

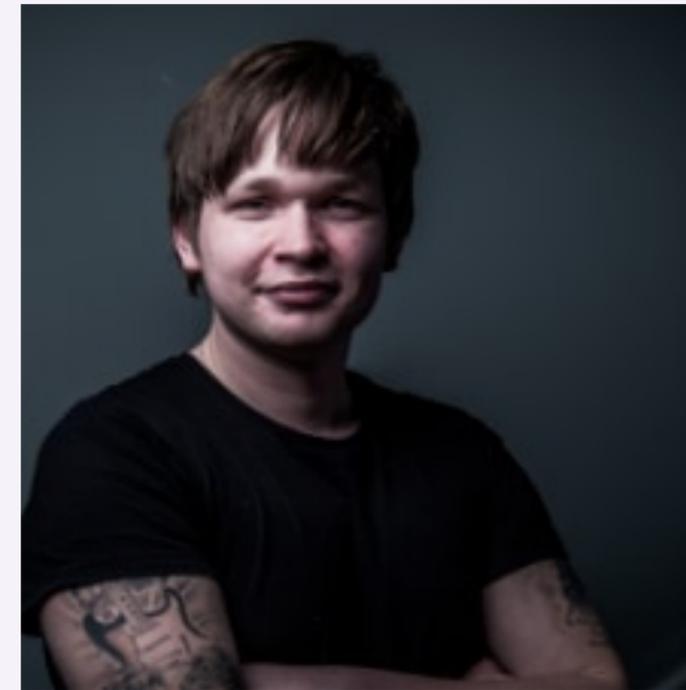
SKF());

TRAINING & GUIDANCE FOR DOING APPSEC RIGHT!



Glenn ten Cate

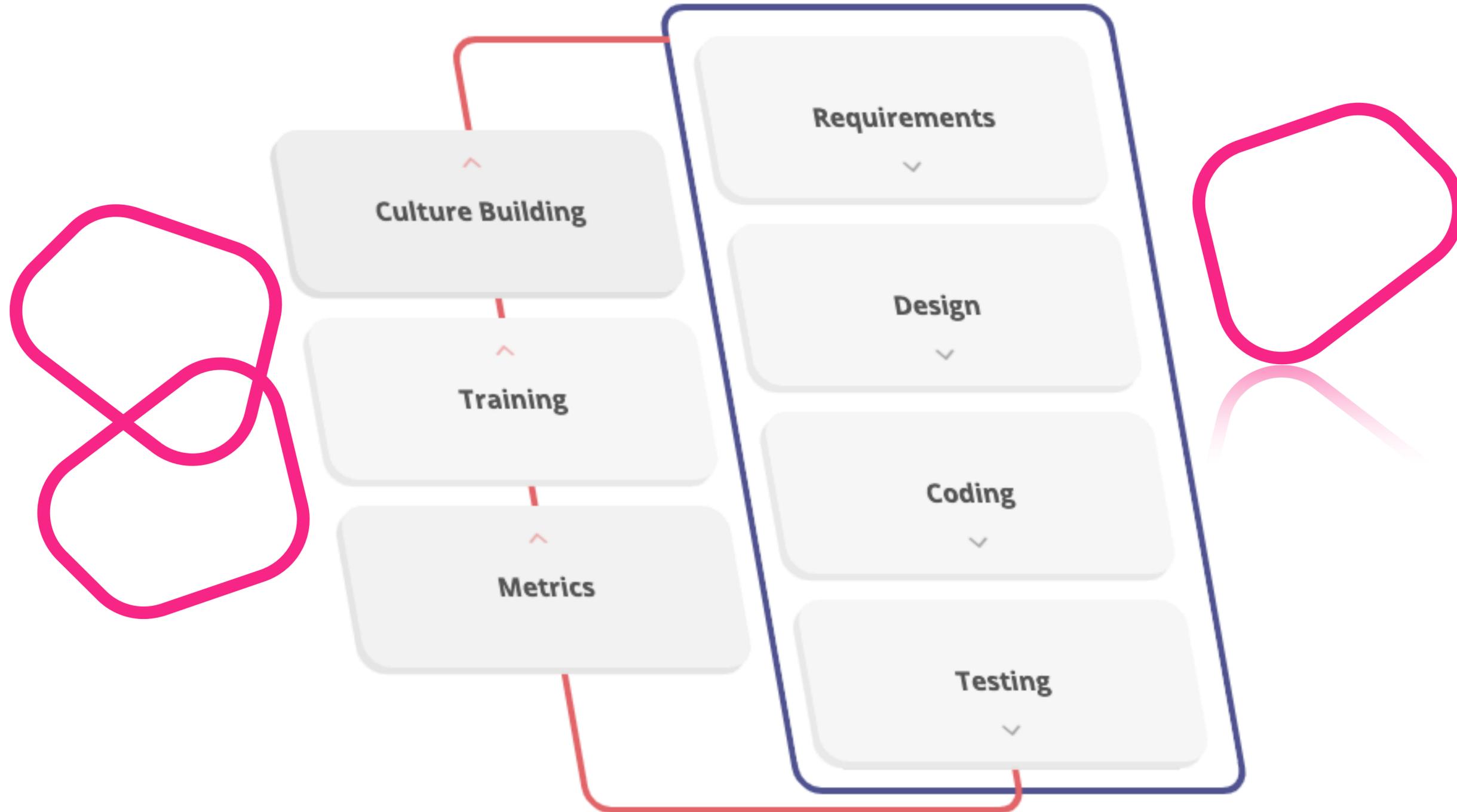
- Almost 20 years of experience in the IT Security field
- Author and creator of OWASP-SKF Flagship project
- Founder of DefDev, a secure coding training company
- OWASP Board of directors member
- Working at ING Belgium as Security chapter lead



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?





