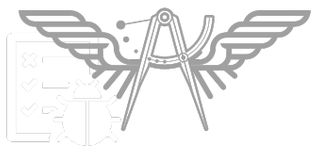
สยามชำนาญกิจ
SIAM CHAMNAN KIT

Security Testing
For Dev and Tester



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Security Testing

\

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Software Testing

\

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

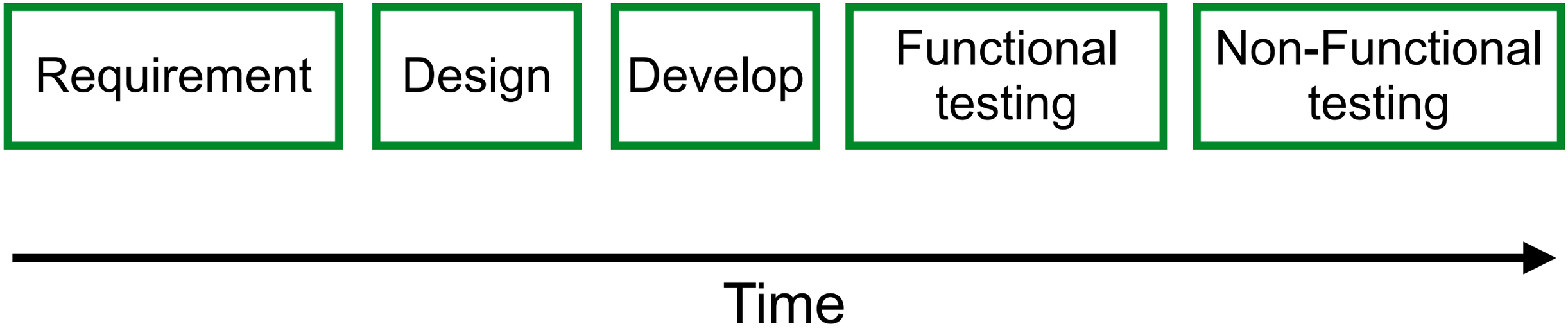
Testing ?

When to test ?
When to secure test ?

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

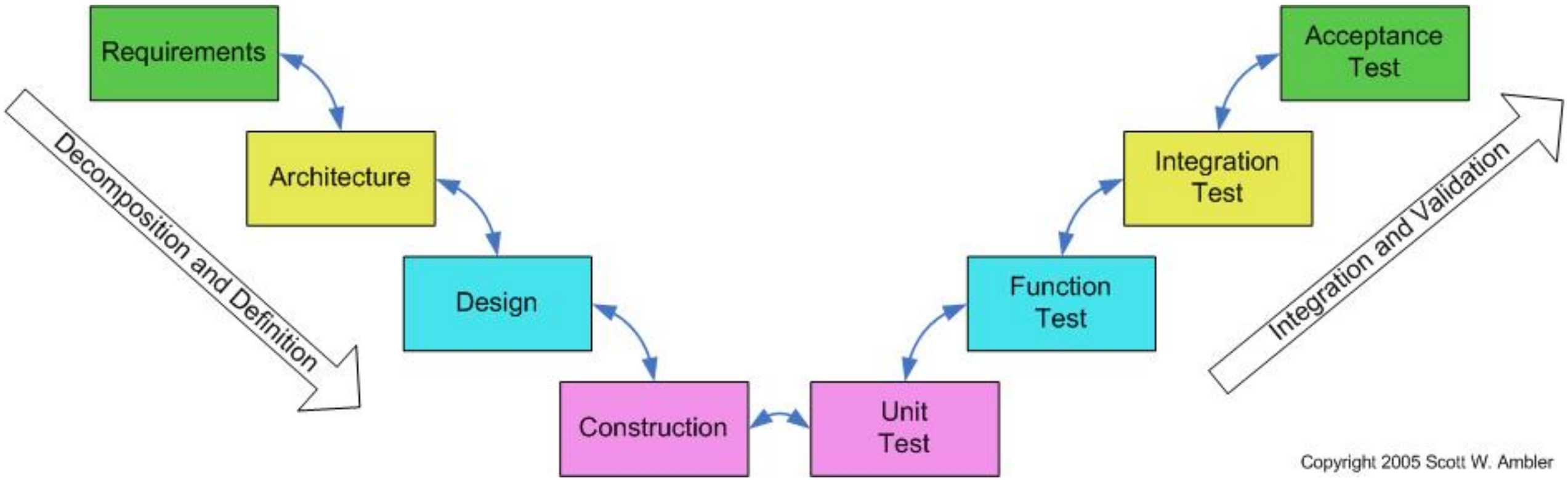
Testing ?

When to test ?
When to secure test ?



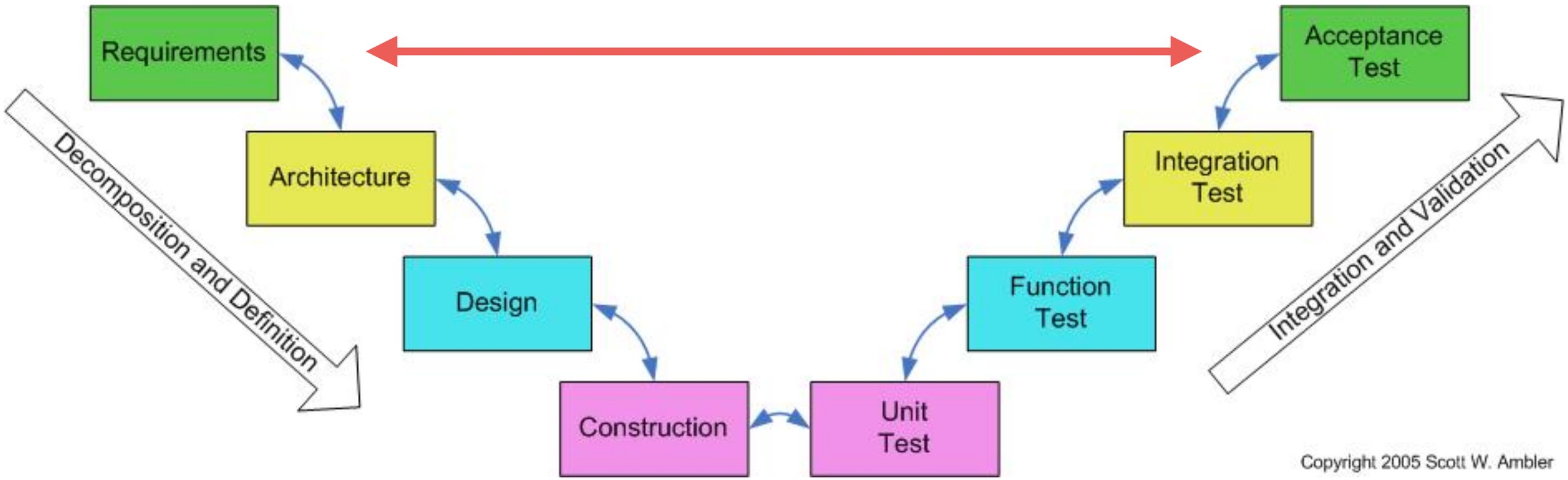
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

V Model



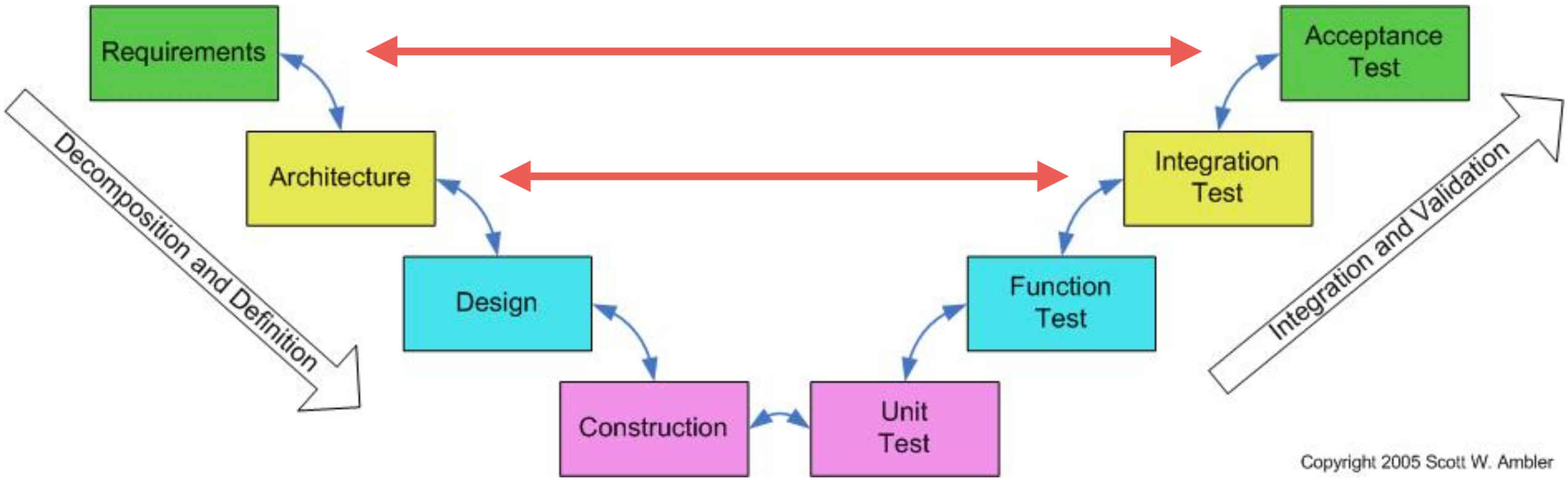
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

V Model



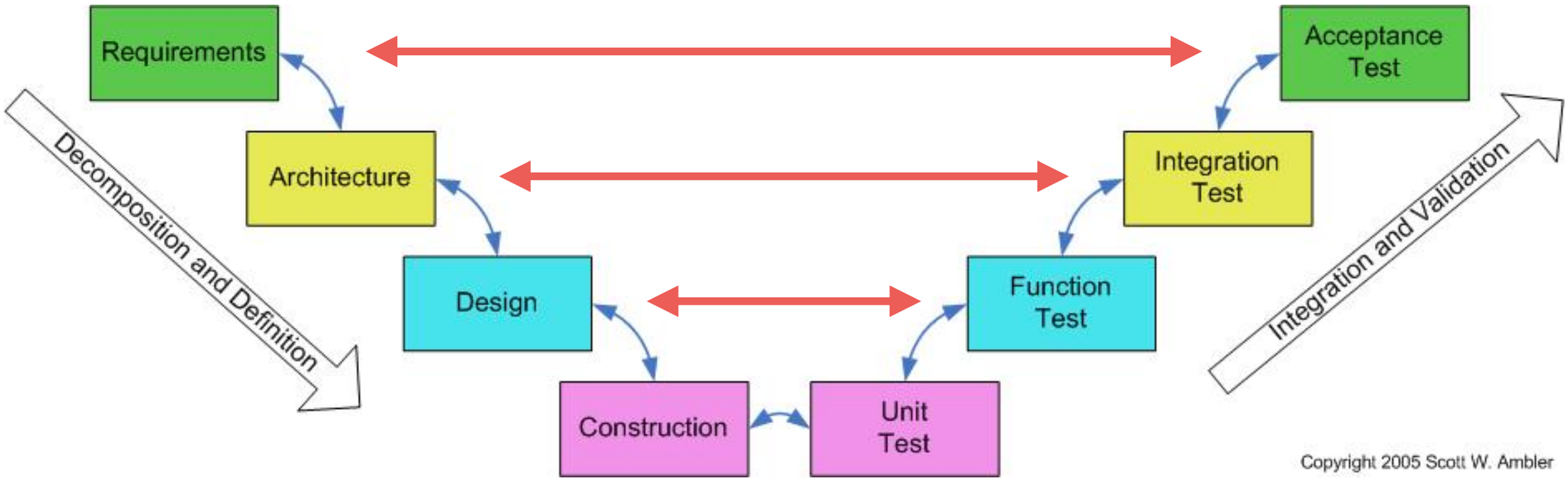
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

V Model



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

V Model

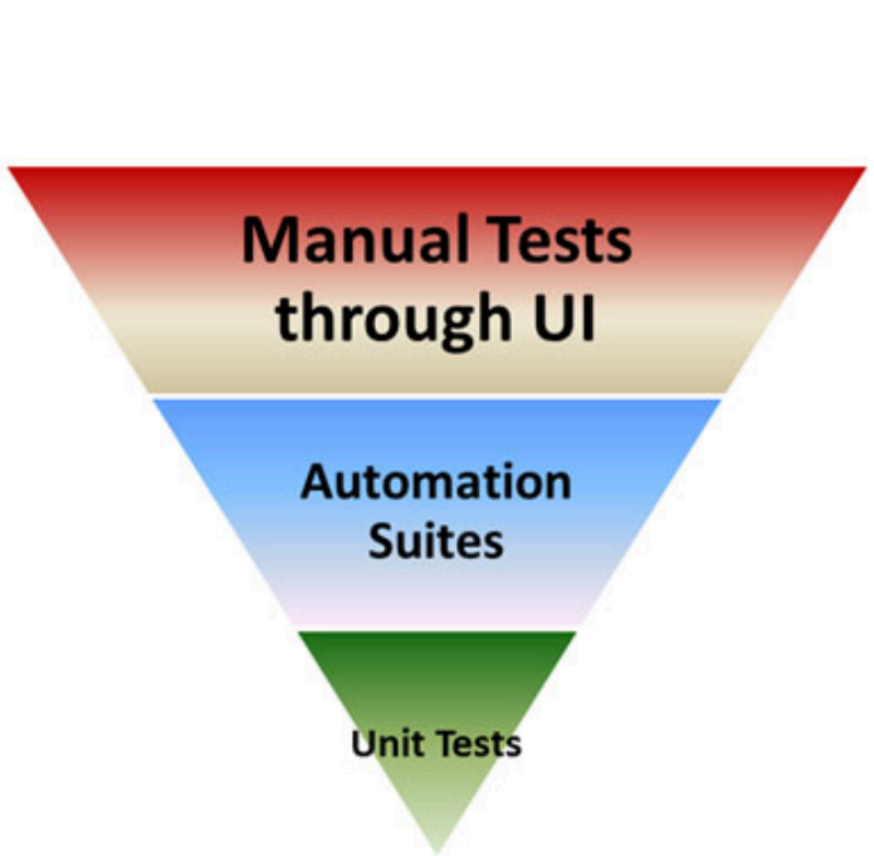


© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

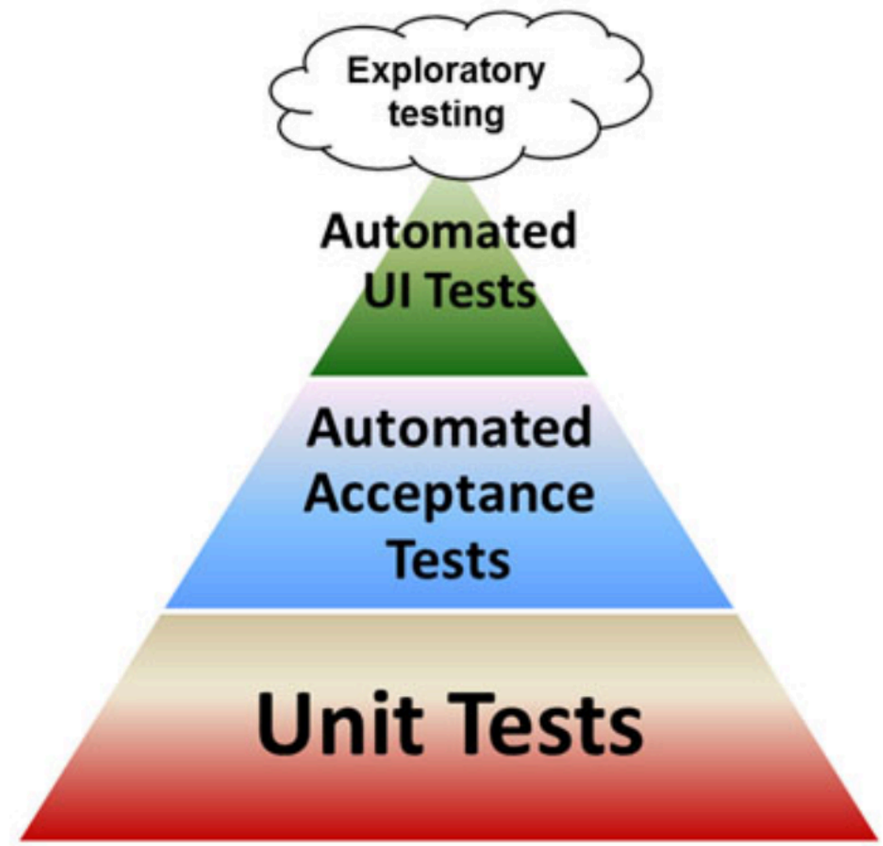
Prevent vs Find

\

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.



Traditional
(find bugs)



Agile
(prevent bugs)

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

BUSINESS FACING

Automated & Manual

Manual

Functional Tests
Examples
Story Tests
Prototypes
Simulations

Q2

Exploratory Testing
Scenarios
Usability Testing
UAT (User Acceptance Testing)
Alpha / Beta

Q3

SUPPORTING THE TEAM

Q1

Unit Tests
Component Tests

Q4

Performance & Load Testing
Security Testing
“ility” Testing

CRITIQUE PRODUCT

Automated

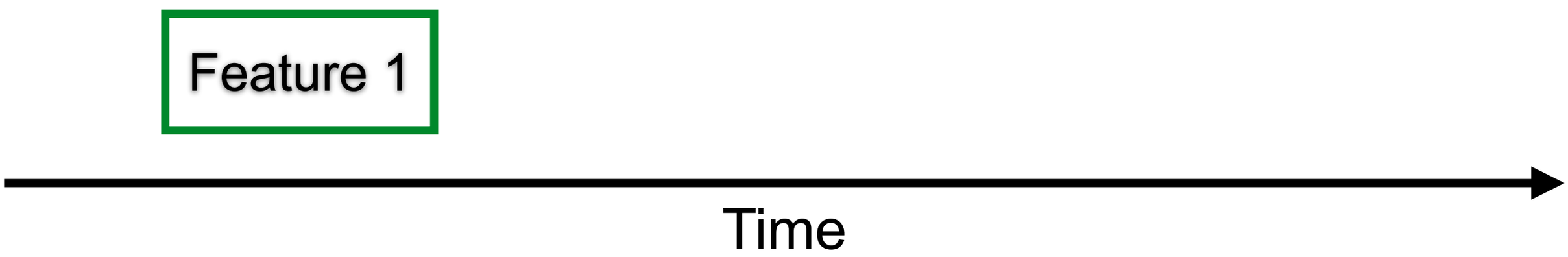
Tools

TECHNOLOGY FACING

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Iterative and incremental process

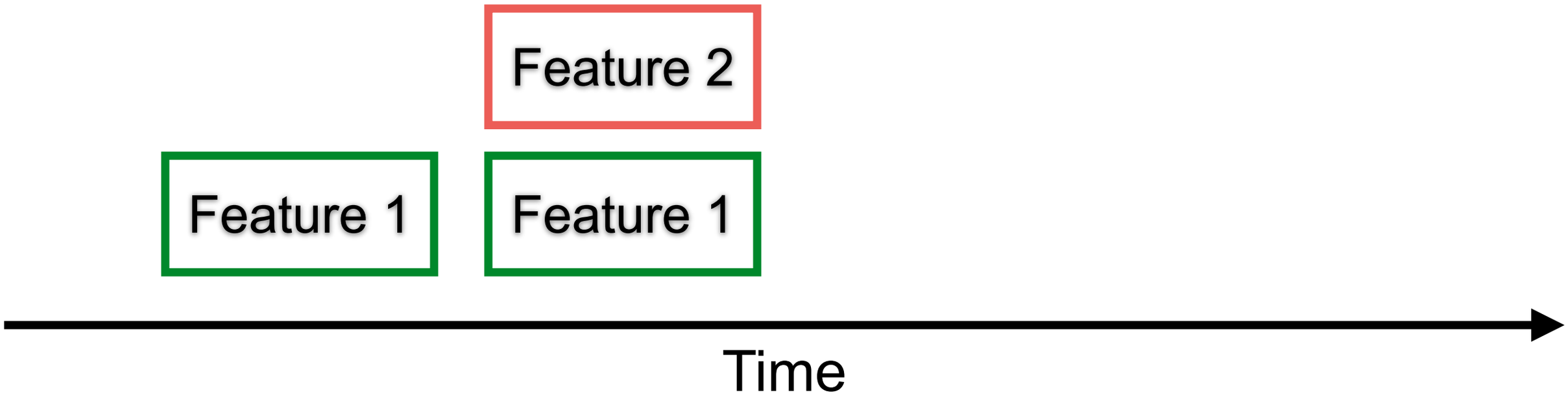
Done = coded and tested



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Iterative and incremental process

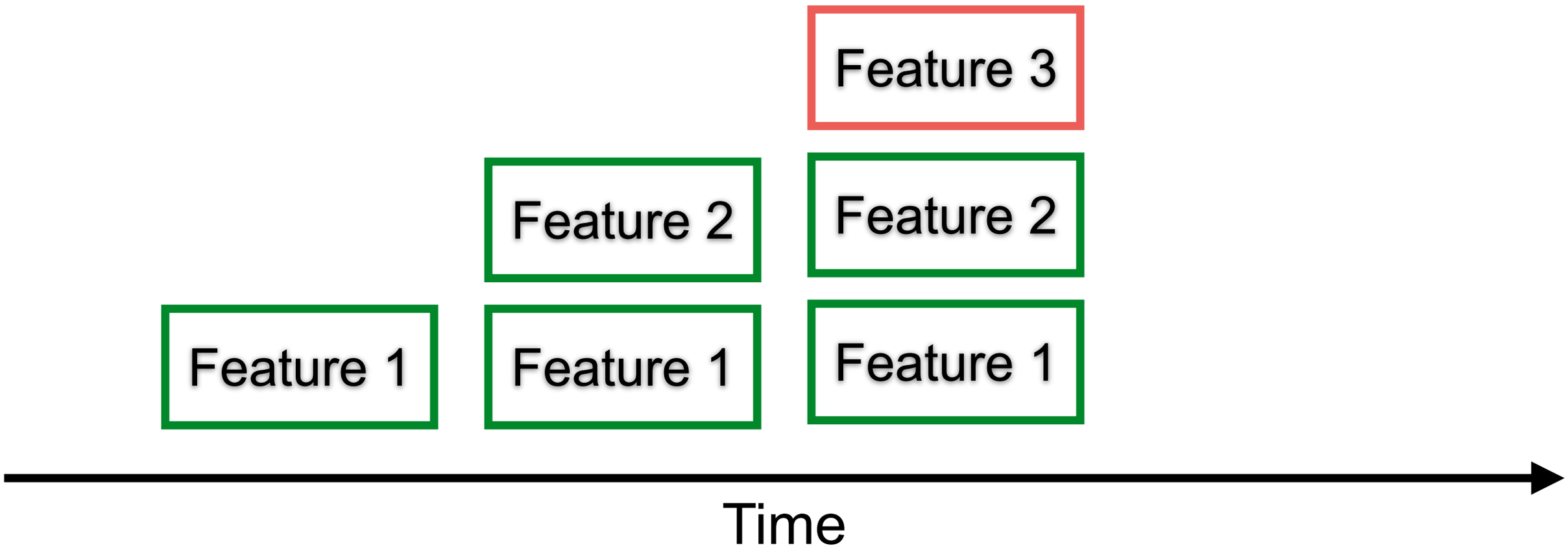
Done = coded and tested



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Iterative and incremental process

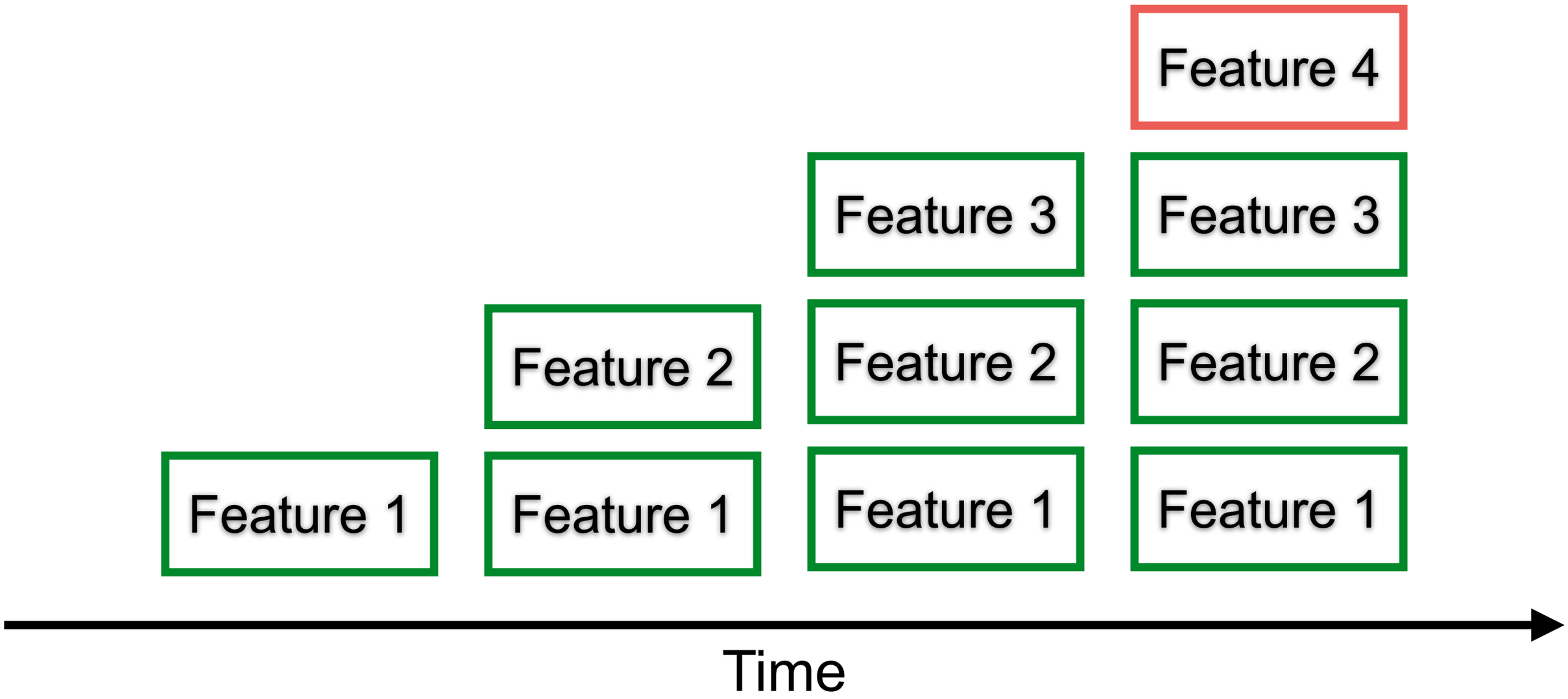
Done = coded and tested



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Iterative and incremental process

