SKF();

TRAINING & GUIDANCE FOR DOING APPSEC RIGHT!

The Team

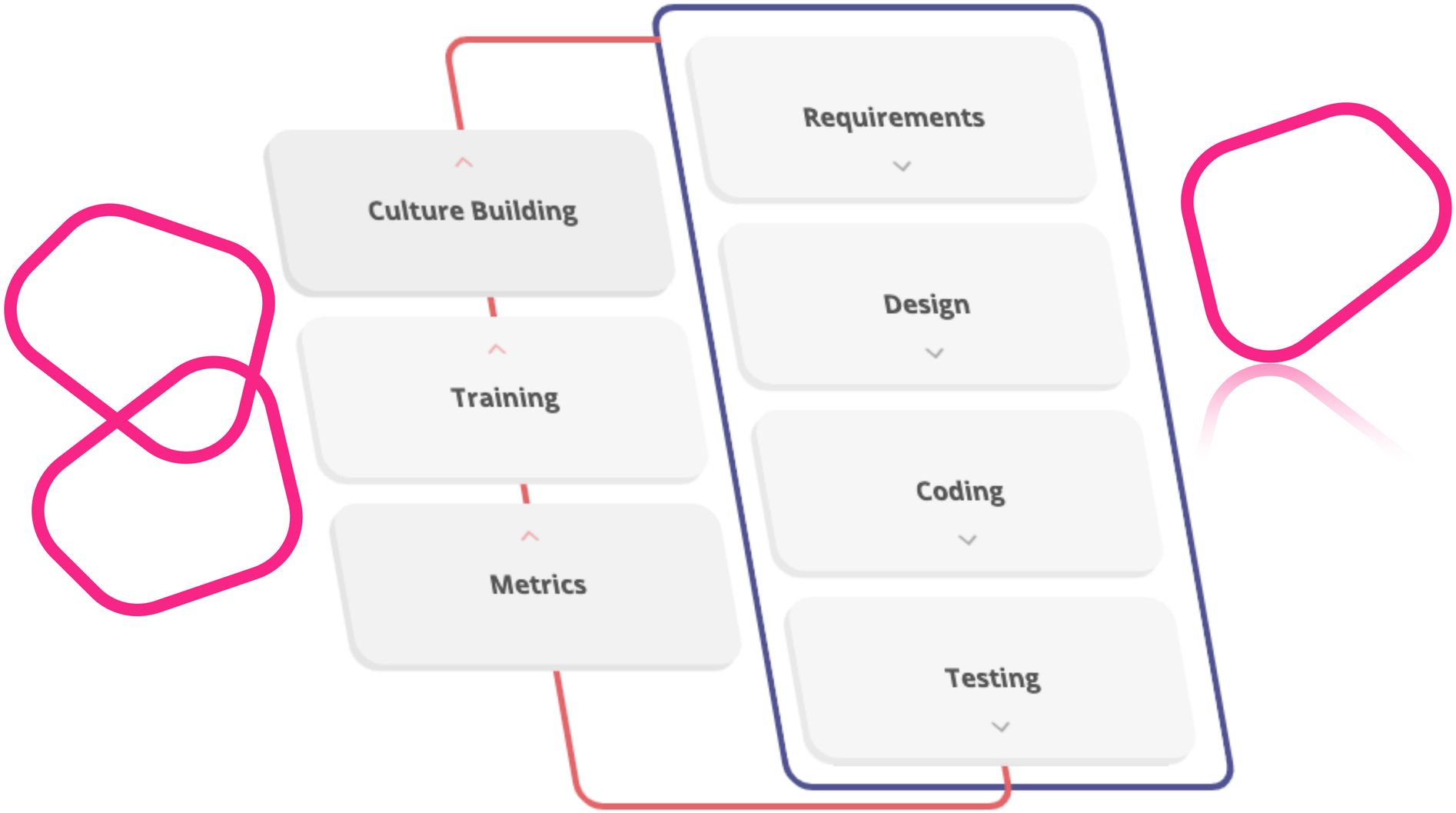
Glenn ten Cate

- Almost 20 years of experience in the IT Security field
- Author and creator of OWASP-SKF Flagship project
- Founder of DefDev, a secure coding training company
- OWASP Board of directors member
- Working at ING Belgium as Security chapter lead

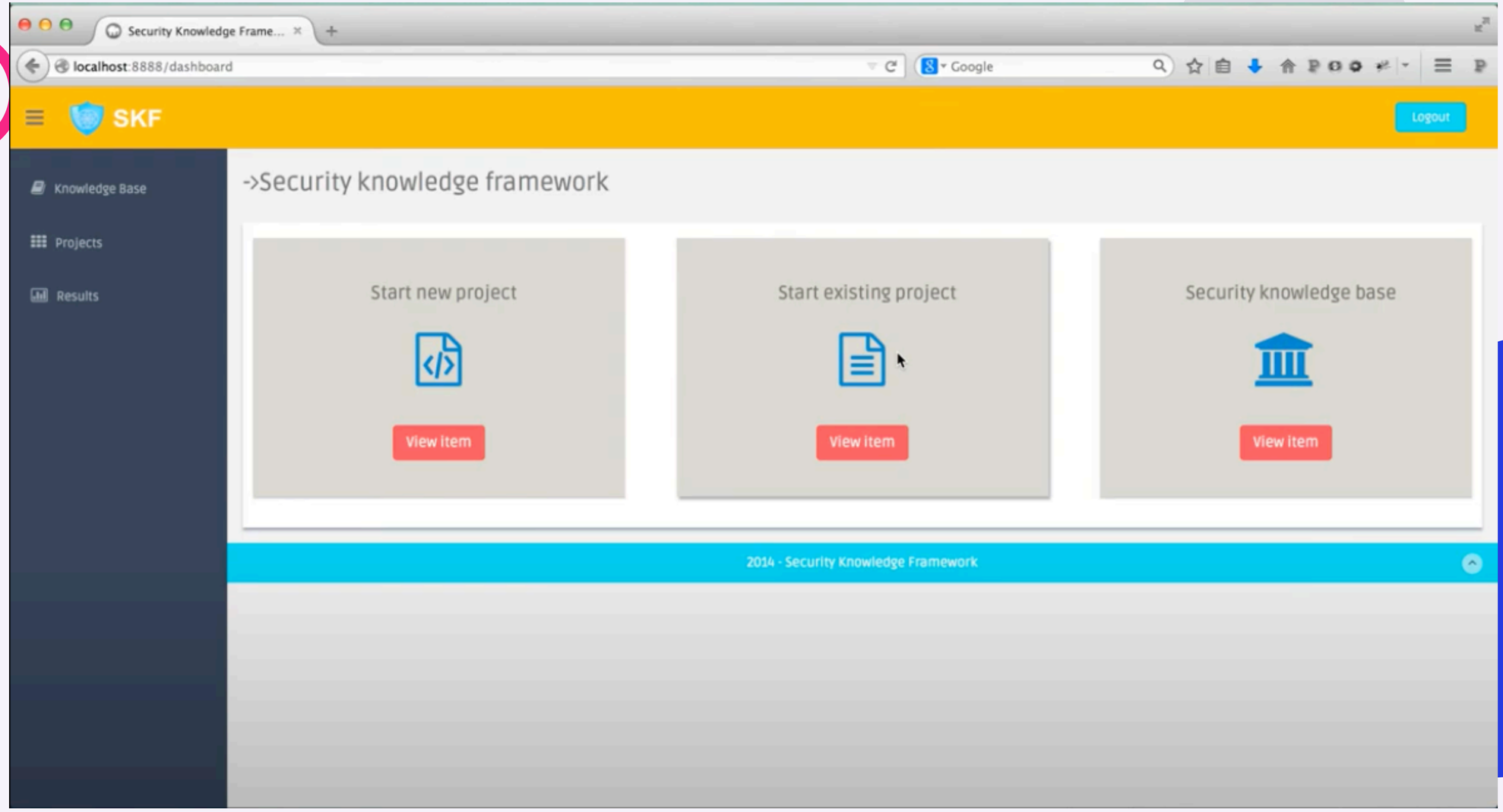
Riccardo ten Cate

- Almost 13 years of experience in the IT Security field
- Author and creator of OWASP-SKF Flagship project
- Lead trainer for secure coding trainings
- Working at Nedap as lead application security engineer

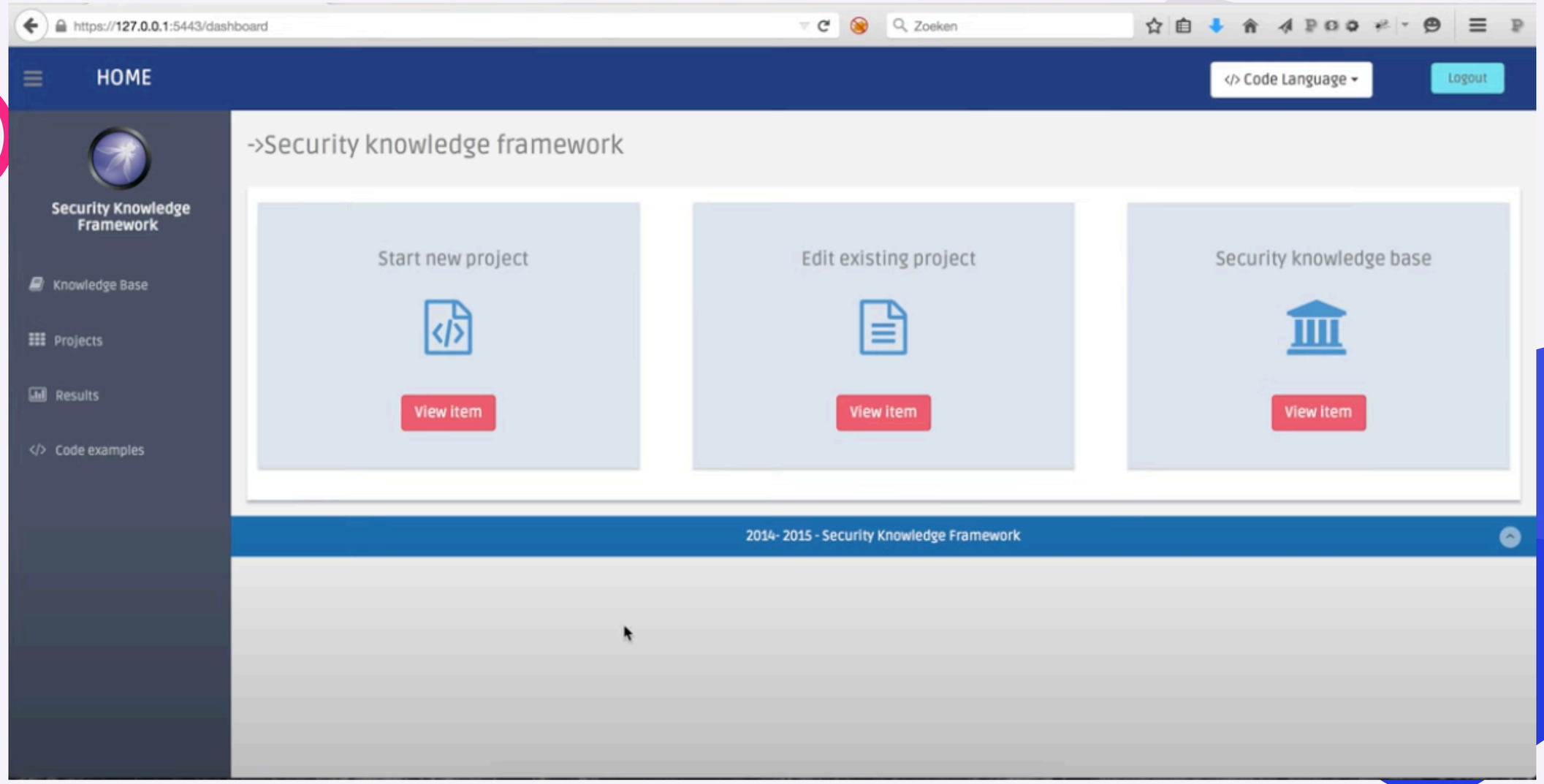
WHAT?