HISTORY

Security Knowledge Frame... x +

localhost:8888/dashboard

Google

SKF Logout

->Security knowledge framework

Knowledge Base

Projects

Results

Start new project

Start existing project

Security knowledge base

View Item

View Item

View Item

2014 - Security Knowledge Framework

HISTORY

https://127.0.0.1:5443/dashboard

HOME

</> Code Language Logout

->Security knowledge framework

Start new project

Edit existing project

Security knowledge base

View item

View item

View item

2014- 2015 - Security Knowledge Framework

Problem #1

The screenshot shows a web browser window with the URL `https://127.0.0.1:5443/project-new`. The page title is "Security Knowledge Framework". The browser's search bar contains the word "Zoeken". The application's navigation menu on the left includes "Projects", "Results", "Knowledge Base", and "Code examples". The main content area features a heading "Security knowledge framework" and a paragraph: "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." Below this text are four circular icons with labels: "Start new project" (code icon), "Edit existing project" (document icon), "Security knowledge base" (book icon), and "Code examples" (code icon). The footer contains the text "© 2015 - Security Knowledge Framework". A status bar at the bottom left of the browser window displays "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

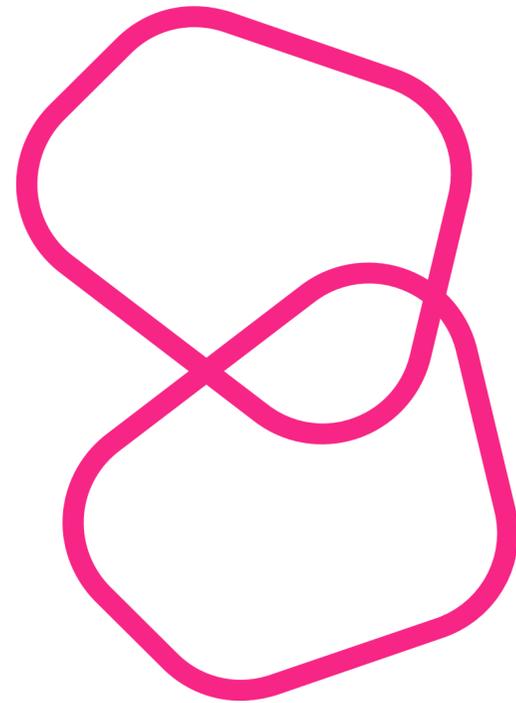
Pentester

Training Labs

Customize Checklist

2022 © Security Knowledge Framework.

SKF is part of: OWASP and OSSF



OpenSSF

OPEN SOURCE SECURITY FOUNDATION



Sign in to your account.

Email:

Password:

[Forgot Password?](#)

LOGIN

Or sign up with



[Don't have an account yet? Sign up](#)



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
```

The image shows a Neo4j graph visualization interface. At the top, a terminal window displays the query `neo4j$ MATCH (n) RETURN n`. The main area shows a graph with a central orange node, several blue nodes, and many purple nodes. Relationships are labeled 'DEFINED_IN' and 'BELONGS_TO'. A sidebar on the left contains icons for 'Graph', 'Table', 'Text', and 'Code'. A right-hand panel titled 'Overview' provides statistics: 'Node labels' (307 total, with Requirement: 286, Section: 20, Chapter: 1) and 'Relationship Types' (82 total, with DEFINED_IN: 76, BELONGS_TO: 6). It also states 'Displaying 307 nodes, 82 relationships.' A tooltip at the bottom center says 'Use Ctrl or Shift + scroll to zoom' and 'Don't show again'.

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

Security Knowledge Framework

Search...

Logout

Dashboard Projects Code Examples Checklists Knowledgebase Labs Training

LABS

Labs / View

Red & Blue Labs

Search Lab

#	Name	Label	Level	Status	Write-up	Action
	Path traversal (LFI)	SKF-labs	1	Lab is Running	Click here	Stop
	Cross Site Scripting	SKF-labs	1		Click here	Start
	Cross site scripting (attribute)	SKF-labs	1		Click here	Start
	Cross site scripting (href)	SKF-labs	1		Click here	Start
	Insecure file upload	SKF-labs	1		Click here	Start
	Clickjacking	SKF-labs	1		Click here	Start
	Rate-limiting	SKF-labs	1		Click here	Start



LIVE DEMONSTRATION!

Local file inclusion/path traversal

Selects Intro ▾

Submit Button

SKF write-ups

- 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