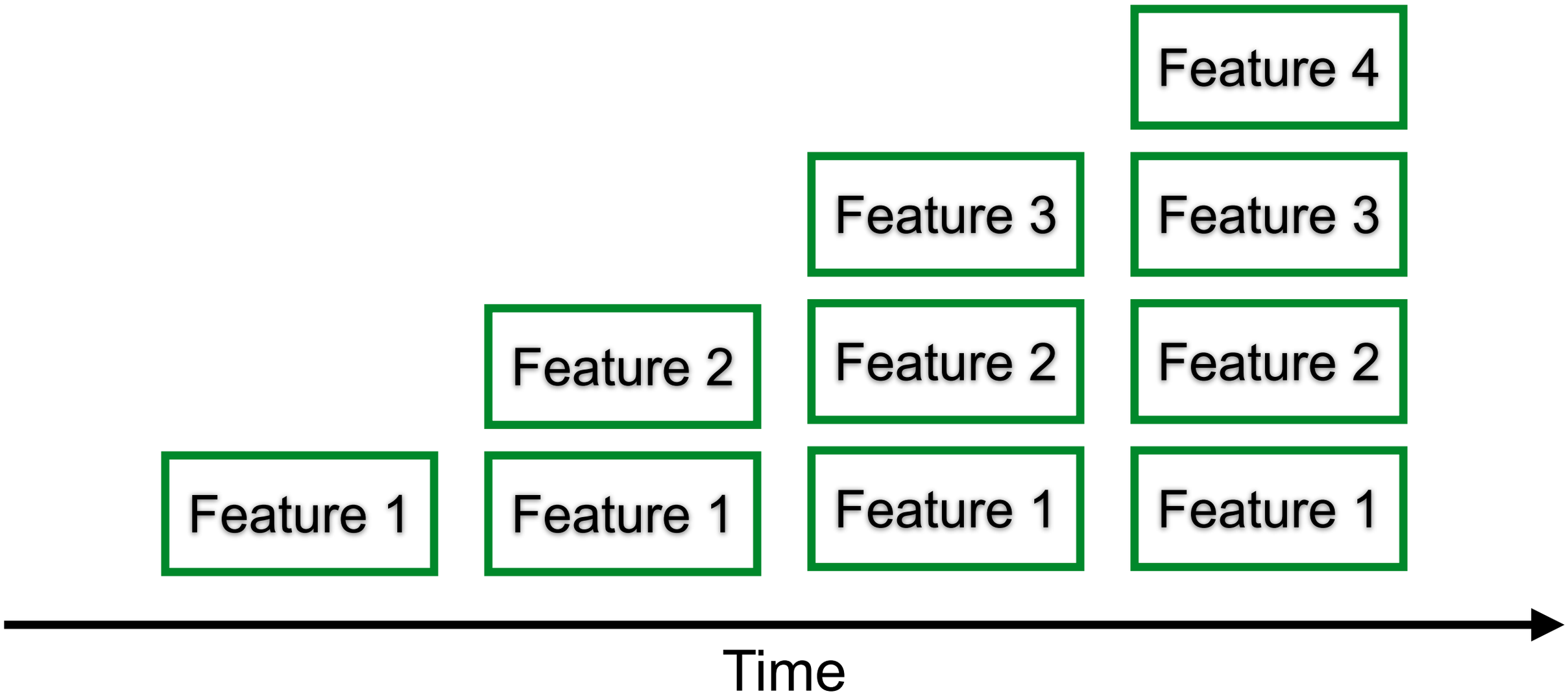
Done = coded and tested



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

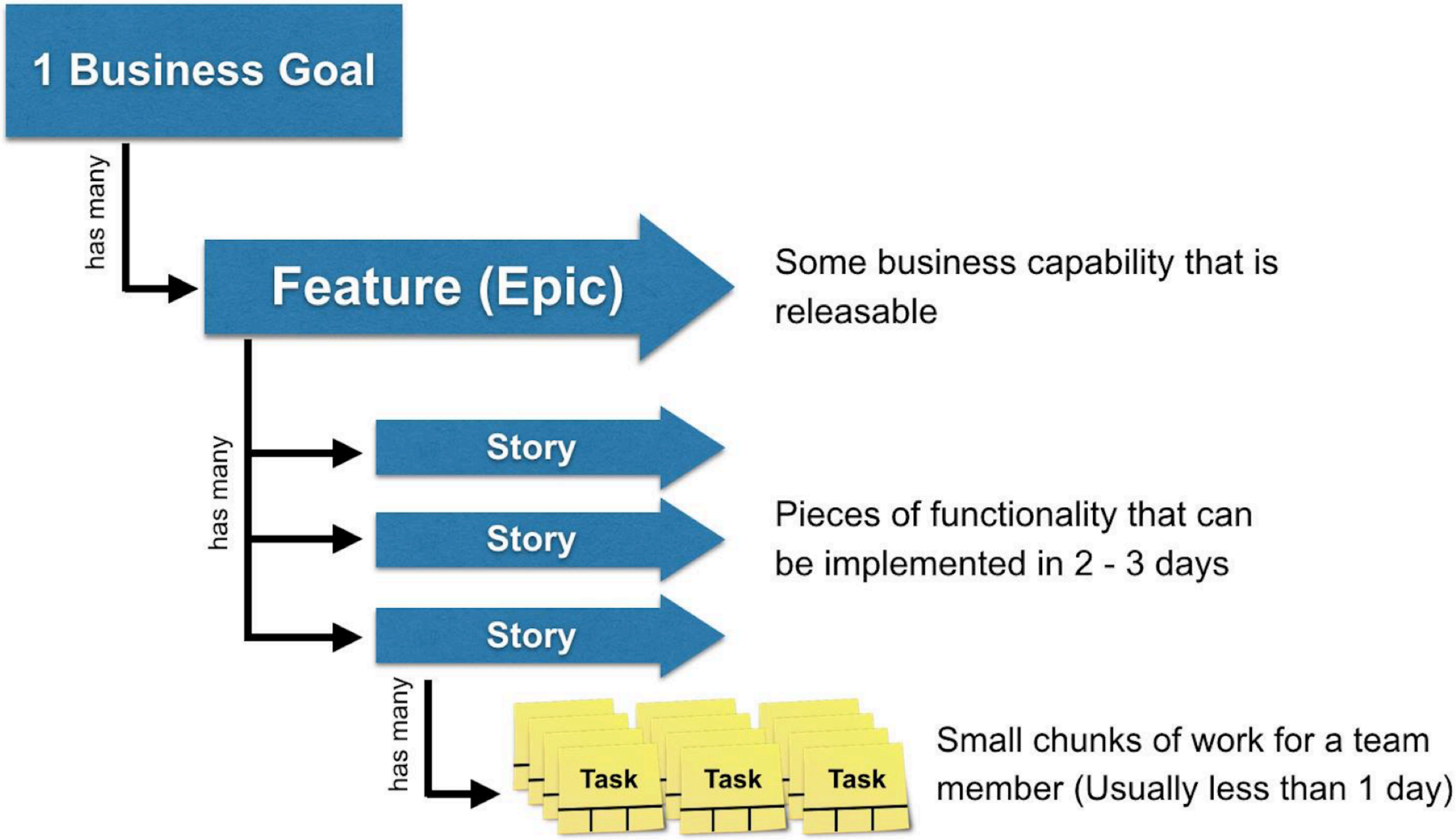
Iterative and incremental process

Done = coded and tested



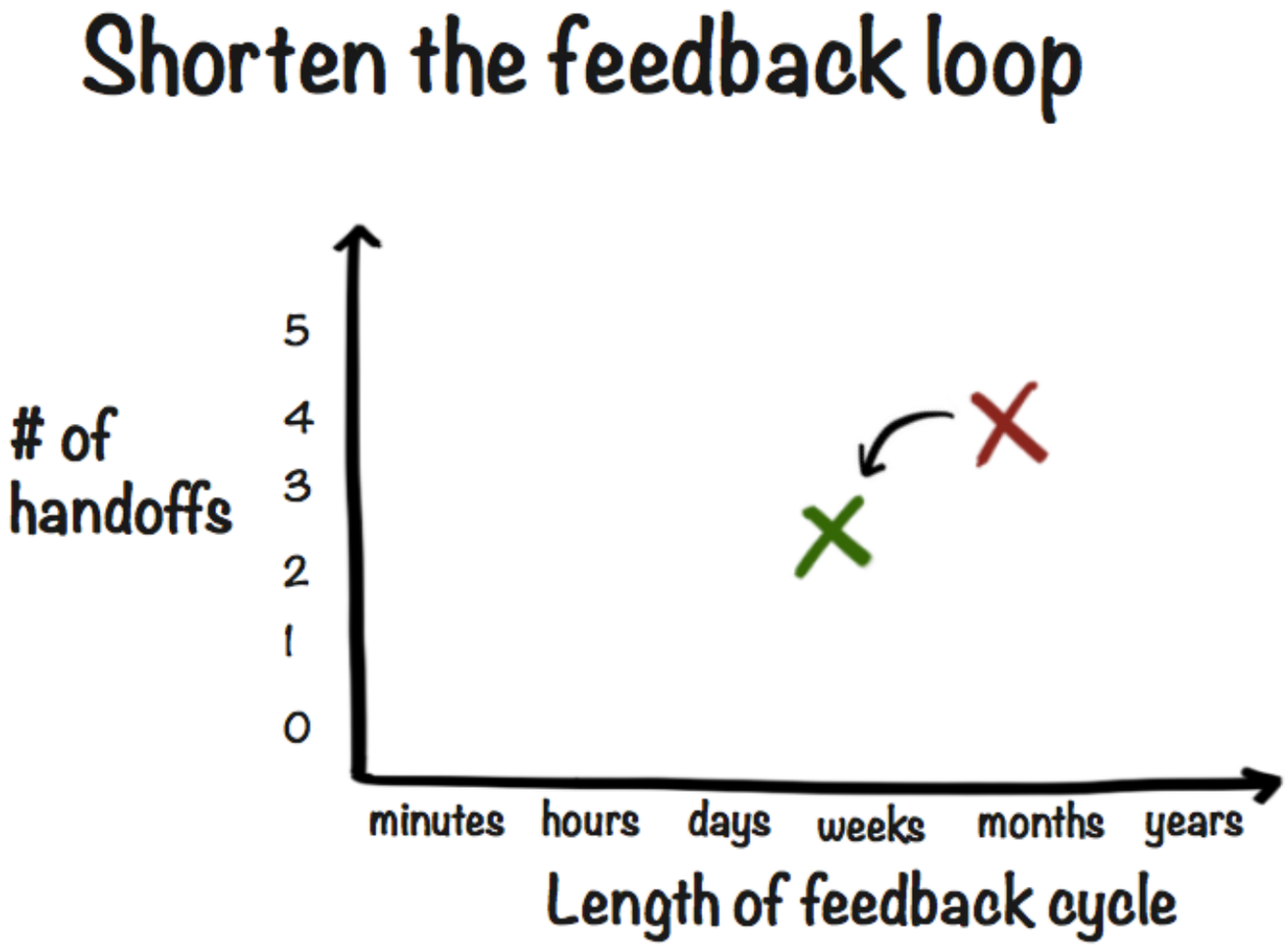
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

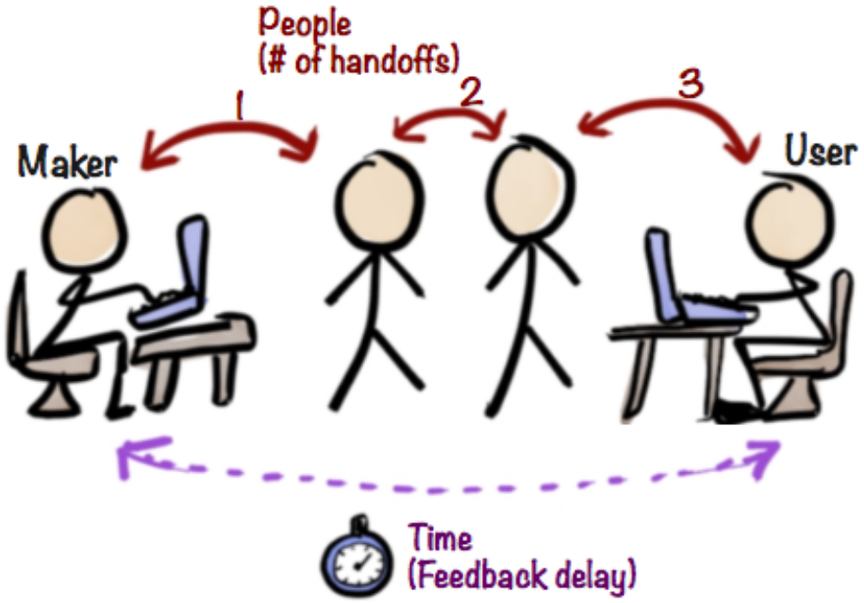
Start with business goal to tasks



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

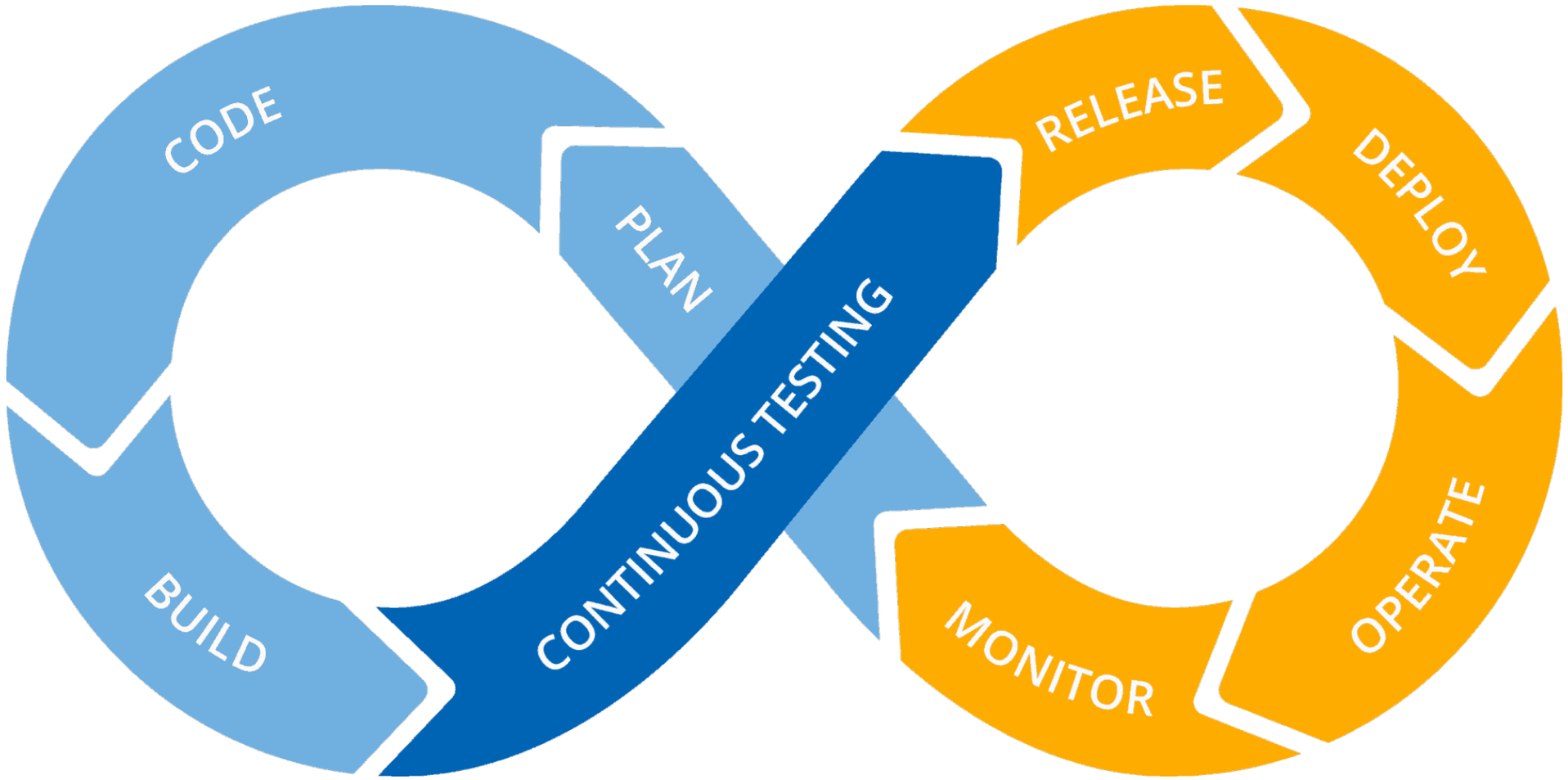
Need Fast Feedback Loop





© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Continuous Testing

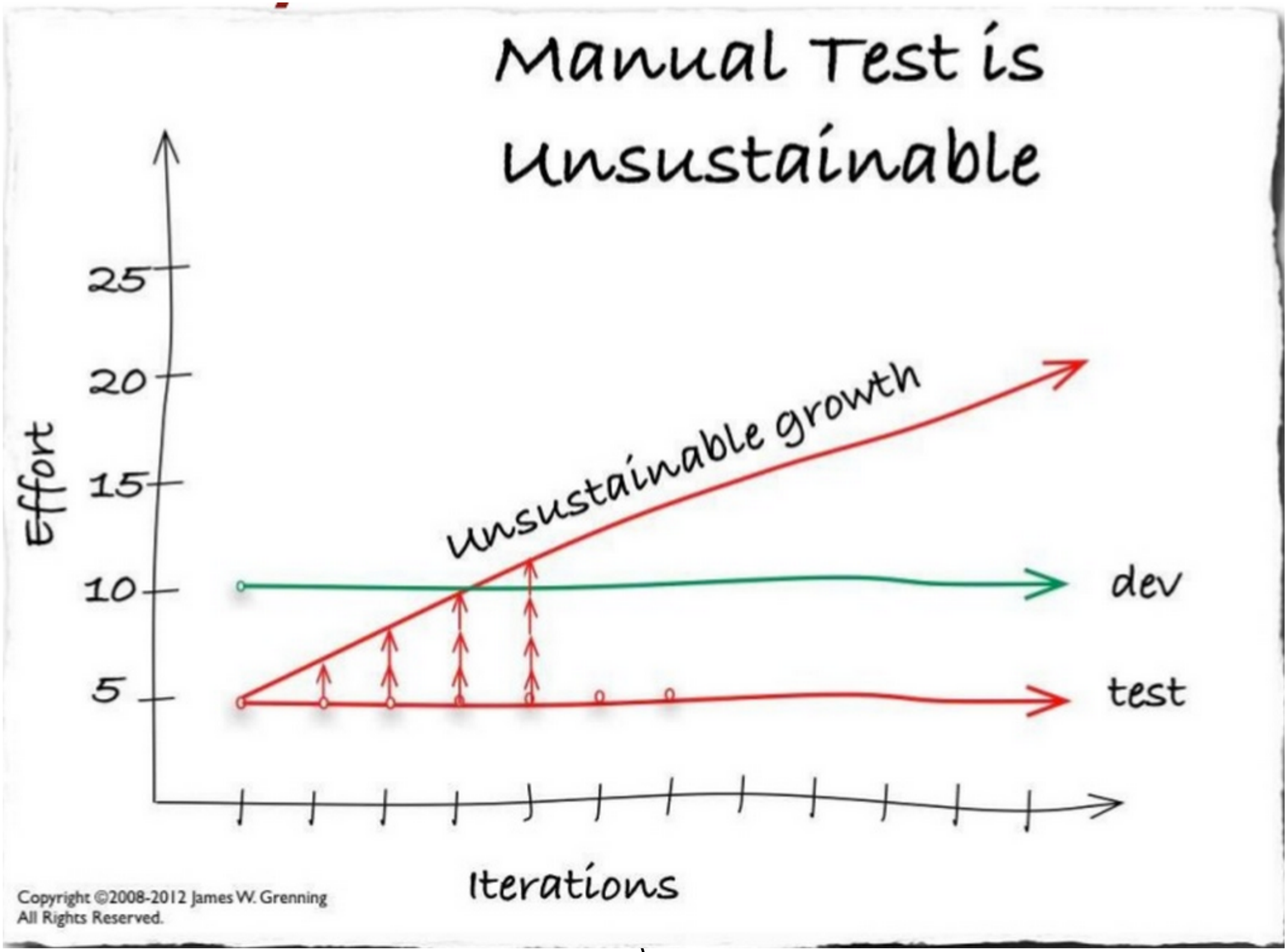


© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Manual vs Automated testing

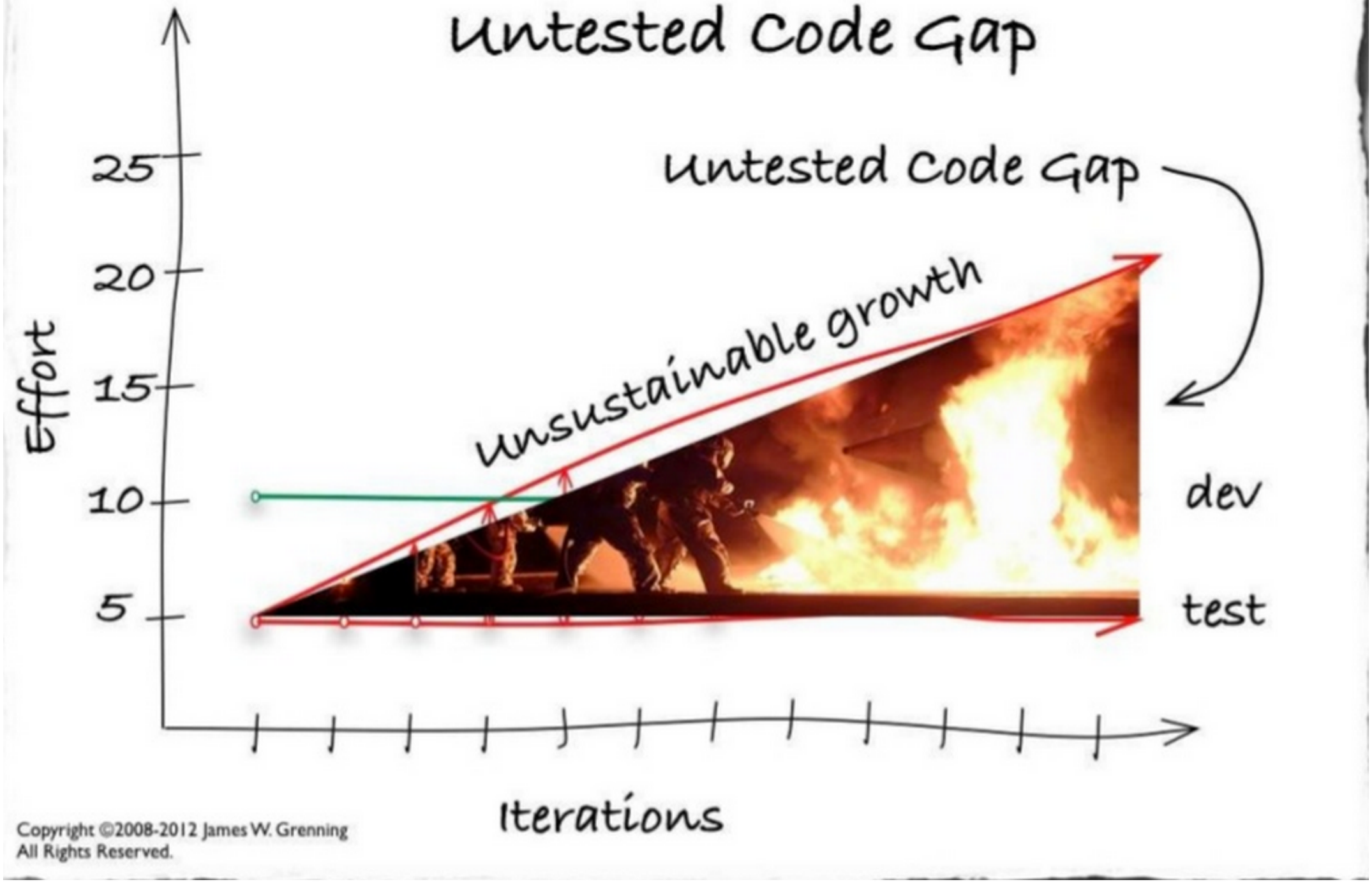
\

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Risk Accumulates in the Untested Code Gap



Copyright ©2008-2012 James W. Grenning
All Rights Reserved.

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Why we need automation ?

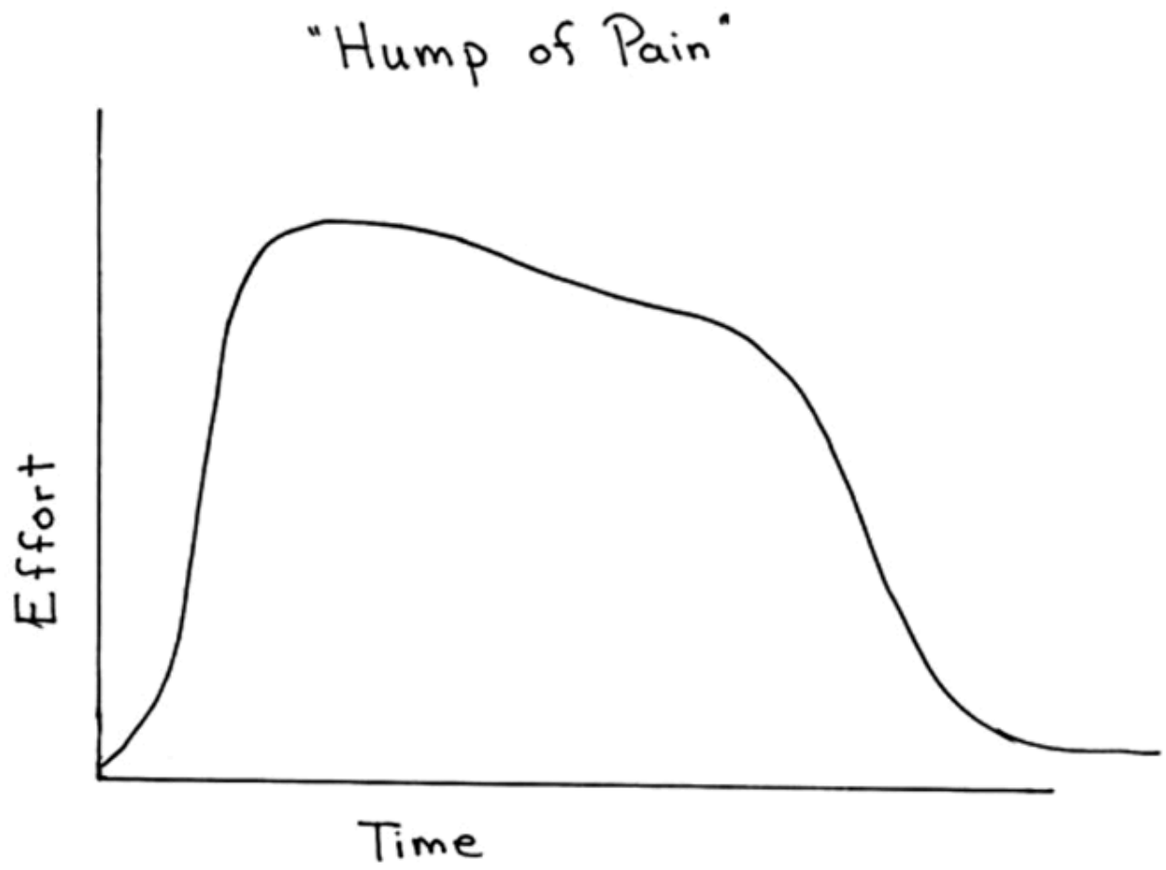
Manual checking take too long
Manual checks are error prone
Free people to do their best work (testing)
Living document
Repeatable and save time

\

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Initial investment !!

Hump of pain



\

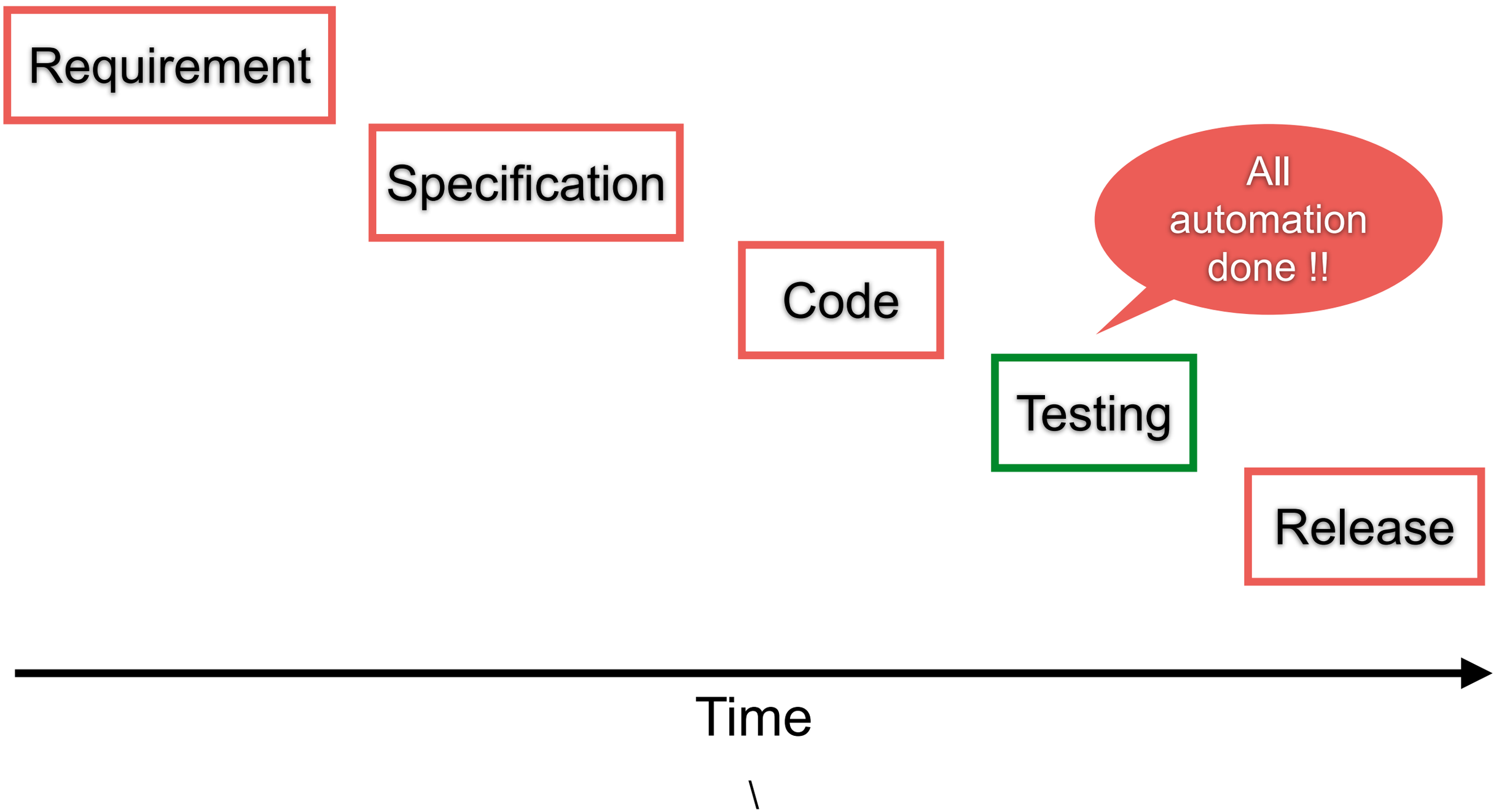
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Automation test strategy

\

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

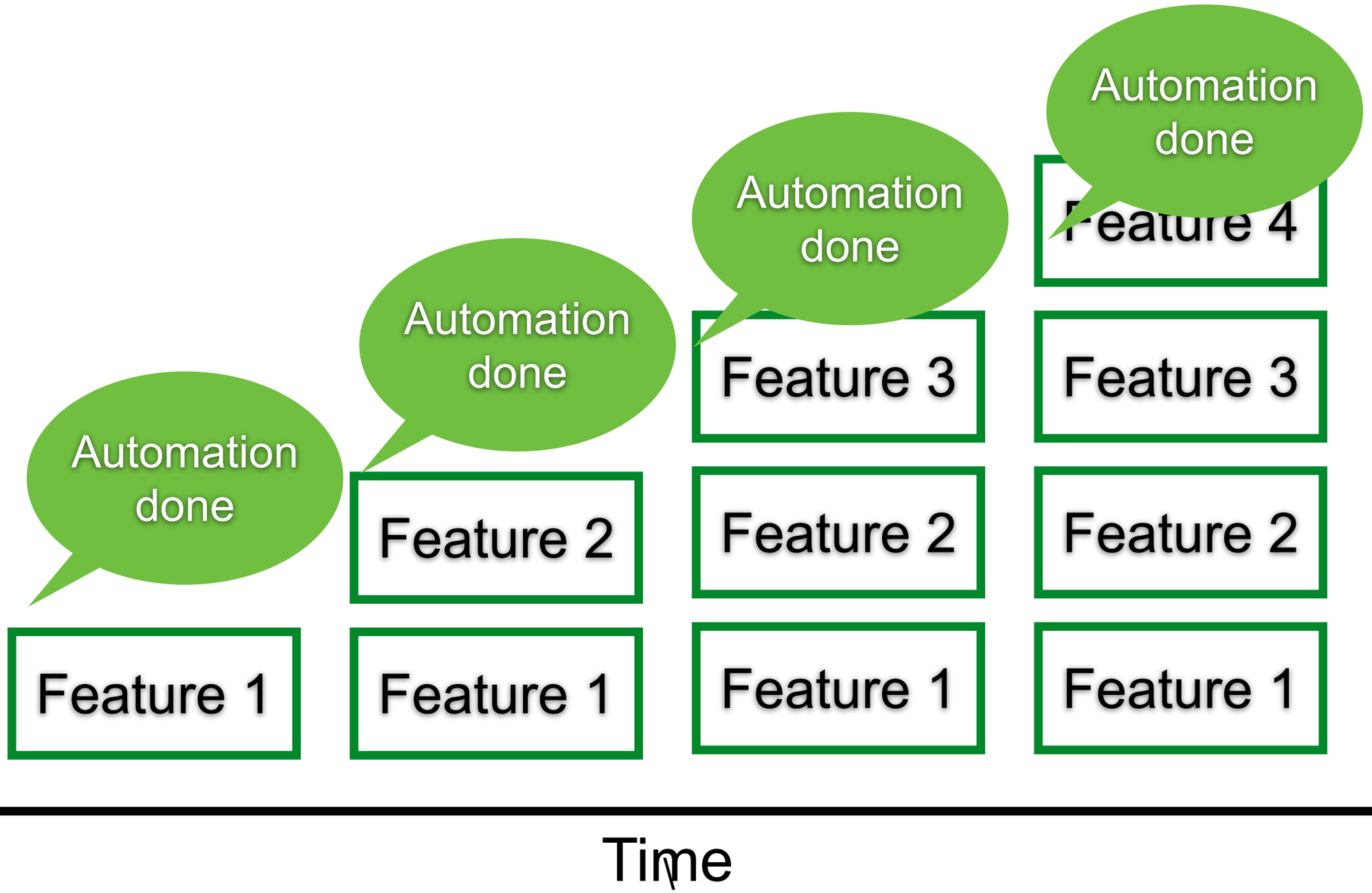
Sequential process



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Iterative and incremental process

Done = coded and tested



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Testing Types

Unit

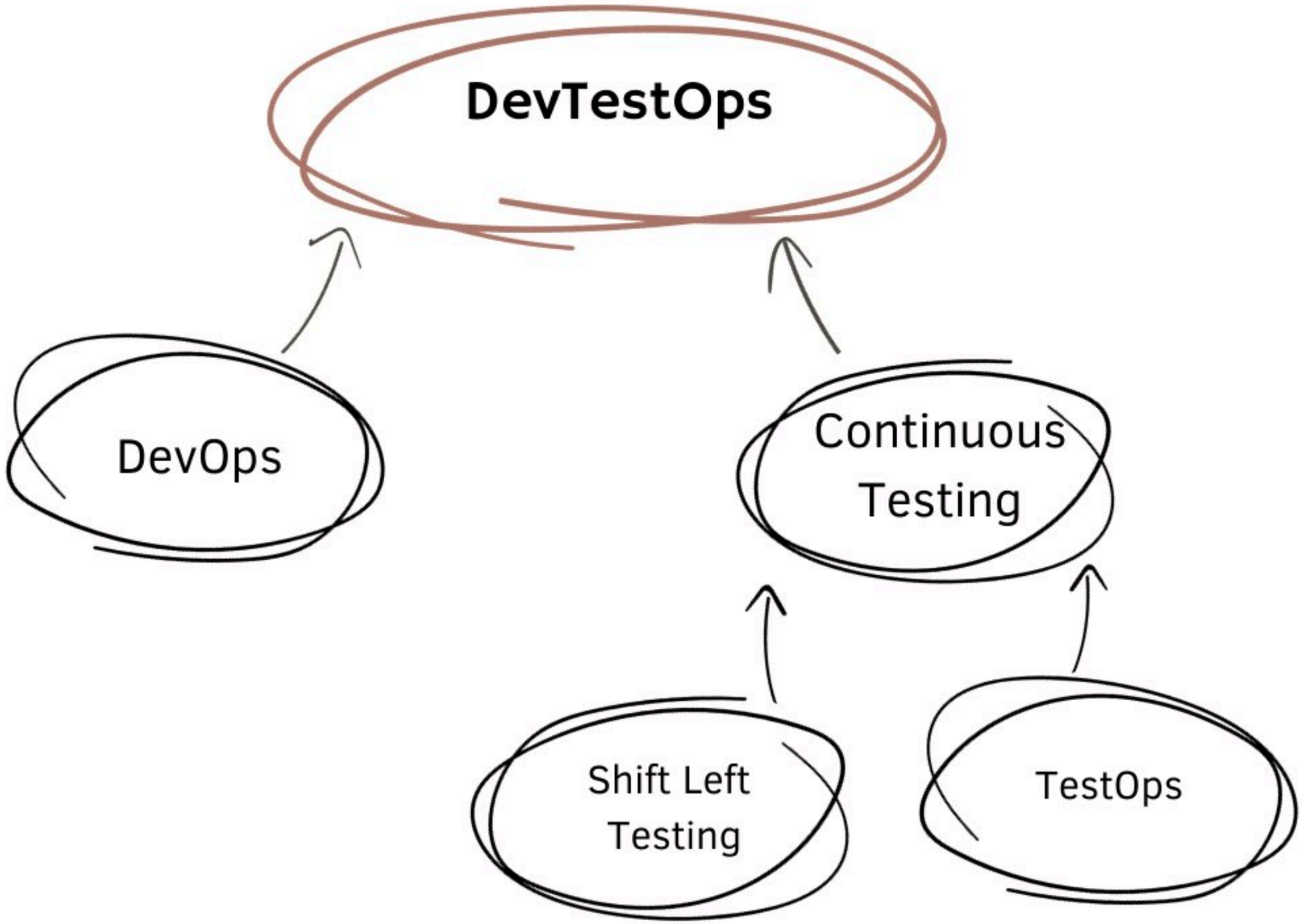
Integration

Component

Contract

End-to-End

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Security Testing

\

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Security Testing ?

