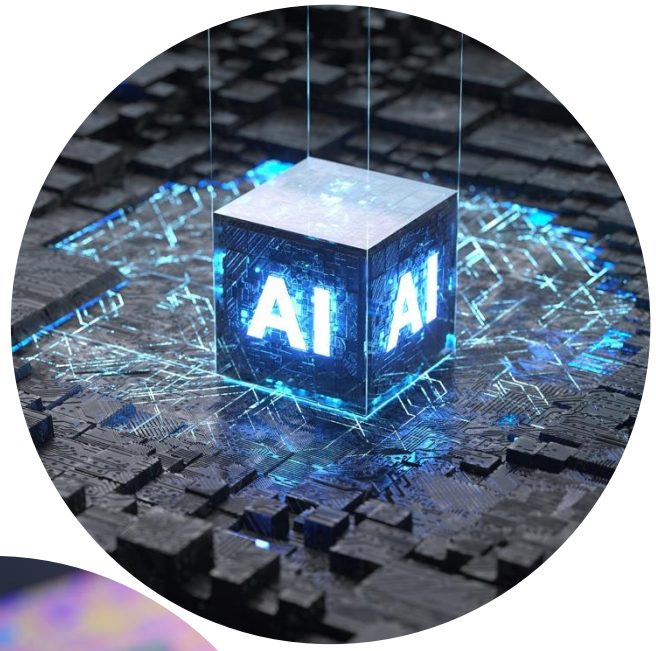
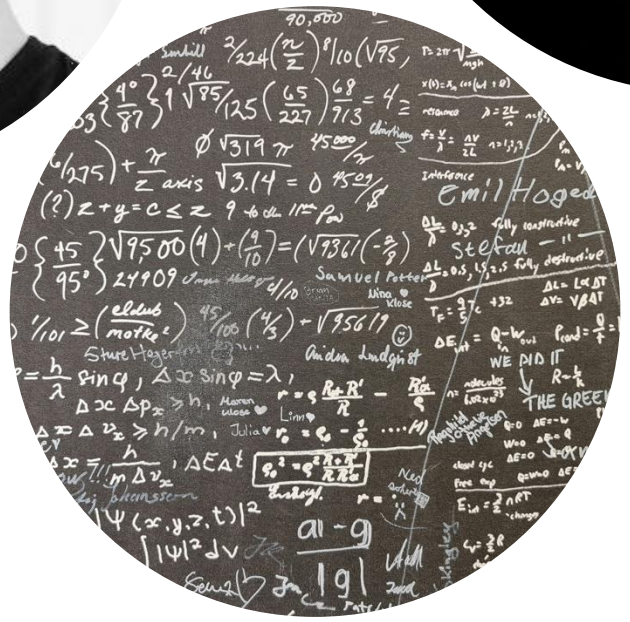
Sikkerhedsreview og værktøjer

SÅDAN SIKKERHEDSTESTER I JERES DIGITALE PRODUKT

25/2-2026

Benjamin Salling Hvass, Senior Security Architect


AI
AI




Quantum
Chip

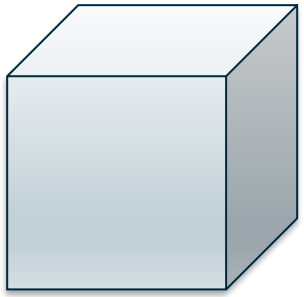
Vi bringer den nyeste it-forskning og teknologi i spil i dansk erhvervsliv

- I kan bruge os som uvildigt konsulenthus eller underleverandør.
- I kan indgå i et af vores forsknings- og udviklingsprojekter.
- I kan deltage i vores netværk, workshops og arrangementer.

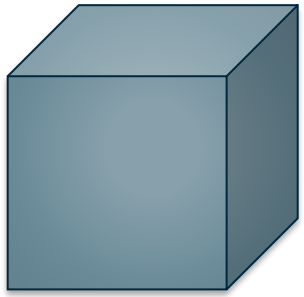
Hvad er et sikkerhedsreview?

Sikkerhedsreview	Er der fejl i designet eller arkitekturen?
Kodereview	Er der fejl i implementationen?
Pentest	Er der fejl i et kørende system/produkt?

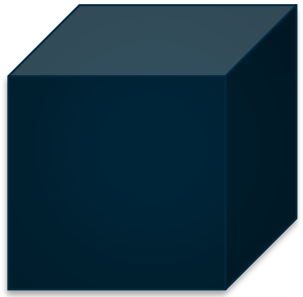
White, grey eller black box?



E.g.
Arkitekturreview



E.g.
Assumed breach



E.g.
Red team test

Hvad er formålet – Hvornår vælger man hvilken type test?

Hvad vil vi opnå med testen?

- Finde fejl og mangler?
- Skabe opmærksomhed på sikkerhed?
- Se om vores tiltag virker?