```
<div class="col-md-6">  
  <form method="post" action="/home" enctype="multipart/form-data">  
    <div class="form-group">  
      <label>Selects</label>  
      <select class="form-control" name="filename">  
        <option value="../../../../etc/passwd">Intro</option>  
        <option value="text/chapter1.txt">Chapter 1</option>  
        <option value="text/chapter2.txt">Chapter 2</option>  
      </select>  
    </div>  
  </form>  
</div>
```

```
Request  
Raw Params Headers Hex  
POST /home HTTP/1.1  
Host: 127.0.0.1:5000  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:64.0) Gecko/20100101 Firefox/64.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Accept-Language: nl,en-US;q=0.7,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://127.0.0.1:5000/home  
Content-Type: multipart/form-data;  
boundary=-----1564649599112855287810126502  
42  
Content-Length: 188  
Connection: close  
Upgrade-Insecure-Requests: 1  
-----156464959911285528781012650242  
Content-Disposition: form-data; name="filename"  
/etc/passwd  
-----156464959911285528781012650242--  
  
Response  
Raw Headers Hex HTML Render  
<center> <n style="font-size:2em;"> ##  
# User Database  
#  
# Note that this file is consulted directly only  
# when the system is running  
# in single-user mode. At other times this  
# information is provided by  
# Open Directory.  
#  
# See the opendirectoryd(8) man page for additional  
# information about  
# Open Directory.  
##  
nobody:*:-2:-2:Unprivileged  