Identify all possible weakness of system
Impacts to system

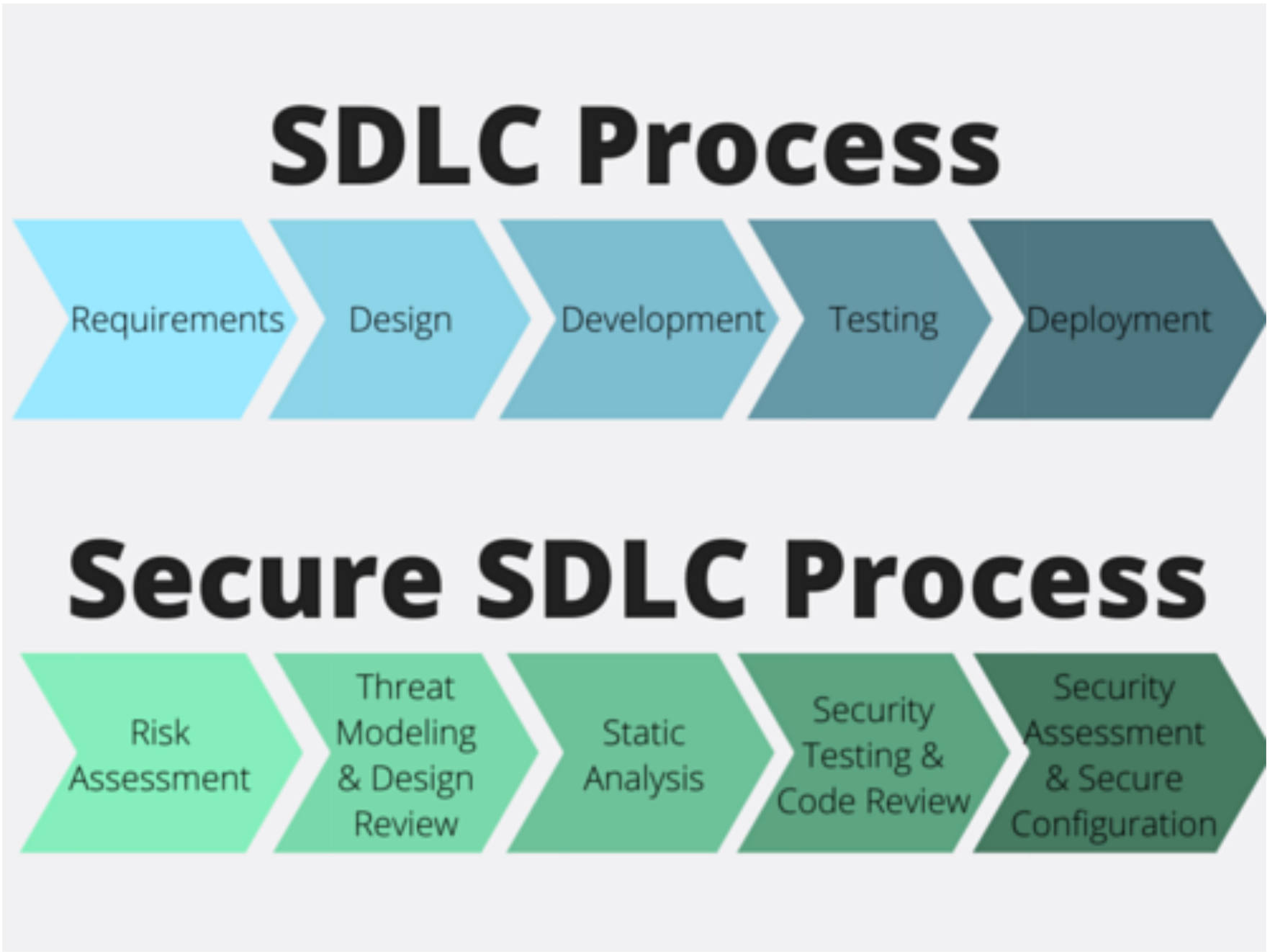
Loss information	Loss revenue	Loss your business

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Types of Security Testing

Vulnerability Scanning	Security scanning	Penetration testing
Security auditing	Posture assignment	Ethical hacking

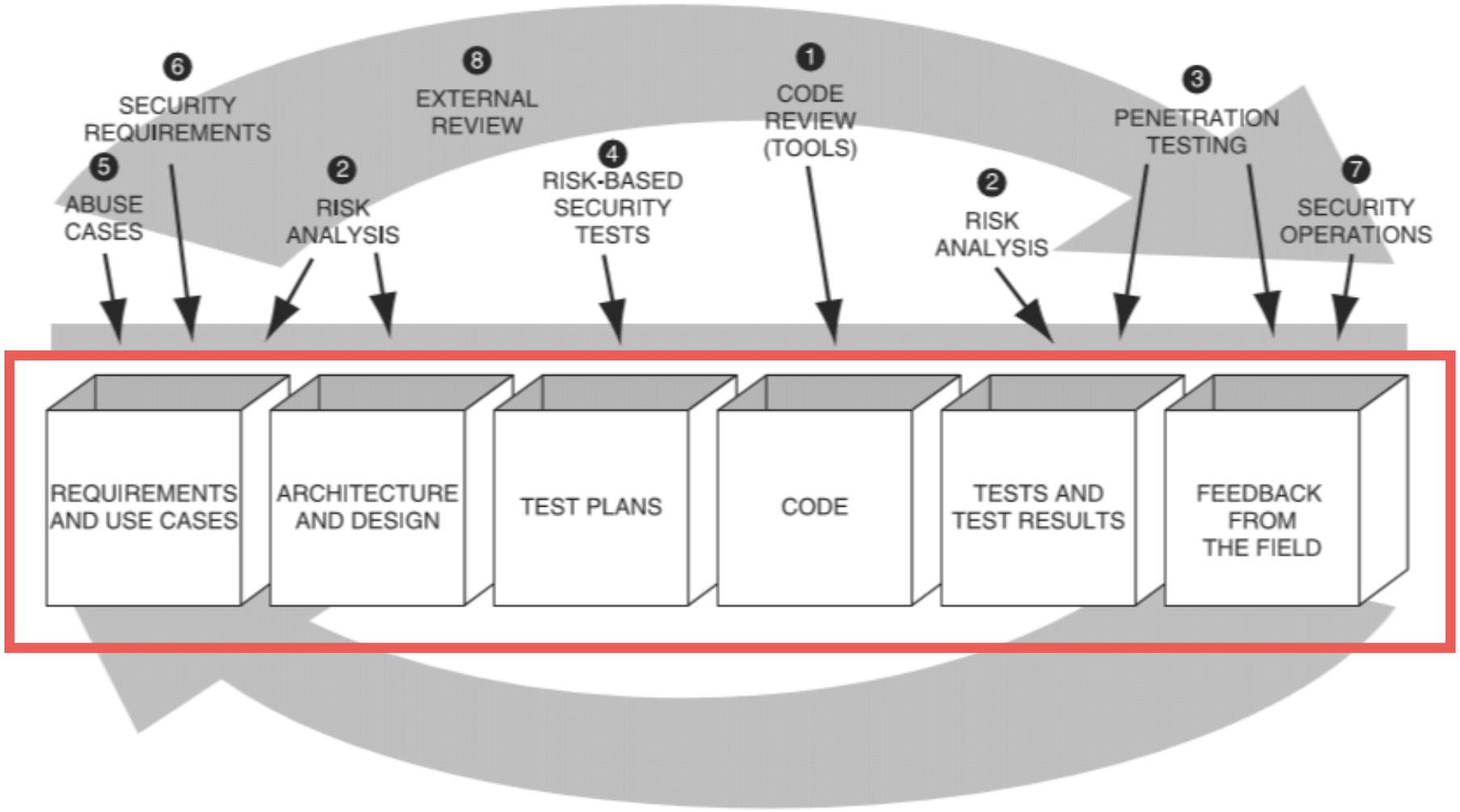
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.



https://checkmarx.com/glossary/a-secure-sdlc-with-static-source-code-analysis-tools/

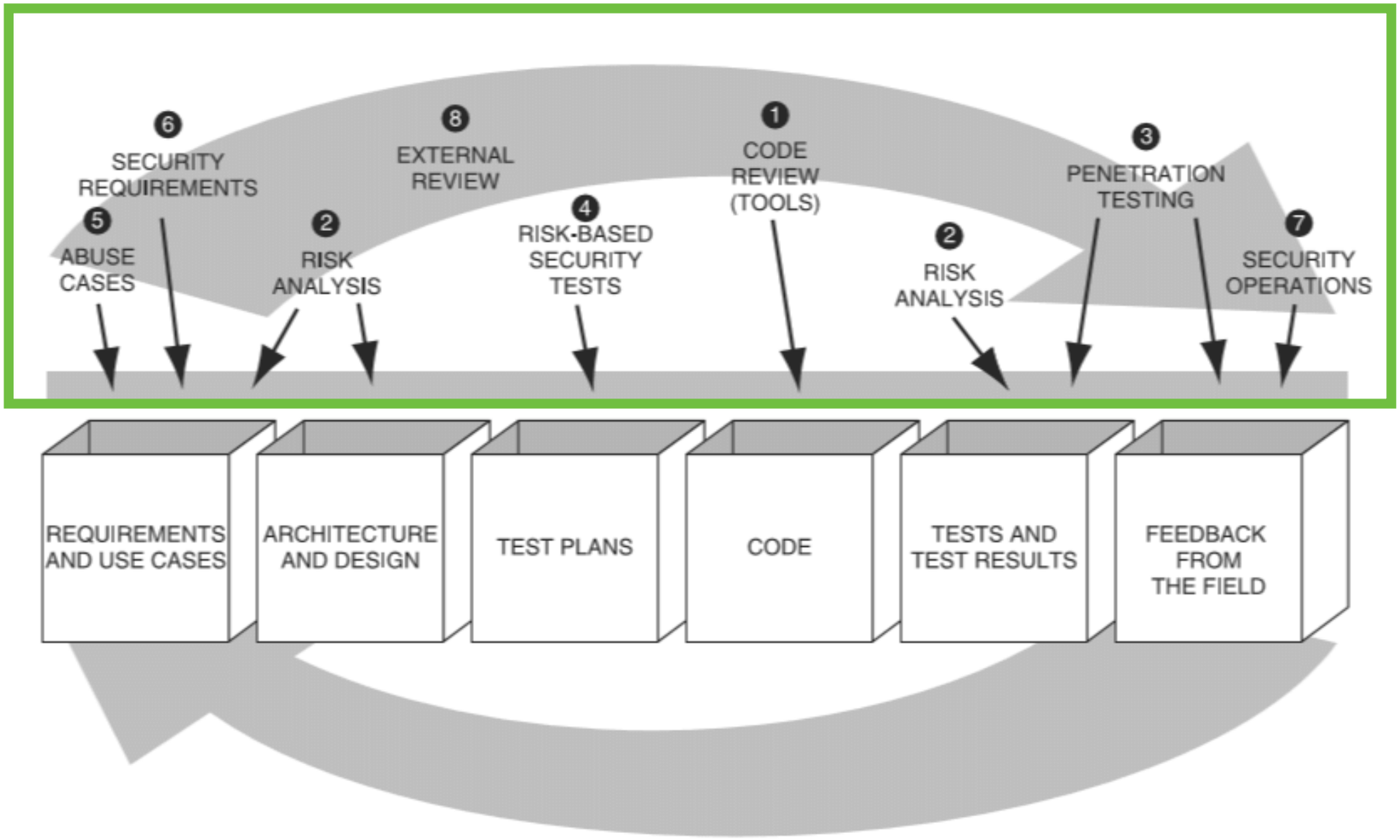
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Secure Software Development process



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Secure Software Development process



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Microsoft Security Development

Education

Administer and track security training

Process

Guide product teams to meet SDL requirements

Accountability

Establish release criteria and sign-off as part of FSR

Incident Response (MSRC)

Training	Requirements	Design	Implementation	Verification	Release	Response
• Core training	• Define quality gates/bug bar • Analyze security and privacy risk	• Attack surface analysis • Threat modeling	• Specify tools • Enforce banned functions • Static analysis	• Dynamic/Fuzz testing • Verify threat models/attack surface	• Response plan • Final security review • Release archive	• Response execution

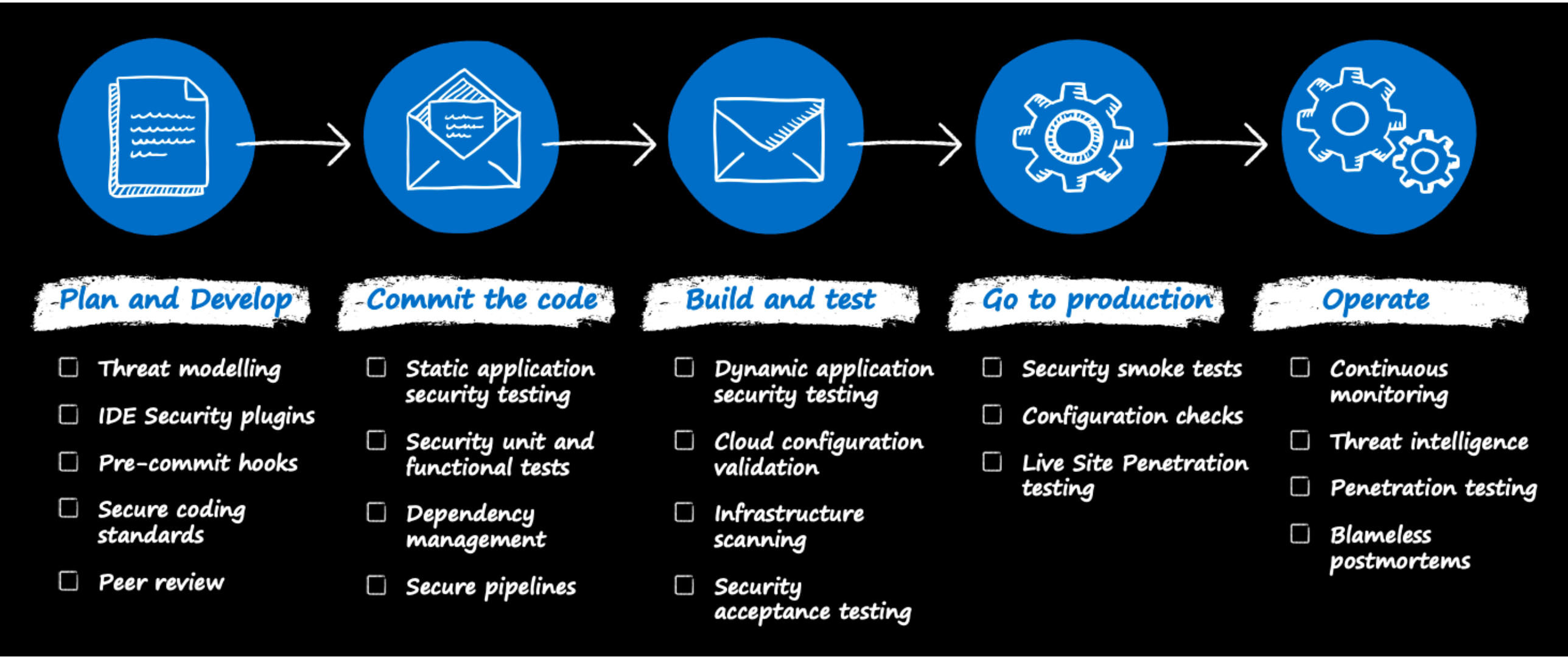
Ongoing Process Improvements

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Risk	People	Roles and responsibility
	Process	Activity, Deliverable, Control gate
	Knowledge	Standard and guideline Compliance
	Tool & Component	Development support Assessment tool Management tools

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

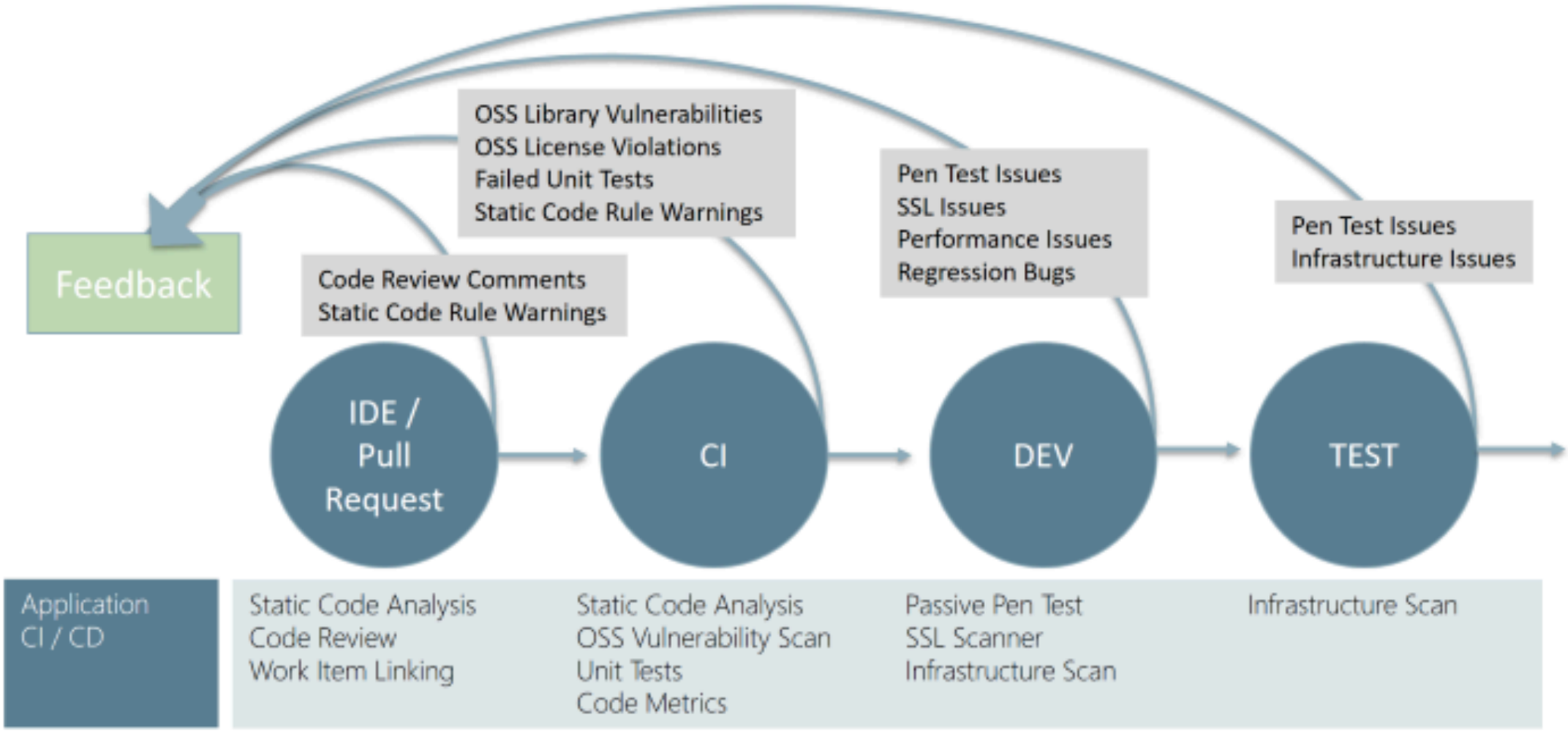
Pipeline to Deliver



https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

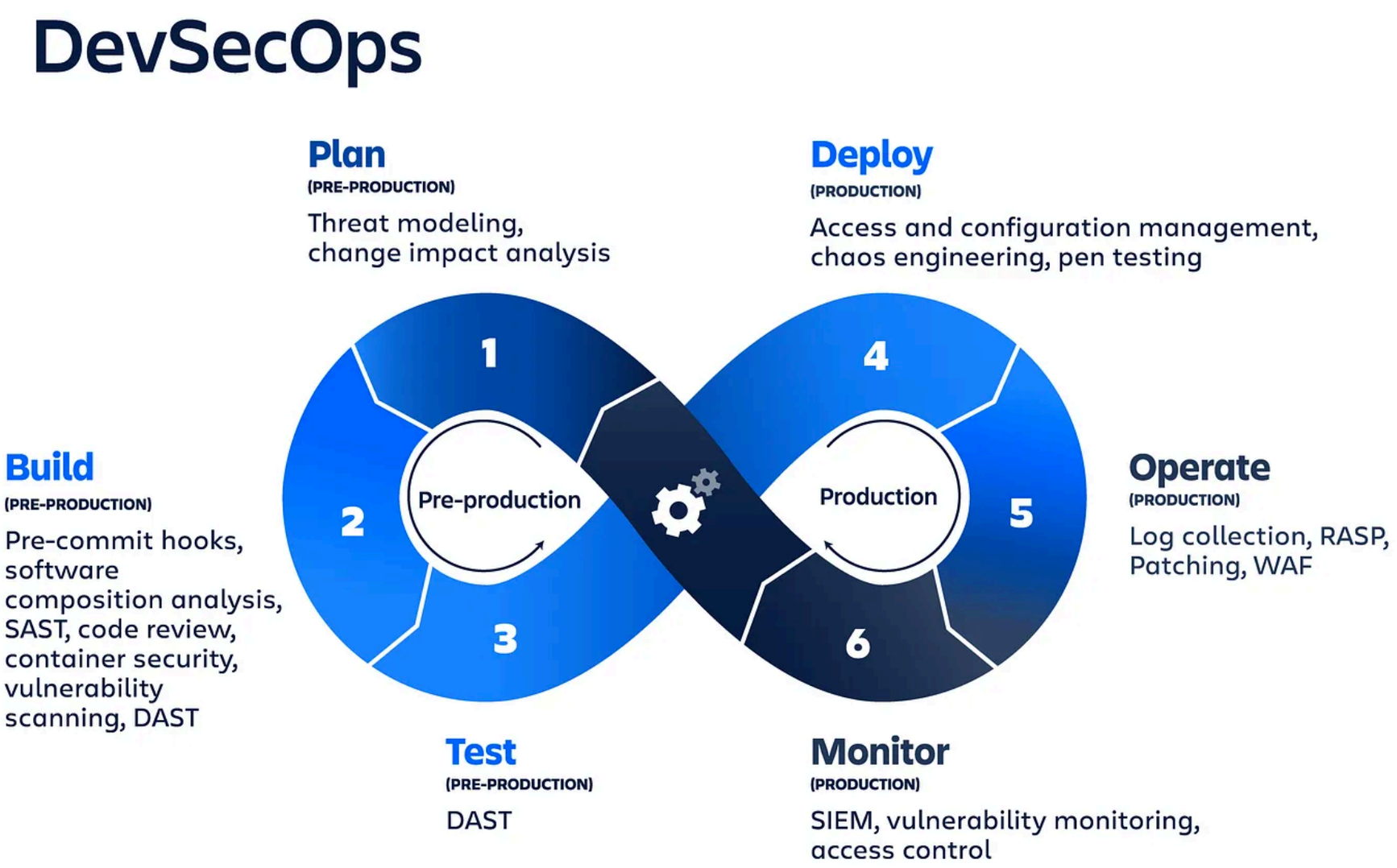
Feedback Loops



https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

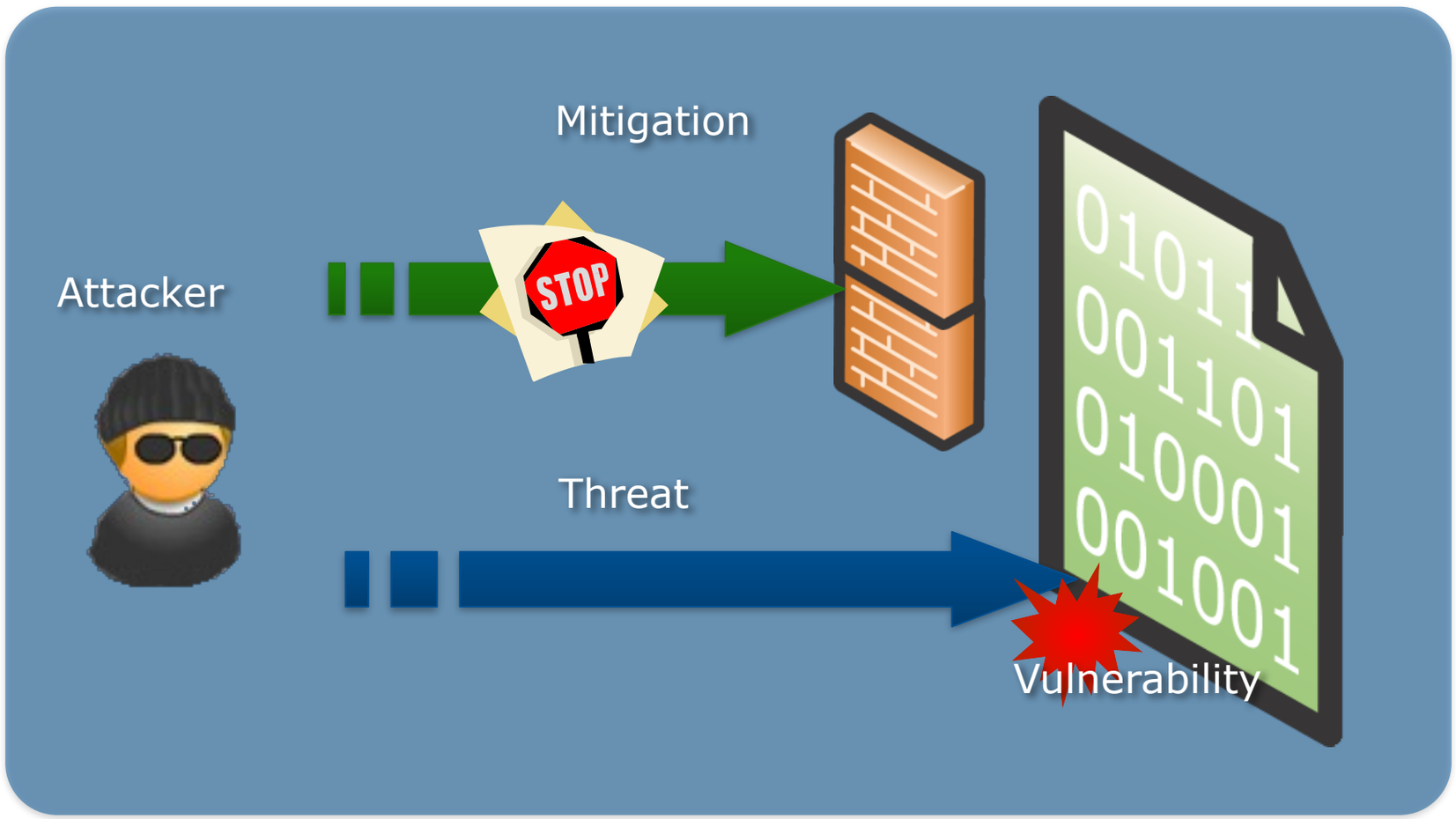
DevSecOps



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

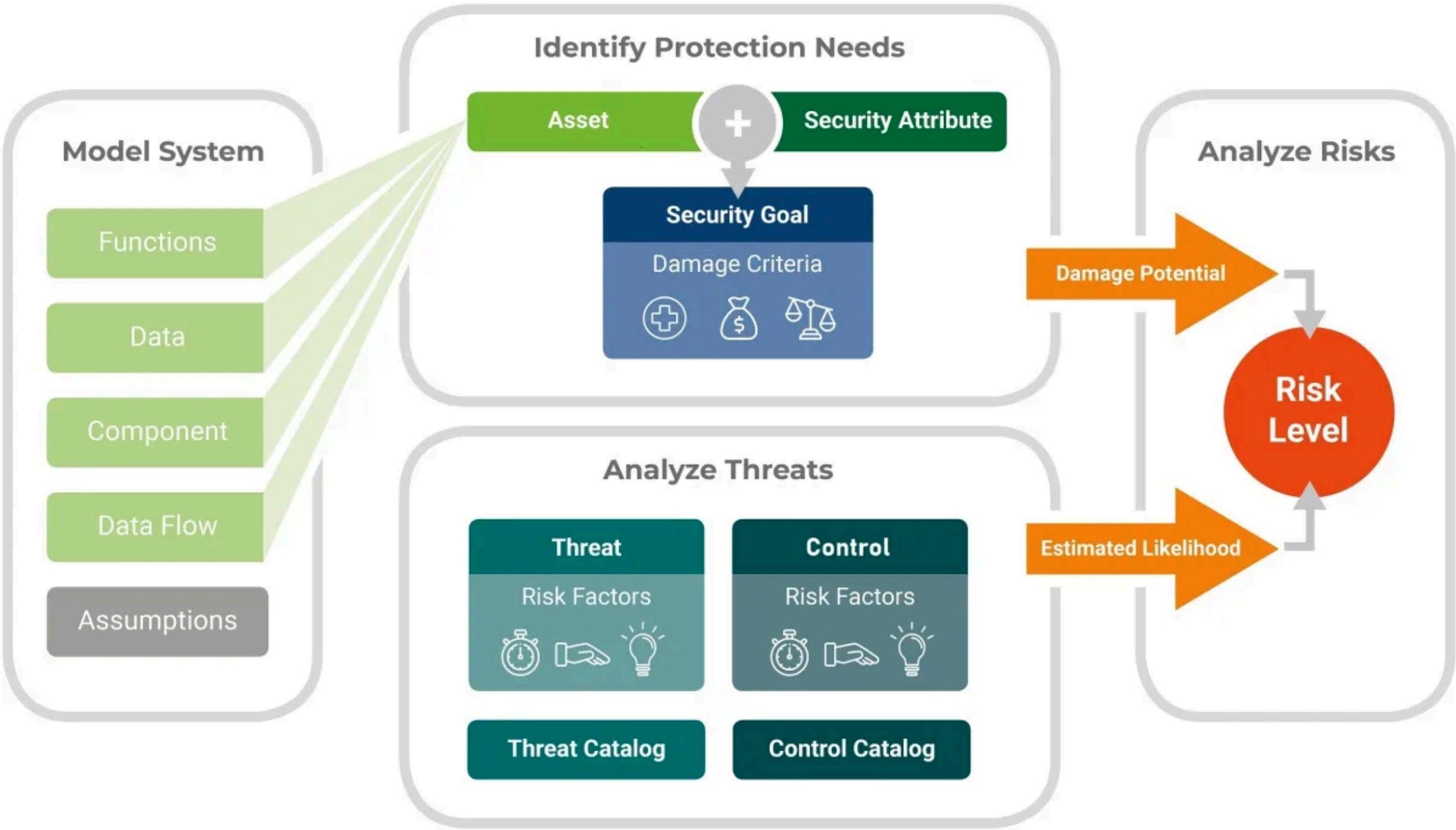
Secure Design

Threat Analysis
Secure software start with understanding the threats



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Threat Analysis



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Threat Modeling from OWASP

What are we working on ?
What can go wrong ?
What are we going to do about it ?
Did we do a good enough job ?

https://owasp.org/www-community/Threat_Modeling

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Test Plan with Security ?