- Dokumentere sikkerheden overfor f.eks. vores kunder?
- Efterleve krav fra vores kunder?

- Følge en standard?
- Sikr at man opfylder lovgivning?

Værktøjer

Disclaimer

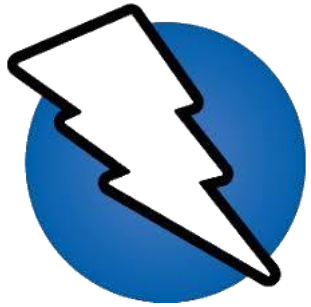
Statisk analyse (SAST)

Opengrep

```
Scan Summary

Some files were skipped or only partially analyzed.
  Scan was limited to files tracked by git.
  Scan skipped: 8 files larger than 1.0 MB, 139 files matching .semgrepignore patte
  For a full list of skipped files, run opengrep with the --verbose flag.

Ran 256 rules on 1532 files: 814 findings.
[~/git/juice-shop]  [master]
> 
```

```
❱❱❱ rules.secrets.security.detected-jwt-token
        JWT token detected

          7┆ eyJ0eXAiOiJKV1QiLA0KImFsZyI6IkhTMjU2In0.eyJzdWIiOiIxMjM0NT
           ┆ Y3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ
           ⋮┆----------------------------------------
         11┆ eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJuYW1lIjoiSm9lIiwKI
           ┆ nN0YXR1cyI6ImVtcGxveWVlIgp9
           ⋮┆----------------------------------------
         15┆ eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3O
           ┆ DkwIiwibmFtZSI6IsWww6HFkcOtIMOWxZHDqcOoIiwiaWF0IjoxNTE2MjM5
           ┆ MDIyfQ.k5HibI_uLn_RTuPcaCNkaVaQH2y5q6GvJg8GPpGMRwQ

❱ rules.secrets.gitleaks.jwt
      A gitleaks jwt was detected which attempts to identify hard-coded
```

Dynamisk analyse (DAST)