User:/var/empty:/usr/bin/false  
root:*:0:0:System Administrator:/var/root:/bin/sh  
daemon:*:1:1:System  
Services:/var/root:/usr/bin/false  
_uucp:*:4:4:Unix to Unix Copy  
Protocol:/var/spool/uucp:/usr/sbin/uucico  
taskgated:*:13:13:Task Gate  
Daemons:/var/empty:/usr/bin/false
```

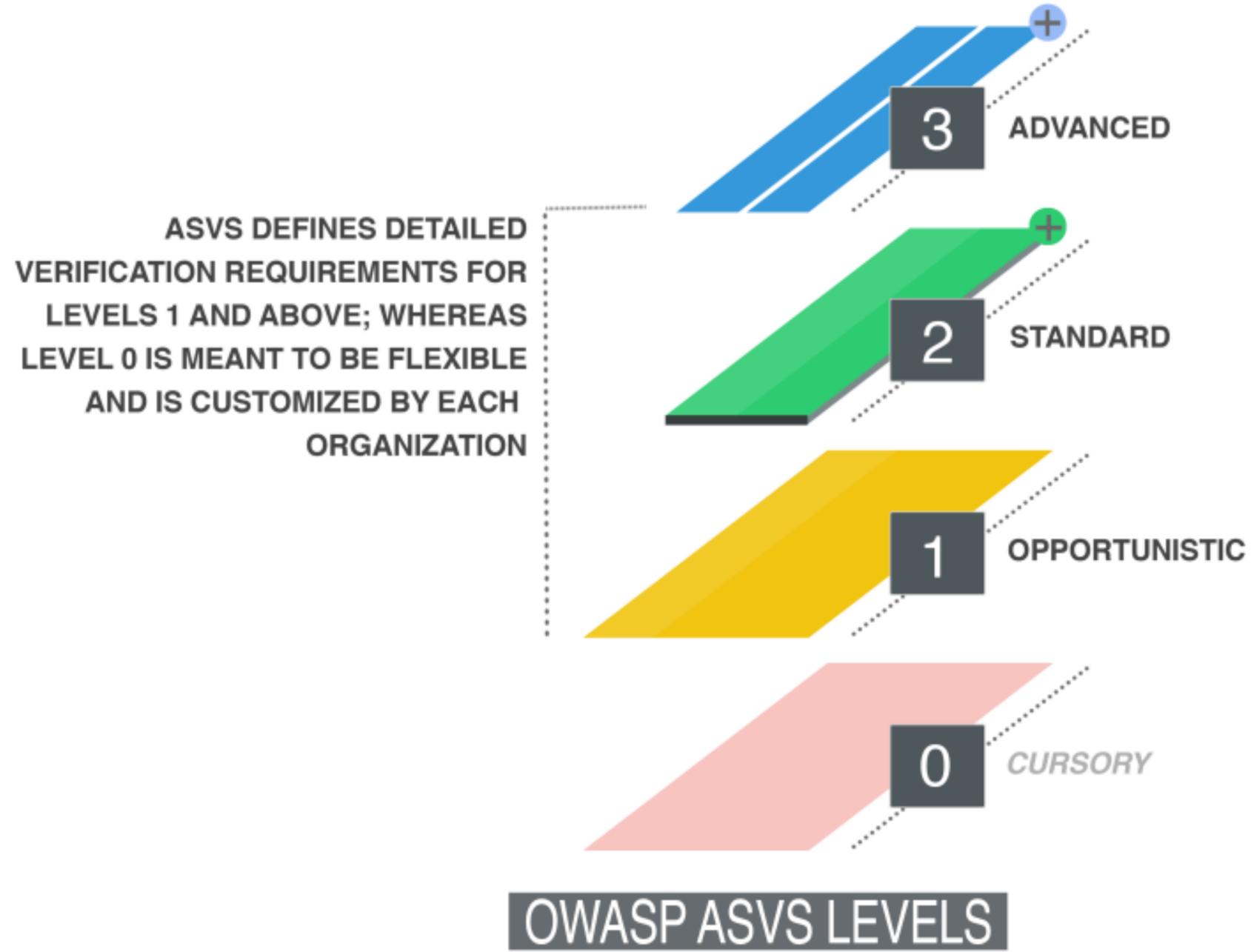
Success! As we observed, we can access the /etc/passwd file through LFI.

Additional sources

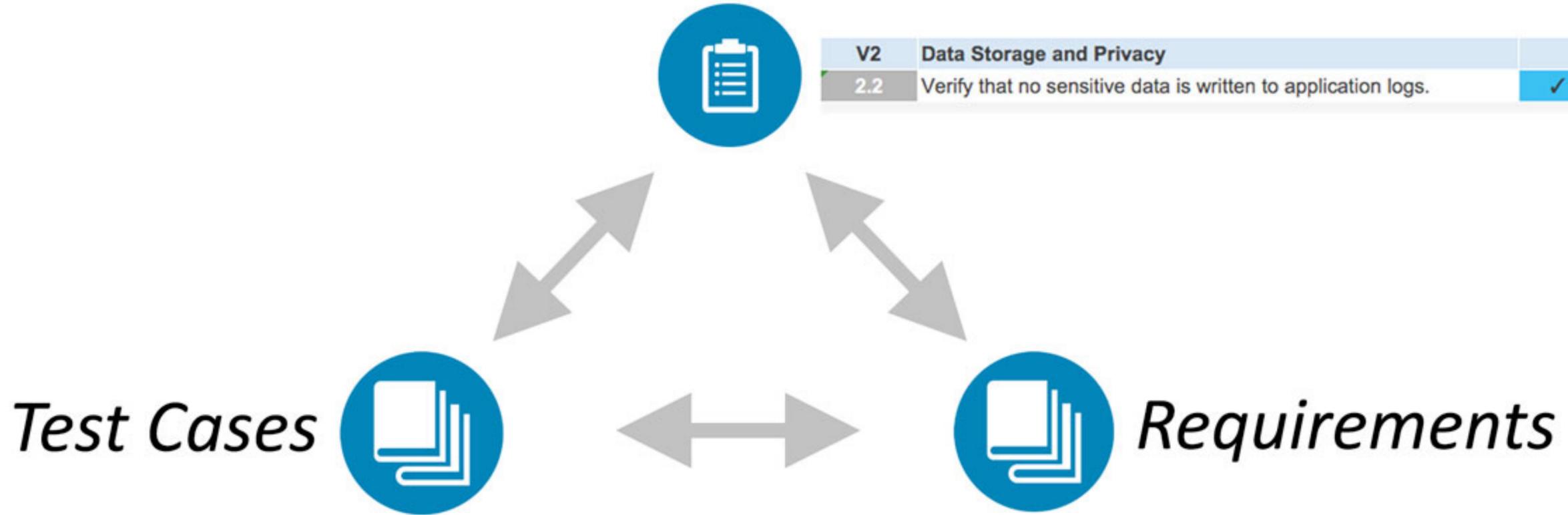
https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion

Mitigation

SKF & ASVS



Checklist



OWASP Mobile Security Testing Guide (MSTG)

OWASP Mobile Application Security Verification Standard (MASVS)

OMTG-DATAST-002: Test for Sensitive Data in Logs

Overview

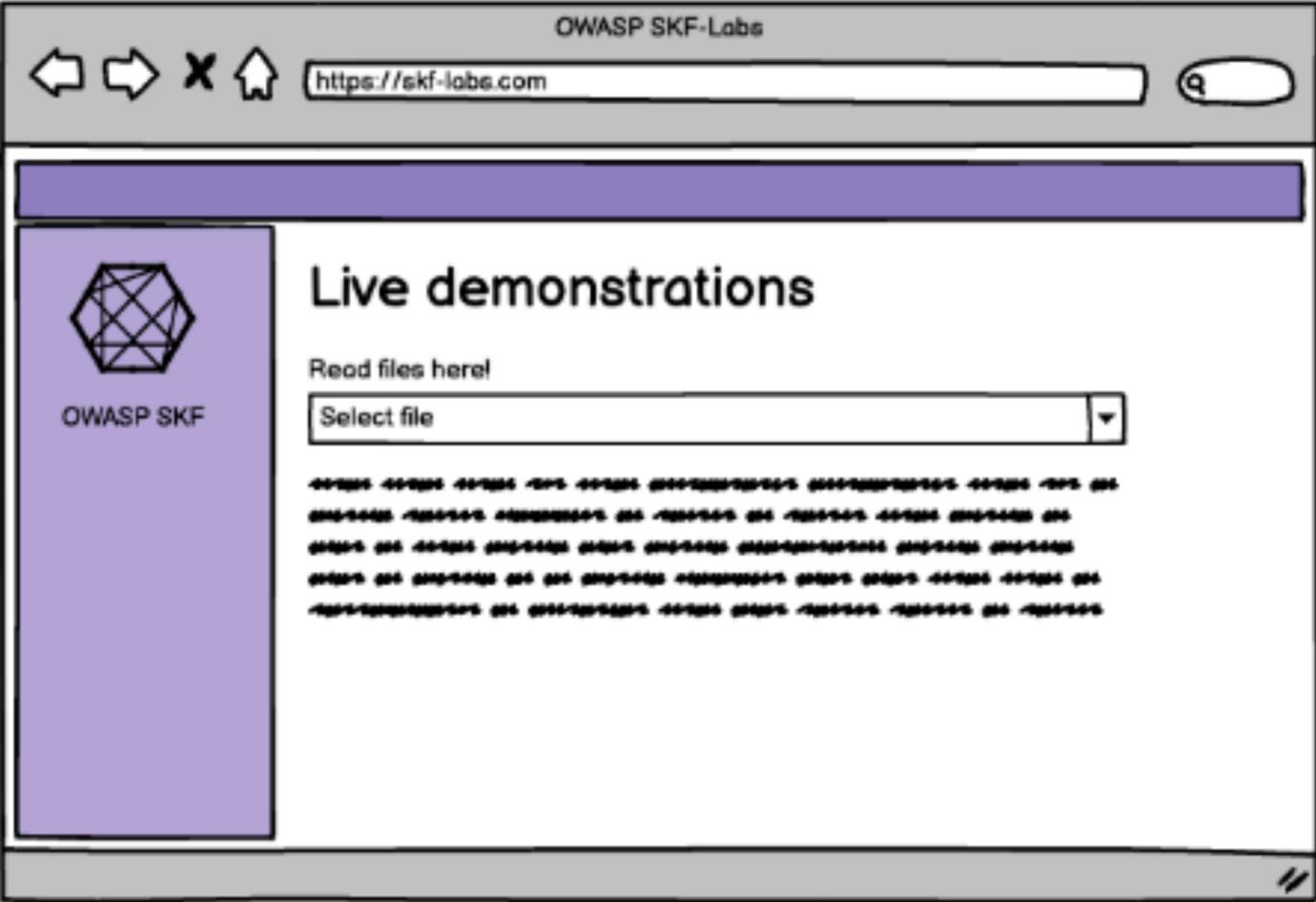
There are many legit reasons to create log files on a mobile device, for example to keep track of crashes or errors that are stored locally when being offline and being sent to the application developer/company once online again or for usage statistics. However, logging sensitive data such as credit card number and session IDs might expose the data to attackers or malicious applications. Log files can be created in various ways on each of the different operating systems. The following list shows the mechanisms that are available on Android:

- Log Class, .log[a-Z]
- Logger Class
- StrictMode