Requirements
Design
Coding
Testing
Culture Building
Training
Metrics

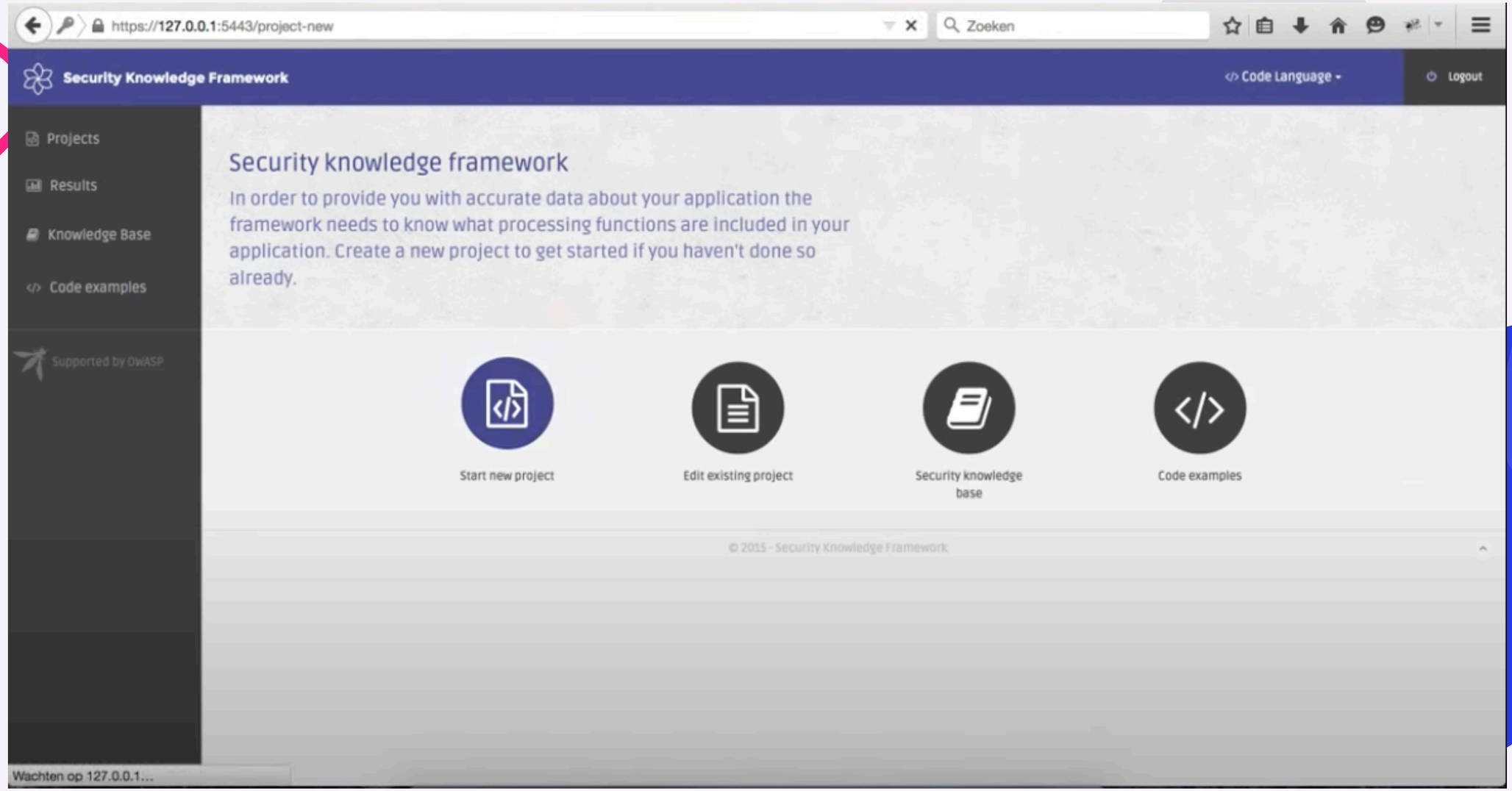
HISTORY


Security Knowledge Frame...
localhost:8888/dashboard
Google
SKF
Logout
Knowledge Base
Projects
Results
->Security knowledge framework
Start new project
View item
Start existing project
View item
Security knowledge base
View item
2014 - Security Knowledge Framework

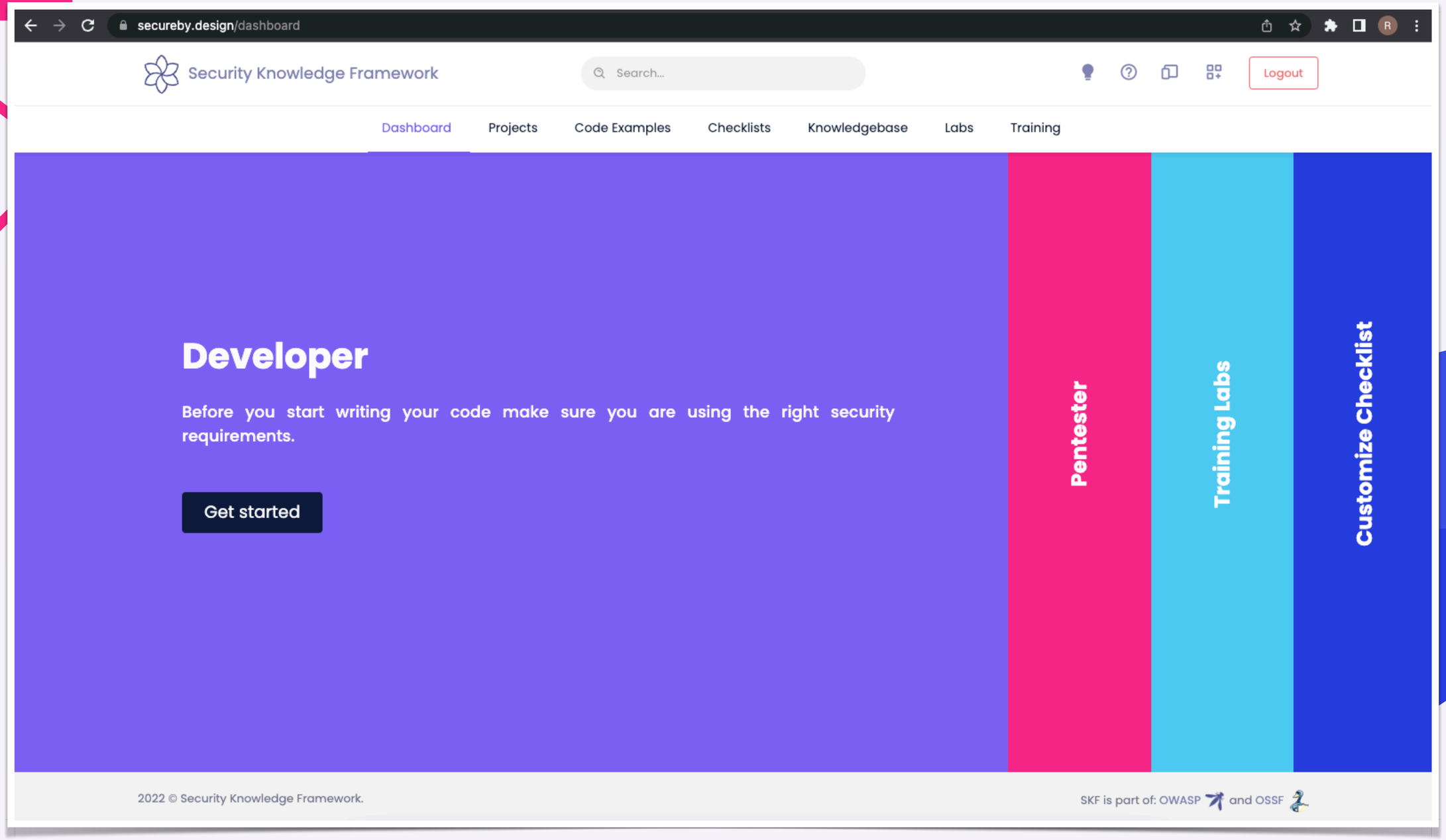
HISTORY


https://127.0.0.1:5443/dashboard
Zoeken
HOME
Code Language
Logout
Security Knowledge Framework
->Security knowledge framework
Knowledge Base
Projects
Results
Code examples
Start new project
View item
Edit existing project
View item
Security knowledge base
View item
2014- 2015 - Security Knowledge Framework

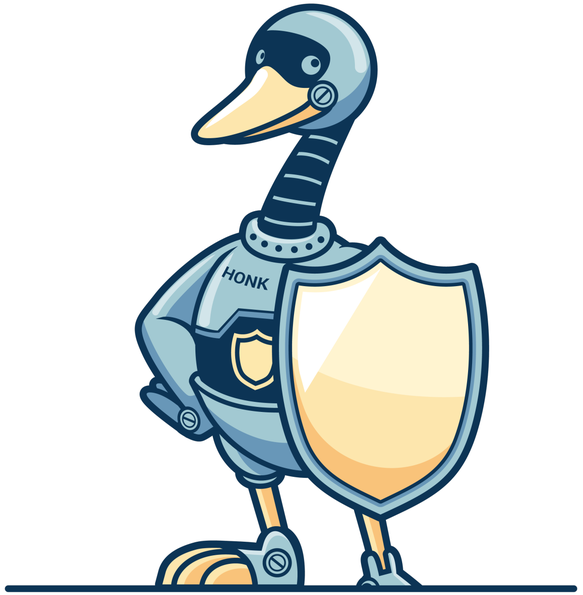
Problem #1


https://127.0.0.1:5443/project-new
Zoeken
Security Knowledge Framework
Code Language
Logout
Projects
Results
Knowledge Base
Code examples
Supported by OWASP
Security knowledge framework
In order to provide you with accurate data about your application the framework needs to know what processing functions are included in your application. Create a new project to get started if you haven't done so already.
Start new project
Edit existing project
Security knowledge base
Code examples
© 2015 - Security Knowledge Framework
Wachten op 127.0.0.1...

