phonebook lists all domains, email addresses, or URLs for the given input domain. Wildcards such as *.gov.uk are allowed. You are searching 100 billion records.

google.com   Submit

Try: cia.gov, cnn.com, netflix.com, *.ru, *.gov.uk, solarwinds.com

○ Domains
● Email Addresses
○ URLs

careers@google.com
info@google.com
        @google.com
        @google.com
    @google.com
    @google.com
usz@google.com
llion@google.com
            @google.com
support@google.com
3qqg53lpj3jqdo6plpp4smnkjq@google.com
support-deutschland@google.com
data-protection-office@google.com
wildabandonstudio@google.com
youremail@google.com
newemail@google.com
    google.com
registrar-abuse@google.com
generationgoogle-na@google.com
noreply+feedproxy@google.com
haihong@google.com
0015175cda8c95db2d047fa5f916@google.com

List of email addresses found on google.com domain.

SSL Labs (TLS check)

On this website you can **analyze the configuration of your SSL certificate**. Here you can easily check out if your server certificate is trusted, what TLS protocols are supported, and what might be the security issues.

Yet again, everyone can check it so be certain that you have all certificate issues covered.

check this tool
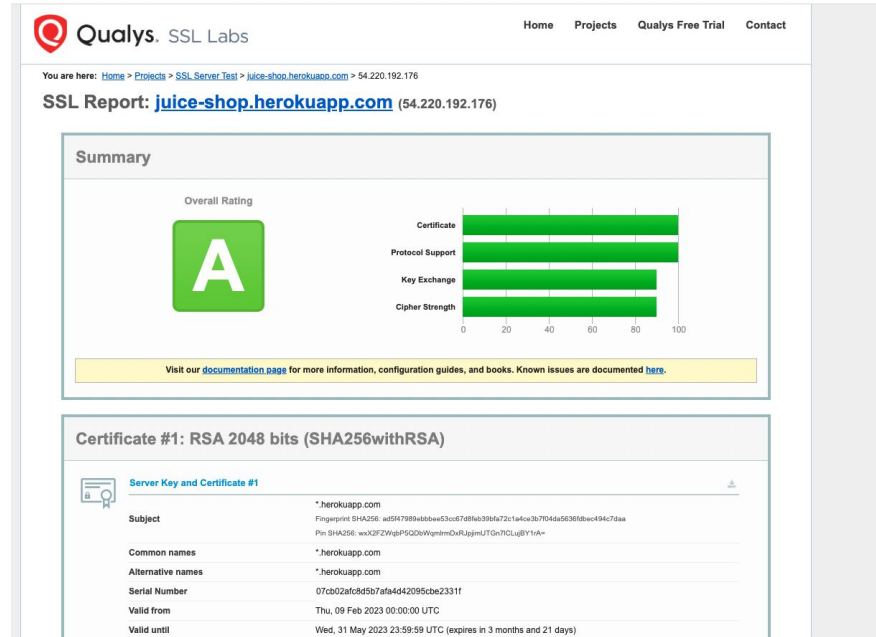
SSL score for Juice Shop example page hosting.

Security Headers

This tool will help you check if your **web app has the correct security headers configured**. Scan your page and then read more information about each header on the site.

check this tool

Security Headers score for Juice Shop example page hosting.
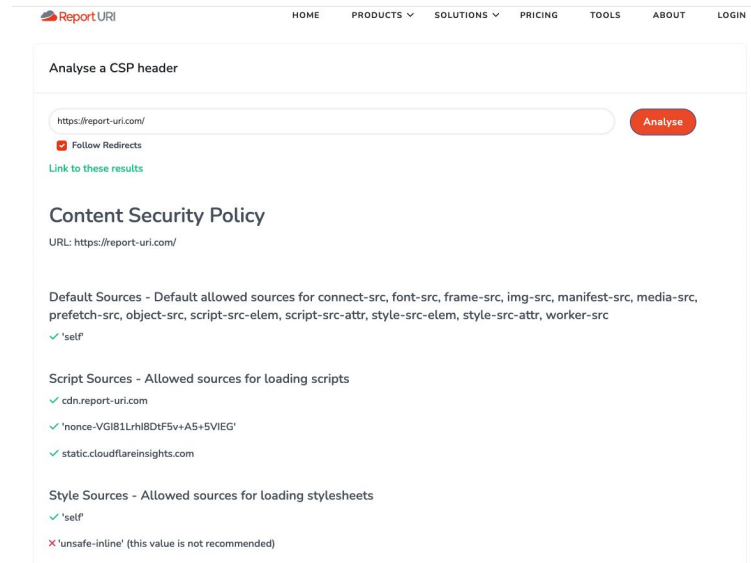
Report URI

When you use the previous tool you will know that the **CSP header might be of use**. 😉 To check it you can use Report URI analyzer.