- System.out/System.err.print

Classification of sensitive information can vary between different industries, countries and their laws and regulations. Therefore laws and regulations need to be known that are applicable to it and to be aware of what sensitive information actually is in the context of the App.

#	
2.2	No sensitive data is written to application logs.

User story - Read files example

Description	<p>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</p>
Benefits	<p>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.</p>
Acceptance criteria	<ul style="list-style-type: none"> 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	 <p>The wireframe depicts a web browser window titled 'OWASP SKF-Labs'. The address bar shows 'https://skf-labs.com'. The page layout includes a purple header bar, a left sidebar with the OWASP SKF logo and name, and a main content area. The main content area features the heading 'Live demonstrations', the text 'Read files here!', and a dropdown menu labeled 'Select file'. Below the dropdown is a block of placeholder text represented by several lines of small, illegible characters. The browser window also shows navigation icons (back, forward, home, refresh) and a search icon.</p>

PROJECTS

[← go back](#)

CHECKLIST



MATURITY LEVEL



CATEGORY



QUESTIONNAIRE



SETUP



FINISH

Platforms

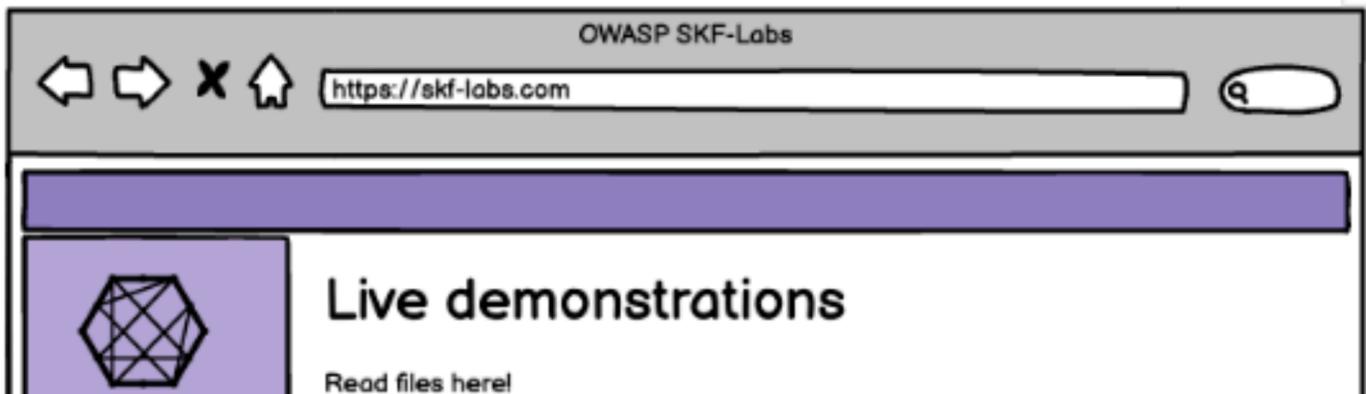
Select checklist type