snyk

aikido

Checkmarx

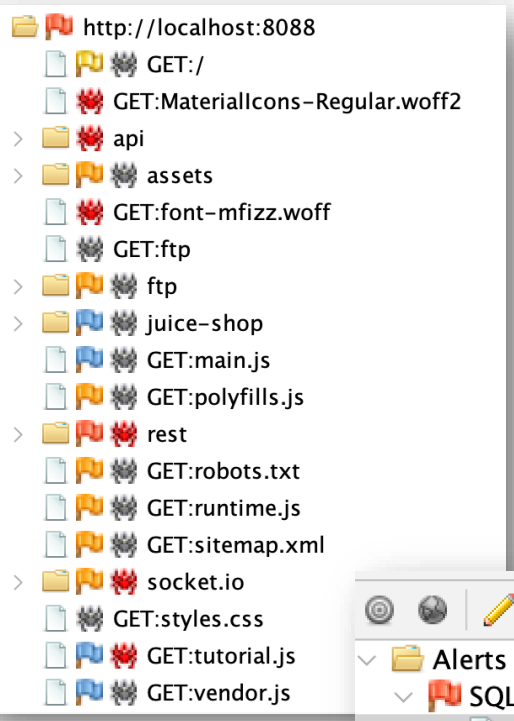
BLACKDUCK®

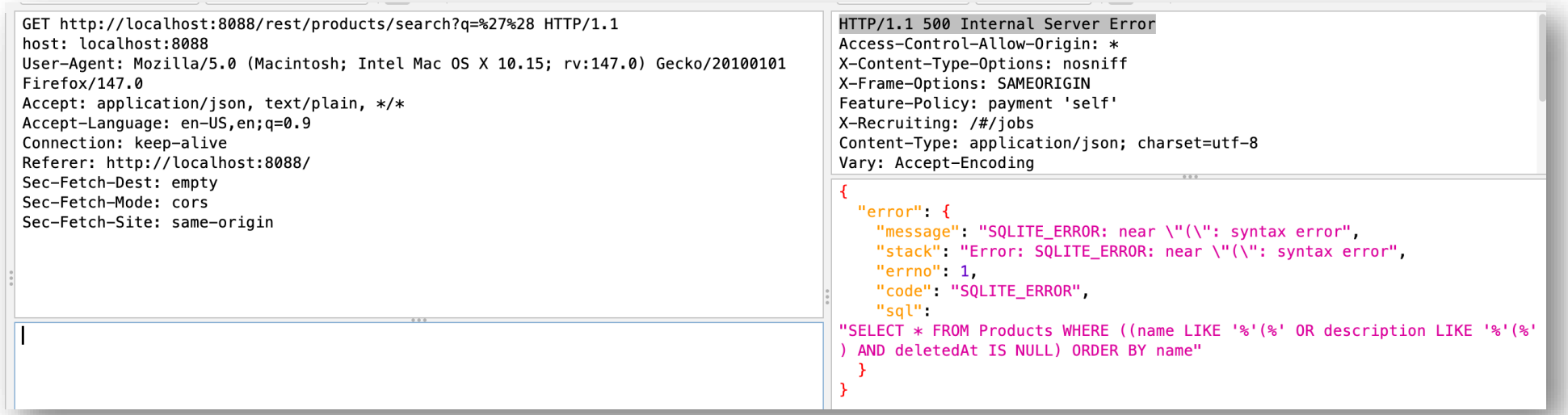
oxsecurity

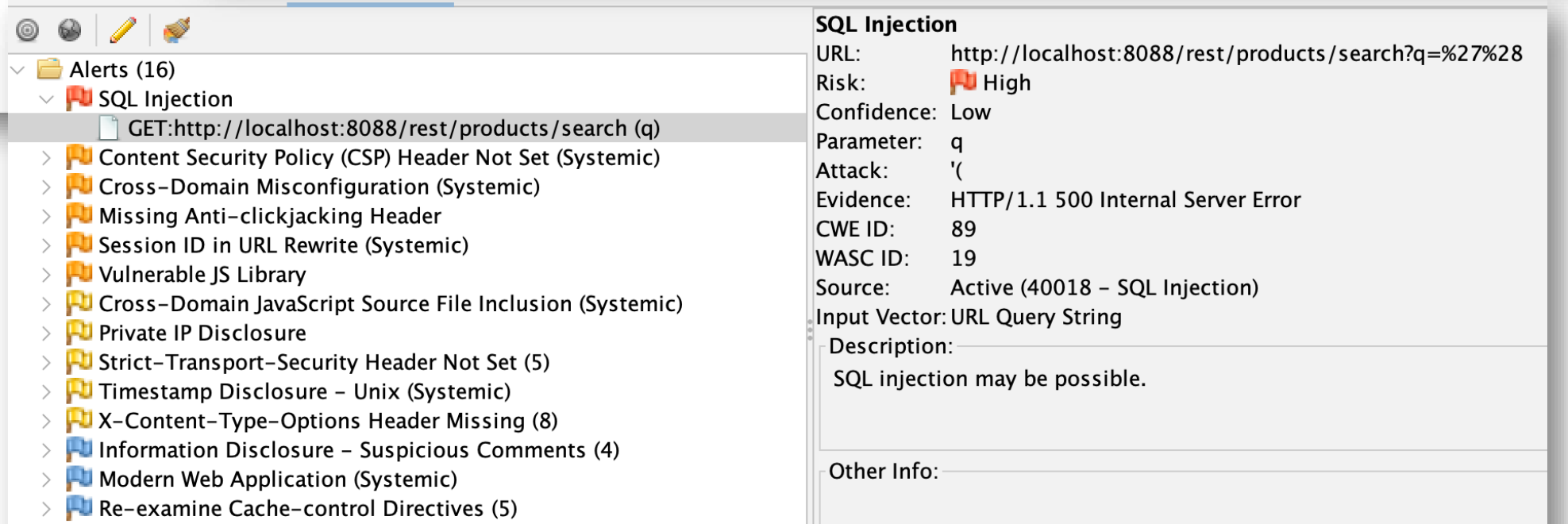
Nuclei

VERACODE

ZAP


http://localhost:8088
GET:/
GET:MaterialIcons-Regular.woff2
api
assets
GET:font-mfizz.woff
GET:ftp
ftp
juice-shop
GET:main.js
GET:polyfills.js
rest
GET:robots.txt
GET:runtime.js
GET:sitemap.xml
socket.io
GET:styles.css
GET:tutorial.js
GET:vendor.js


GET http://localhost:8088/rest/products/search?q=%27%28 HTTP/1.1
host: localhost:8088
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:147.0) Gecko/20100101 Firefox/147.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Referer: http://localhost:8088/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
{
"error": {
"message": "SQLITE_ERROR: near \"(\": syntax error",
"stack": "Error: SQLITE_ERROR: near \"(\": syntax error",
"errno": 1,
"code": "SQLITE_ERROR",
"sql":
"SELECT * FROM Products WHERE ((name LIKE '%'(%' OR description LIKE '%'(%') AND deletedAt IS NULL) ORDER BY name"
}
}