<div>check this tool</div>

Content Security Policy (CSP)

It is a security header, sent by the backend which specifies the security policy that the client should follow when loading scripts, styles, images, etc. It might stop e.g. XSS attack when a script is loaded from a malicious site.

CSP header check on example page.

Report URI

To **generate a policy** (even based on existing data) you can use <u>Report URI generator</u>.

CSP header generator.
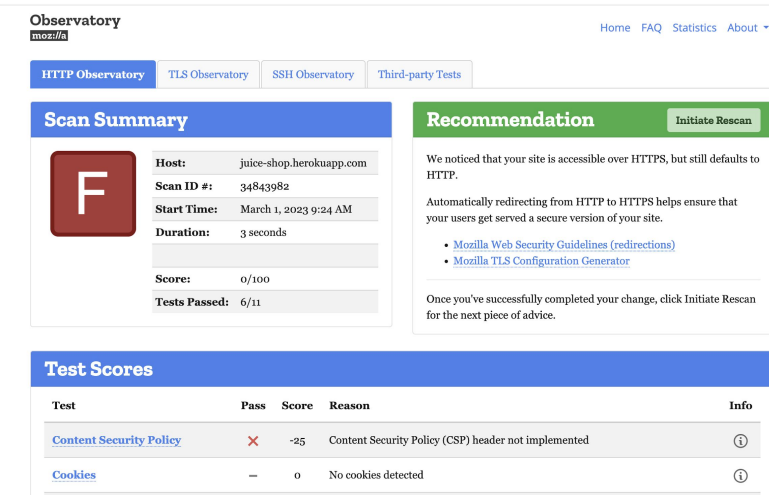
Mozilla Observatory

The tool, in a way, aggregates previous websites so you get an option to **check headers, do TLS scan, and see third parity analysis**.

check this tool

Scan summary for Juice Shop.

chapter 6

infrastructure security

Apart from using the security tools, you should also **follow grand rules** which will help you **maintain your infrastructure secure**.

At Bright Inventions we mostly use AWS as a cloud infrastructure provider, thus will present some security features based on it. These are the only tools mentioned in this ebook which are paid (no free trials included), because they are a part of AWS cloud services.

OWASP Kubernetes Top 10

Standards for one of main deployment and management of containerized apps. It might also be worth taking a look into OWASP Container Security Verification Standard (similar to ASWS but for containers). Last but not least OWASP Cheat Sheet Series might be your friend here.

check more

AWS Foundational Security Best Practices standard

In 2020 AWS provided it as a part of Security Hub, so similar to SAST you can have automatic checks in place. You can also download this list as a document to do a checklist for your environment.

If you want to do a quick check-up, here is also a shorter checklist for your use:

check more

OUT-OF-THE-BOX CLOUD SECURITY

FREE EBOOK FOR DEVELOPERS, APP OWNERS, STARTUPS AND LARGER COMPANIES

AWS Shield

A distributed denial-of-service (DDoS) protection for your AWS apps. By default standard plan is activated.

Distributed denial-of-service (DDoS)

A flooding server with malicious requests to exceed. As a result, its capacity to handle requests is unavailable.

check more

AWS WAF (Web Application Firewall)

A web application firewall. It helps you **define a rule set of which requests should be blocked and which ones should go through.**

Imagine that your app is prone to SQL injection. If you have AWS WAF with OWASP rules enabled, WAF will detect such a malicious request and block it.

check more

AWS KMS (Key Management Service)

KMS is used for encrypting/decrypting your data. By using it, **you can encrypt your secrets or environmental variables**. Also, thanks to KMS your data can be encrypted at rest when stored in S3, RDS or EBS.

check more

A Tip for App Owners

Encryption of sensitive private data is usually legally required. Check what data you should encrypt and do it easily with KMS.

AWS ECR (Elastic Container Registry)

When storing Docker images in ECR you can enable automatic security scans of your docker images.

check more

The power of backup

Make use of backups as a malicious actor can delete or encrypt your resources.

AWS IAM

AWS GuardDuty

You can use IAM (Identity and Access Management) to control the access of users to your infrastructure. Allow only for session manager access when login in to machines, enable SSO etc. which all allows for better granularity and security.