TODAY


secureby.design/dashboard
Security Knowledge Framework
Search...
Logout
Dashboard
Projects
Code Examples
Checklists
Knowledgebase
Labs
Training
Developer
Before you start writing your code make sure you are using the right security requirements.
Get started
Pentester
Training Labs
Customize Checklist
2022 © Security Knowledge Framework.
SKF is part of: OWASP and OSSF

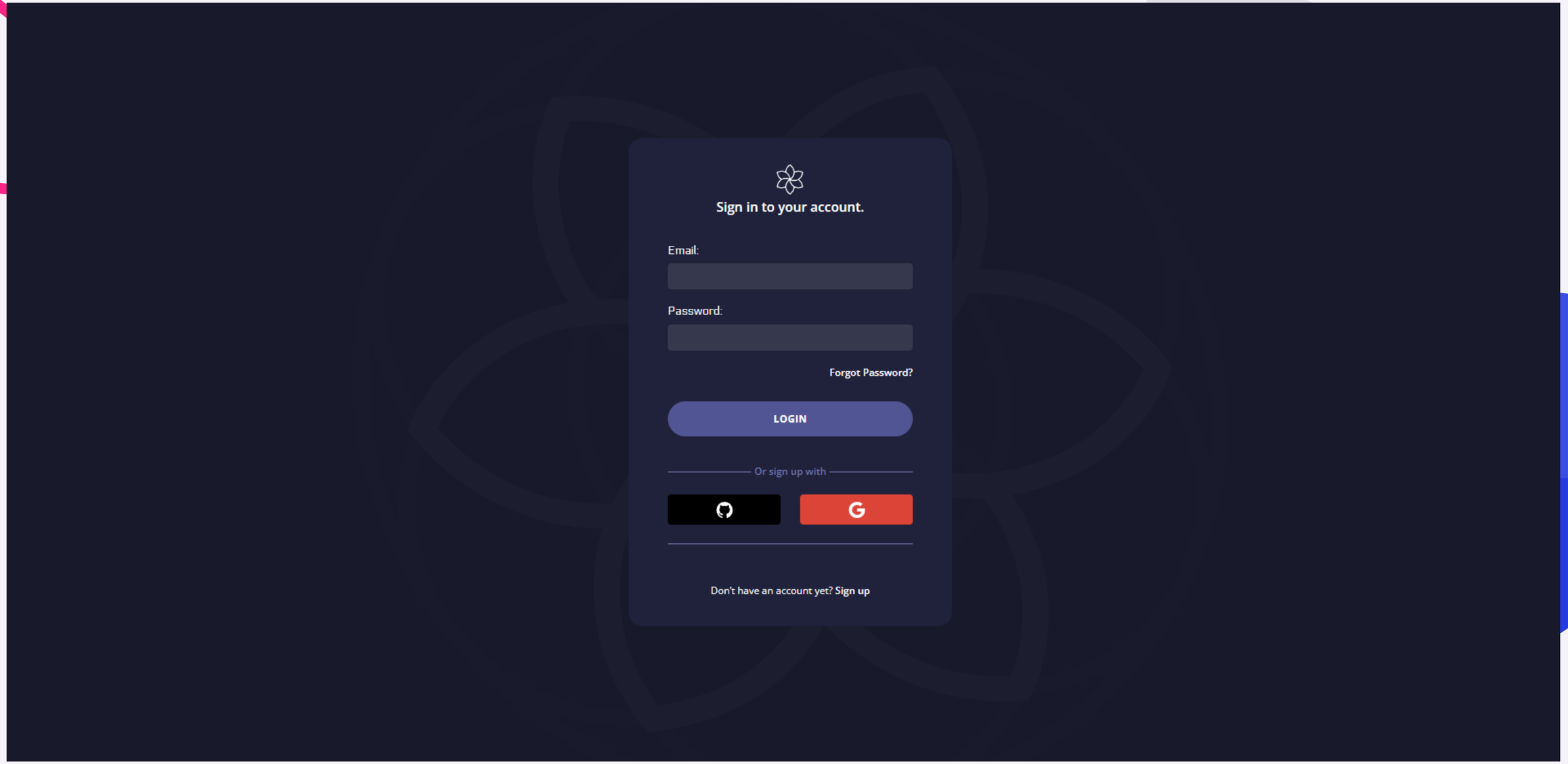
COLLAB



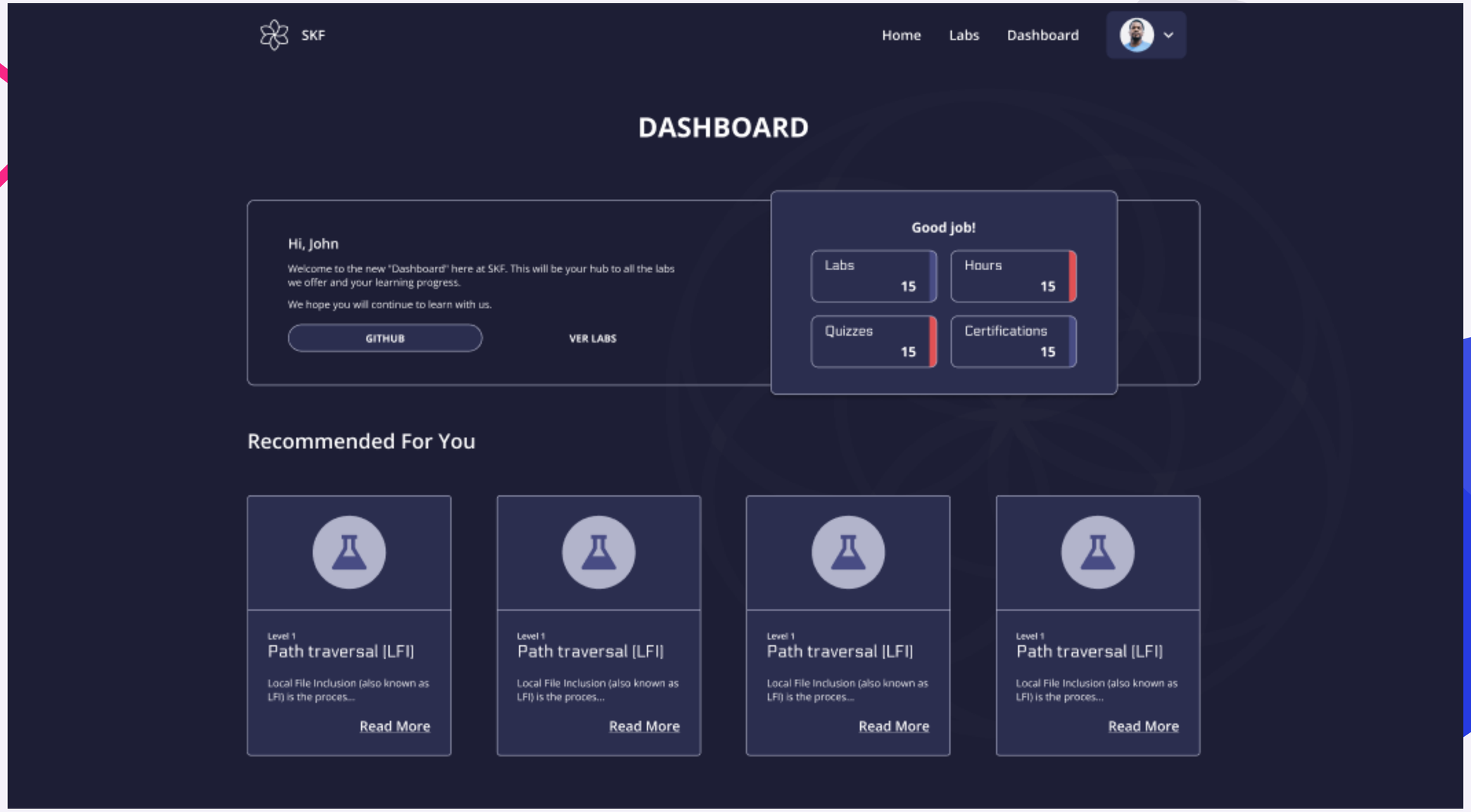
OpenSSF

OPEN SOURCE SECURITY FOUNDATION

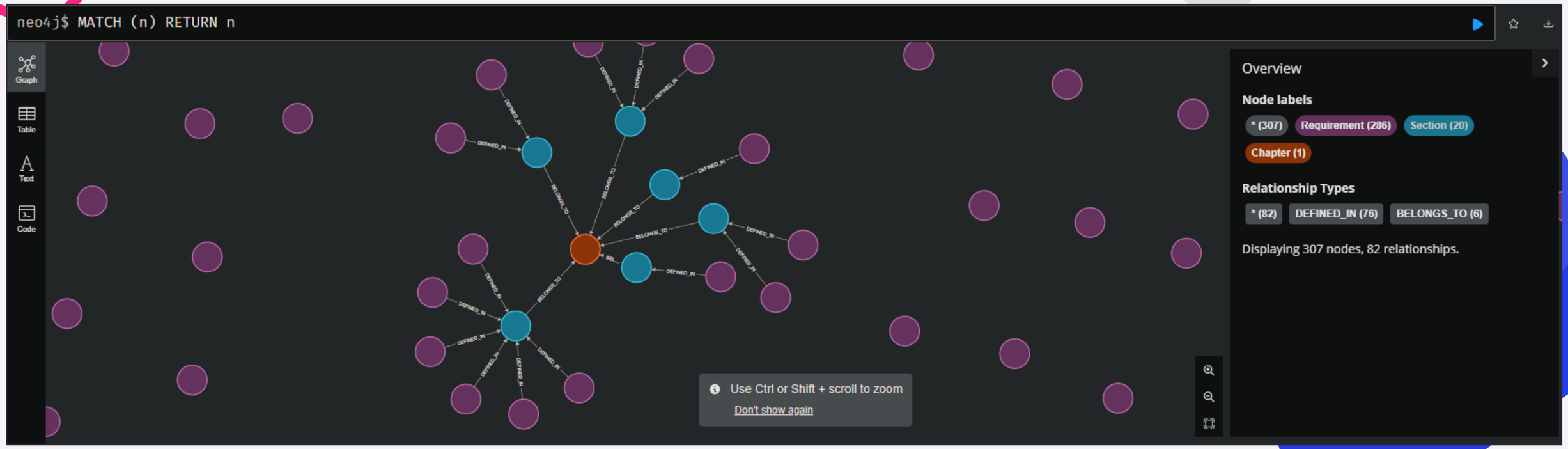
FUTURE


Sign in to your account.
Email:
Password:
Forgot Password?
LOGIN
Or sign up with
Don't have an account yet? Sign up