\

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Test Plan with Security ?

Security related test cases and scenarios
Test data related to security testing
Test tools required for security testing
Analysis of various test outputs from security tools

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Example of test scenarios

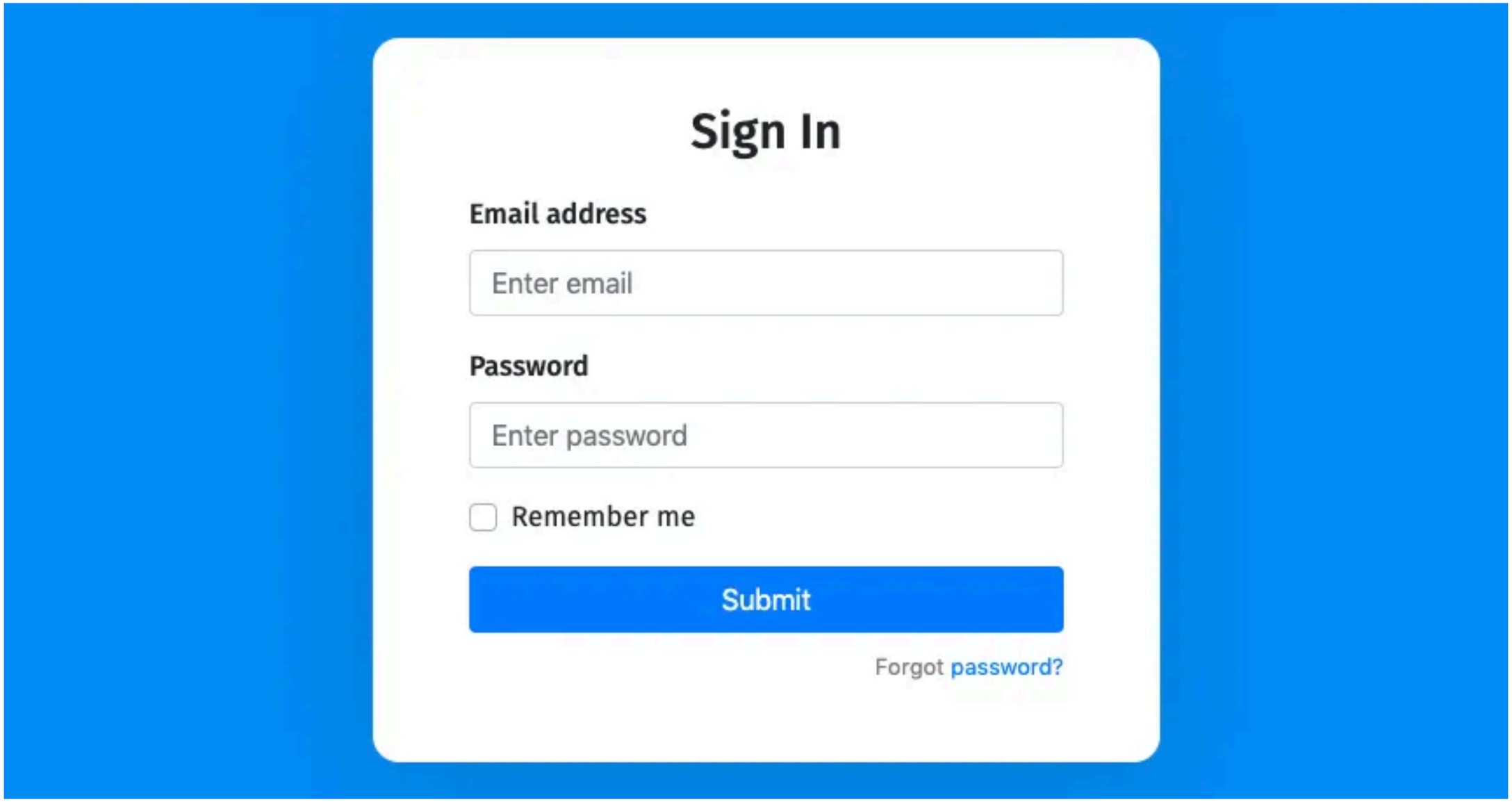
Password should be in encrypt format

System should not allow invalid users

Check data in web browser eg. Cookie, local storage

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Workshop with Login Page

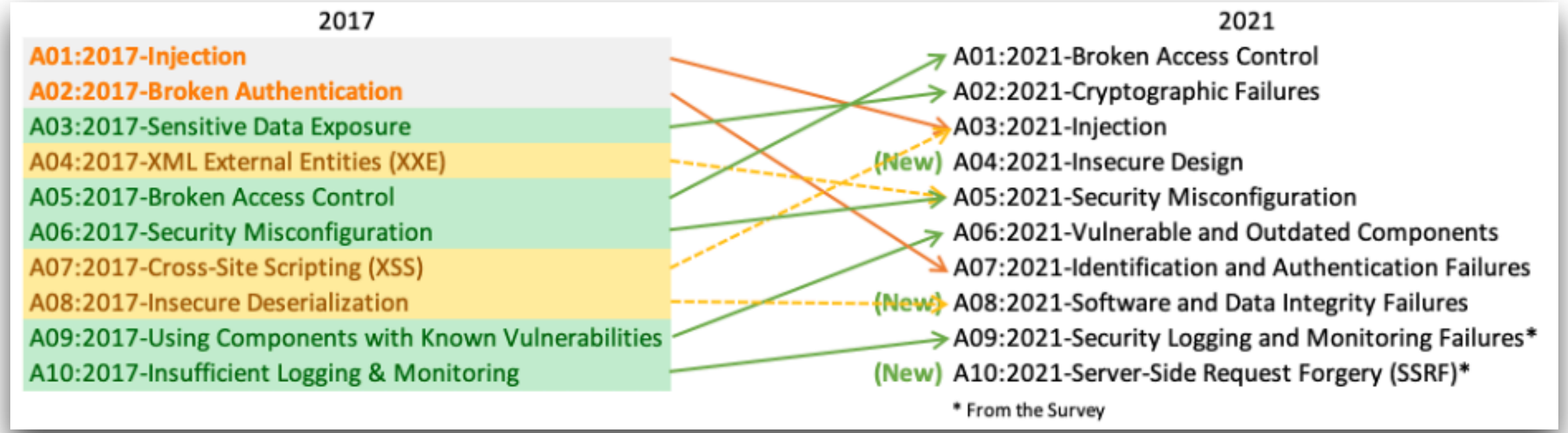


© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Design test scenarios with security ?

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

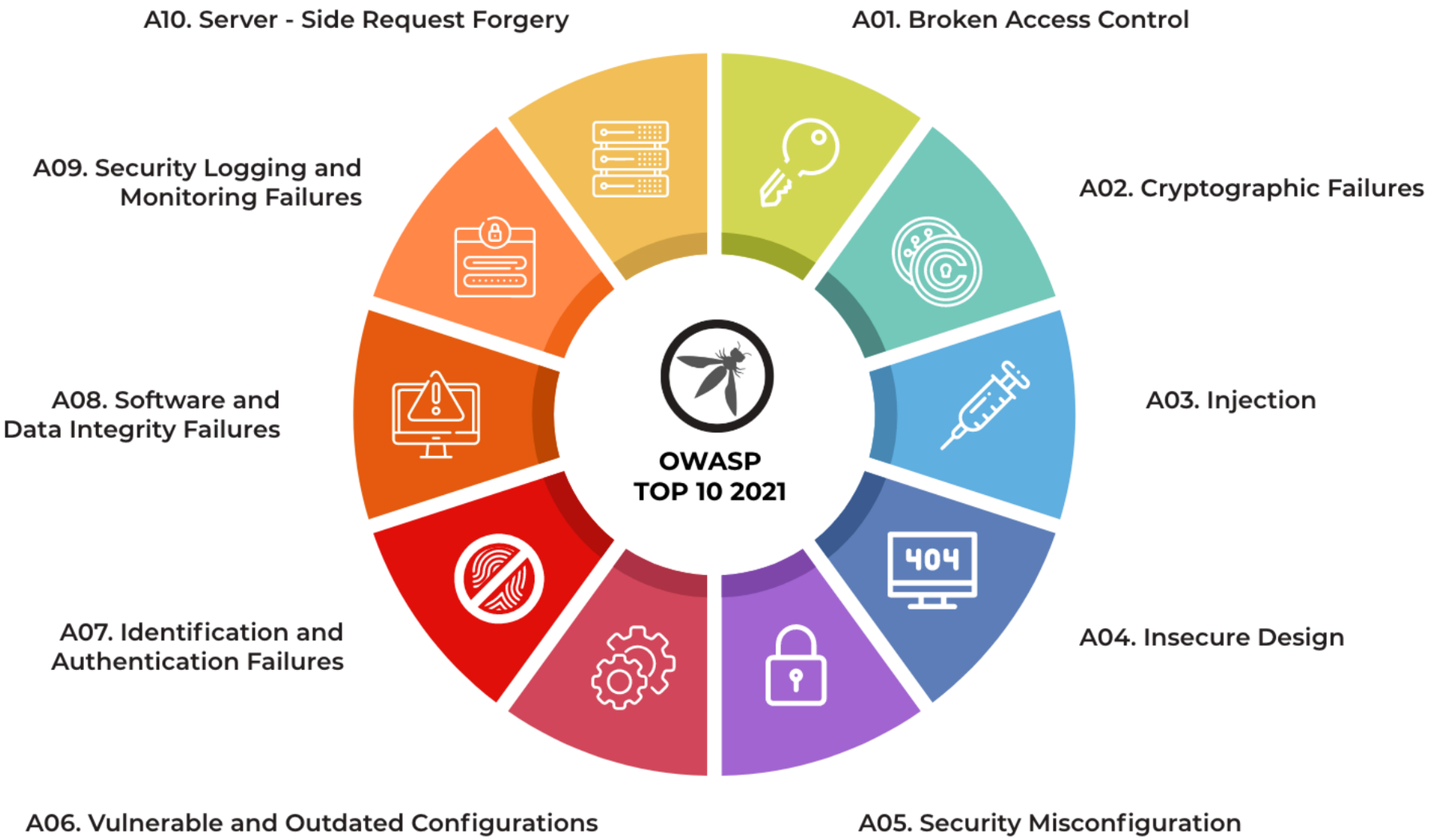
Top 10 Web Application Security Risks



https://owasp.org/www-project-top-ten/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Top 10 Web Application Security Risks



https://owasp.org/www-project-top-ten/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

What to test ?

HTTPS and data encryption

Data/SQL Injection

Cross-Site Scripting (XSS)

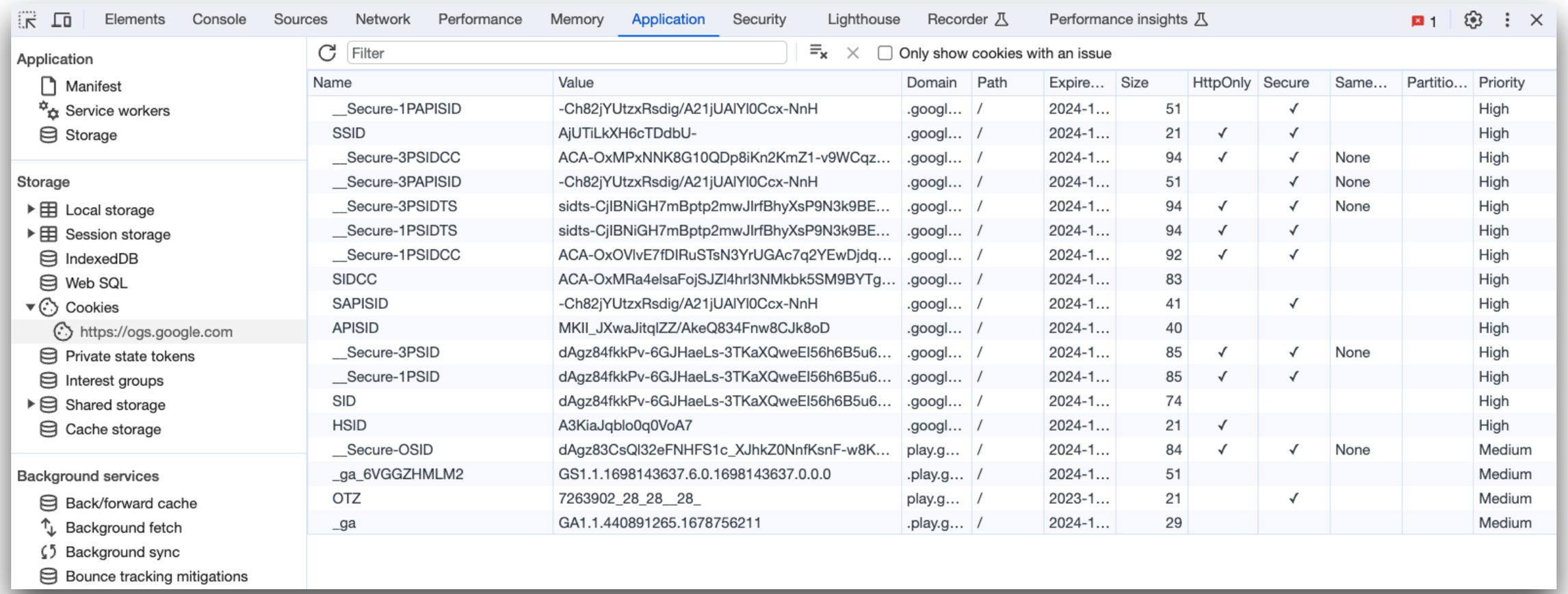
Brute-force attack

Secure cookie in browser, HttpOnly

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Google Chrome

Inspect -> Application



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

OWASP Application Security Verification Standard

Input Validation, Sanitization and Encoding

Control Objective

The most common web application security weakness is the failure to properly validate input coming from the client or the environment before directly using it without any output encoding. This weakness leads to almost all of the significant vulnerabilities in web applications, such as Cross-Site Scripting (XSS), SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

Ensure that a verified application satisfies the following high-level requirements:

- Input validation and output encoding architecture have an agreed pipeline to prevent injection attacks.
- Input data is strongly typed, validated, range or length checked, or at worst, sanitized or filtered.
- Output data is encoded or escaped as per the context of the data as close to the interpreter as possible.

With modern web application architecture, output encoding is more important than ever. It is difficult to provide robust input validation in certain scenarios, so the use of safer API such as parameterized queries, auto-escaping templating frameworks, or carefully chosen output encoding is critical to the security of the application.

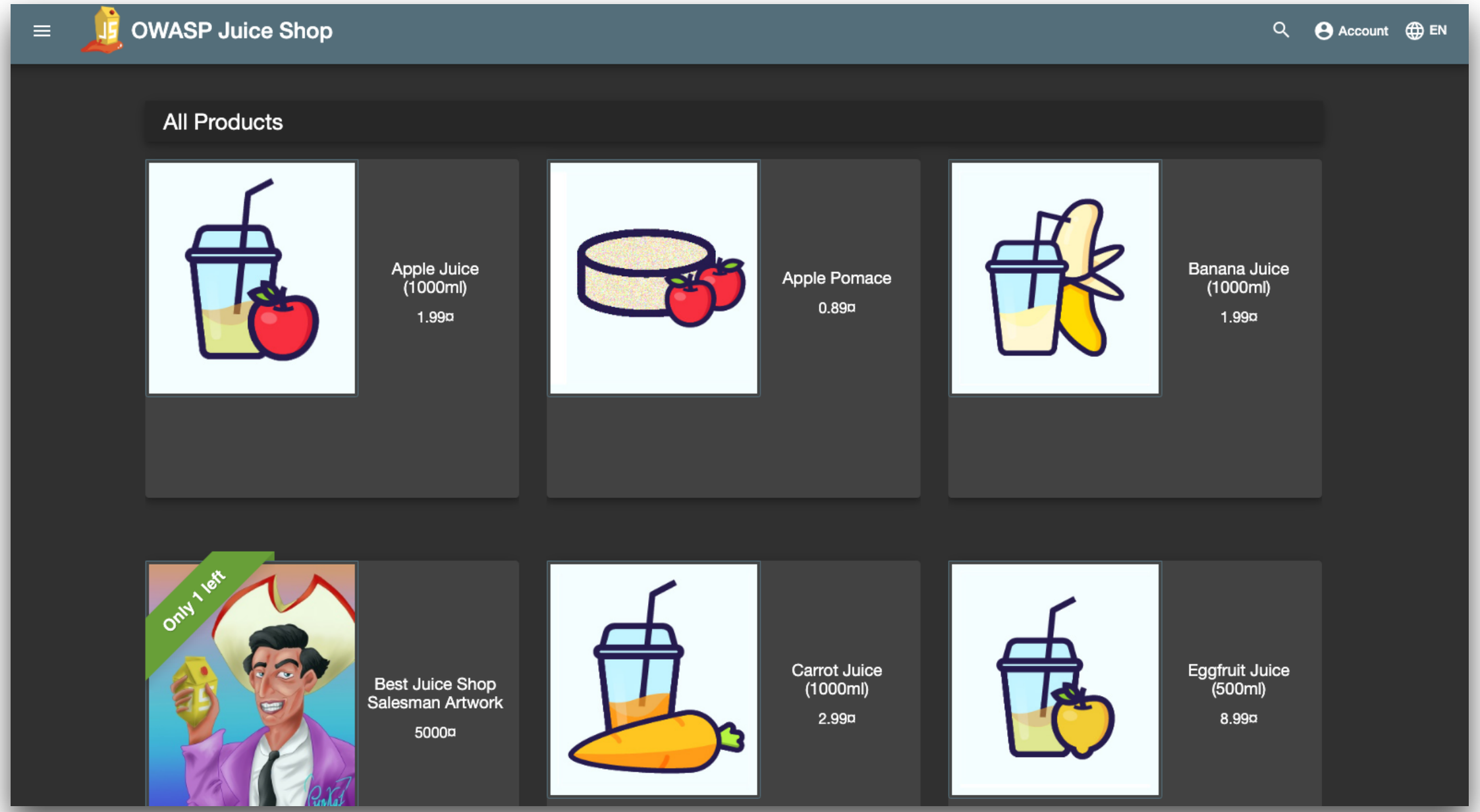
https://owasp.org/www-project-application-security-verification-standard/
https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Workshop

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

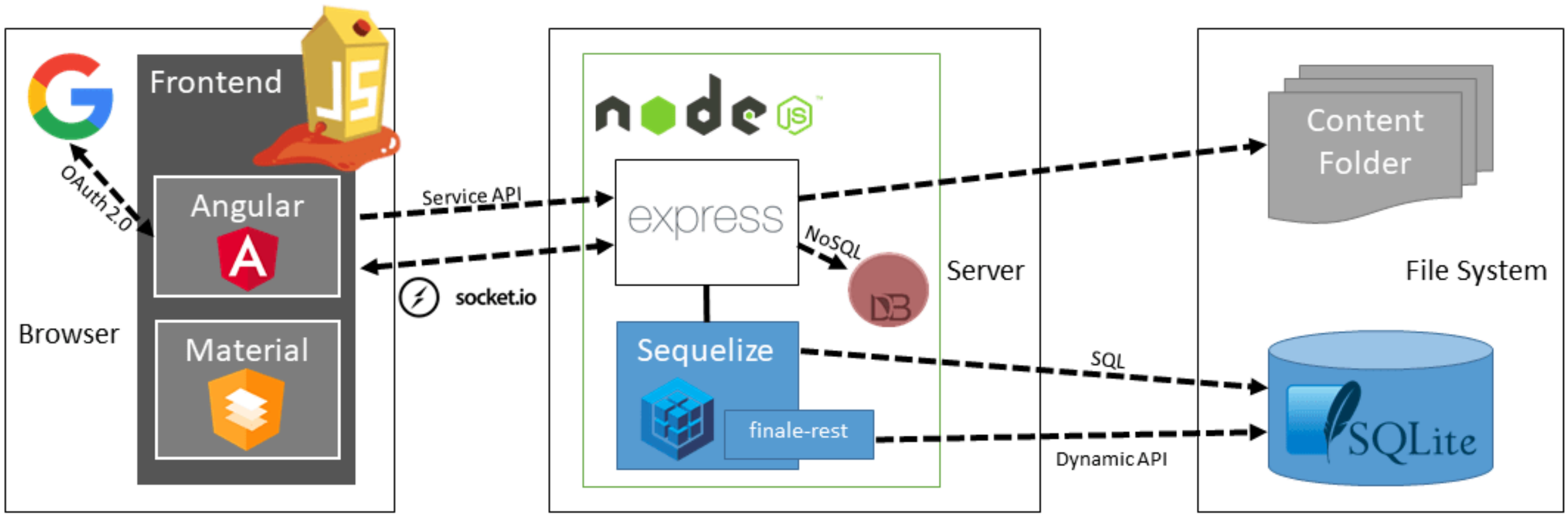
OWASP Juice Shop



https://demo.owasp-juice.shop/#/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

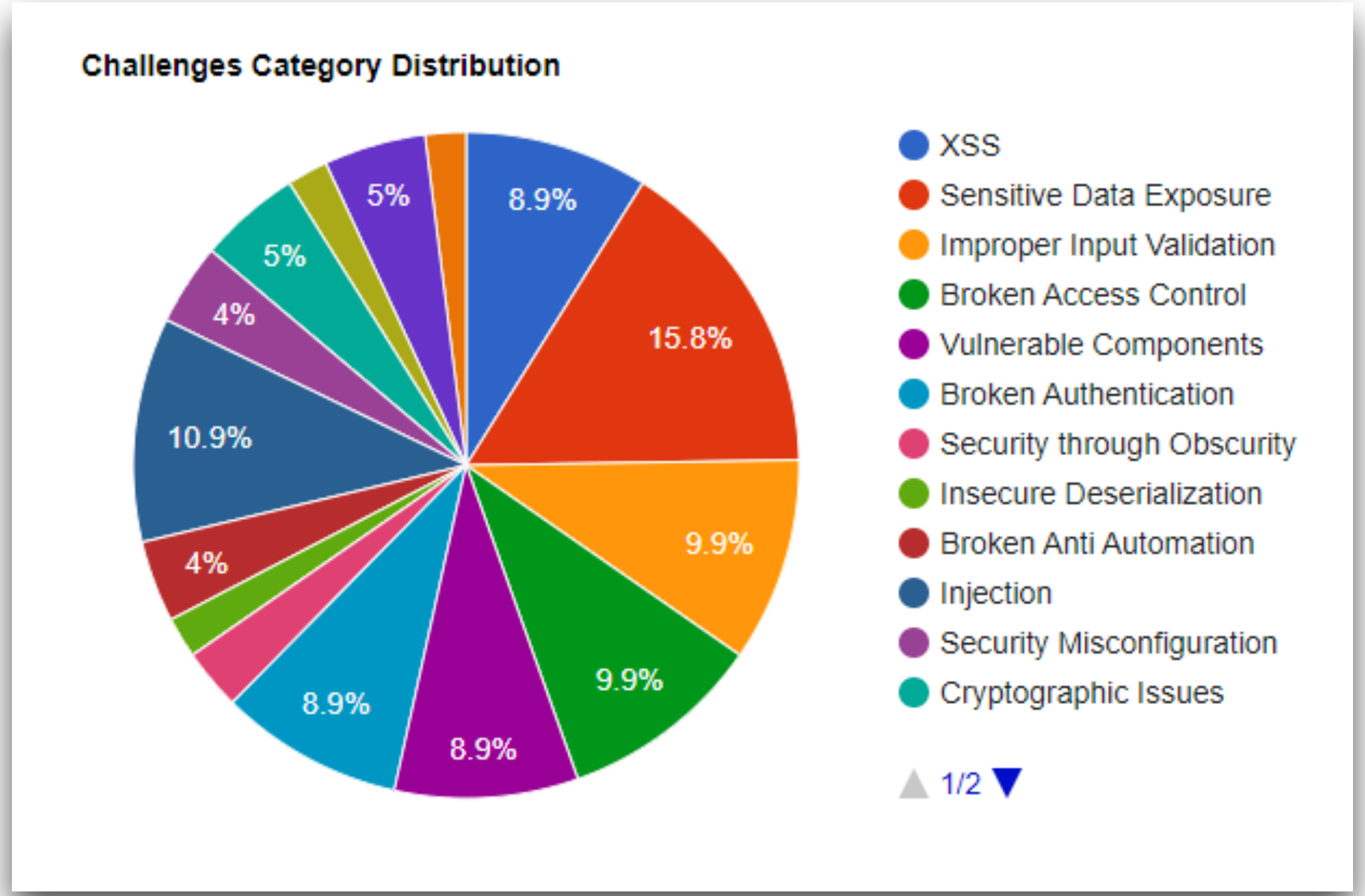
OWASP Juice Shop



https://owasp.org/www-project-juice-shop/

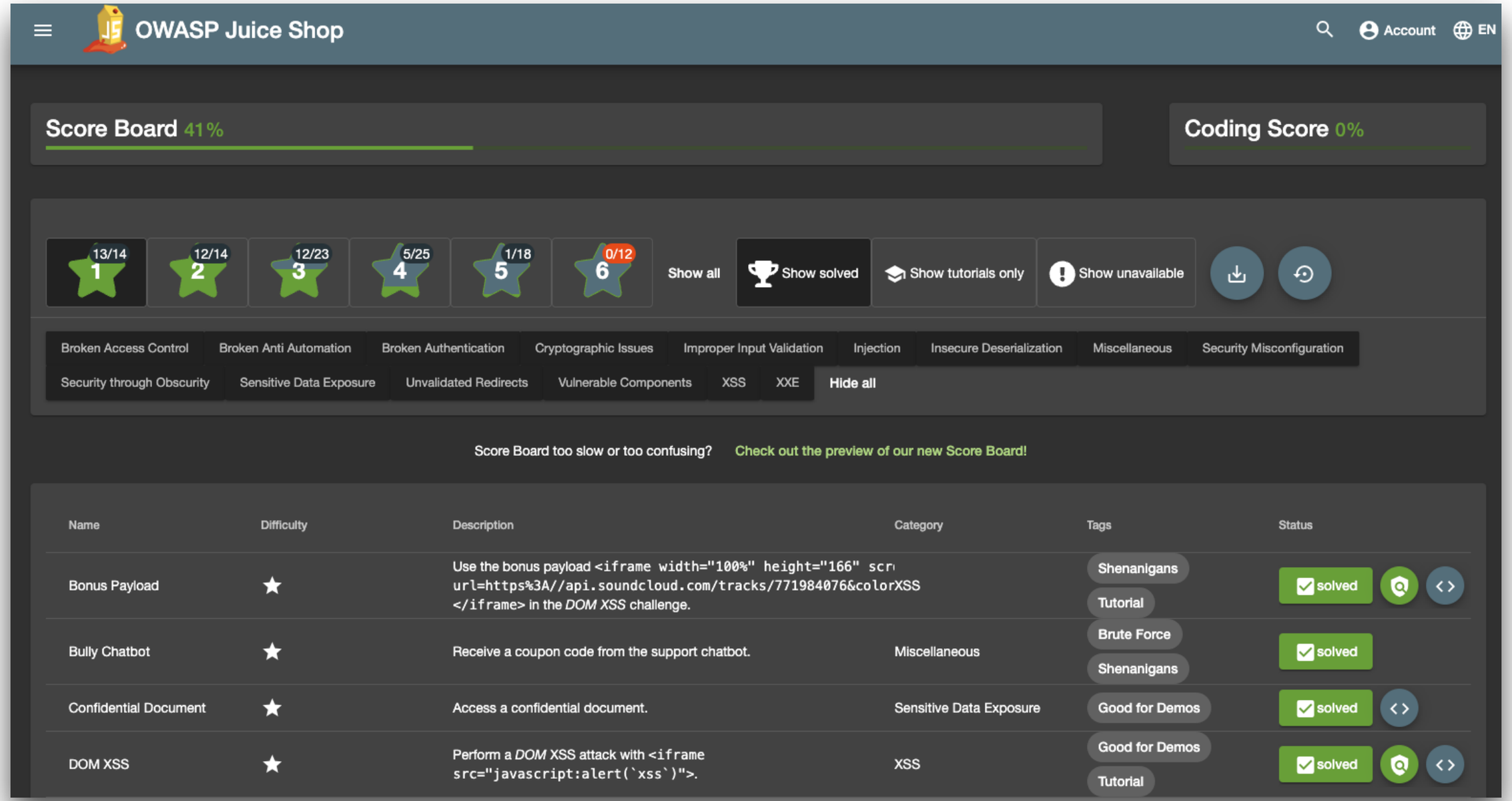
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