AWS GuardDuty uses ML to analyze anomaly detection.

It's worth to mention that this tool ultimately informed LastPass about suspicious behaviour during recent cyber attack according to the company's update.

check more

check more

Infrastructure security – final thoughts

There are also many other tools for infrastructure security. You will find a full list of those at aws.amazon.com.

All those tools are paid (more or less) but are easy to activate and use within your organization. Consider activating some of them when your app requires certain things legally or when it grows bigger and becomes a target for attackers.

Are you building something on AWS and do not know where to start with security? Check this curated list from AWS.

chapter 7

security
monitoring

We've shown you how to deeply analyze your apps and how to make crucial security improvements. Now what?

Find tips on **what and how to monitor in order to prevent future vulnerabilities & breaches**.

Log security issues to monitor

Examples:

- authorization failures,
- authentication failures,
- password attempts for account exceeded,
- rate limit for endpoint exceeded,
- failure of input validation.

Avoid this mistake 👇

Facebook Bug Allows 2FA Bypass Via Instagram

The Instagram rate-limiting bug, found by a rookie hunter, could be exploited to bypass Facebook 2FA in vulnerable apps, researcher reports.

Dark Reading Staff
Dark Reading

January 30, 2023

Source: darkreading.com

73

Business activity logs to monitor

Examples:

- user who authorized some actions,
- log of users' actions, warning if some actions threshold is exceeded,
- user who canceled some actions.

Avoid this mistake 👇

Hackers breach MailChimp's internal tools to target crypto customers

By **Lawrence Abrams**   April 4, 2022   10:53 AM

Source: bleepingcomputer.com

Infrastructure logs to monitor

Examples:

- who deleted some resources,
- who and when checked some resources,
- who logged in to some machine.

Log those actions as events in logs and use your cloud provider dashboards and alarms. Consider enabling extra protection from your Cloud provider. For AWS use CloudTrail or AWS GuardDuty.

When logging, use centralized place to do it and do a sanitization of the logs.

Avoid this mistake 👇

SECURITY / POLICY / TECH

LastPass reveals attackers stole password vault data by hacking an employee's home computer

Source: theverge.com

Do not log sensible information

Examples:

- passwords,
- keys,
- login credentials,
- biometric information.

Do not log too much information. We cannot express it enough. Don't make it that easy for a possible attacker. As always, **if looking for more information, refer to OWASP Cheat Sheet**.

the end

Now you know the **tools and tactics to ensure your app's higher quality.** We believe that security is a part of quality assurance. You should **pay attention to security, just like you pay attention to testing** (we hope you do 🙂).

Don't forget to check the Tool directory where we listed every mentioned tool.

Also, find Software security resources gathered in one place for you.

If you have any questions or want to share some feedback, contact us via info@brightinventions.pl or find us on Facebook, LinkedIn and Instagram.

author

**Rafał Hofman,
Fullstack Developer
@ bright inventions**

Software Developer with over 5 years of experience. A maritime navigator by profession who decided to become a fullstack developer with a strong focus on web security. He specializes in Ethereum blockchain development. He believes that security is an integral part of quality assurance.

Do you want to know more about Rafał? Read an interview.

Editorial support: Izabela Pawlik, Digital Marketing Specialist @ bright inventions

Bright Inventions is a software consulting studio based in Gdansk, Poland **operating since 2012**. Our expertise in **mobile, web, blockchain and IOT** systems has been highly appreciated by our clients from **UK, Germany, Netherlands, Norway, Israel** and more.

Contact us if you want to estimate your software solution.

brightinventions.pl

info@brightinventions.pl

bright
inventions.

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
Snyk	SAST tool	No	Yes	$0-98 per dev/month	Scanning code for security issues.	Automated security testing
Semgrep	SAST tool	Yes	Yes	Prices aren't listed on the website.	Easy to set up and connect to CI/CD. Built-in as a security scanner in Gitlab.	Automated security testing
SonarQube	SAST tool	Yes	Yes	Developer Plan starts from 150$ per month	Setting up a free community edition server on the local machine.	Automated security testing

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
OWASP ZAP	DAST tool	Yes	-	-	Running the ZAP proxy with a browser of your choice.	Automated security testing
Burp Suite Community Edition	DAST tool	No	Yes, as a Community Edition	Pro version costs €449.00 / per user yearly.	A free version of Burp Suite Professional. It has more extensions and better community support compared to OWASP Zap.	Automated security testing
Dependabot	Dependency tracking tool	Yes	-	-	Out of the box for Github users. Free to use for all GitHub repositories.	Automated security testing