FUTURE

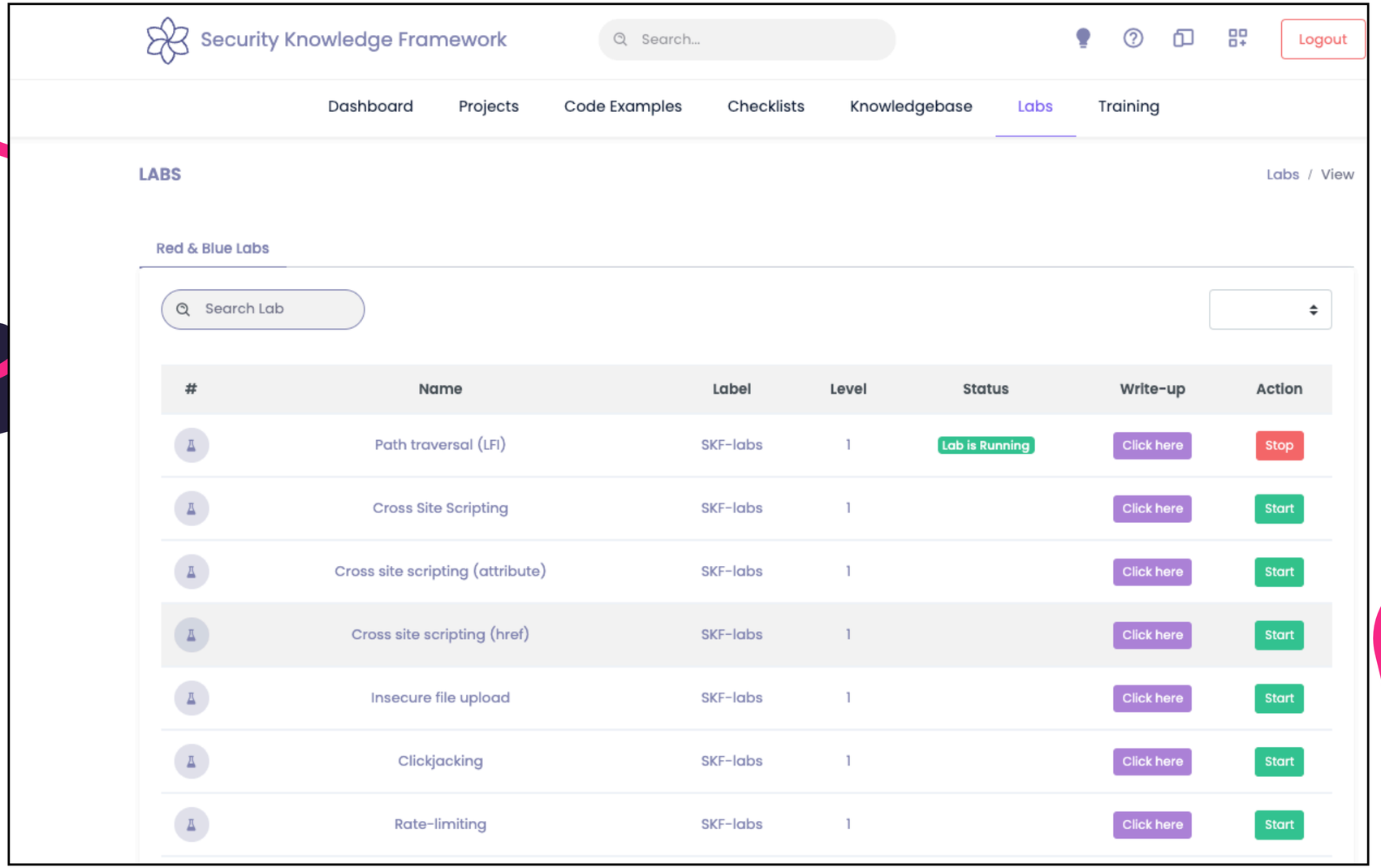

SKF
Home
Labs
Dashboard
DASHBOARD
Hi, John
Welcome to the new "Dashboard" here at SKF. This will be your hub to all the labs we offer and your learning progress.
We hope you will continue to learn with us.
GITHUB
VER LABS
Good job!
Labs
15
Hours
15
Quizzes
15
Certifications
15
Recommended For You
Level 1
Path traversal [LFI]
Local File Inclusion (also known as LFI) is the proces...
Read More
Level 1
Path traversal [LFI]
Local File Inclusion (also known as LFI) is the proces...
Read More
Level 1
Path traversal [LFI]
Local File Inclusion (also known as LFI) is the proces...
Read More
Level 1
Path traversal [LFI]
Local File Inclusion (also known as LFI) is the proces...
Read More

FUTURE

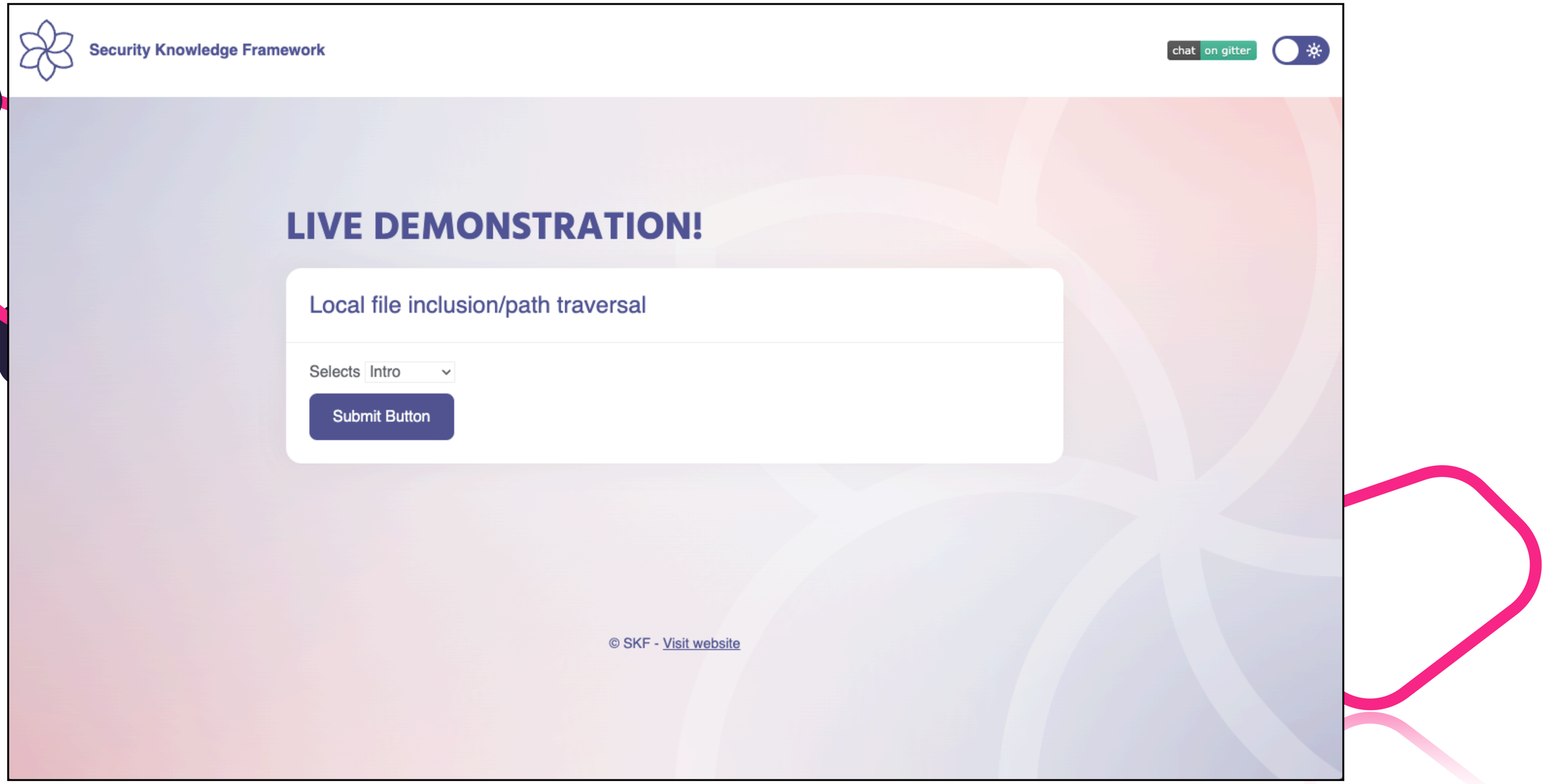

neo4j$ MATCH (n) RETURN n
Graph
Table
Text
Code
Overview
Node labels
* (307)
Requirement (286)
Section (20)
Chapter (1)
Relationship Types
* (82)
DEFINED_IN (76)
BELONGS_TO (6)
Displaying 307 nodes, 82 relationships.
Use Ctrl or Shift + scroll to zoom
Don't show again