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.

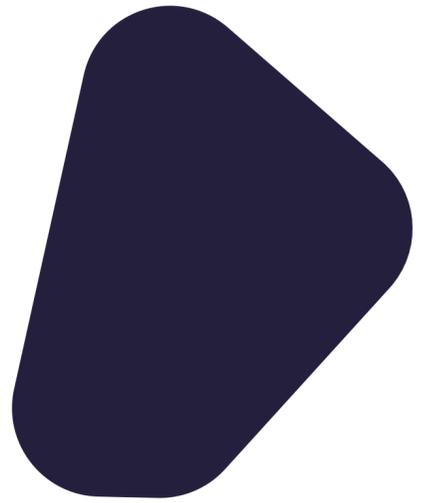
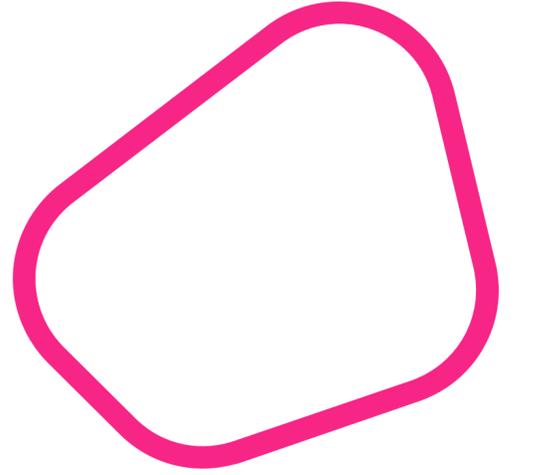
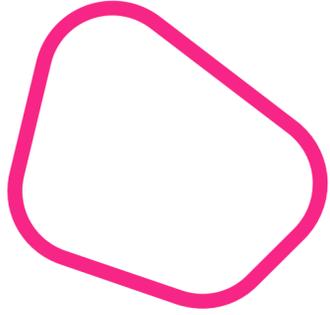
[Next](#)

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	<table border="1"><thead><tr><th>Item</th><th>Control</th></tr></thead><tbody><tr><td>5.1.3</td><td>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)</td></tr><tr><td>5.1.4</td><td>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).</td></tr><tr><td>5.3.9</td><td>Verify that the application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.</td></tr><tr><td>7.4.1</td><td>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.</td></tr></tbody></table>	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.
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	 <p>The wireframe shows a browser window with the title 'OWASP SKF-Labs'. The address bar contains 'https://skf-labs.com'. Below the address bar is a purple navigation bar. Underneath, there is a section with a purple background and a white geometric logo on the left. To the right of the logo, the text reads 'Live demonstrations' in a large font, and 'Read files here!' in a smaller font below it.</p>										

Automation

ZAP



Standard Mode

Sites Scripts

Quick Start Request Response Script Console

Header: Text Body: Text

- Contexts
- Sites
 - https://lfi-d946ea71-f492-4873-9f83-112c6ff5e7d8.securityknowledgeframework-labs.org/home