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
OWASP Dependency Check	Dependency tracking tool	Yes	-	-	It can be incorporated in CI/CD pipeline to generate an HTML report about dependencies.	Automated security testing
Retire.js	Dependency tracking tool	Yes	-	-	It also works as a Chrome extension to analyze visited websites.	Automated security testing
Gitleaks	Secret leak detection tools	Yes	-	-	In all Gitlab plans available for free as Secret Leaks scanning tool.	Automated security testing

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
TruffleHog	Secret leak detection tools	Yes	Yes	Prices aren't listed on the website.	It works as a Chrome extension which shows secret leaks on websites.	Automated security testing
GitHub Secret Scanning	Secret leak detection tools	No	-	Free on all public repositories.	Secret scanning alerts for GitHub repositories.	Automated security testing
crt.sh	Infrastructure reconnaissance tools	Yes	-	-	Here you can insert your domain to see all subdomains.	Infrastructure reconnaissance

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
VirusTotal	Infrastructure reconnaissance tools	No	-	-	A subdomain reconnaissance tool which also shows domain IPs.	Infrastructure reconnaissance
Censys	Infrastructure reconnaissance tools	No	Yes	Prices aren't listed on the website.	An search engine that could be used for Infra reconnaissance.	Infrastructure reconnaissance
Phonebook.cz	Infrastructure reconnaissance tools	No	-	-	It lists domains and shows email addresses from the scanned domains.	Infrastructure reconnaissance

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
SSL Labs	Infrastructure reconnaissance tools	No	-	-	It analyzes the configuration of SSL certificate.	Infrastructure reconnaissance
Security Headers	Infrastructure reconnaissance tools	No	-	-	It checks if the web app has the correct security headers configured	Infrastructure reconnaissance
Report URI	Infrastructure reconnaissance tools	No	-	-	It analyzes a CSP header.	Infrastructure reconnaissance

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
Mozilla Observatory	Infrastructure reconnaissance tools	Yes	-	-	HTTP, TLS, SSH Observatory and Third-party tests.	Infrastructure reconnaissance
AWS Shield	Infrastructure security tools	No	Yes As AWS Shield Standard	$3,000.00 / per month for AWS Shield Advanced	DDoS protection for your AWS apps.	Infrastructure security
AWS WAF	Infrastructure reconnaissance tools	No	Yes	Depends on many factors. Better to verify on AWS website.	A web application firewall.	Infrastructure security

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
AWS KMS	Infrastructure security tools	No	Yes	$1/month (prorated hourly)	It is used used for encrypting/decrypting data.	Infrastructure security
AWS ECR	Infrastructure security tools	No	Yes	Storage is $0.10 per GB / month for data stored in private or public repositories.	Automatic security scans of your docker images	Infrastructure security
AWS IAM	Infrastructure security tools	No	No	If you already use AWS services, you can use IAM with no additional charge.	It helps to control the access of users to your infrastructure.	Infrastructure security

Tools directory

Tool	Type	Open source	Free trial	Price range	Main feature	Ebook chapter
AWS GuardDuty	Infrastructure security tools	No	Yes	Depends on many factors. Better to verify on AWS website.	It analyzes anomaly detection.	Infrastructure security

Software security resources

Resource	About	Ebook chapter
OWASP TOP 10	10 most popular dependencies to be discovered in web apps.	Introduction to OWASP
OWASP ASVS	A standard checklist by OWASP. Follow the list and step-by-step check if your app meets dozens of security standards described by OWASP.	Introduction to OWASP
OWASP MASVS	Another OWASP standard checklist made exclusively for mobile application security.	Infrastructure reconnaissance
OWASP Cheat Sheet	Top security standards and processes in a nutshell.	Introduction to OWASP
OWASP Kubernetes Top 10	Standards for one of main deployment and management of containerized apps.	Infrastructure security

Software security resources

Resource	About	Ebook chapter
OWASP Container Security Verification Standard	A framework of security requirements for Docker Containers.	Infrastructure security
AWS Foundational Security Best Practices standard	A security checklist provided by AWS.	Infrastructure security
AWS Security Documentation	AWS documentation that shows how to configure AWS services to meet security standards.	Infrastructure security
OWASP Logging Cheat Sheet	Security best practices for logging information.	Infrastructure security
Bright Inventions blog	A place where you can read about security, QA, mobile and web development.	-