Exploitation

EXPLOITATION



EXPLOITATION



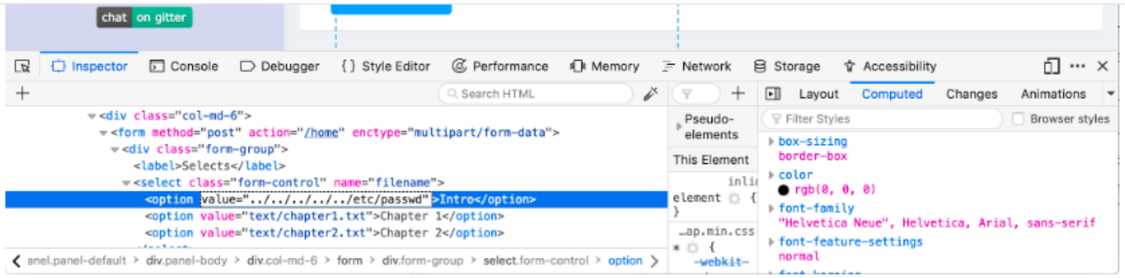
EXPLOITATION

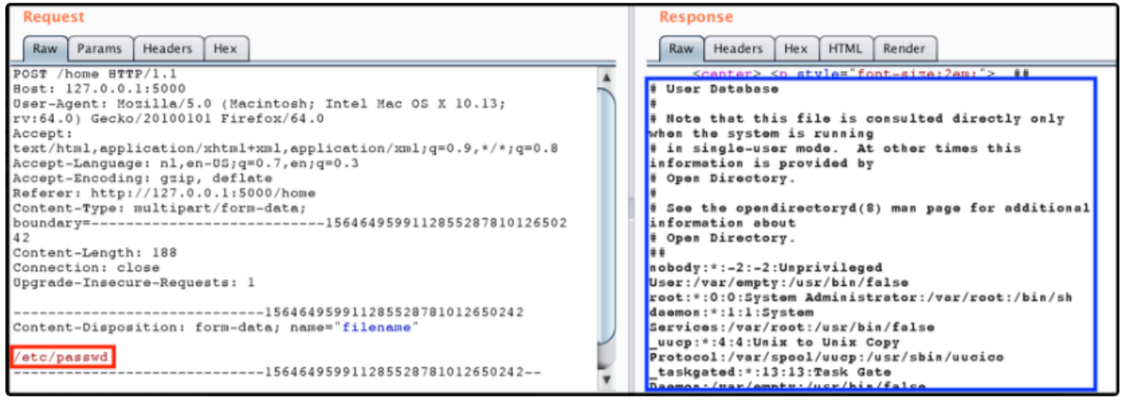
SKF write-ups

Search... ⌘K

- Introduction
- Cross Site Scripting (XSS)
- Cross Site Scripting - Attribute (XSS-Attribute)
- Cross Site Scripting - href (XSS-href)
- Cross Site Scripting - DOM (XSS-DOM)
- Cross Site Scripting - DOM-2 (XSS-DOM-2)
- CSRF
- CSRF - Samesite
- CSRF - Weak
- XML External Entity (XXE)
- File upload
- Clickjacking
- Ratelimiting (Brute-force login)
- HttpOnly Session Hijacking XSS
- Host Header Injection

Powered By GitBook





Success! As we observed, we can access the /etc/passwd file through LFI.