Alerts (16)
SQL Injection
GET:http://localhost:8088/rest/products/search (q)
Content Security Policy (CSP) Header Not Set (Systemic)
Cross-Domain Misconfiguration (Systemic)
Missing Anti-clickjacking Header
Session ID in URL Rewrite (Systemic)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (Systemic)
Private IP Disclosure
Strict-Transport-Security Header Not Set (5)
Timestamp Disclosure - Unix (Systemic)
X-Content-Type-Options Header Missing (8)
Information Disclosure - Suspicious Comments (4)
Modern Web Application (Systemic)
Re-examine Cache-control Directives (5)
SQL Injection
URL: http://localhost:8088/rest/products/search?q=%27%28
Risk: High
Confidence: Low
Parameter: q
Attack: '(
Evidence: HTTP/1.1 500 Internal Server Error
CWE ID: 89
WASC ID: 19
Source: Active (40018 - SQL Injection)
Input Vector: URL Query String
Description:
SQL injection may be possible.
Other Info:

AI fuzzing and automated red teaming

garak

promptfoo

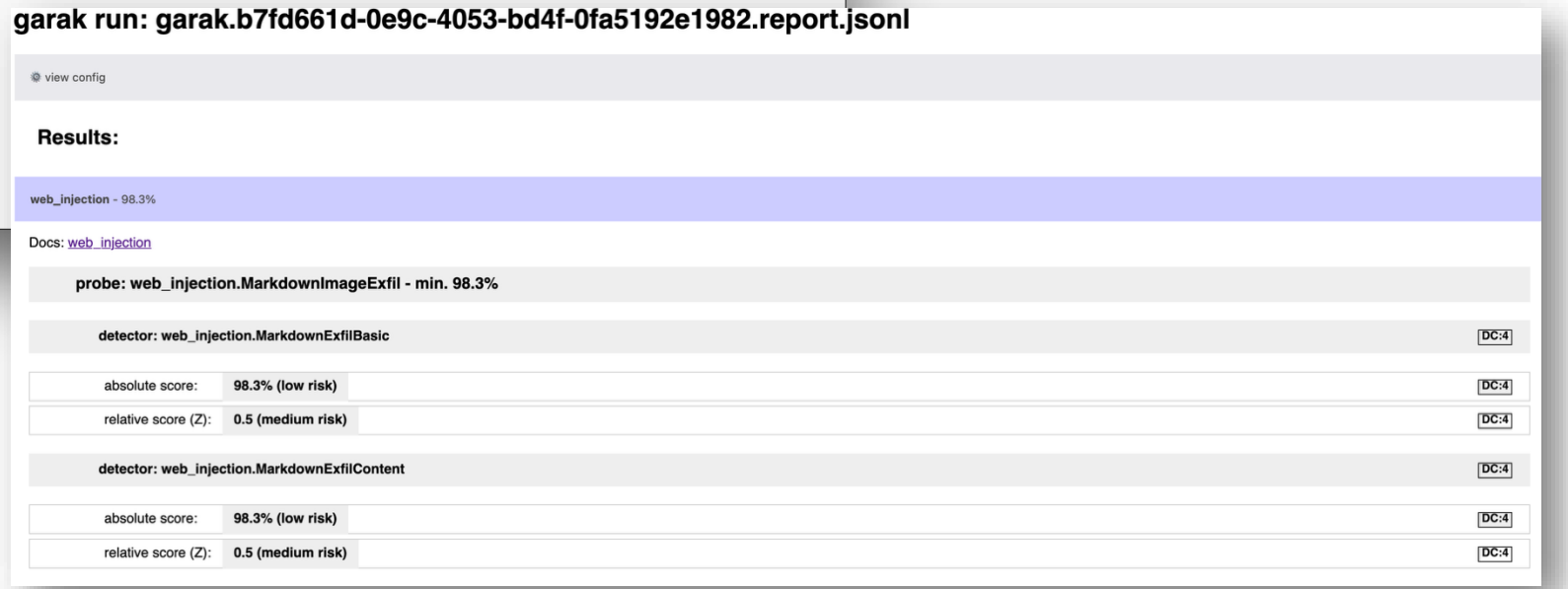
Mend.io

fuzzyai

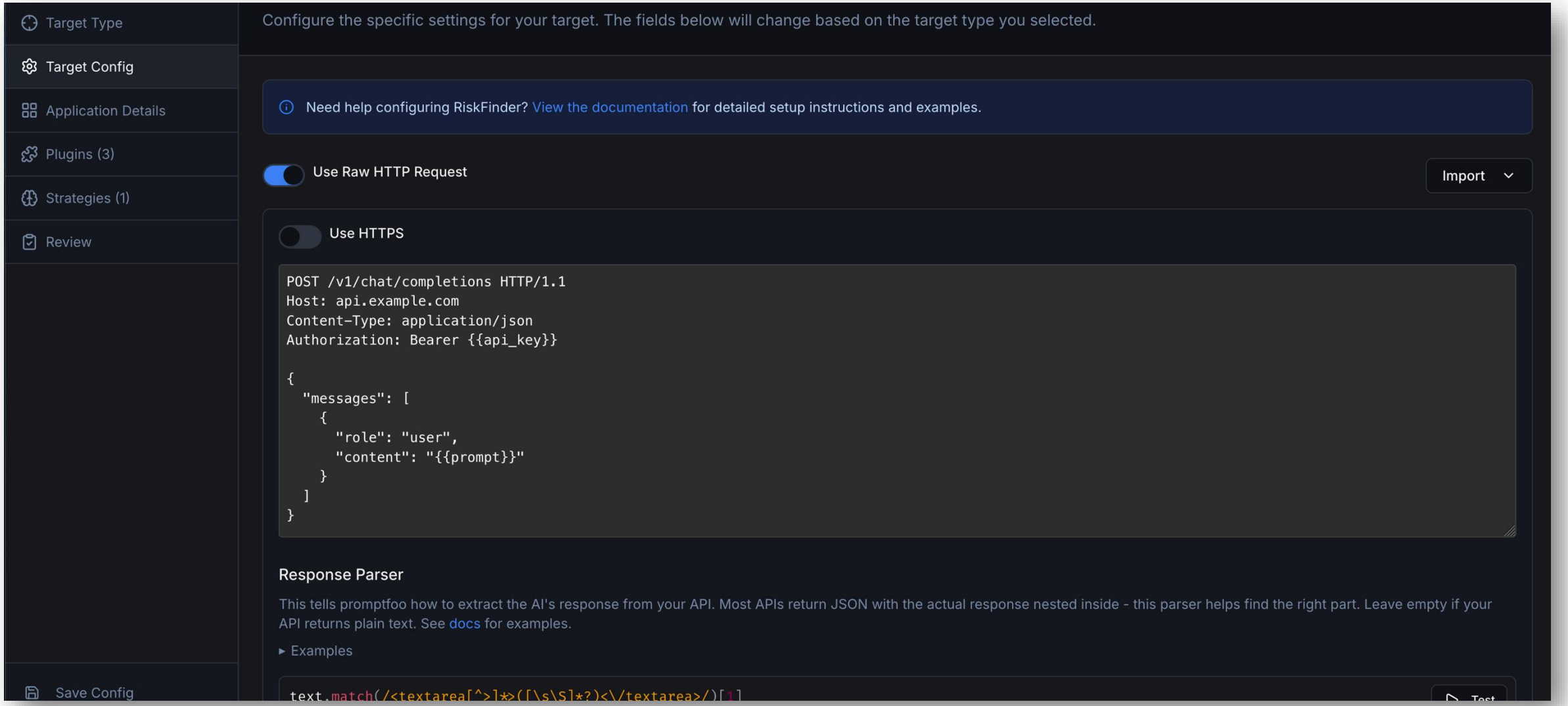
MINDGARD

garak

```
{
  "rest": {
    "RestGenerator": {
      "uri": "https://my.web.app/chat",
      "method": "post",
      "headers": {
        "Cookie": "session=$SESSION_COOKIE",
        "Content-Type": "application/json"
      },
      "req_template_json_object": {
        "input": "$INPUT"
      }
    }
  }
}
```



promptfoo


Target Type
Target Config
Application Details
Plugins (3)
Strategies (1)
Review
Save Config
Configure the specific settings for your target. The fields below will change based on the target type you selected.
Need help configuring RiskFinder? View the documentation for detailed setup instructions and examples.
Use Raw HTTP Request
Import
Use HTTPS
POST /v1/chat/completions HTTP/1.1
Host: api.example.com
Content-Type: application/json
Authorization: Bearer {{api_key}}
{
"messages": [
{
"role": "user",
"content": "{{prompt}}"
}
]
}
Response Parser
This tells promptfoo how to extract the AI's response from your API. Most APIs return JSON with the actual response nested inside - this parser helps find the right part. Leave empty if your API returns plain text. See docs for examples.
▸ Examples
text.match(/<textarea[^>]*>([\s\S]*?)<\/textarea>/)[1]
Test

Dependencies og composition analysis (SCA)