OWASP Juice Shop covers all vulnerabilities



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

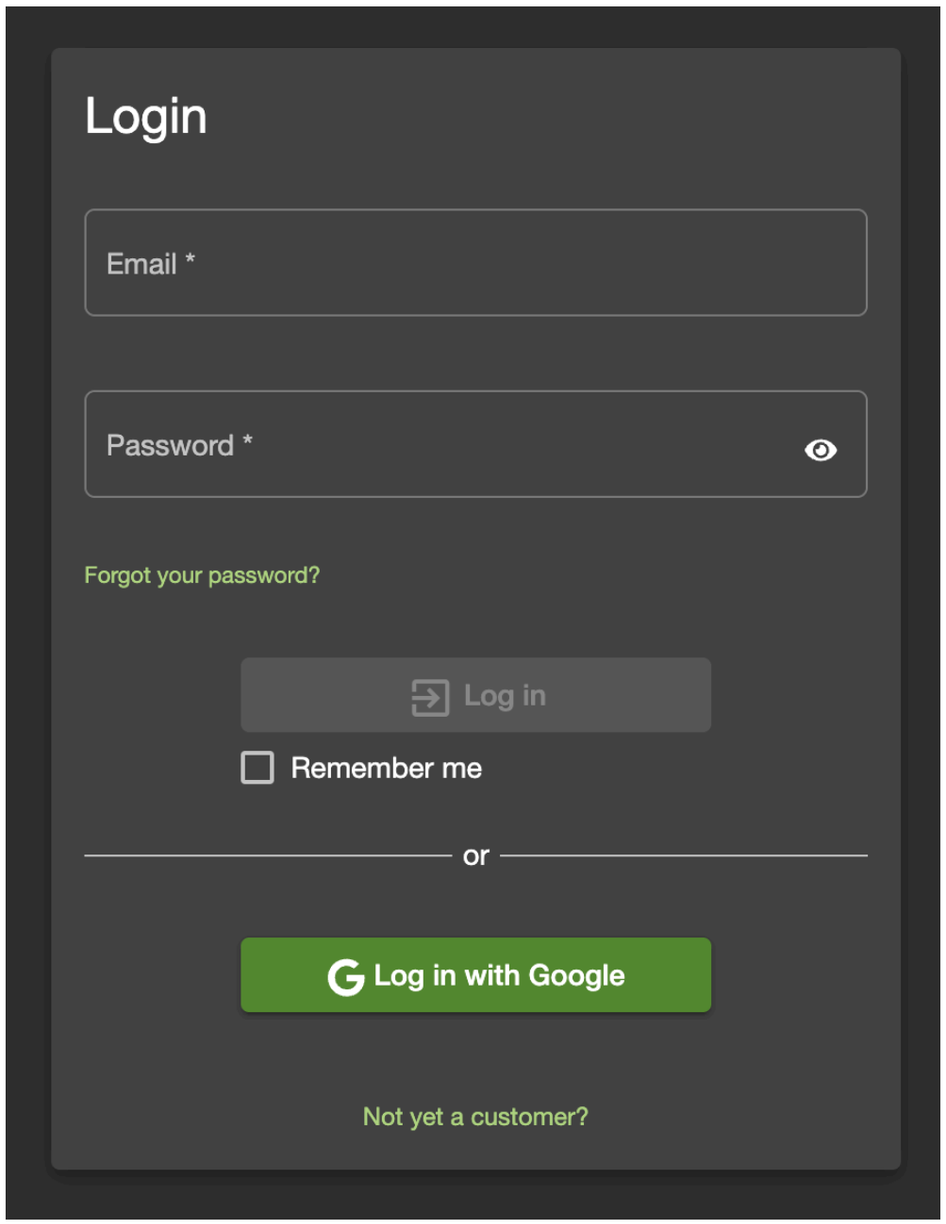
Score Board



https://demo.owasp-juice.shop/#/score-board

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Try to login



https://demo.owasp-juice.shop/#/login

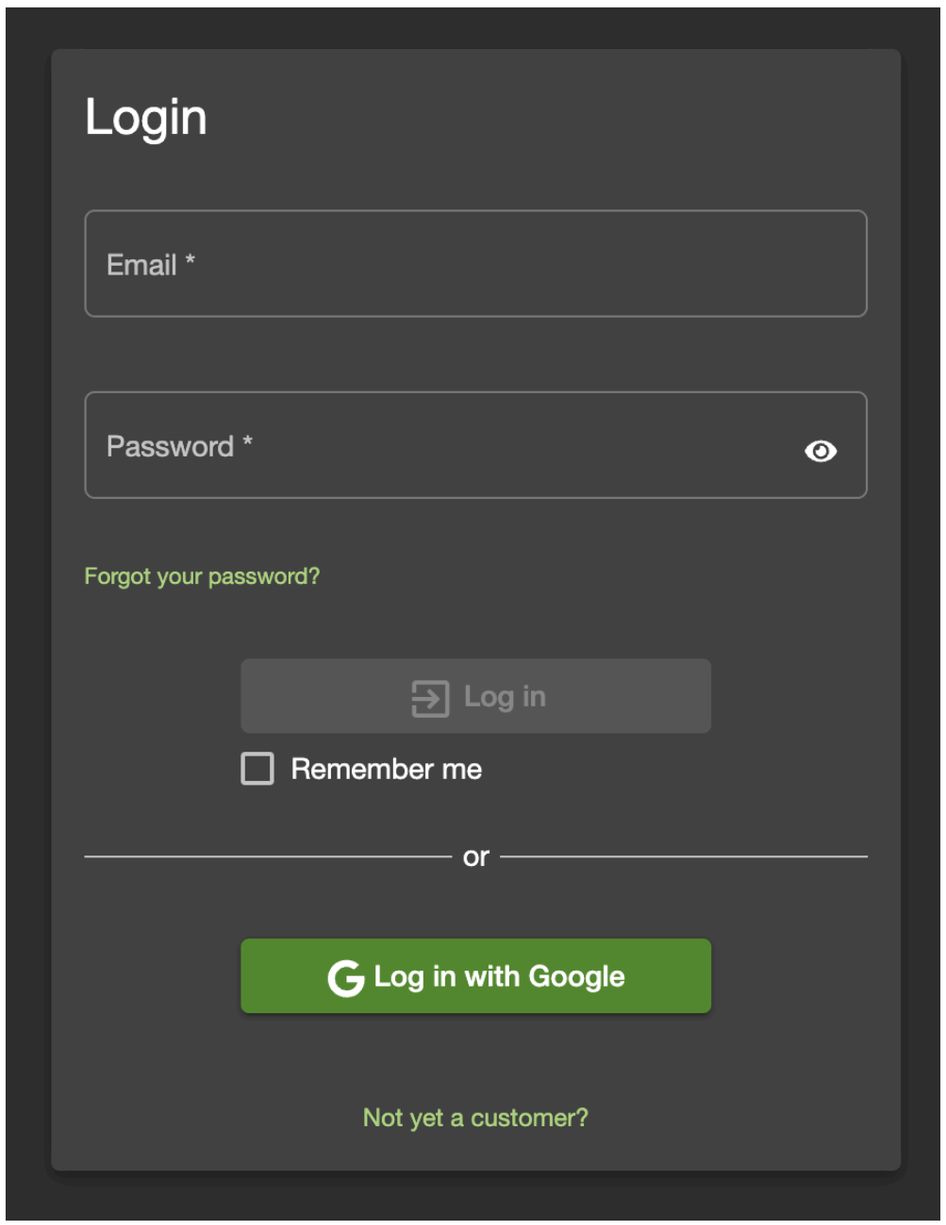
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Test cases

Group of test	Test cases name	Test data
Success case	Valid email and password	
Failure case	Wrong email	
	Wrong password	
	Wrong both email and password	
Edge case	Empty email and password	
	Maximum length of email and password	
Security case	SQL injection in email and password	' OR ‘1'='1 --
	XSS in email and password	<script>alert('XSS')</ script>@example.com

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Try to login with SQL Injection



https://demo.owasp-juice.shop/#/login

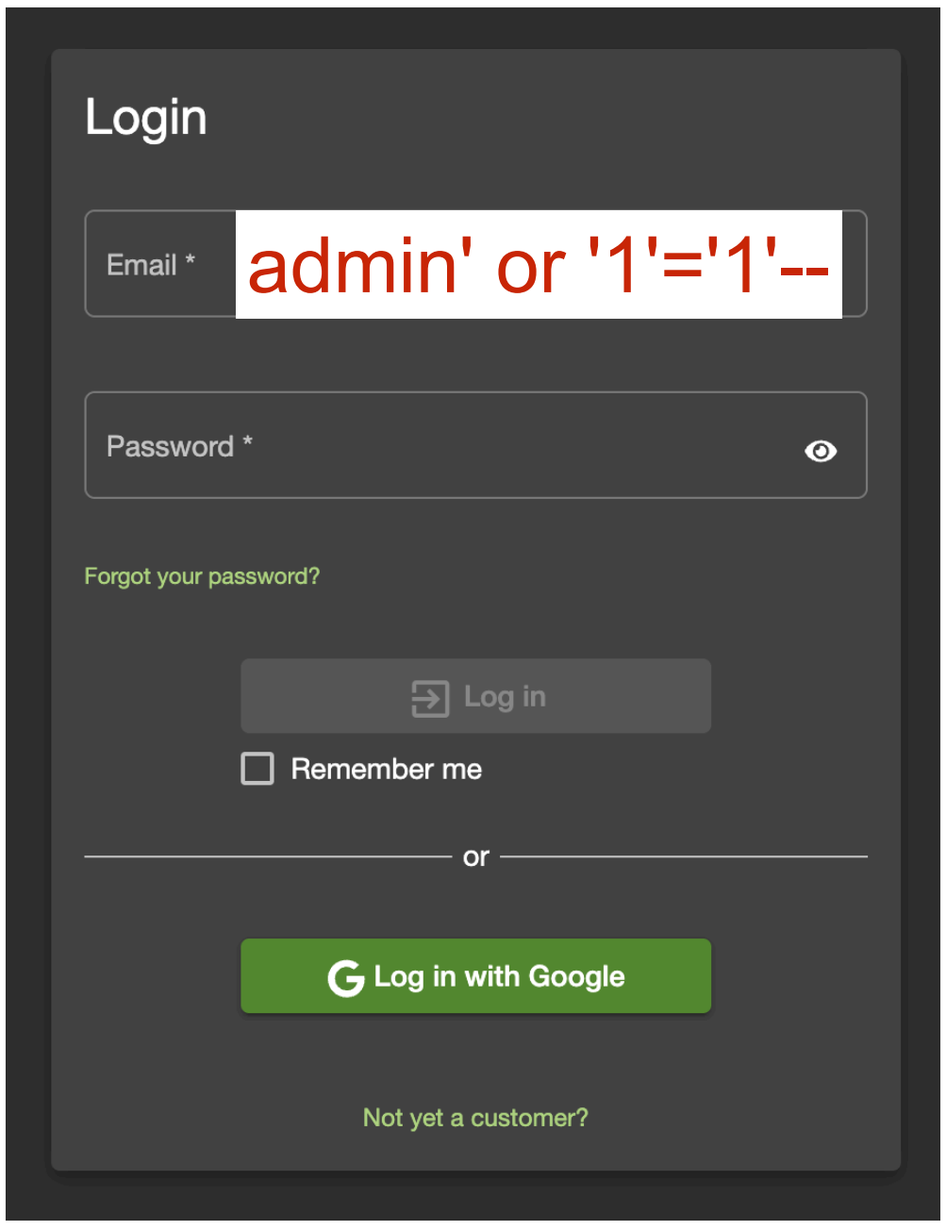
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Example of Inputs

Input	Comments
OR '1'='1	
admin' --	-- = comment in sql
; DROP TABLE users; --	
admin' OR '1'='1	
admin' or '1'='1'--	
"><script>alert('Injected')</script>	Code Injection
; DROP TABLE users; --	

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

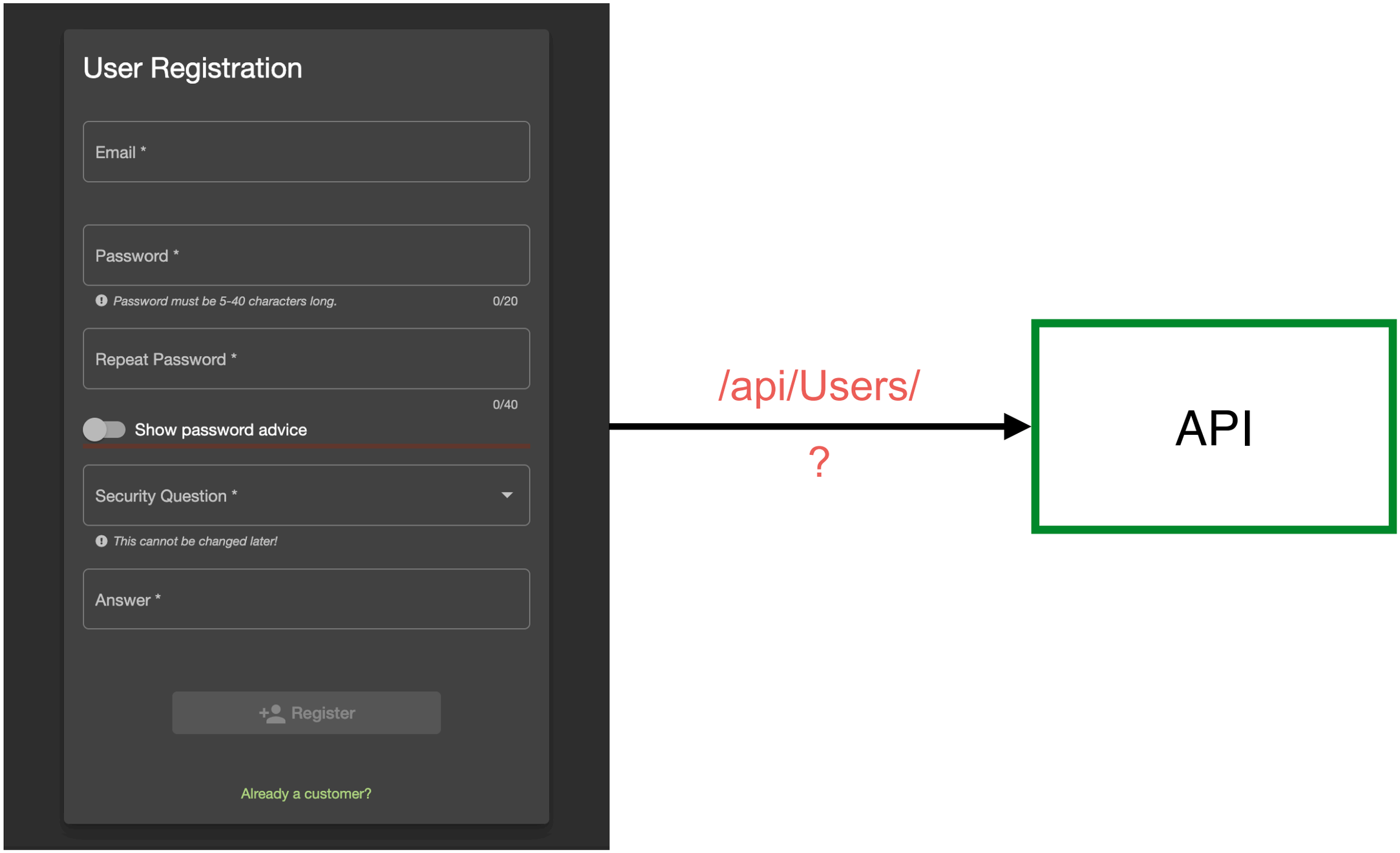
Try to login with SQL Injection



https://demo.owasp-juice.shop/#/login

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Register



https://demo.owasp-juice.shop/#/register

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Secure User Login ?

Password hashing

Salt the hash

Use HTTPS

Account lock

2FA

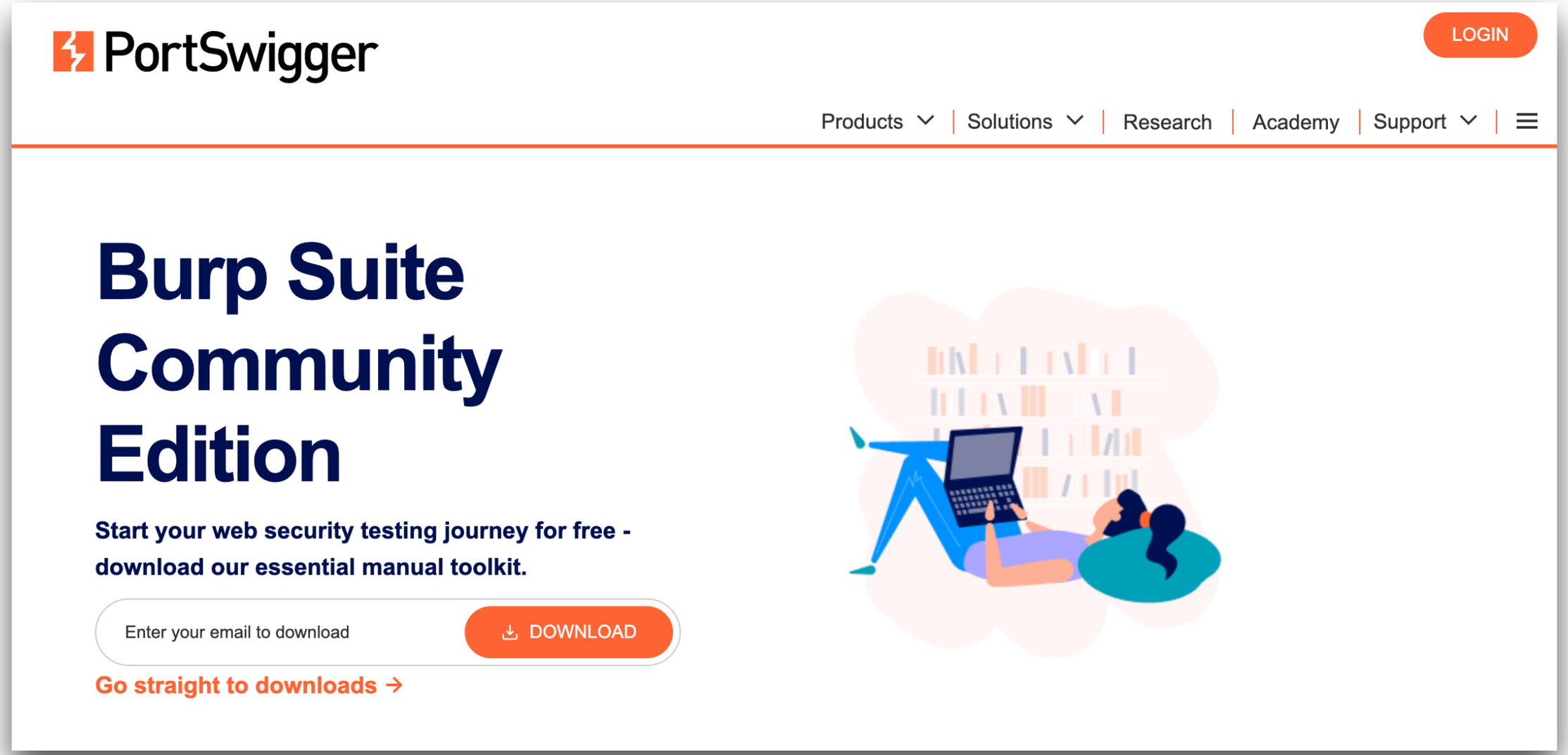
Password policy

Secure cookies

Avoid information leak

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Tools

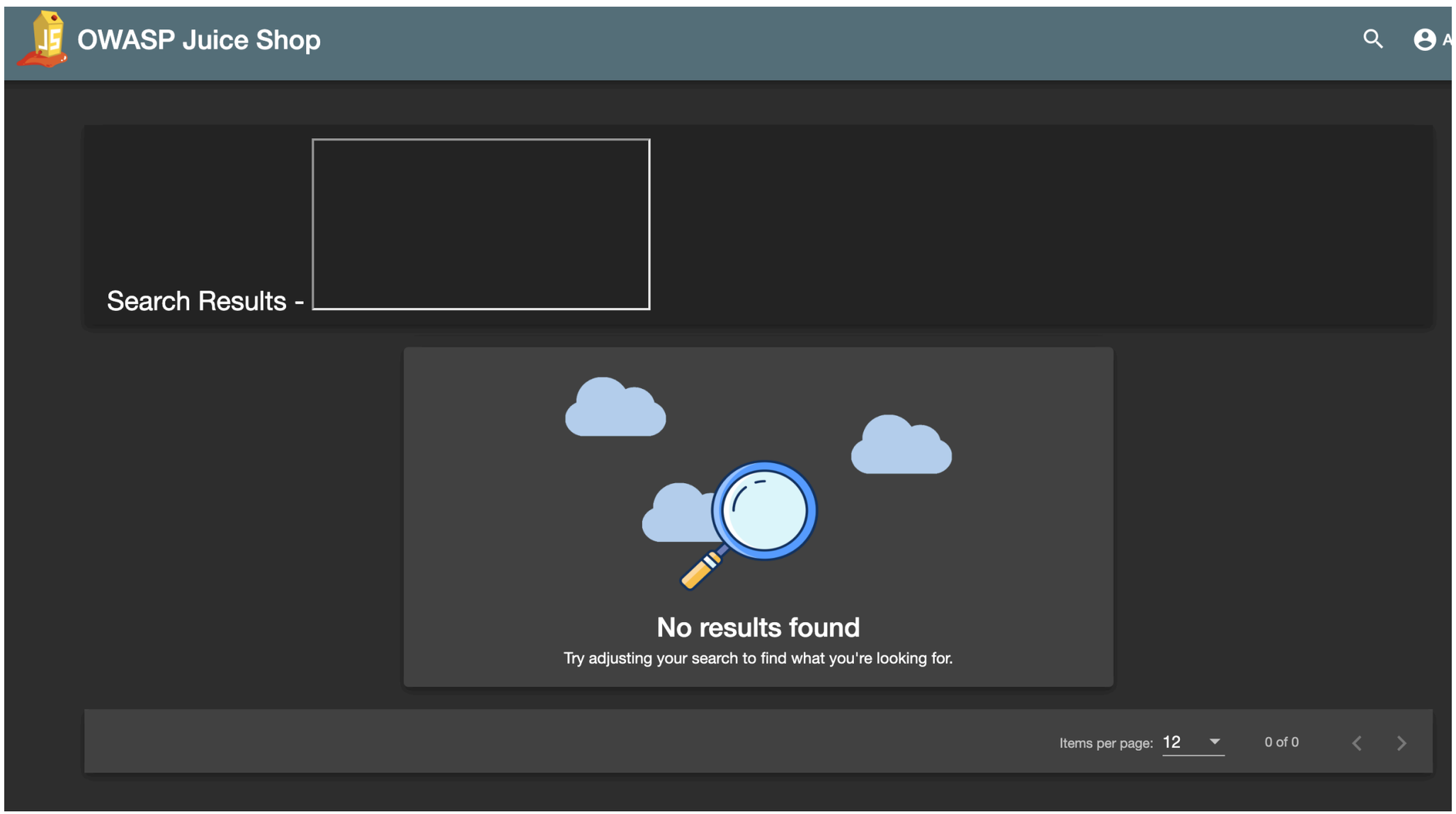


https://portswigger.net/burp/communitydownload

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Cross Site Scripting (XSS)

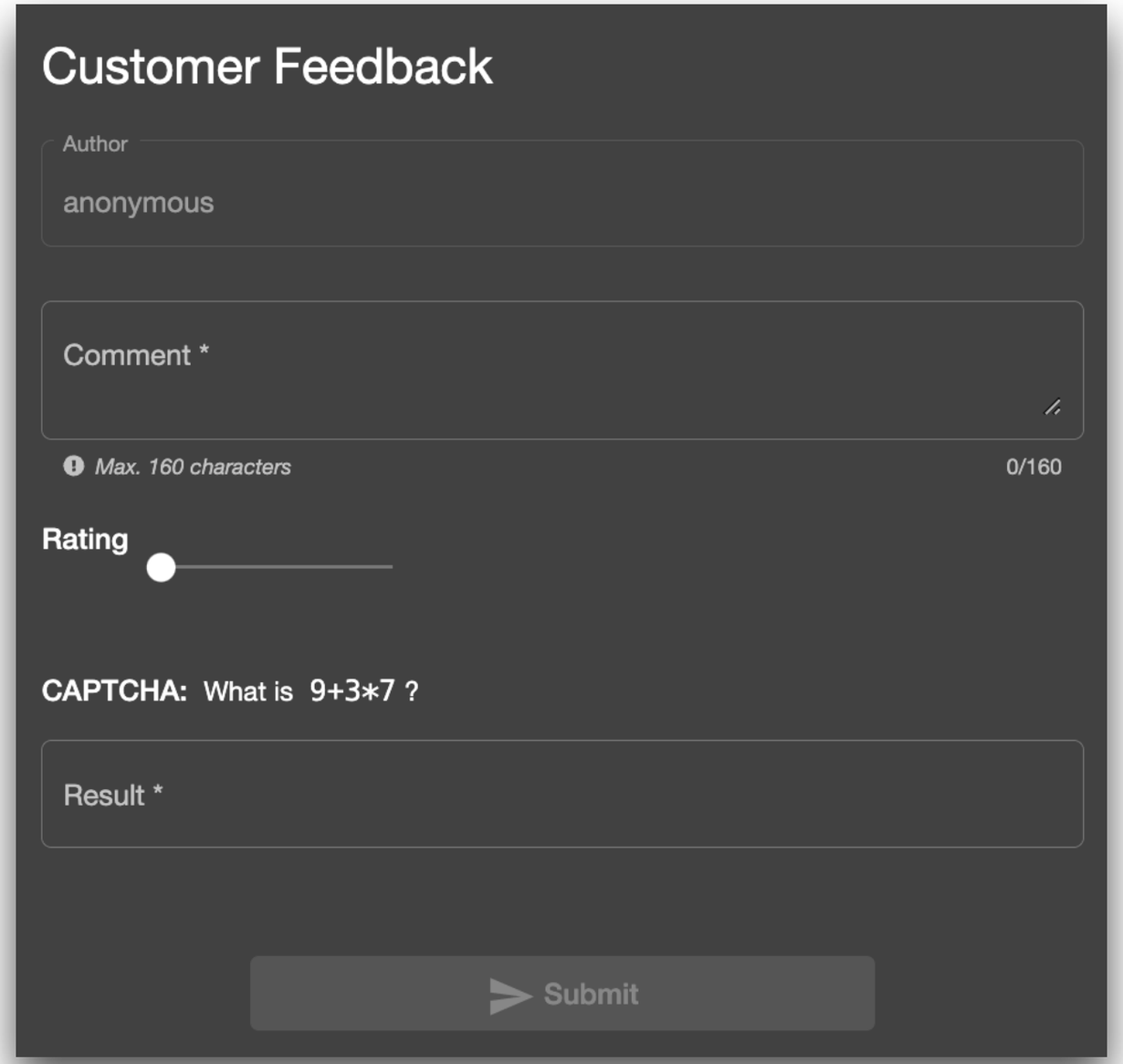
<iframe src="javascript:alert(`data all over this screen that wasnt planned`)">



https://demo.owasp-juice.shop/#/search?q=apple

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Feedback



https://demo.owasp-juice.shop/#/contact

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Broken Access Control

https://owasp.org/Top10/A01_2021-Broken_Access_Control/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