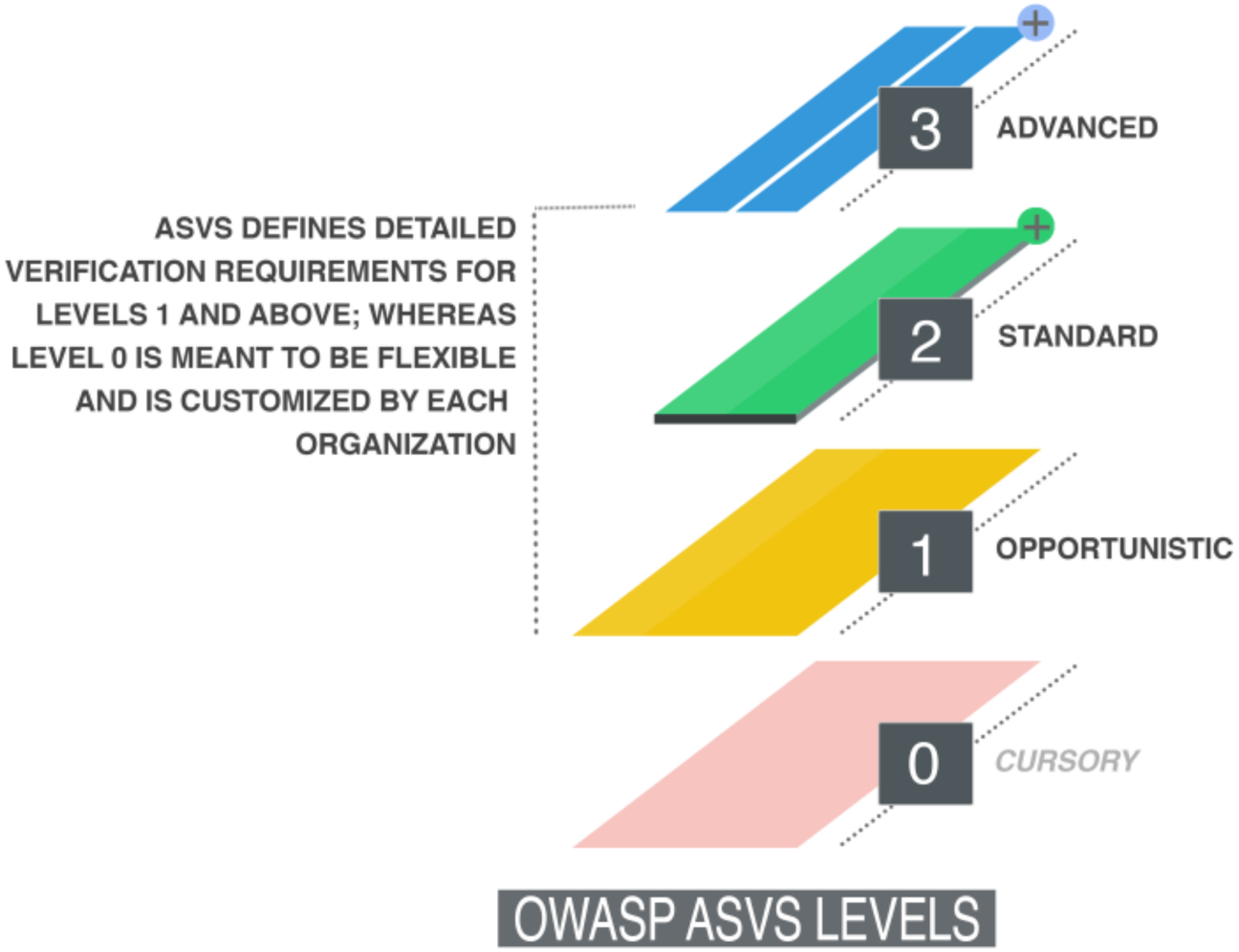
Additional sources

https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion

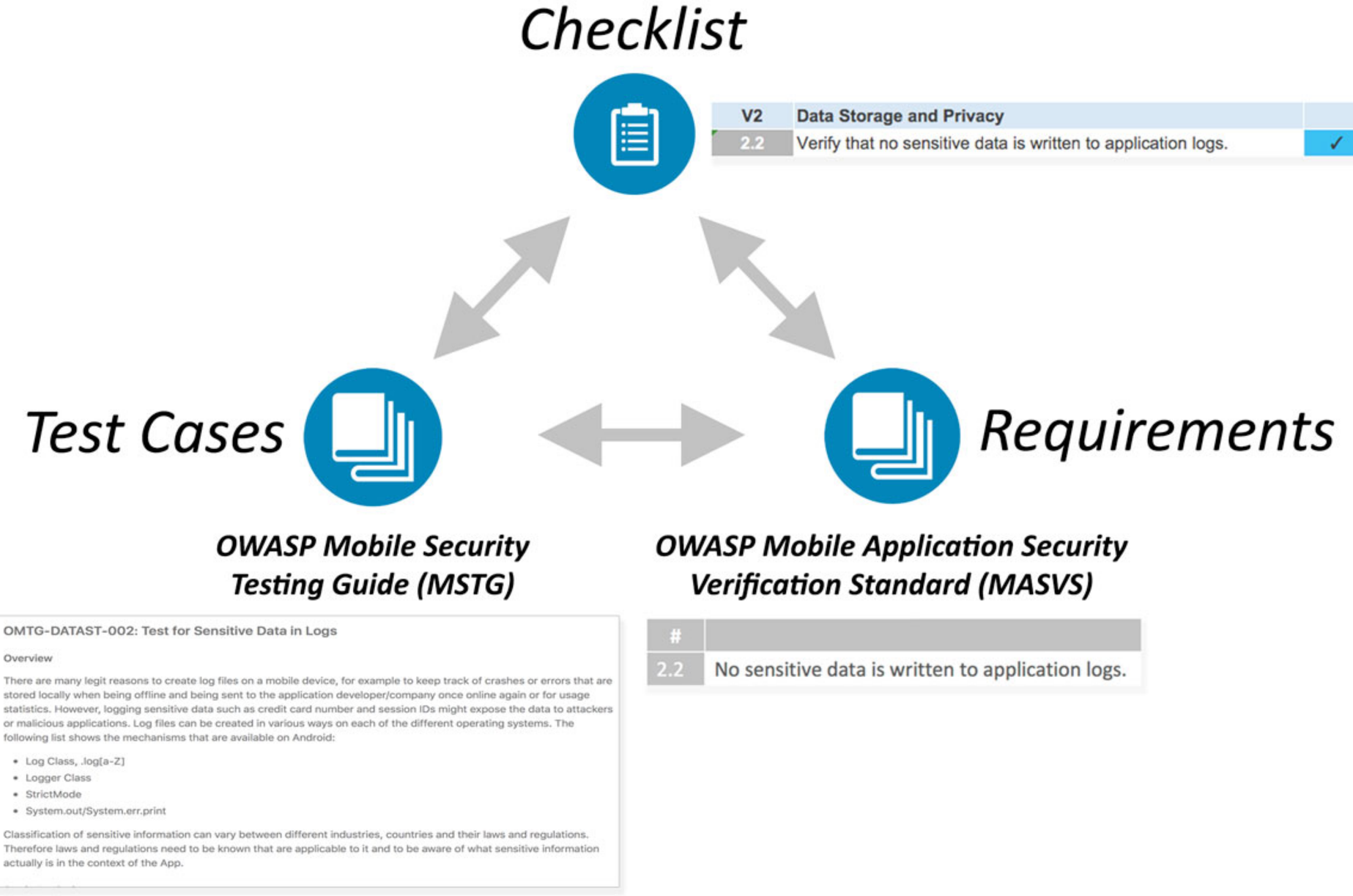
Mitigation

SKF && ASVS

complementary

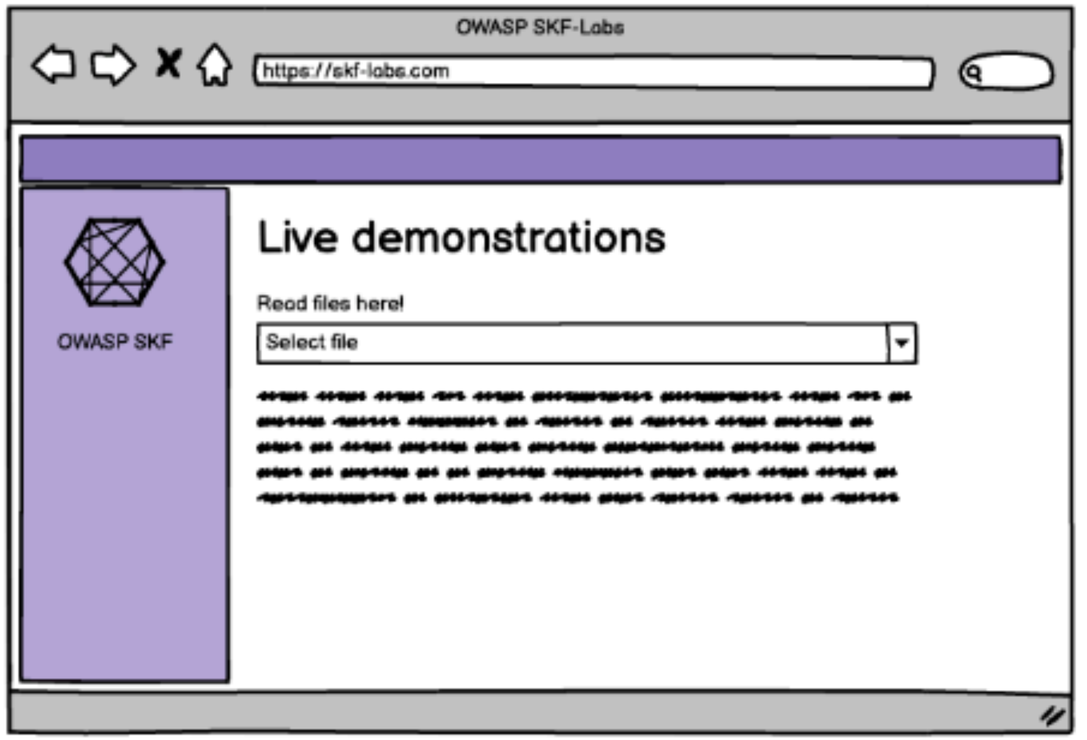


complementary



Story time!

User story - Read files example

Description	**As a** visitor **I want to** be able to browse through text files on the server **so that** I can read the content and extend my knowledge
Benefits	There are a lot of text files uploaded to the application with interesting information. We want users to be able to read all the files and benefit from the knowledge.
Acceptance criteria	a) Given that i select a document i want to read b) When i select a title from a dropdown list c) The current page displays the information
Wireframe	

SKF

PROJECTS

go back

1 CHECKLIST — 2 MATURITY LEVEL — 3 CATEGORY — 4 QUESTIONNAIRE — 5 SETUP — 6 FINISH

Platforms

Select checklist type

--Select--

Security Category selection

- The security category selection gives you a different set of checklists that are correlated to different levels.
- By default SKF comes with the OWASP-ASVS for the web/api security controls and OWASP-MASVS for mobile security controls.
- Also you can modify the controls of the existing checklists in SKF or create your own new security checklist from scratch.

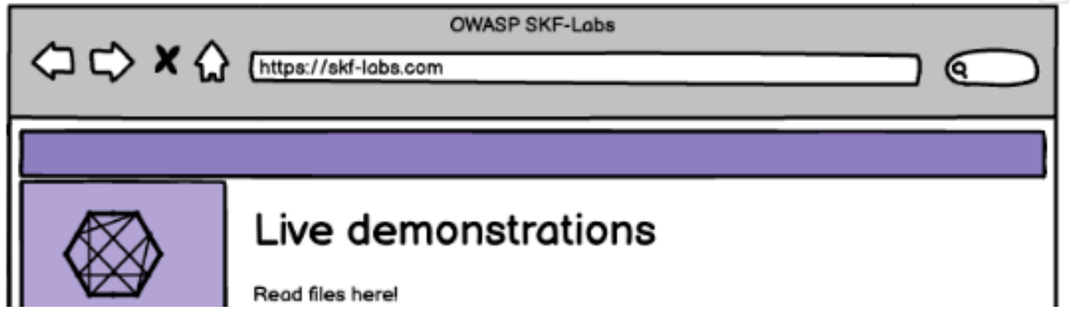
Next

User story - Read files example

Description	**As a** visitor **I want to** be able to browse through text files on the server **so that** I can read the content and extend my knowledge
Benefits	There are a lot of text files uploaded to the application with interesting information. We want users to be able to read all the files and benefit from the knowledge.
Acceptance criteria	a) Given that i select a document i want to read b) When i select a title from a dropdown list c) The current page displays the information
Security controls	

Item	Control
5.1.3	Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (whitelisting)
5.1.4	Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).
5.3.9	Verify that the application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.
7.4.1	Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate.

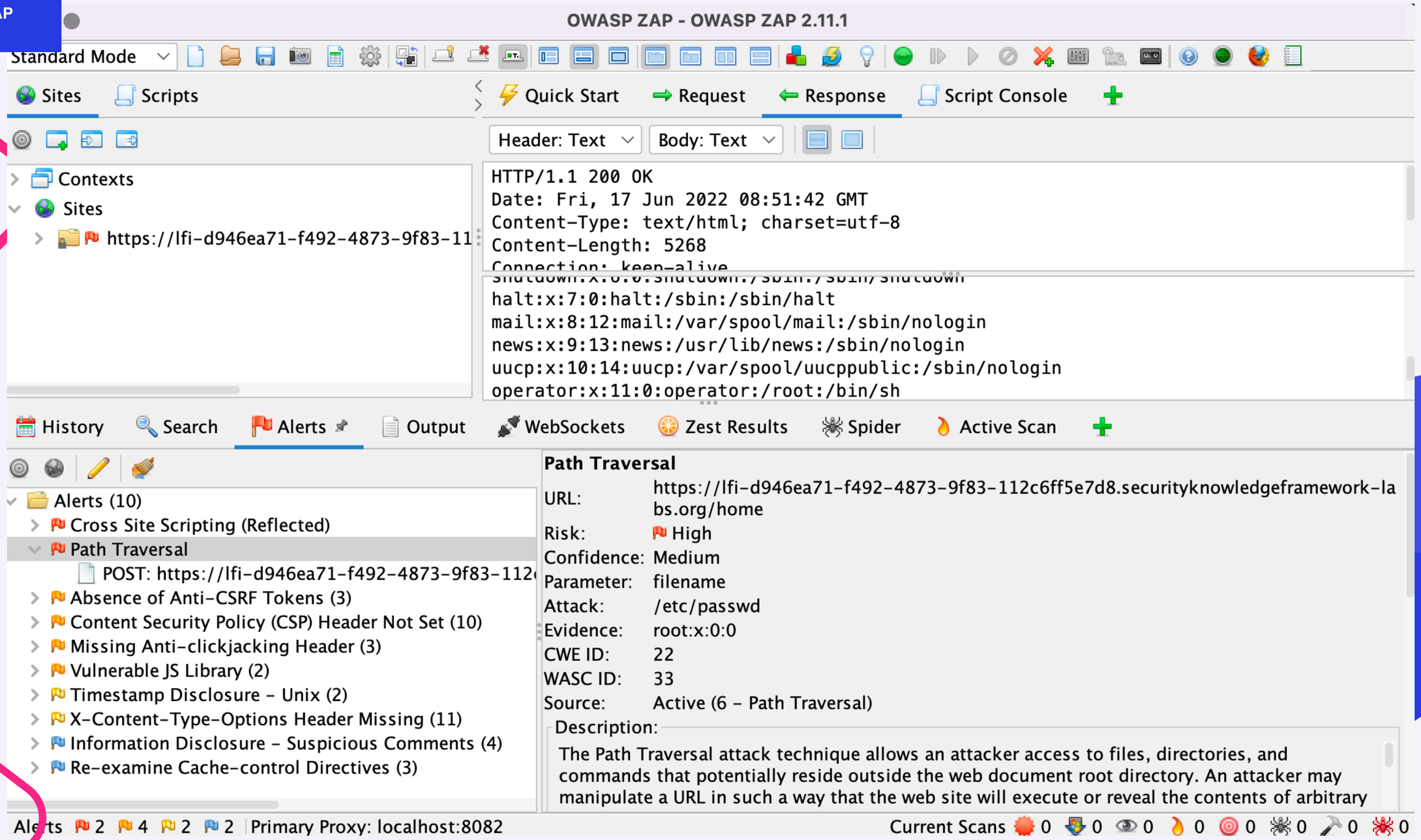
Wireframe



Automation

ZAP

ZAP


OWASP ZAP - OWASP ZAP 2.11.1
Standard Mode
Sites
Scripts
Quick Start
Request
Response
Script Console
Header: Text
Body: Text
Contexts
Sites
https://lfi-d946ea71-f492-4873-9f83-11
HTTP/1.1 200 OK
Date: Fri, 17 Jun 2022 08:51:42 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 5268
Connection: keep-alive
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh
History
Search
Alerts
Output
WebSockets
Zest Results
Spider
Active Scan
Alerts (10)
Cross Site Scripting (Reflected)
Path Traversal
POST: https://lfi-d946ea71-f492-4873-9f83-112
Absence of Anti-CSRF Tokens (3)
Content Security Policy (CSP) Header Not Set (10)
Missing Anti-clickjacking Header (3)
Vulnerable JS Library (2)
Timestamp Disclosure - Unix (2)
X-Content-Type-Options Header Missing (11)
Information Disclosure - Suspicious Comments (4)
Re-examine Cache-control Directives (3)
Path Traversal
URL: https://lfi-d946ea71-f492-4873-9f83-112c6ff5e7d8.securityknowledgeframework-labs.org/home
Risk: High
Confidence: Medium
Parameter: filename
Attack: /etc/passwd
Evidence: root:x:0:0
CWE ID: 22
WASC ID: 33
Source: Active (6 - Path Traversal)
Description:
The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary
Alerts 2 4 2 2 Primary Proxy: localhost:8082
Current Scans 0 0 0 0 0 0 0 0

SKF

Zest

Zest is an experimental specialized scripting language (also known as a domain-specific language) originally developed by the Mozilla security team and is intended to be used in web oriented security tools.