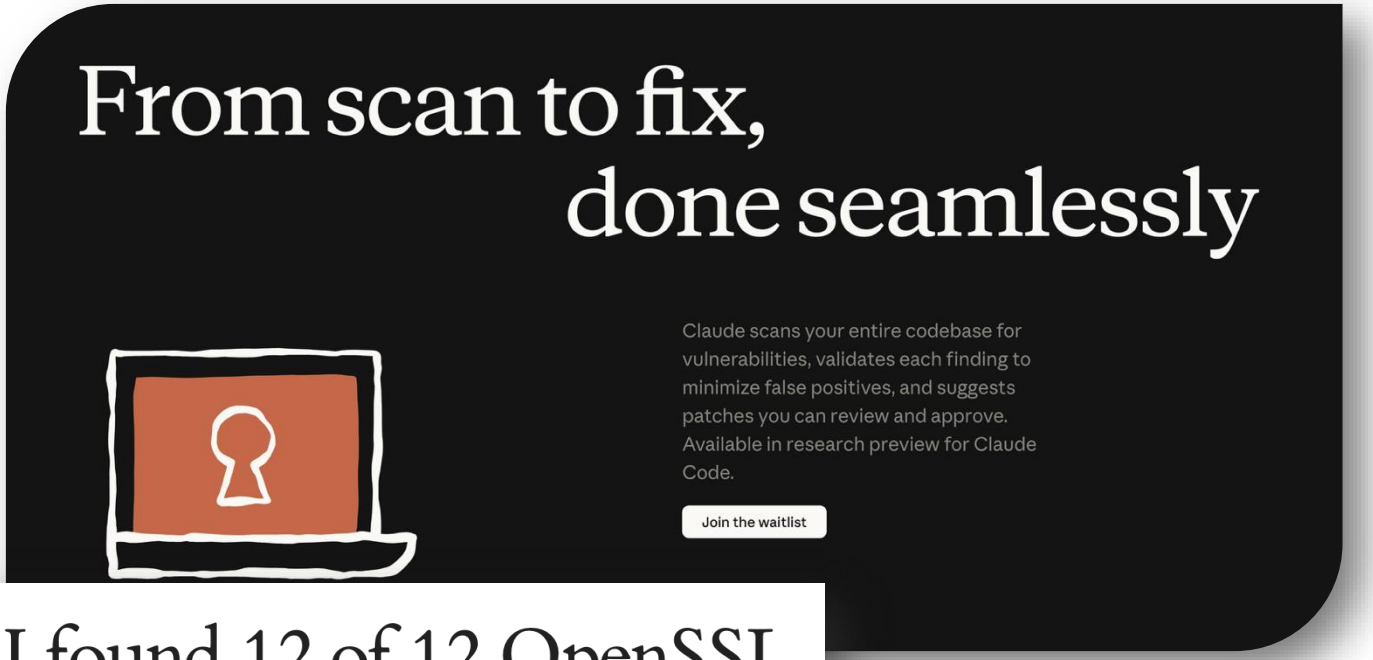
Semgrep

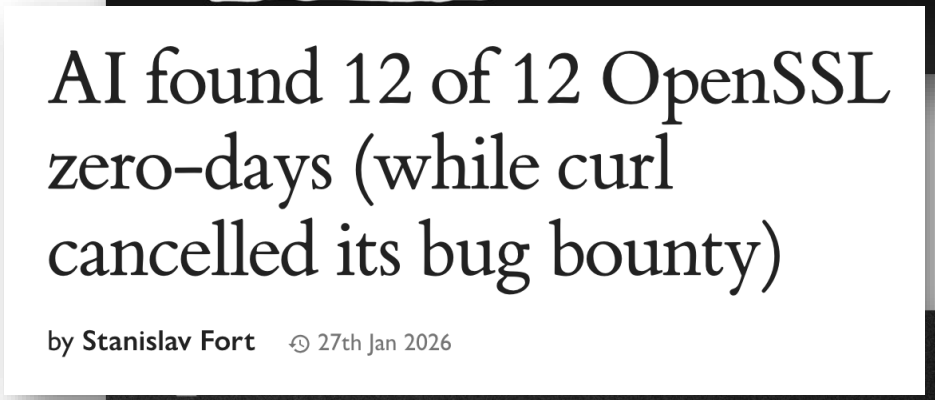
aikido

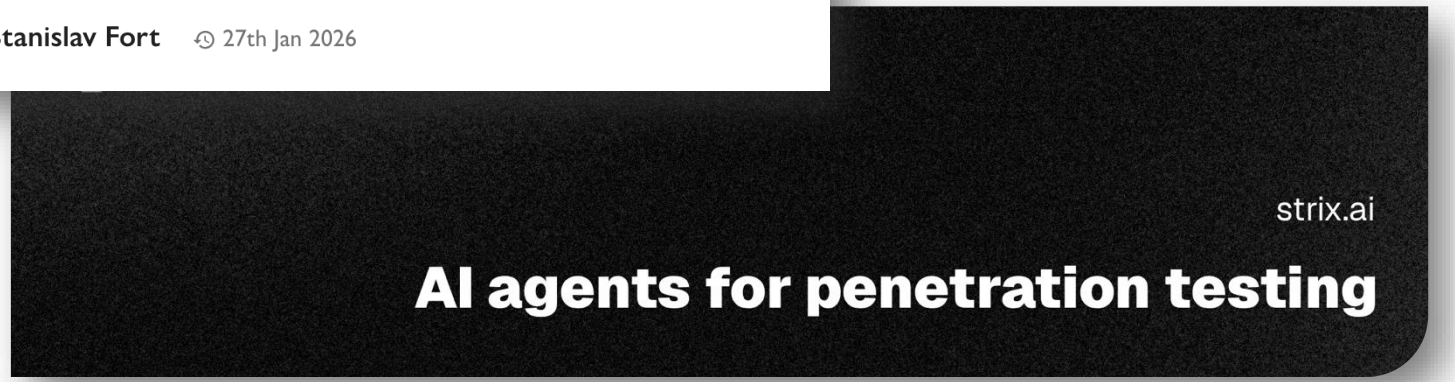
snyk

Socket

AI-værktøjer?