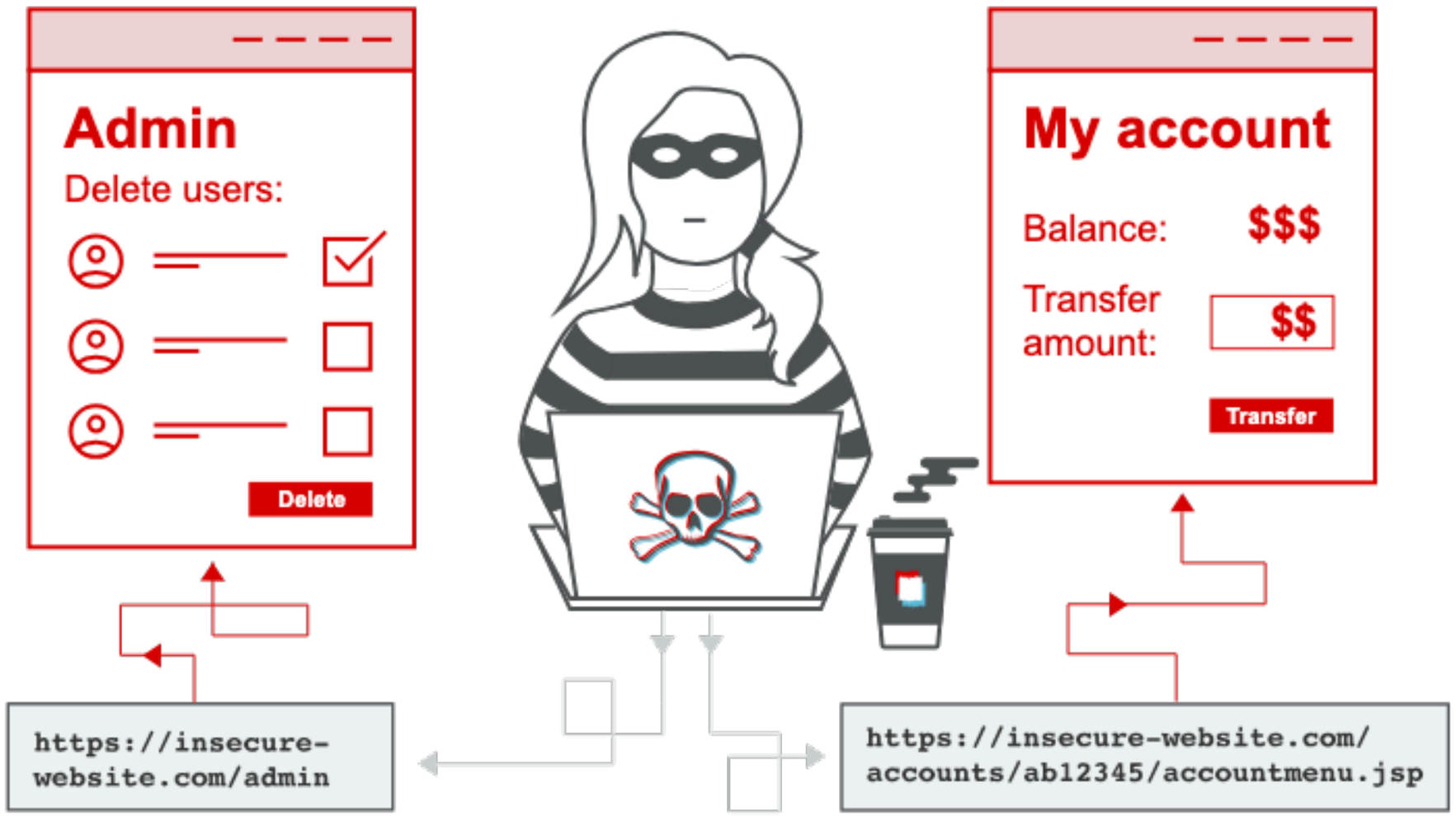
Broken Access Control

Users can access resources that they are not supposed to be able to

Authentication	Session management	Access control

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Broken Access Control



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Broken Access Control

In juice shop

Forged review

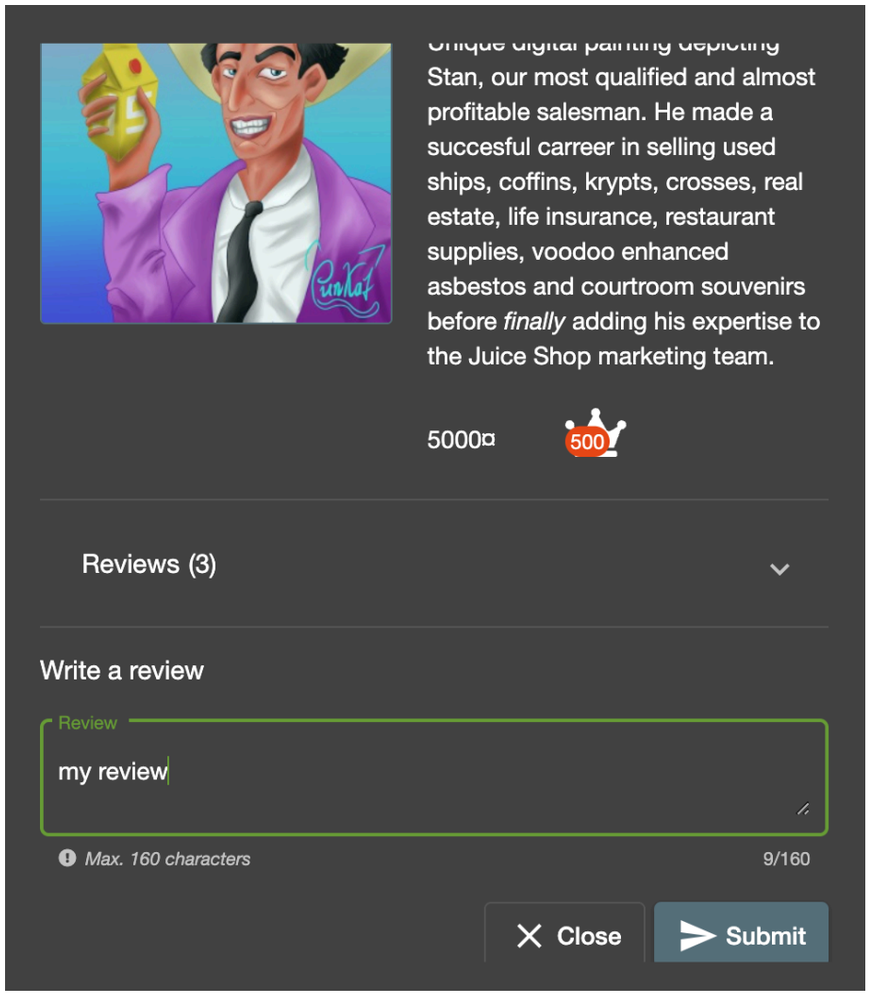
Forged feedback

Add product to other basket

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Forged review

User can write a review.



rest/products/24/reviews

?

API

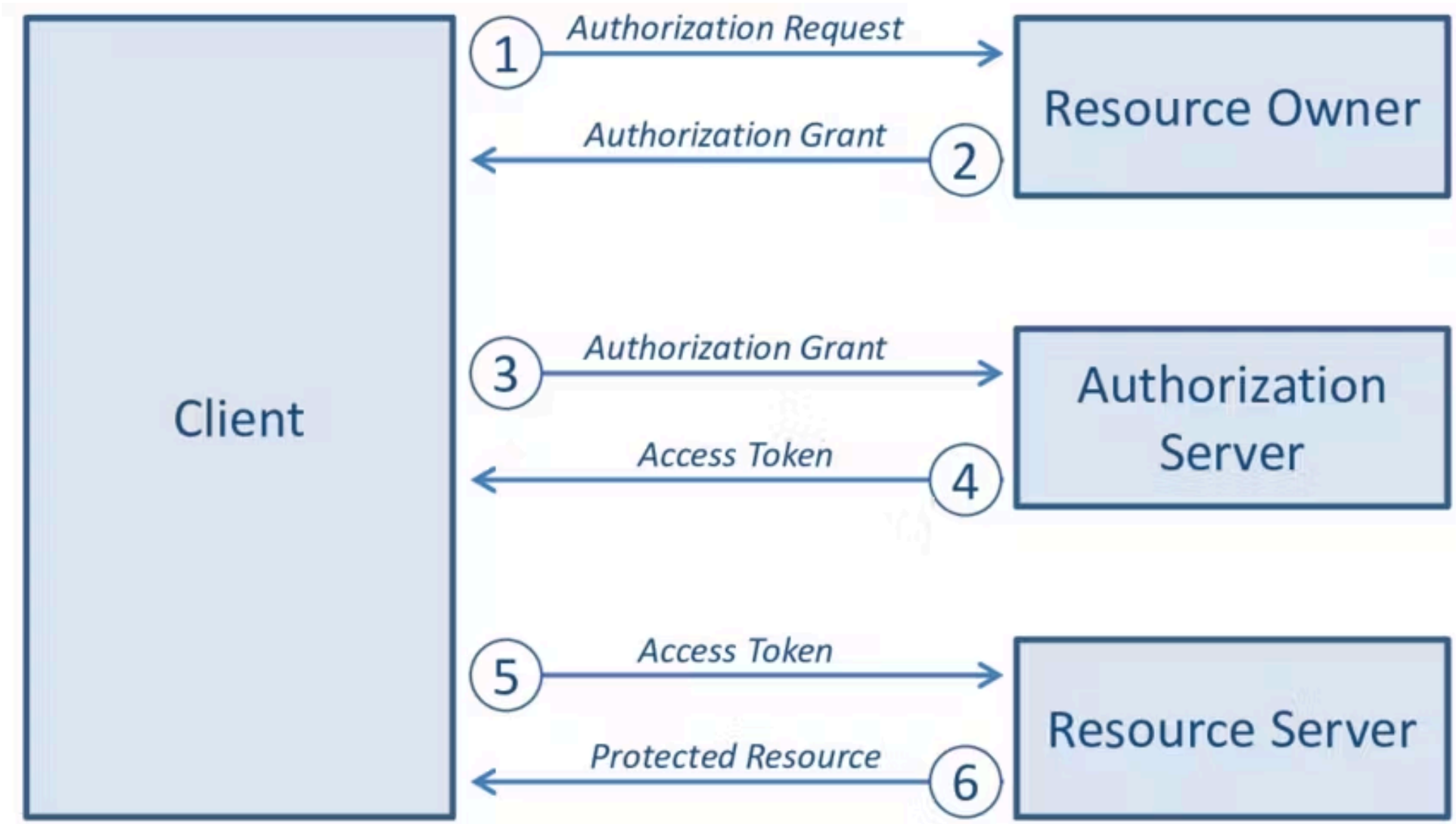
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

How to prevent ?

User can write a review.

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

OAuth 2.0



https://oauth.net/2/

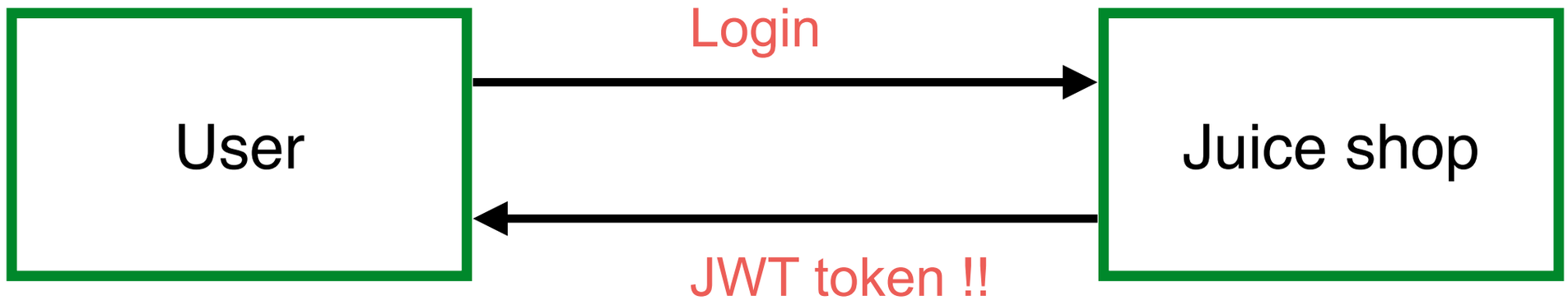
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Unsigned JWT Token

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Forged Signed JWT

JWT Token !!

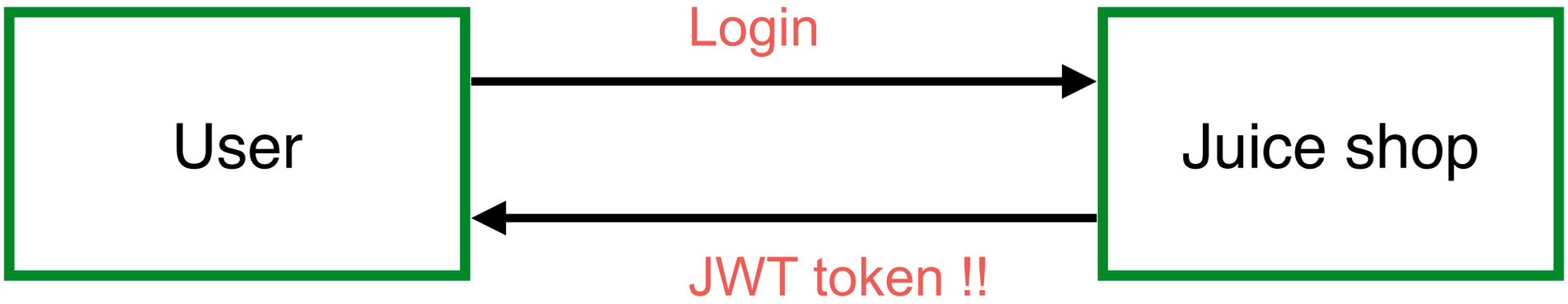


https://pwning.owasp-juice.shop/companion-guide/latest/part2/vulnerable-components.html#_forge_an_almost_properly_rsa_signed_jwt_token

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Log in to system

email=jwtn3d@juice-sh.op
password=123456



https://pwning.owasp-juice.shop/companion-guide/latest/part2/vulnerable-components.html#_forge_an_almost_properly_rsa_signed_jwt_token

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Open JWT Token

Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.ey
JzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZ
CI6MzYsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJy
c2FfbG9yZEBqdWljZS1zaC5vcCIsInBhc3N3b3J
kIjoiODI3Y2NiMGVlYThhNzA2YzRjMzRhMTY4OT
FmODRlN2IiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZ
Wx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoi
MC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3N
ldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZm
F1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQ
WN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIz
LTExLTE2IDEyOjA4OjA1Ljk3MCArMDA6MDAiLCJ
1cGRhdGVkQXQiOiIyMDIzLTExLTE2IDEyOjA4Oj
A1Ljk3MCArMDA6MDAiLCJkZWxldGVkQXQiOm51b
Gx9LCJpYXQiOjE3MDAxMzY0OTh9.G0EIm8kSikB
1ji9VPbgWgME4sZuBIJi2HxUc1-
4RXEGMXyqbgmtVireNahJvFrt-
m3HogkZyIYgKvccayrHc0j6e0TR3-
8lGhny70vxG-qMQDFcKmJOAZW-
qro3K29ORyC5k-
xW0ibk8rK3LWYkdsG9cvaL8UVUkknLfUEe9t8E
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256"
}
```

PAYLOAD: DATA