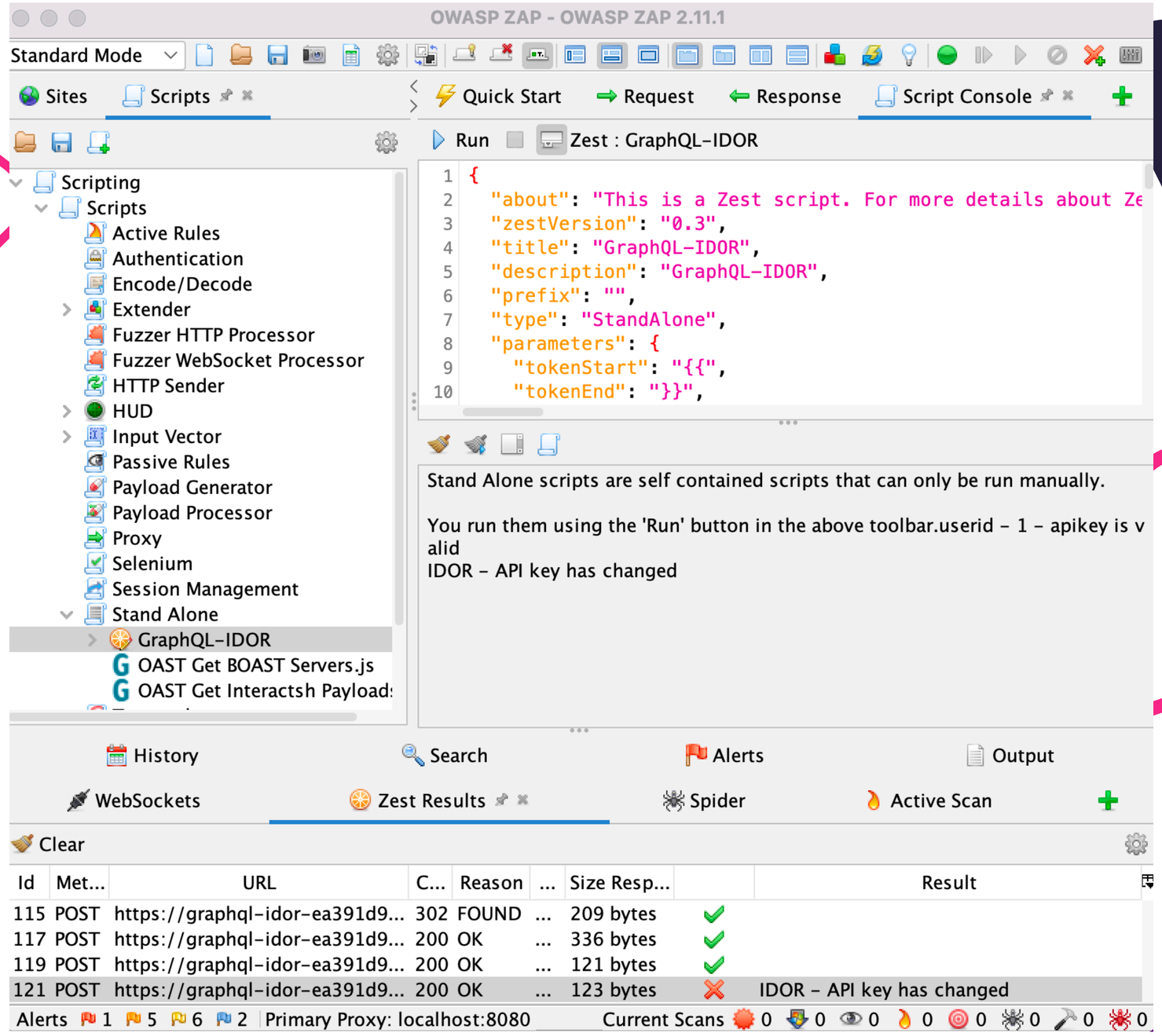
It is included by default with ZAP.

Creating Zest scripts

There are a variety of ways to create Zest scripts:

Record a new Zest script Button

SKF


OWASP ZAP - OWASP ZAP 2.11.1
Standard Mode
Sites
Scripts
Quick Start
Request
Response
Script Console
Run
Zest : GraphQL-IDOR
Scripting
Scripts
Active Rules
Authentication
Encode/Decode
Extender
Fuzzer HTTP Processor
Fuzzer WebSocket Processor
HTTP Sender
HUD
Input Vector
Passive Rules
Payload Generator
Payload Processor
Proxy
Selenium
Session Management
Stand Alone
GraphQL-IDOR
OAST Get BOAST Servers.js
OAST Get Interactsh Payload
{
"about": "This is a Zest script. For more details about Ze
"zestVersion": "0.3",
"title": "GraphQL-IDOR",
"description": "GraphQL-IDOR",
"prefix": "",
"type": "StandAlone",
"parameters": {
"tokenStart": "{{",
"tokenEnd": "}}",
Stand Alone scripts are self contained scripts that can only be run manually.
You run them using the 'Run' button in the above toolbar.userid - 1 - apikey is valid
IDOR - API key has changed
History
Search
Alerts
Output
WebSockets
Zest Results
Spider
Active Scan
Clear
Id Met... URL C... Reason ... Size Resp... Result
115 POST https://graphql-idor-ea391d9... 302 FOUND ... 209 bytes
117 POST https://graphql-idor-ea391d9... 200 OK ... 336 bytes
119 POST https://graphql-idor-ea391d9... 200 OK ... 121 bytes
121 POST https://graphql-idor-ea391d9... 200 OK ... 123 bytes IDOR - API key has changed
Alerts 1 5 6 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

```
# OWASP ZAP automation configuration file, for more details see https://www.zaproxy.org/docs/automate/automation-framework/
:                                  # The environment, mandatory
ontexts :                          # List of 1 or more contexts, mandatory
- name: skf-labs                   # Name to be used to refer to this context in other jobs, mandatory
  urls: ["http://192.168.1.16:4444"]
  includePaths:                    # An optional list of regexes to include
  excludePaths:                    # An optional list of regexes to exclude
jobs:
- type: script
  parameters:
    action: add
    type: standalone
    engine: Mozilla Zest
    name: Session-hijacking-xss
    file: /Users/riccardotencate/zap-tests/zest/Session-hijacking-xss.zst
- type: script
  parameters:
    action: run
    type: standalone
    engine: Mozilla Zest
    name: Session-hijacking-xss
    file: /Users/riccardotencate/zap-tests/zest/Session-hijacking-xss.zst
- type: activeScan                  # The active scanner - this actively attacks the target so should only be used with permission
==
snip, some active scan setup config
==
    rules:                          # A list of one or more active scan rules and associated settings which override the defaults
    - id:                          40012
      name:                        # String: The name of the rule for documentation purposes - this is not required or actually used
      strength: Low
      threshold:
- type: passiveScan-config          # Passive scan configuration
  parameters:
    maxAlertsPerRule: 10           # Int: Maximum number of alerts to raise per rule
    scanOnlyInScope: true          # Bool: Only scan URLs in scope (recommended)
    maxBodySizeInBytesToScan:      # Int: Maximum body size to scan, default: 0 - will scan all messages
    enableTags: false              # Bool: Enable passive scan tags, default: false - enabling them can impact performance
```

AF

```
./zap.sh -cmd -addonupdate
./zap.sh -cmd -autorun zap.yaml <any other ZAP options>
```

If you are using the framework in the ZAP stable docker image then the recommended approach is to run ZAP in this way:

```
docker run -v $(pwd):/zap/wrk/:rw -t owasp/zap2docker-stable bash -c "zap.sh -cmd -addonupdate; zap.sh -cmd -autorun /zap/wrk/zap.yaml"
```

SEMGREP

Semgrep

Get Started

6.7k v0.98.0 (2 days ago)

Static analysis at ludicrous speed

Find bugs and enforce code standards

Open source, works on 20+ languages

Not proprietary and not only for legacy languages

Scan with 1,500+ community rules

Not vendor controlled

Write rules that look like your code

No painful and complex DSL

Quickly get results in the terminal, editor, or CI/CD

RULE

Open in Playground

```yaml
rules:
  - id: python-no-prints-in-prod
    pattern: old_print($X)
    message: Use logging.debug() instead of old_print()
    severity: INFO
    fix: logging.debug($X)
    languages:
      - python
```

TEST CODE

Python

```python
import old_print as oldp

def hello_world():
    skynet.init()
    # TODO Change this to logging framework before prod
    oldp(
        '--> debug, skynet init vector is {skynet.iv}'
    )
    # oldp('don't detect this, it\'s commented')
```