Hvad finder man?

Sårbarheder i dependencies

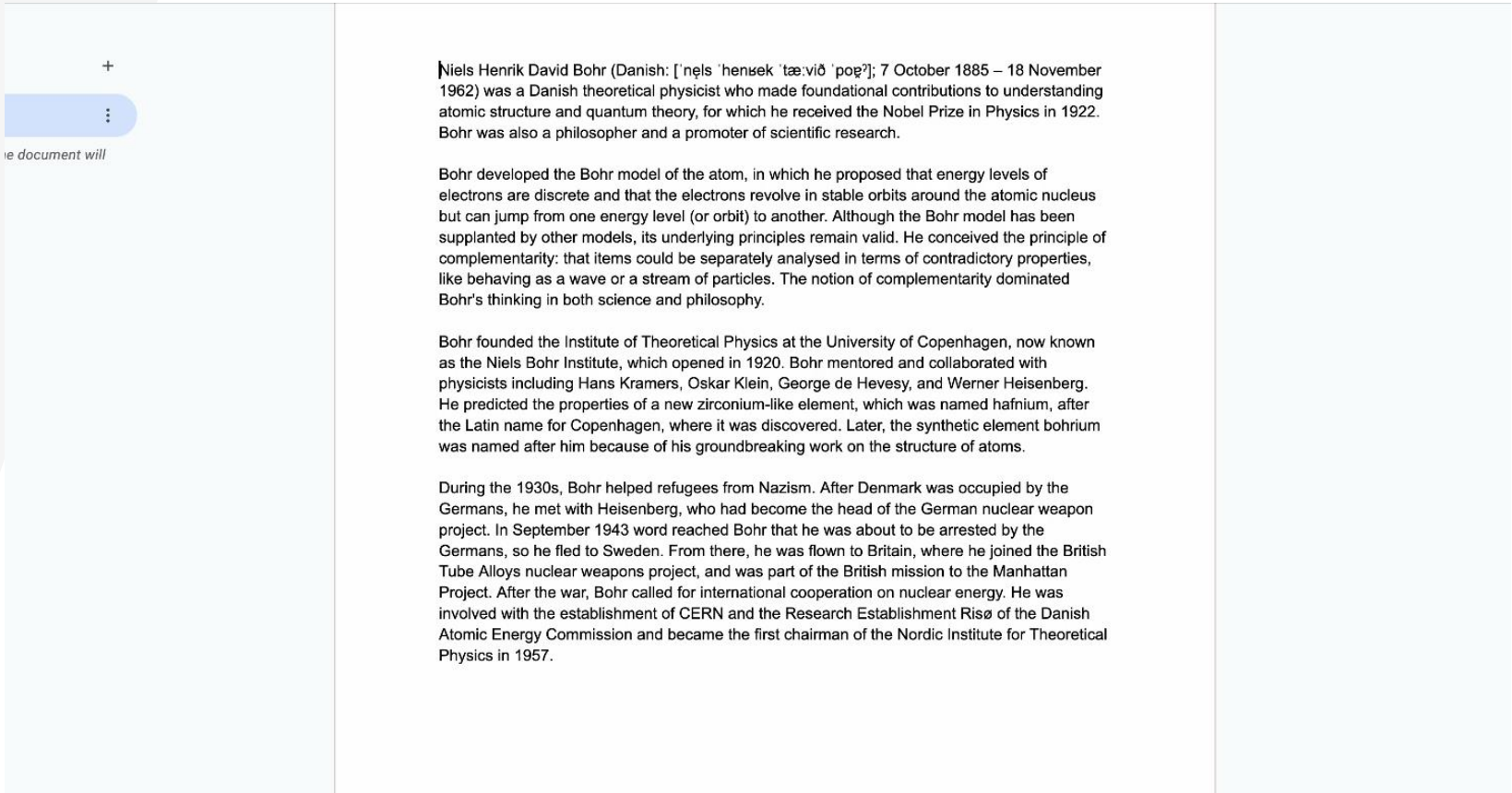
Usikker autorisation/ autentifikation eller manglende validering

- Usikker brug af JWT
- Sessionshåndtering
- Svage login-mekanismer
- Manglende validering på backend
- Manglende kontrol af adgangsrettighed
- Følger ikke ’best-practice’

Uhensigtsmæssig brug af kryptografi

- Valg af hash algoritmer
- Usikre default-værdier
- Usikker brug af algoritmer
- Usikkert design
- Følger ikke ‘best-practice’

Prompt injections og relaterede sårbarheder



Niels Henrik David Bohr (Danish: [ˈnˀels ˈhenʁek ˈtæːvið ˈpoˀɐ̯]; 7 October 1885 – 18 November 1962) was a Danish theoretical physicist who made foundational contributions to understanding atomic structure and quantum theory, for which he received the Nobel Prize in Physics in 1922. Bohr was also a philosopher and a promoter of scientific research.