```
{
  "status": "success",
  "data": {
    "id": 36,
    "username": "",
    "email": "rsa_lord@juice-sh.op",
    "password": "827ccb0eea8a706c4c34a16891f84e7b",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "0.0.0.0",
    "profileImage":
"/assets/public/images/uploads/default.svg",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2023-11-16 12:08:05.970 +00:00",
    "updatedAt": "2023-11-16 12:08:05.970 +00:00",
    "deletedAt": null
  },
  "iat": 1700136498
}
```

VERIFY SIGNATURE

https://jwt.io/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Create Unsigned JWT Token !!

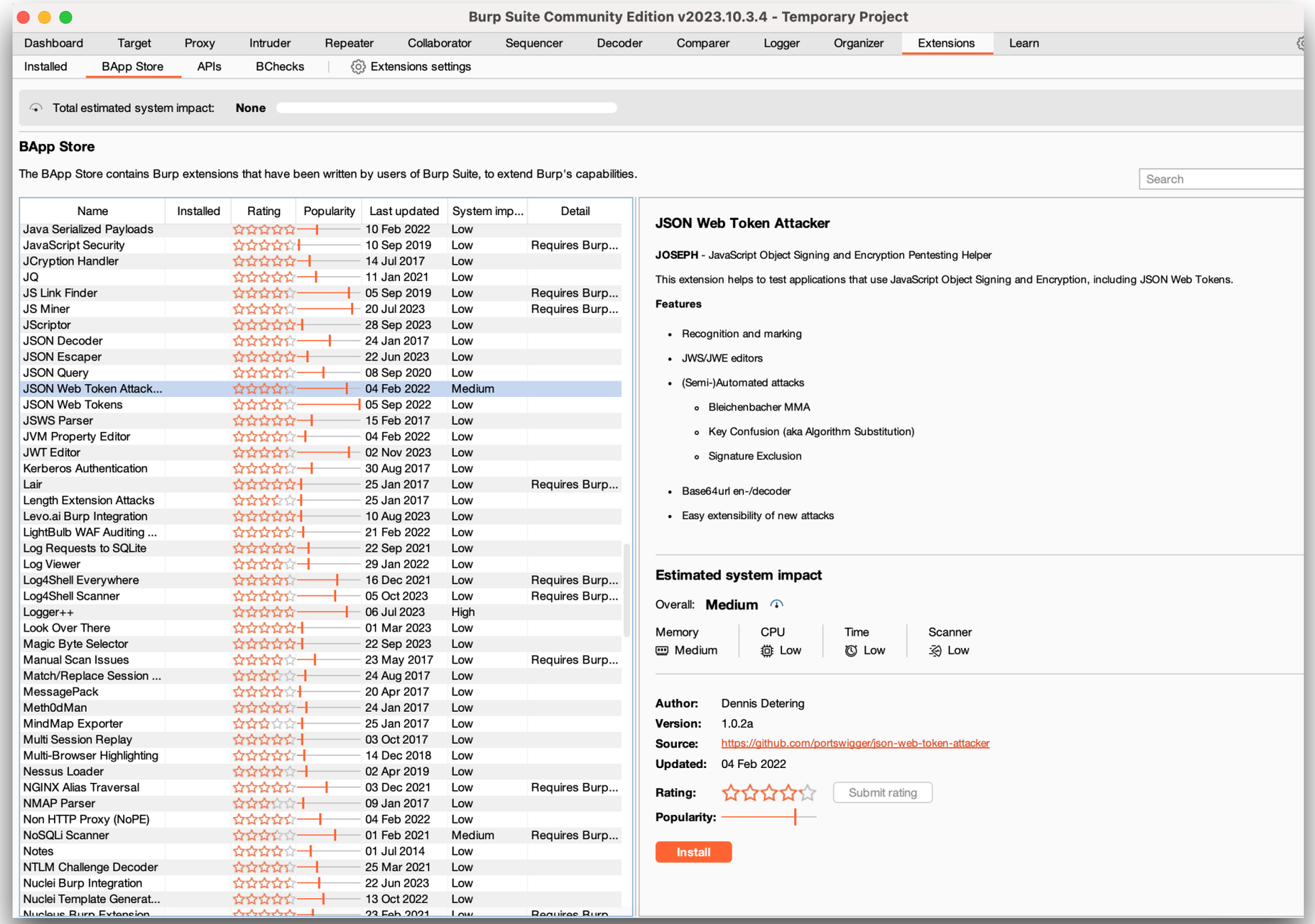
Update alg=“none”

Header.Payload.

https://gchq.github.io/CyberChef/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

JSON Web Token Attack



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Security Test Tools

Static

Dynamic

https://github.com/GoVanguard/main-security-testing-tools

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Static Analysis Security Testing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Static Analysis Security Testing

Dev, Ops

Code and Config

Lint

Dependency Check

Static code Analysis

Security Code Scan

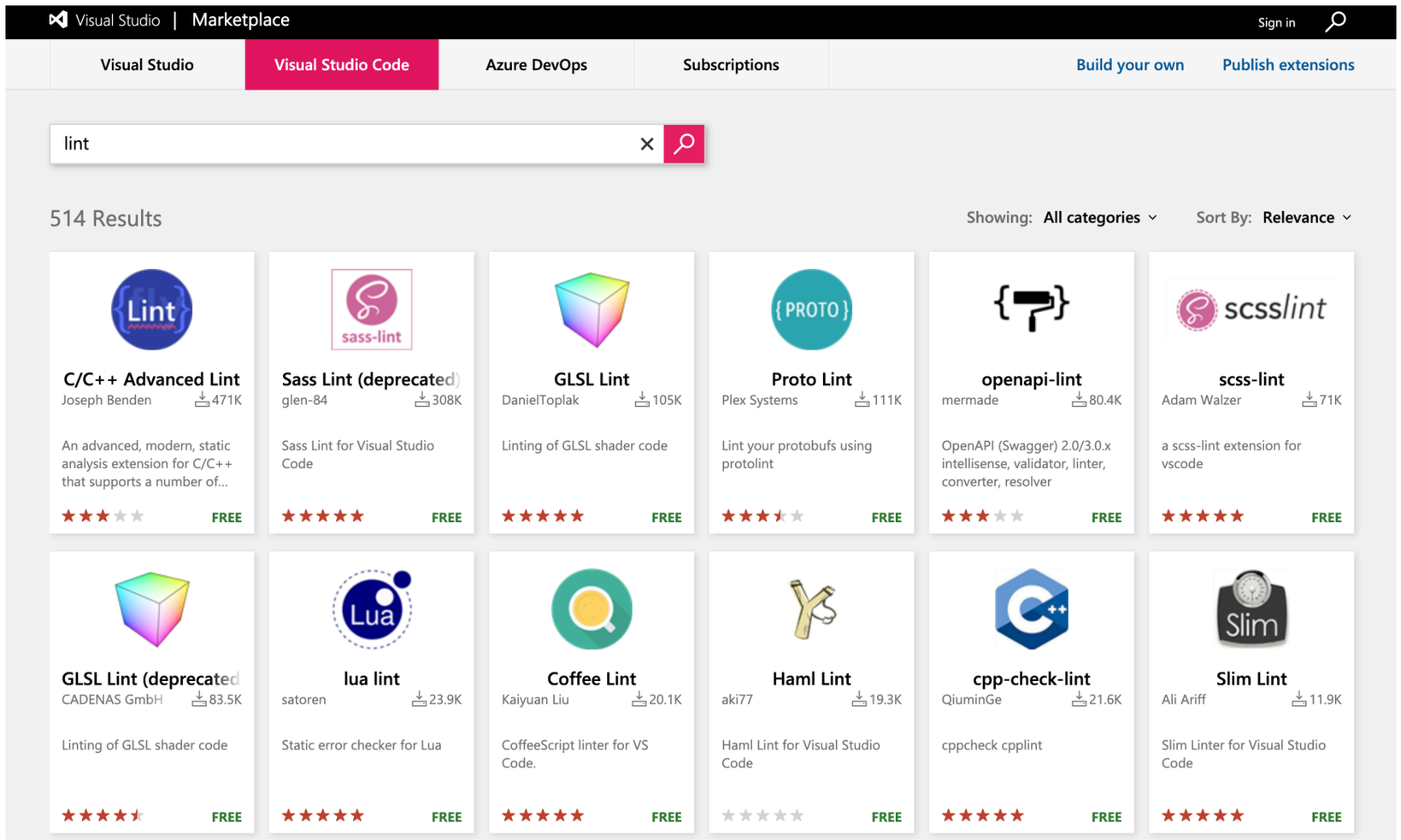
Detect secret

Detect vulnerable components

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Lint Tools

Integrate tools with Text editor or IDE



https://marketplace.visualstudio.com/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Source Code Analysis Tools

Help to analyze source code or compiled code to find security flaws

Scalable

Identified well-known vulnerability (Injection, Buffer overflow)

Output helps developer

Authentication problem

Access control issue

Insecure use of cryptography

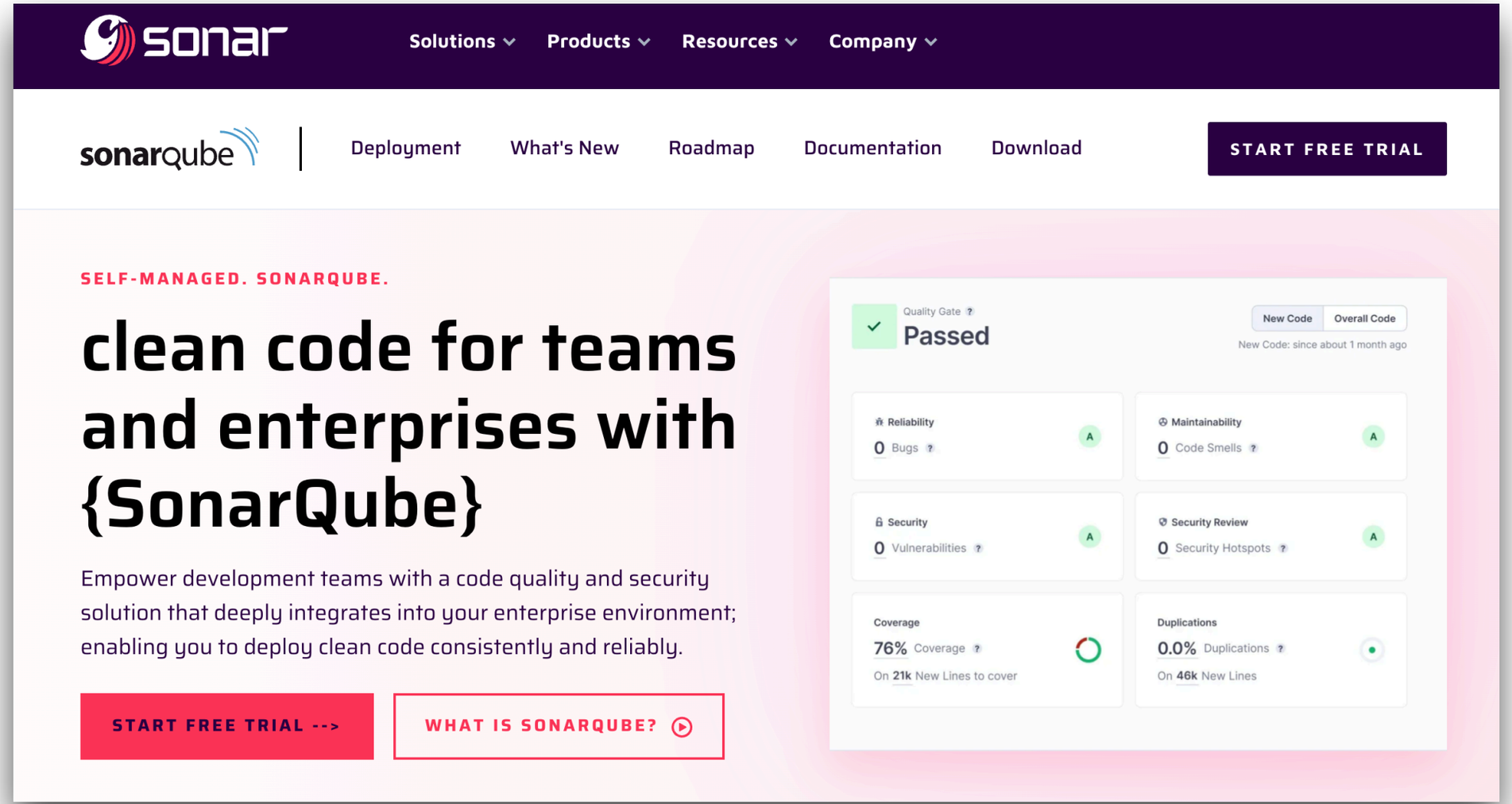
High number of false positive

https://owasp.org/www-community/Source_Code_Analysis_Tools

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Static Code Analysis

SonarQube is popular tool

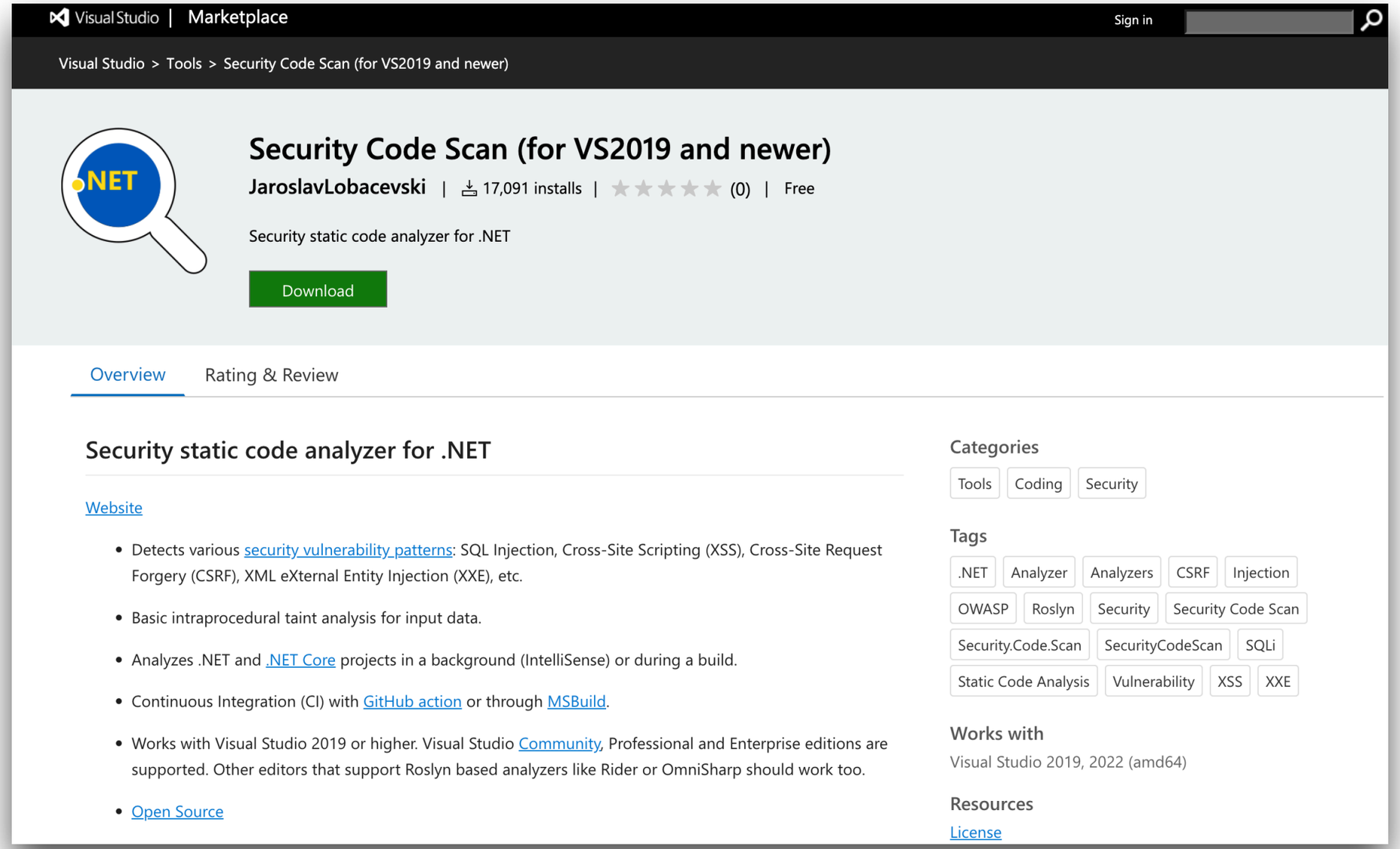


https://www.sonarsource.com/products/sonarqube/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Security Code Scan

For .NET project

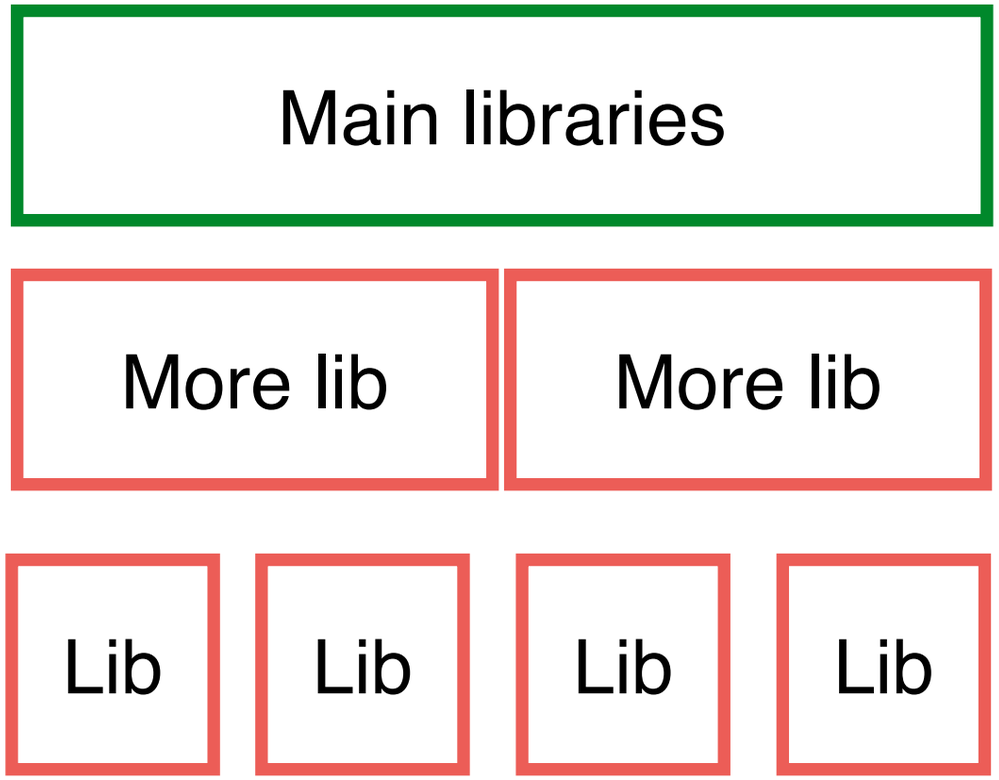


https://marketplace.visualstudio.com/items?itemName=JaroslavLobacevski.SecurityCodeScanVS2019

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Dependency Check

Check your libraries/dependencies in project

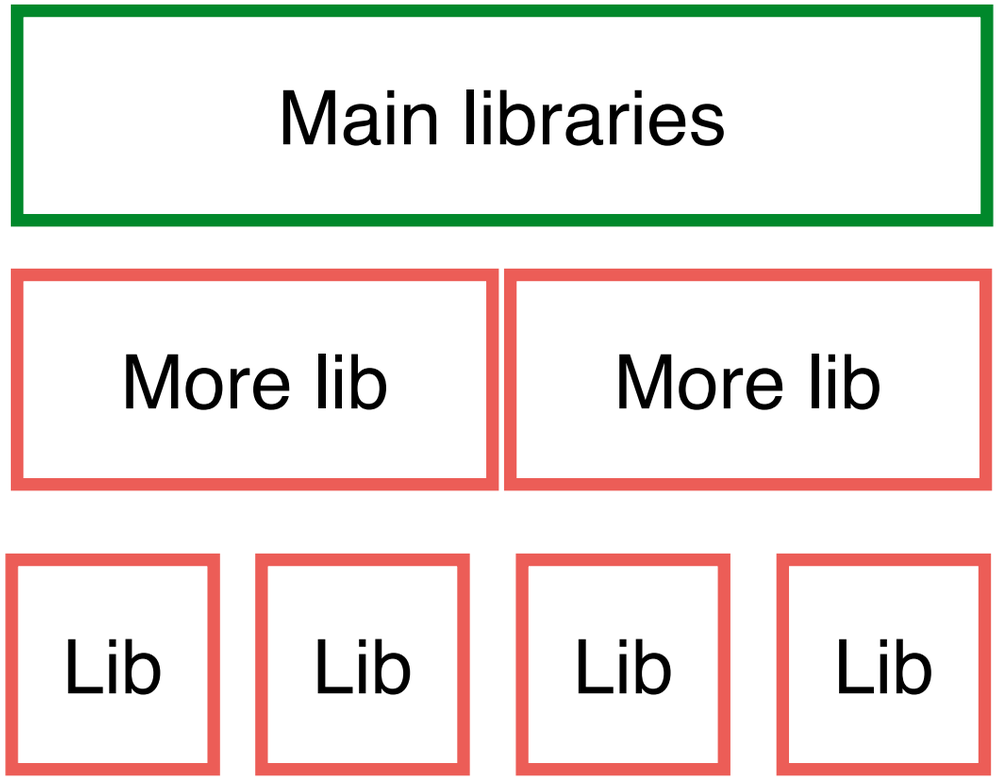


https://owasp.org/www-project-dependency-check/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Dependabot from GitHub

Check your libraries/dependencies in GitHub project



https://docs.github.com/en/code-security/getting-started/dependabot-quickstart-guide

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Example with Log4Shell

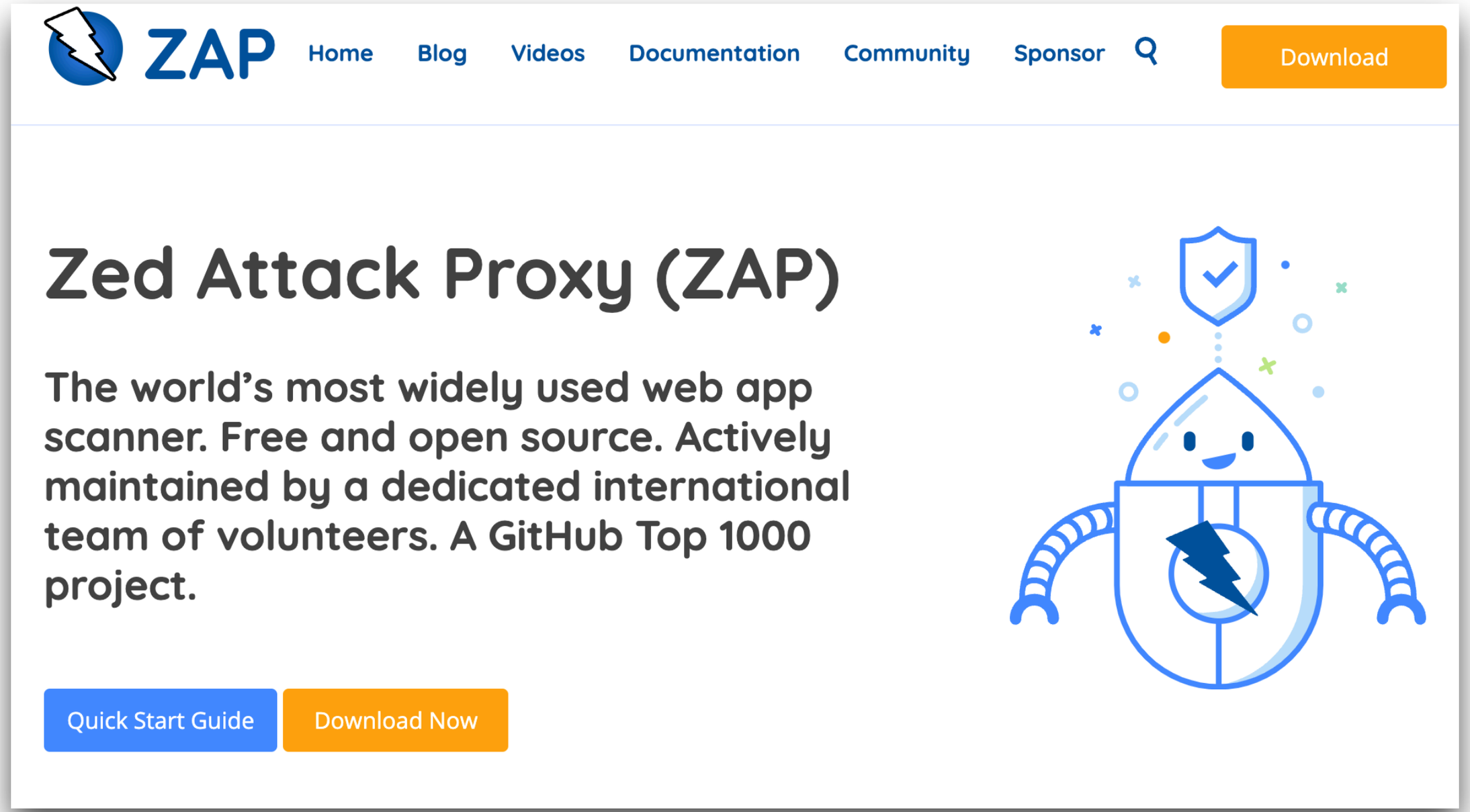
https://www.lunasec.io/docs/blog/log4j-zero-day/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Dynamic Analysis Security Testing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

OWASP ZAP

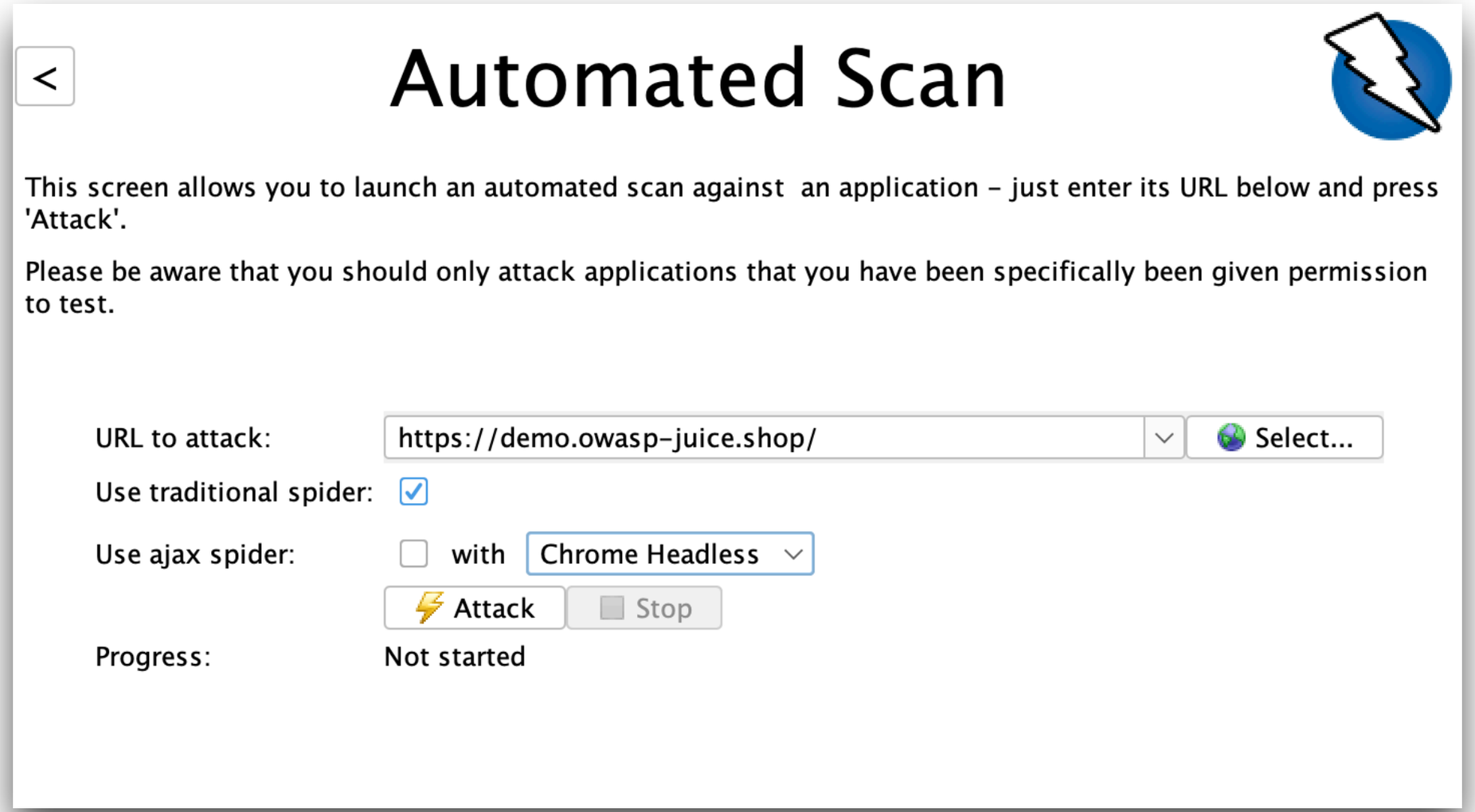


https://www.zaproxy.org/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

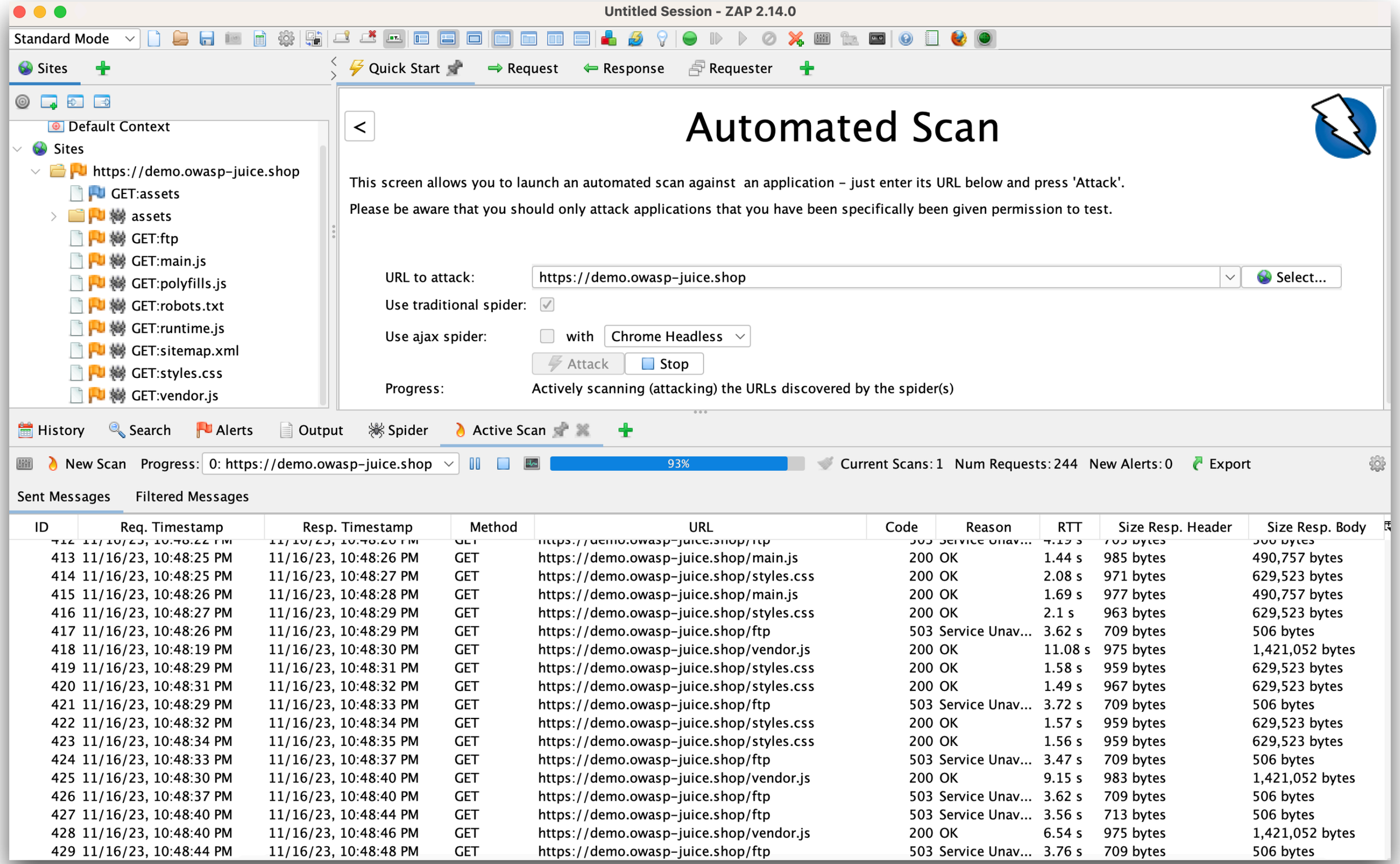
OWASP ZAP

Automated Scan to target url



https://www.zaproxy.org/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

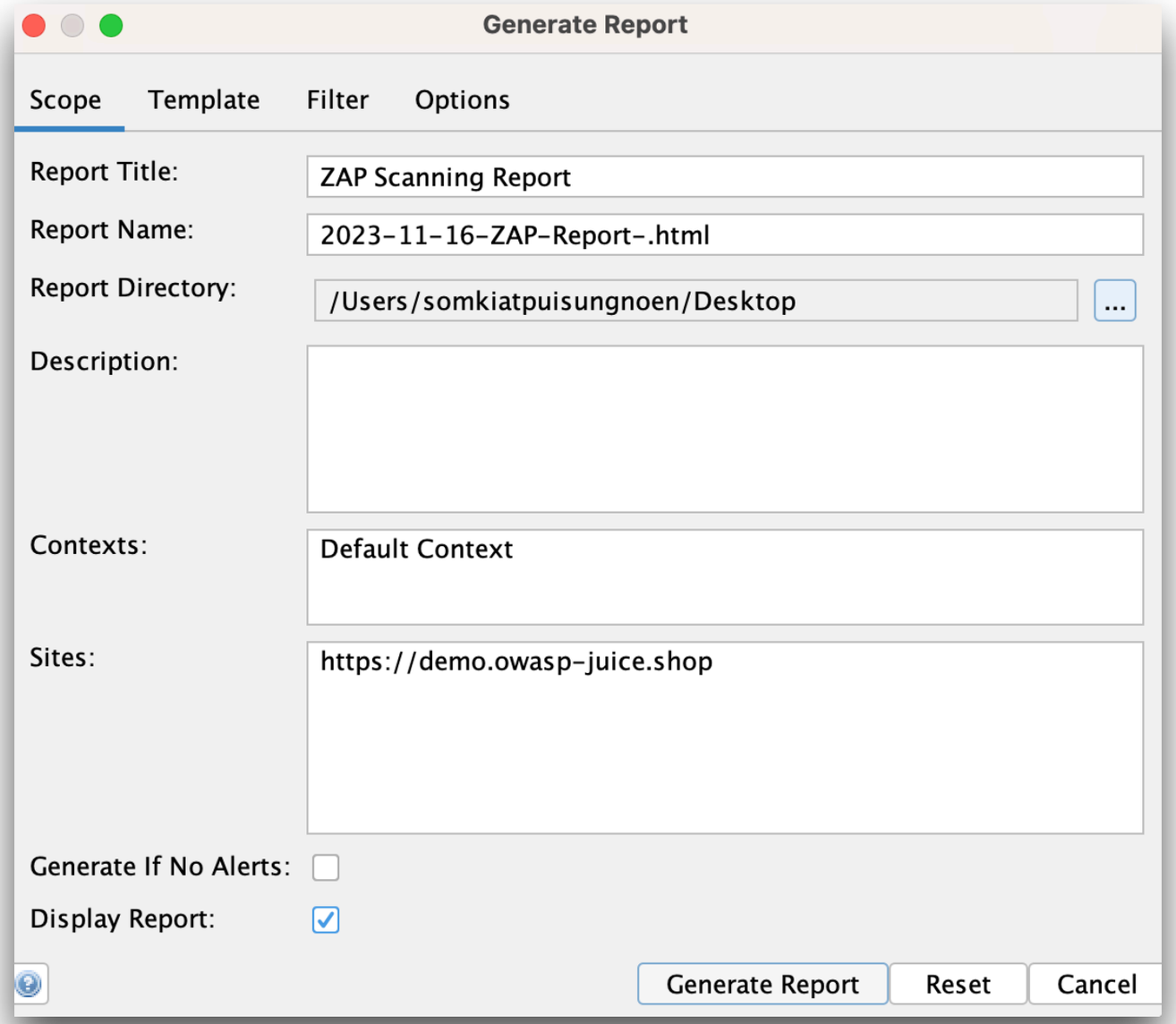


ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
413	11/16/23, 10:48:25 PM	11/16/23, 10:48:26 PM	GET	https://demo.owasp-juice.shop/main.js	200	OK	1.44 s	985 bytes	490,757 bytes
414	11/16/23, 10:48:25 PM	11/16/23, 10:48:27 PM	GET	https://demo.owasp-juice.shop/styles.css	200	OK	2.08 s	971 bytes	629,523 bytes