Run

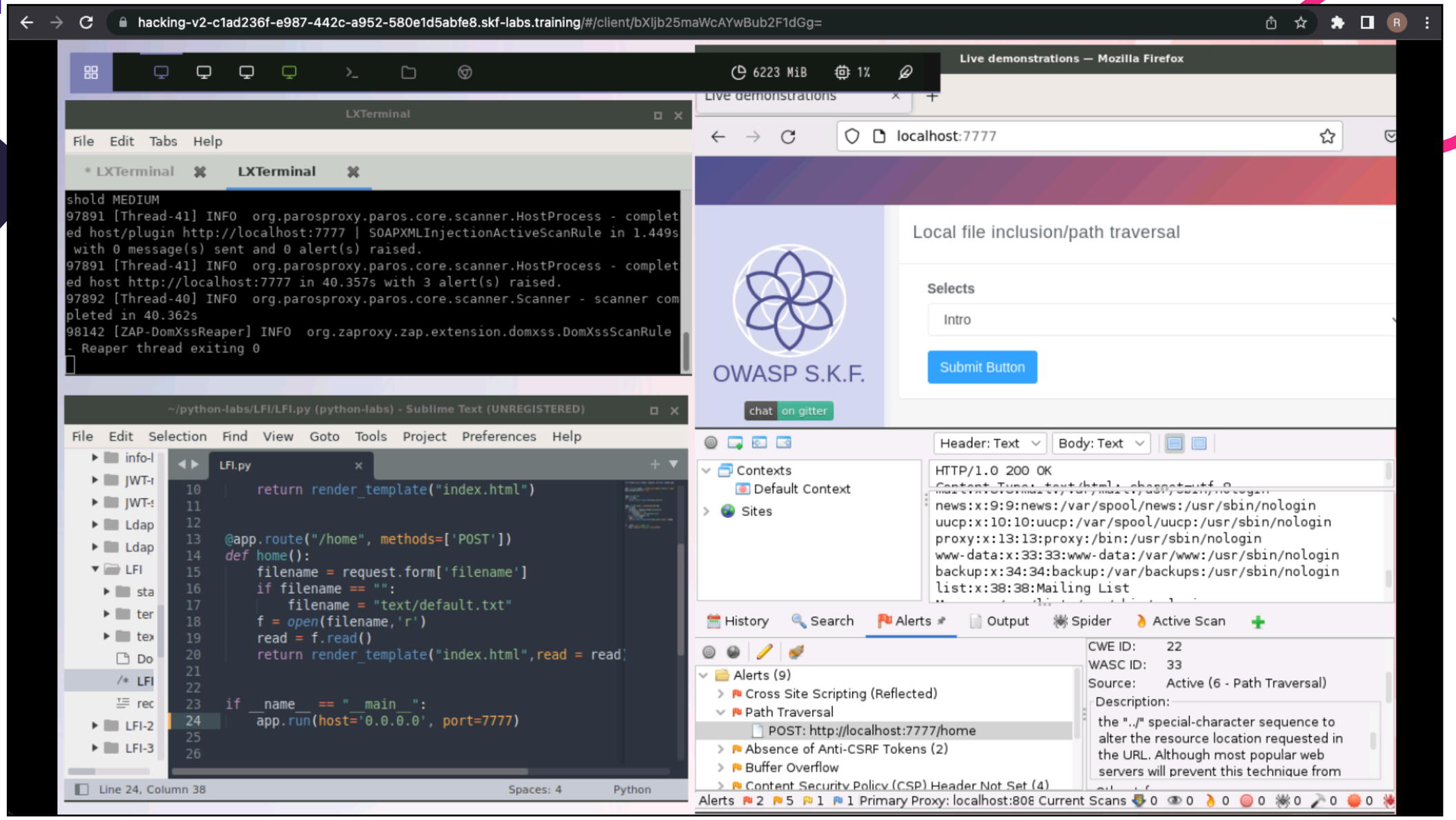
https://semgrep.dev/

SEMGREP

```
riccardo.tencate@nvc3406 LFI % docker run -v $(pwd):/src returntocorp/semgrep semgrep --config p/python
METRICS: Using configs from the Registry (like --config=p/ci) reports pseudonymous rule metrics to semgrep.dev.
To disable Registry rule metrics, use "--metrics=off".
Using configs only from local files (like --config=xyz.yml) does not enable metrics.

More information: https://semgrep.dev/docs/metrics

Fetching rules from https://semgrep.dev/registry.
Scanning 1 file with 34 python rules.

Findings:

  LFI.py
     python.flask.security.injection.path-traversal-open.path-traversal-open
        Found request data in a call to 'open'. Ensure the request data is validated or sanitized,
        otherwise it could result in path traversal attacks.
        Details: https://sg.run/PJRW

         18┆ f = open(filename,'r')

Some files were skipped or only partially analyzed.
  Scan was limited to files tracked by git.

Ran 34 rules on 1 file: 1 finding.

A new version of Semgrep is available. See https://semgrep.dev/docs/upgrading
riccardo.tencate@nvc3406 LFI %
```

https://semgrep.dev/

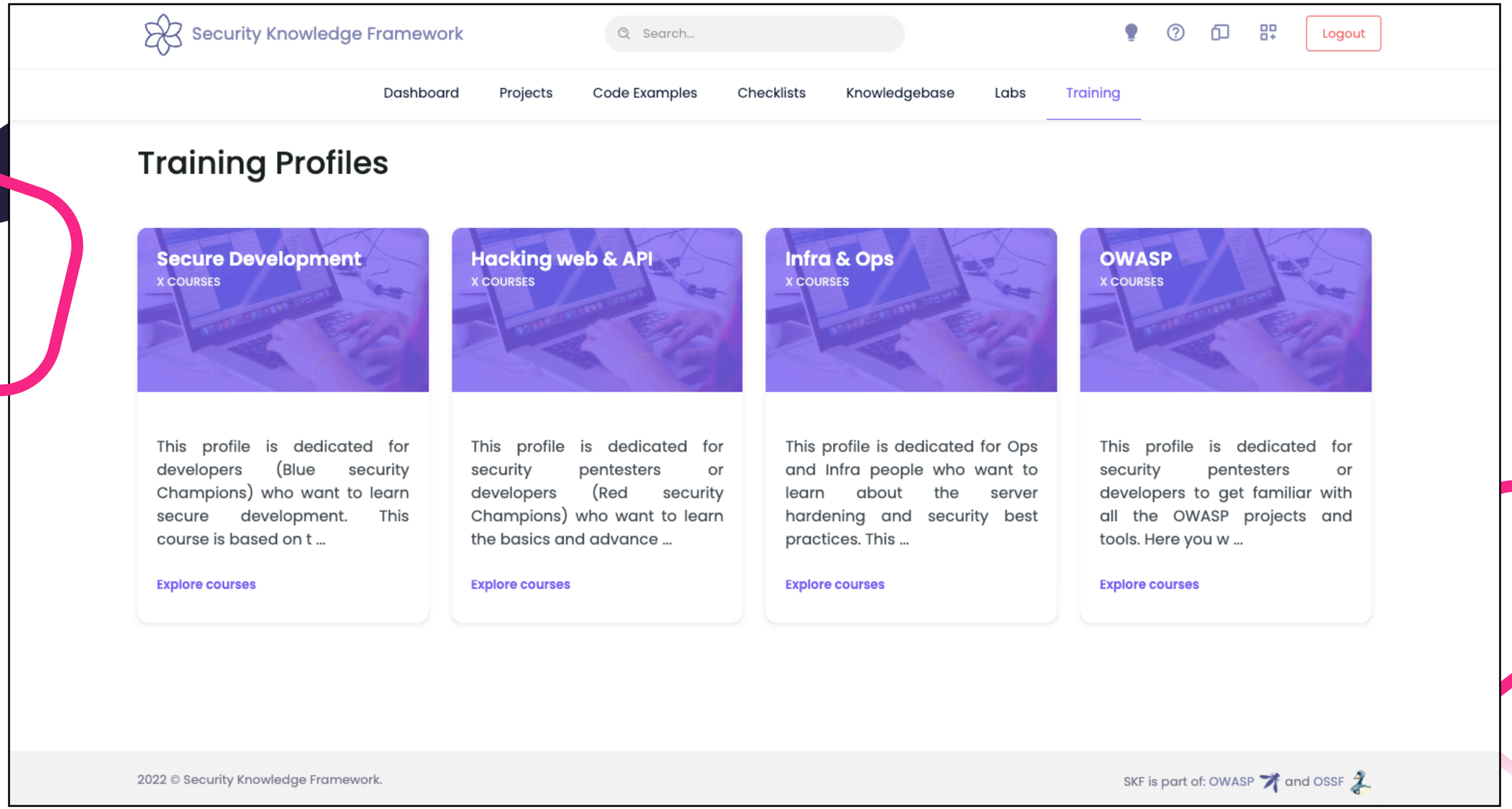
SEMGREP



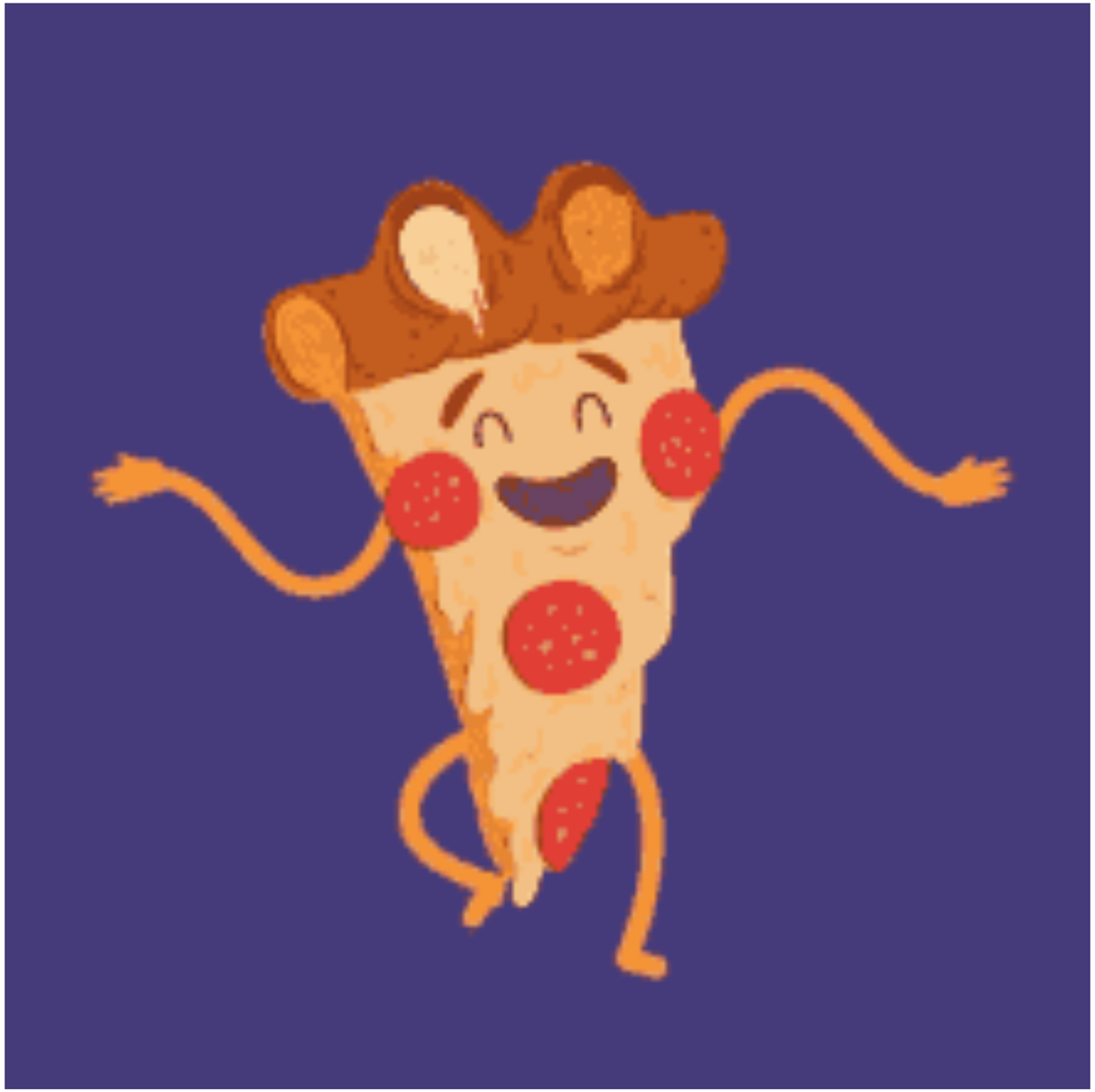
https://semgrep.dev/

Training

EXPLOITATION



DEMO



Links

- https://github.com/blabla1337/skf-flask
- https://github.com/blabla1337/skf-labs
- https://github.com/blabla1337/skf-labs-zap
- https://secureby.design/
- https://securityknowledgeframework.org/
- https://owasp.org/www-project-security-knowledge-framework/
- https://github.com/ossf/wg-best-practices-os-developers

Closing_