```
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
shutdowm:x:0:0:shutdowm:/sbin:/sbin/shutdowm
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
 - 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

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 [↗](#)

OWASP ZAP - OWASP ZAP 2.11.1

Standard Mode

Sites Scripts

Quick Start Request Response Script Console

Run Zest : GraphQL-IDOR

```
1 {
2   "about": "This is a Zest script. For more details about Ze
3   "zestVersion": "0.3",
4   "title": "GraphQL-IDOR",
5   "description": "GraphQL-IDOR",
6   "prefix": "",
7   "type": "StandAlone",
8   "parameters": {
9     "tokenStart": "{",
10    "tokenEnd": "}"
11 }
```

Stand Alone scripts are self contained scripts that can only be run manually.

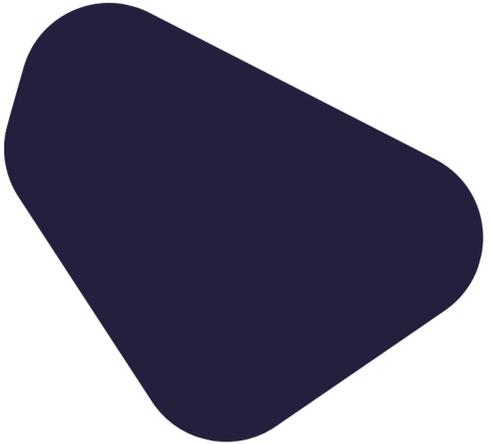
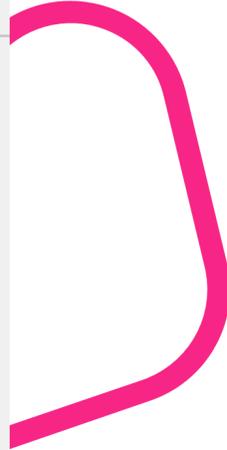
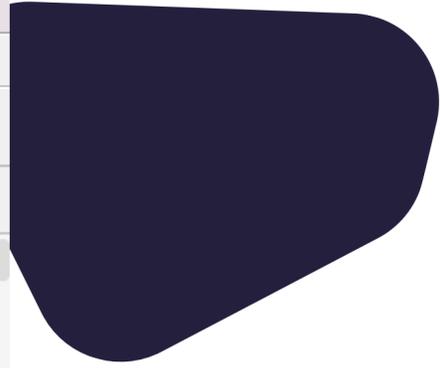
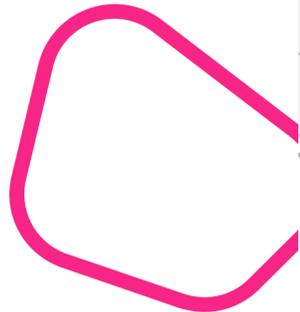
You run them using the 'Run' button in the above toolbar.userid - 1 - apikey is v
alid
IDOR - API key has changed

History Search Alerts Output

WebSockets Zest Results Spider Active Scan

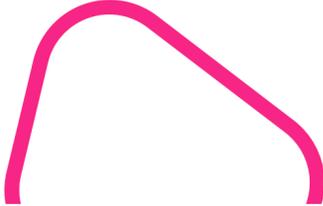
Id	Met...	URL	C...	Reason	...	Size Resp...	Result
115	POST	https://graphql-idor-ea391d9...	302	FOUND	...	209 bytes	✓
117	POST	https://graphql-idor-ea391d9...	200	OK	...	336 bytes	✓
119	POST	https://graphql-idor-ea391d9...	200	OK	...	121 bytes	✓
121	POST	https://graphql-idor-ea391d9...	200	OK	...	123 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

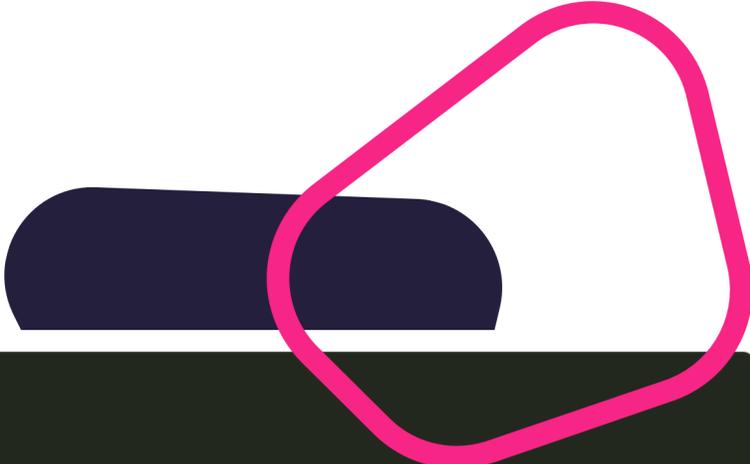


AF

```
# OWASP ZAP automation configuration file, for more details see https://www.zaproxy.org/docs/automate/automation-framework/
: # The environment, mandatory
contexts : # 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
```



```
./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

[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](#)

```
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 ▾

```
1 import old_print as oldp
2
3 def hello_world():
4     skynet.init()
5     # TODO Change this to logging framework before prod
6     oldp(
7         '--> debug, skynet init vector is {skynet.iv}'
8     )
9     # oldp('don't detect this, it\'s commented!')
```

[Run](#)

```
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 % █
```

SEMGREP

The screenshot displays a development environment with three main components:

- LXTerminal:** Shows log output from a scanner. Key messages include:

```
should MEDIUM
97891 [Thread-41] INFO org.parosproxy.paros.core.scanner.HostProcess - completed host/plugin http://localhost:7777 | SOAPXMLInjectionActiveScanRule in 1.449s with 0 message(s) sent and 0 alert(s) raised.
97891 [Thread-41] INFO org.parosproxy.paros.core.scanner.HostProcess - completed host http://localhost:7777 in 40.357s with 3 alert(s) raised.
97892 [Thread-40] INFO org.parosproxy.paros.core.scanner.Scanner - scanner completed in 40.362s
98142 [ZAP-DomXssReaper] INFO org.zaproxy.zap.extension.domxss.DomXssScanRule - Reaper thread exiting 0
```
- Web Browser (Mozilla Firefox):** Displays a page titled "Local file inclusion/path traversal" with the OWASP S.K.F. logo. It features a "Selects" dropdown menu with "Intro" selected and a "Submit Button". The browser's address bar shows "localhost:7777".
- Code Editor (Sublime Text):** Shows the Python code for the web application in "LFI.py":

```
10 return render_template("index.html")
11
12
13 @app.route("/home", methods=['POST'])
14 def home():
15     filename = request.form['filename']
16     if filename == "":
17         filename = "text/default.txt"
18     f = open(filename, 'r')
19     read = f.read()
20     return render_template("index.html", read = read)
21
22
23 if __name__ == "__main__":
24     app.run(host='0.0.0.0', port=7777)
25
26
```

At the bottom right, a security tool interface shows a list of alerts, including "Path Traversal" and "Content Security Policy (CSP) Header Not Set". A detailed description for the Path Traversal alert is visible:

```
CWE ID: 22
WASC ID: 33
Source: Active (6 - Path Traversal)
Description:
the "." special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from
```

<https://semgrep.dev/>

Training

Training Profiles

Secure Development
X COURSES



This profile is dedicated for developers (Blue security Champions) who want to learn secure development. This course is based on t...