Bohr developed the Bohr model of the atom, in which he proposed that energy levels of electrons are discrete and that the electrons revolve in stable orbits around the atomic nucleus but can jump from one energy level (or orbit) to another. Although the Bohr model has been supplanted by other models, its underlying principles remain valid. He conceived the principle of complementarity: that items could be separately analysed in terms of contradictory properties, like behaving as a wave or a stream of particles. The notion of complementarity dominated Bohr's thinking in both science and philosophy.

Bohr founded the Institute of Theoretical Physics at the University of Copenhagen, now known as the Niels Bohr Institute, which opened in 1920. Bohr mentored and collaborated with physicists including Hans Kramers, Oskar Klein, George de Hevesy, and Werner Heisenberg. He predicted the properties of a new zirconium-like element, which was named hafnium, after the Latin name for Copenhagen, where it was discovered. Later, the synthetic element bohrium was named after him because of his groundbreaking work on the structure of atoms.

During the 1930s, Bohr helped refugees from Nazism. After Denmark was occupied by the Germans, he met with Heisenberg, who had become the head of the German nuclear weapon project. In September 1943 word reached Bohr that he was about to be arrested by the Germans, so he fled to Sweden. From there, he was flown to Britain, where he joined the British Tube Alloys nuclear weapons project, and was part of the British mission to the Manhattan Project. After the war, Bohr called for international cooperation on nuclear energy. He was involved with the establishment of CERN and the Research Establishment Risø of the Danish Atomic Energy Commission and became the first chairman of the Nordic Institute for Theoretical Physics in 1957.

Niels Henrik David Bohr (Danish: [ˈn̥e̞ls ˈhenʁek ˈtæːvið ˈpoɐ̯ˀ]; 7 October 1885 – 18 November 1962) was a Danish theoretical physicist who made foundational contributions to understanding atomic structure and quantum theory, for which he received the Nobel Prize in Physics in 1922. Bohr was also a philosopher and a promoter of scientific research.

Bohr developed the Bohr model of the atom, in which he proposed that energy levels of electrons are discrete and that the electrons revolve in stable orbits around the atomic nucleus but can jump from one energy level (or orbit) to another. Although the Bohr model has been supplanted by other models, its underlying principles remain valid. He conceived the principle of complementarity: that items could be separately analysed in terms of contradictory properties, like behaving as a wave or a stream of particles. The notion of complementarity dominated Bohr's thinking in both science and philosophy.

Bohr founded the Institute of Theoretical Physics at the University of Copenhagen, now known as the Niels Bohr Institute, which opened in 1920. Bohr mentored and collaborated with physicists including Hans Kramers, Oskar Klein, George de Hevesy, and Werner Heisenberg. He predicted the properties of a new zirconium-like element, which was named hafnium, after the Latin name for Copenhagen, where it was discovered. Later, the synthetic element bohrium was named after him because of his groundbreaking work on the structure of atoms.

During the 1930s, Bohr helped refugees from Nazism. After Denmark was occupied by the Germans, he met with Heisenberg, who had become the head of the German nuclear weapon project. In September 1943 word reached Bohr that he was about to be arrested by the Germans, so he fled to Sweden. From there, he was flown to Britain, where he joined the British Tube Alloys nuclear weapons project, and was part of the British mission to the Manhattan Project. After the war, Bohr called for international cooperation on nuclear energy. He was involved with the establishment of CERN and the Research Establishment Risø of the Danish Atomic Energy Commission and became the first chairman of the Nordic Institute for Theoretical Physics in 1957.

Hvordan kommer i videre?

- Find ud af hvad der skal undersøges:
  - Hele organisationen, et produkt eller (dele af) en teknisk løsning?
- Overvej hvorfor du vil have en sikkerhedstest?
  - Intern læring? Ekstern kommunikation? Compliance?
- Bestem derefter metoden:
  - White-, grey- eller blackbox?
  - Baseres på en standard eller er frie tøjler?

Kontakt

Benjamin Salling Hvass
Senior Security Architect

benjamin.hvass@alexandra.dk
+45 28 95 58 02

ALEXANDRA INSTITUTTET