[Explore courses](#)

Hacking web & API
X COURSES



This profile is dedicated for security pentesters or developers (Red security Champions) who want to learn the basics and advance ...

[Explore courses](#)

Infra & Ops
X COURSES



This profile is dedicated for Ops and Infra people who want to learn about the server hardening and security best practices. This ...

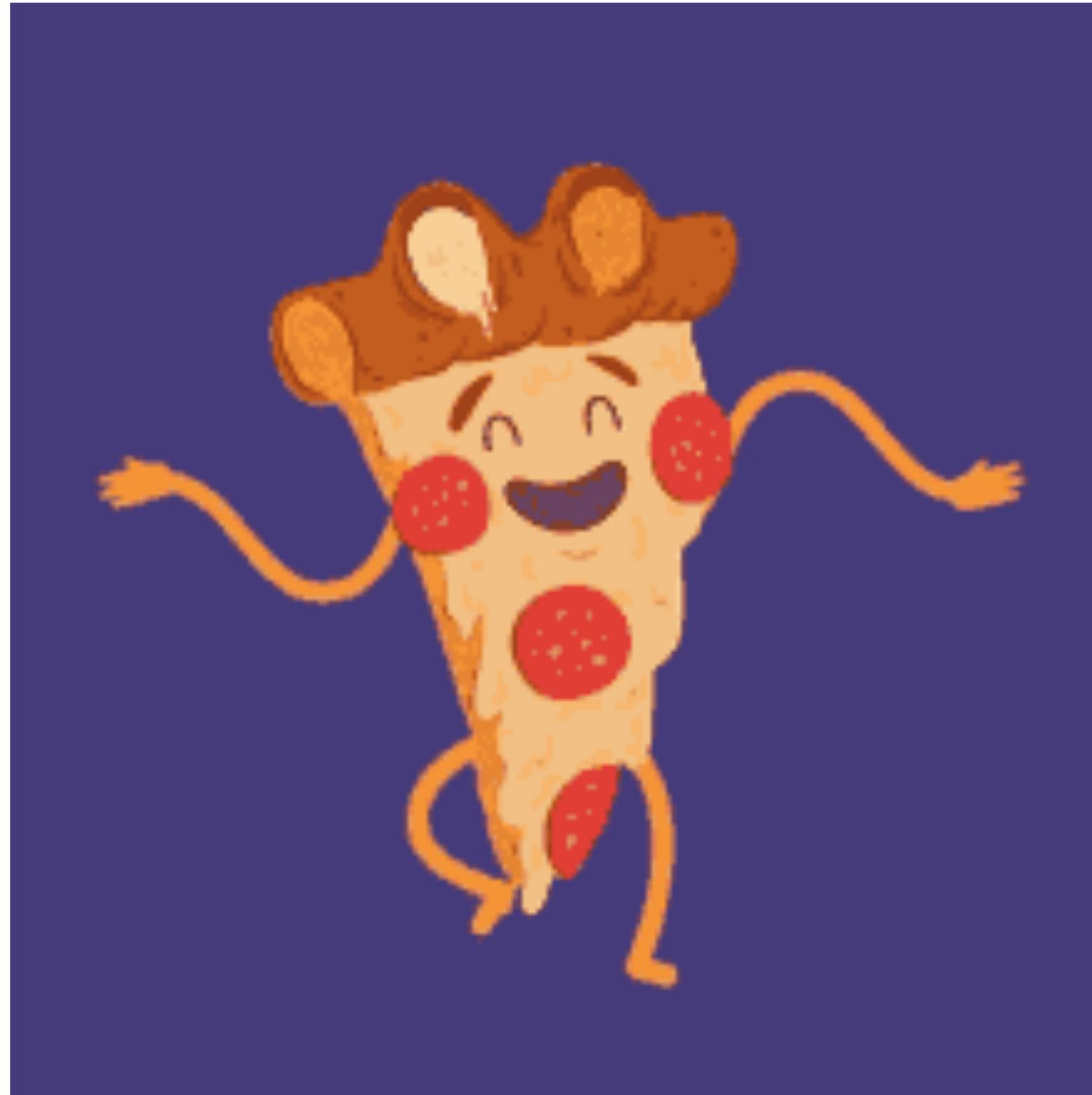
[Explore courses](#)

OWASP
X COURSES



This profile is dedicated for security pentesters or developers to get familiar with all the OWASP projects and tools. Here you w ...

[Explore courses](#)



- <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_