415	11/16/23, 10:48:26 PM	11/16/23, 10:48:28 PM	GET	https://demo.owasp-juice.shop/main.js	200	OK	1.69 s	977 bytes	490,757 bytes
416	11/16/23, 10:48:27 PM	11/16/23, 10:48:29 PM	GET	https://demo.owasp-juice.shop/styles.css	200	OK	2.1 s	963 bytes	629,523 bytes
417	11/16/23, 10:48:26 PM	11/16/23, 10:48:29 PM	GET	https://demo.owasp-juice.shop/ftp	503	Service Unav...	3.62 s	709 bytes	506 bytes
418	11/16/23, 10:48:19 PM	11/16/23, 10:48:30 PM	GET	https://demo.owasp-juice.shop/vendor.js	200	OK	11.08 s	975 bytes	1,421,052 bytes
419	11/16/23, 10:48:29 PM	11/16/23, 10:48:31 PM	GET	https://demo.owasp-juice.shop/styles.css	200	OK	1.58 s	959 bytes	629,523 bytes
420	11/16/23, 10:48:31 PM	11/16/23, 10:48:32 PM	GET	https://demo.owasp-juice.shop/styles.css	200	OK	1.49 s	967 bytes	629,523 bytes
421	11/16/23, 10:48:29 PM	11/16/23, 10:48:33 PM	GET	https://demo.owasp-juice.shop/ftp	503	Service Unav...	3.72 s	709 bytes	506 bytes
422	11/16/23, 10:48:32 PM	11/16/23, 10:48:34 PM	GET	https://demo.owasp-juice.shop/styles.css	200	OK	1.57 s	959 bytes	629,523 bytes
423	11/16/23, 10:48:34 PM	11/16/23, 10:48:35 PM	GET	https://demo.owasp-juice.shop/styles.css	200	OK	1.56 s	959 bytes	629,523 bytes
424	11/16/23, 10:48:33 PM	11/16/23, 10:48:37 PM	GET	https://demo.owasp-juice.shop/ftp	503	Service Unav...	3.47 s	709 bytes	506 bytes
425	11/16/23, 10:48:30 PM	11/16/23, 10:48:40 PM	GET	https://demo.owasp-juice.shop/vendor.js	200	OK	9.15 s	983 bytes	1,421,052 bytes
426	11/16/23, 10:48:37 PM	11/16/23, 10:48:40 PM	GET	https://demo.owasp-juice.shop/ftp	503	Service Unav...	3.62 s	709 bytes	506 bytes
427	11/16/23, 10:48:40 PM	11/16/23, 10:48:44 PM	GET	https://demo.owasp-juice.shop/ftp	503	Service Unav...	3.56 s	713 bytes	506 bytes
428	11/16/23, 10:48:40 PM	11/16/23, 10:48:46 PM	GET	https://demo.owasp-juice.shop/vendor.js	200	OK	6.54 s	975 bytes	1,421,052 bytes
429	11/16/23, 10:48:44 PM	11/16/23, 10:48:48 PM	GET	https://demo.owasp-juice.shop/ftp	503	Service Unav...	3.76 s	709 bytes	506 bytes

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Generate Report

Report -> Generate Report



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

HTML Report

ZAP Scanning Report

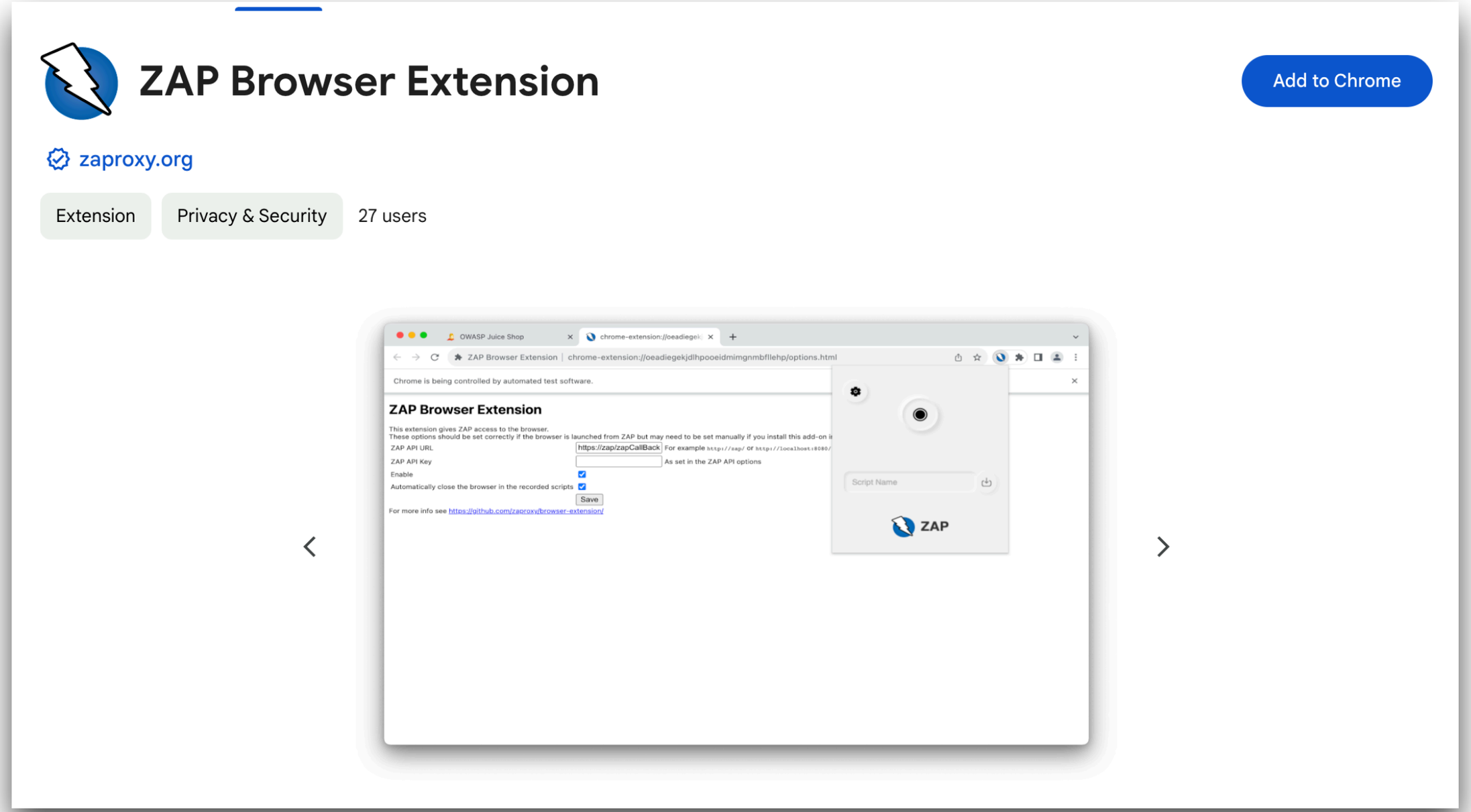
Generated with ZAP on Thu 16 Nov 2023, at 22:51:06

ZAP Version: 2.14.0

Contents

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

ZAP on Google Chrome



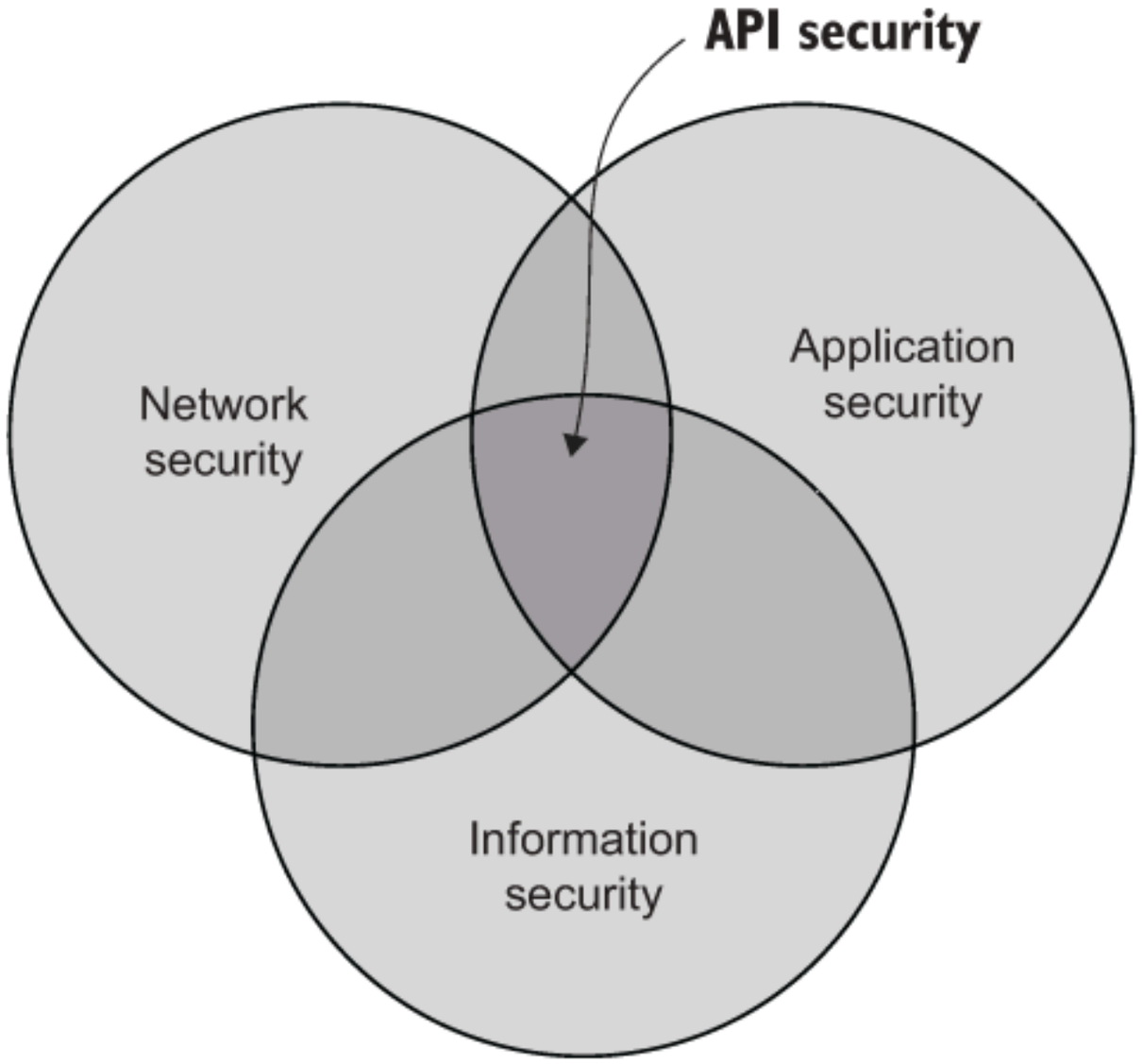
https://chromewebstore.google.com/detail/zap-browser-extension/cnmficmodhagepcmhogkbdakncebckho?pli=1

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Architecture

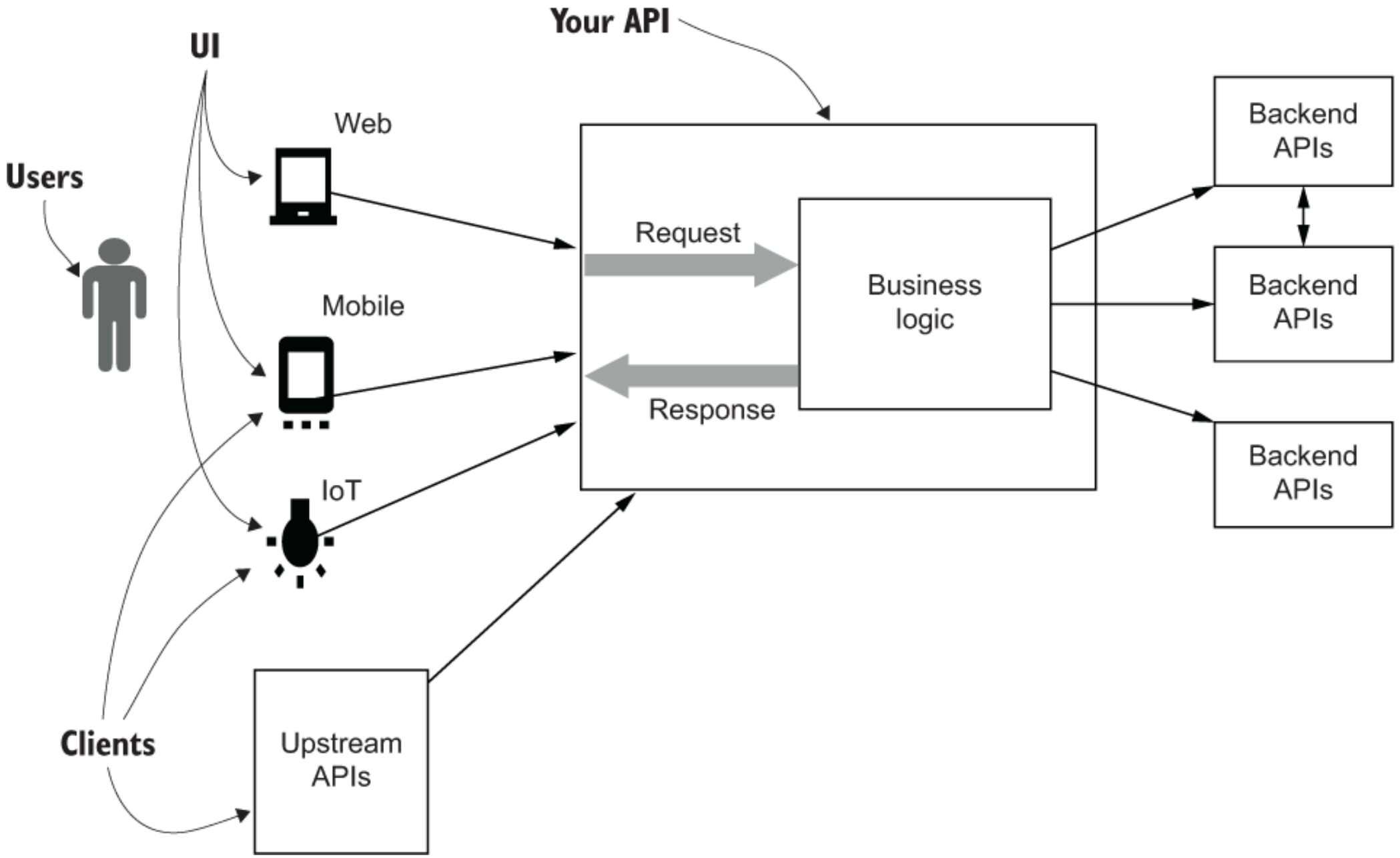
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

API Security

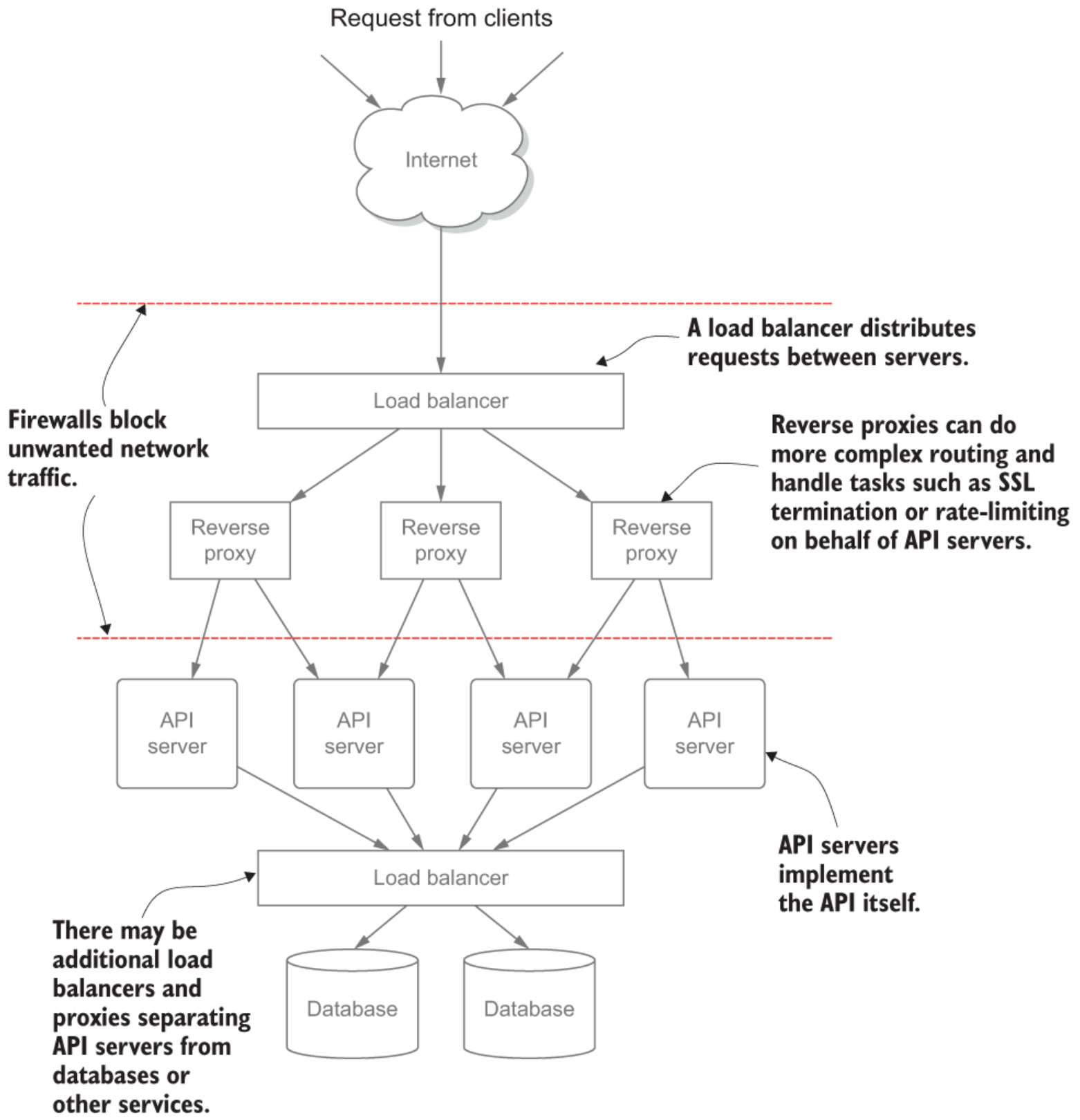


© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Simple Architecture



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Security Mechanisms

Authorization

Authentication

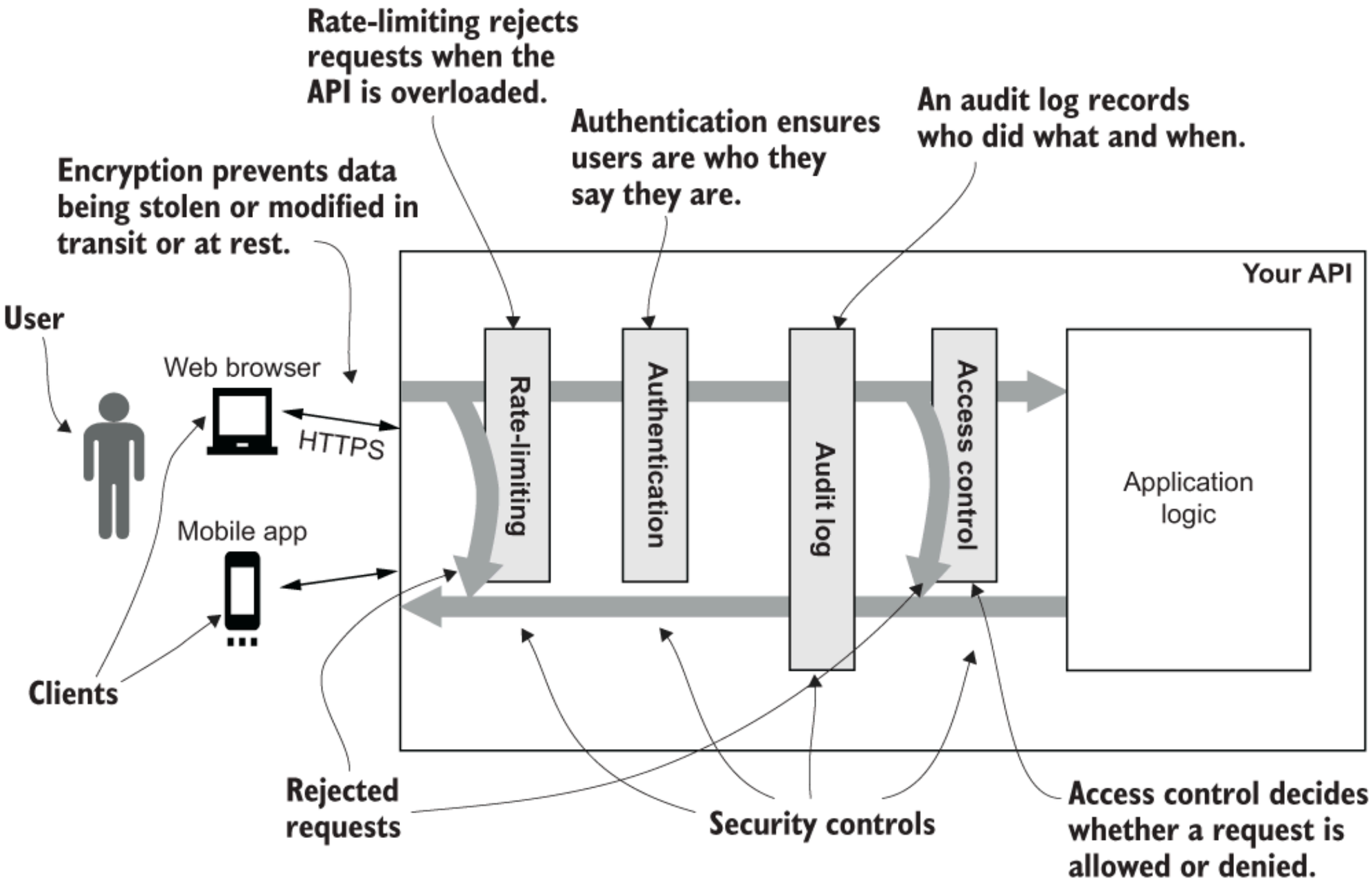
Encryption

Audit logging

Rate limiting

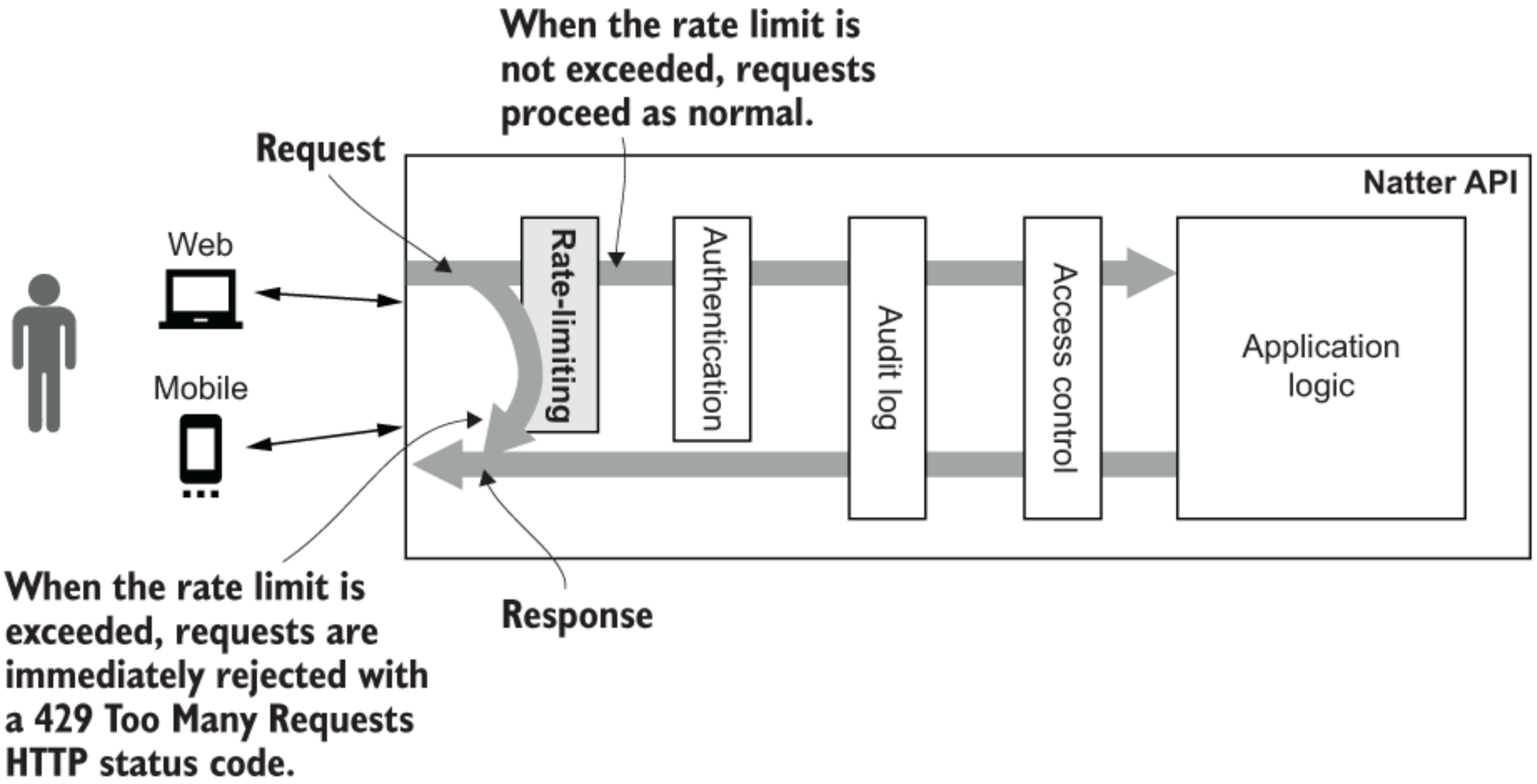
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Security Mechanisms



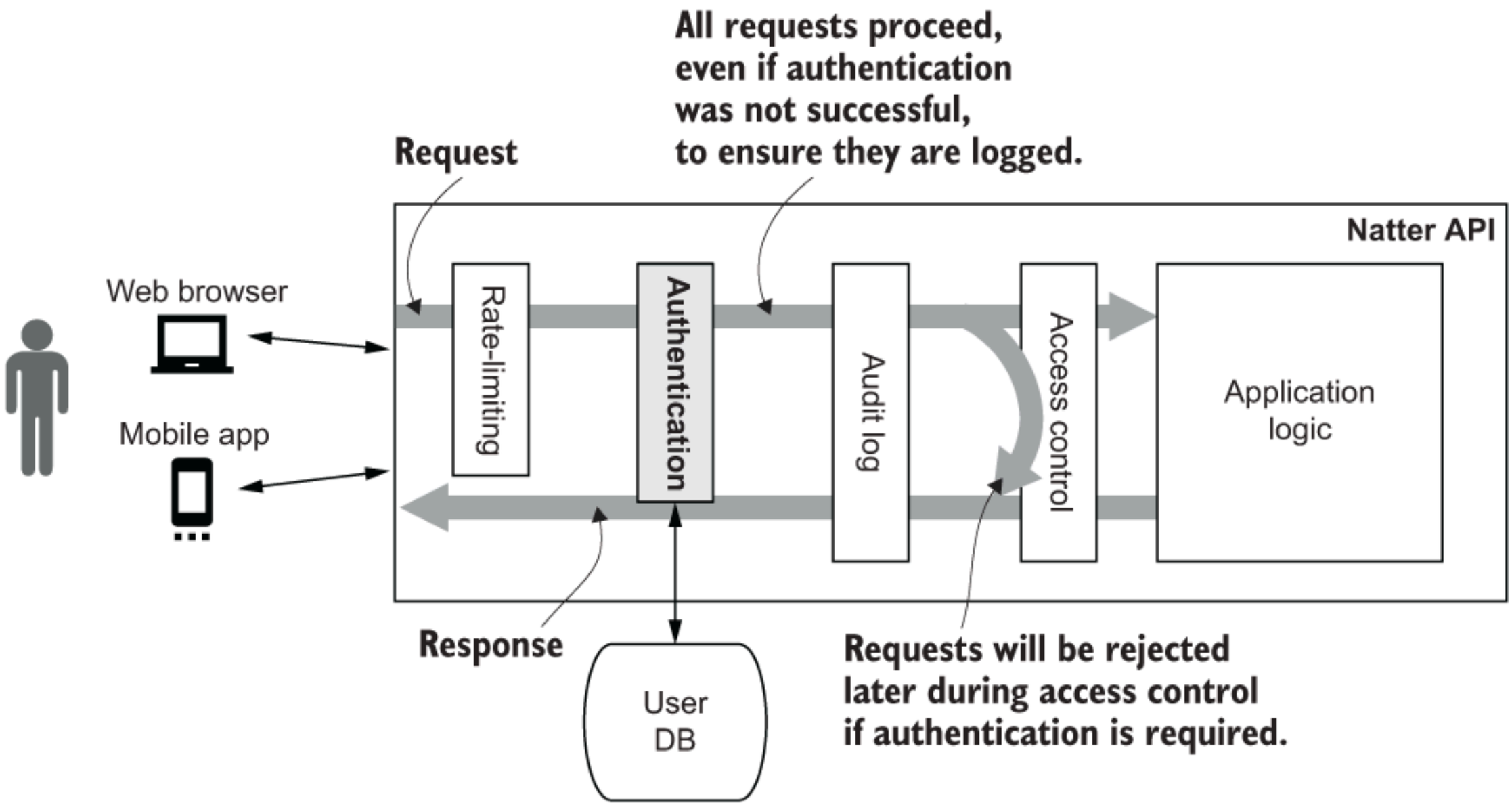
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Rate Limiting for Availability



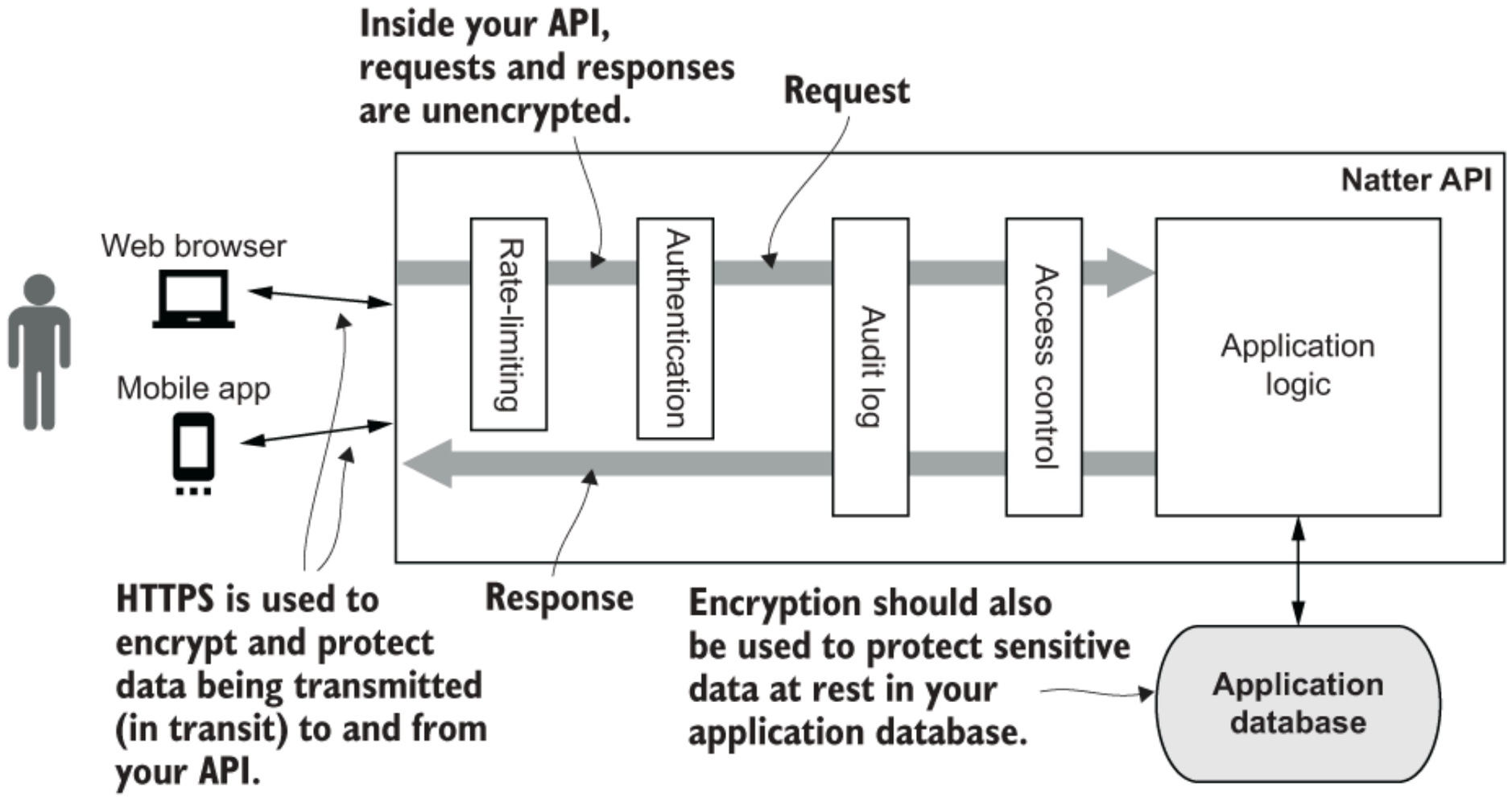
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Authentication



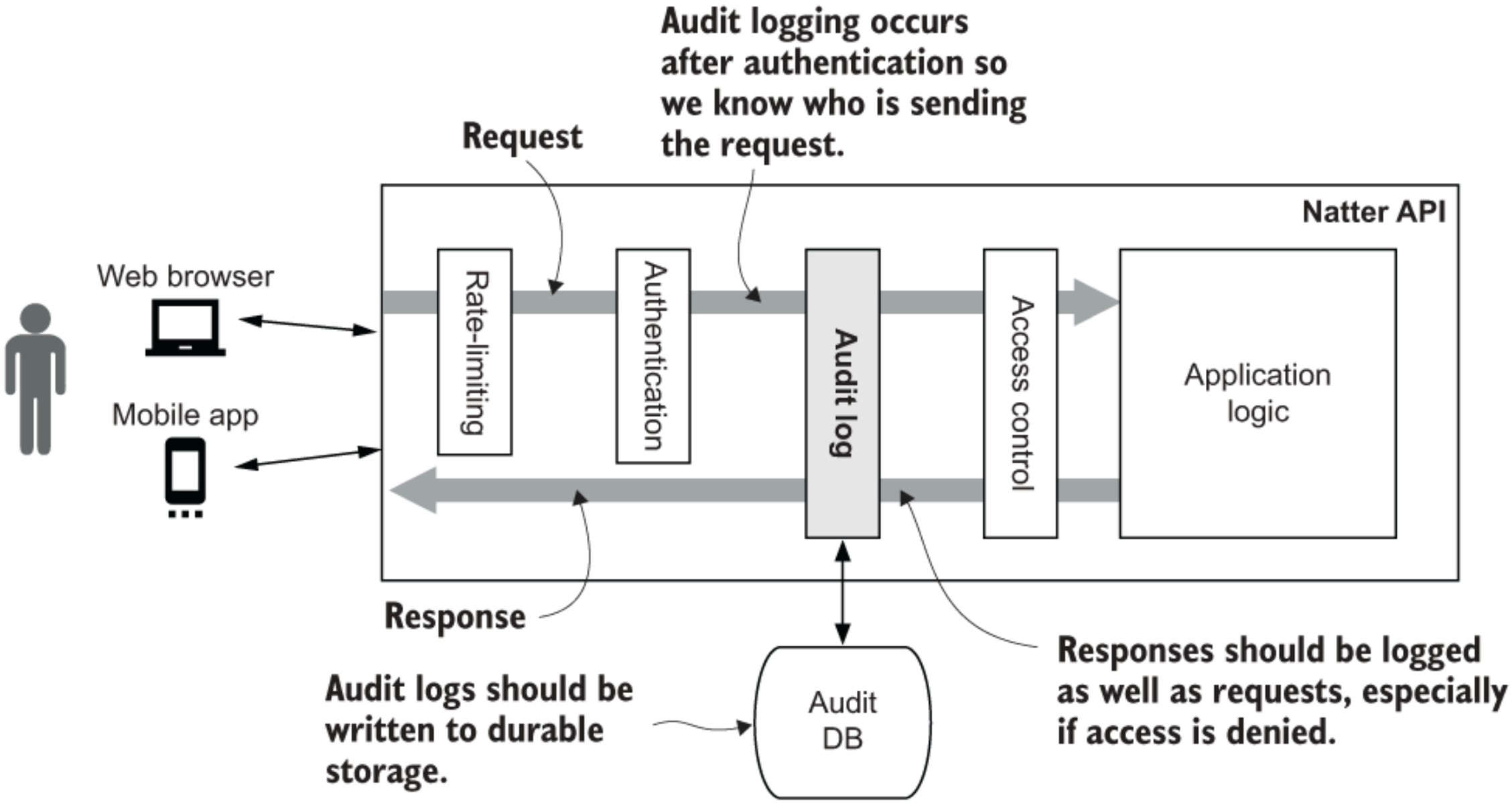
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Use encryption to keep data private



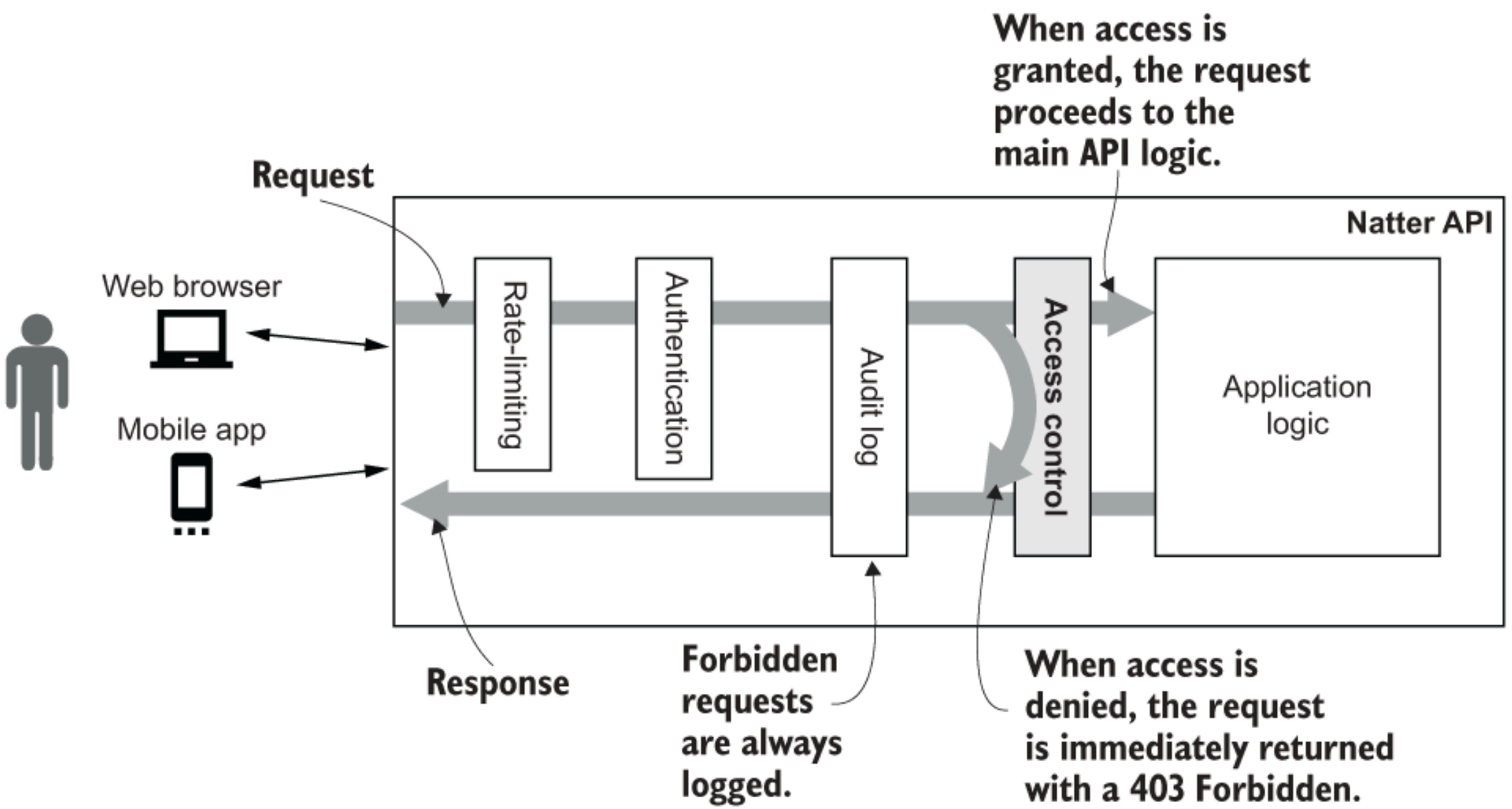
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Audit logging for accountability



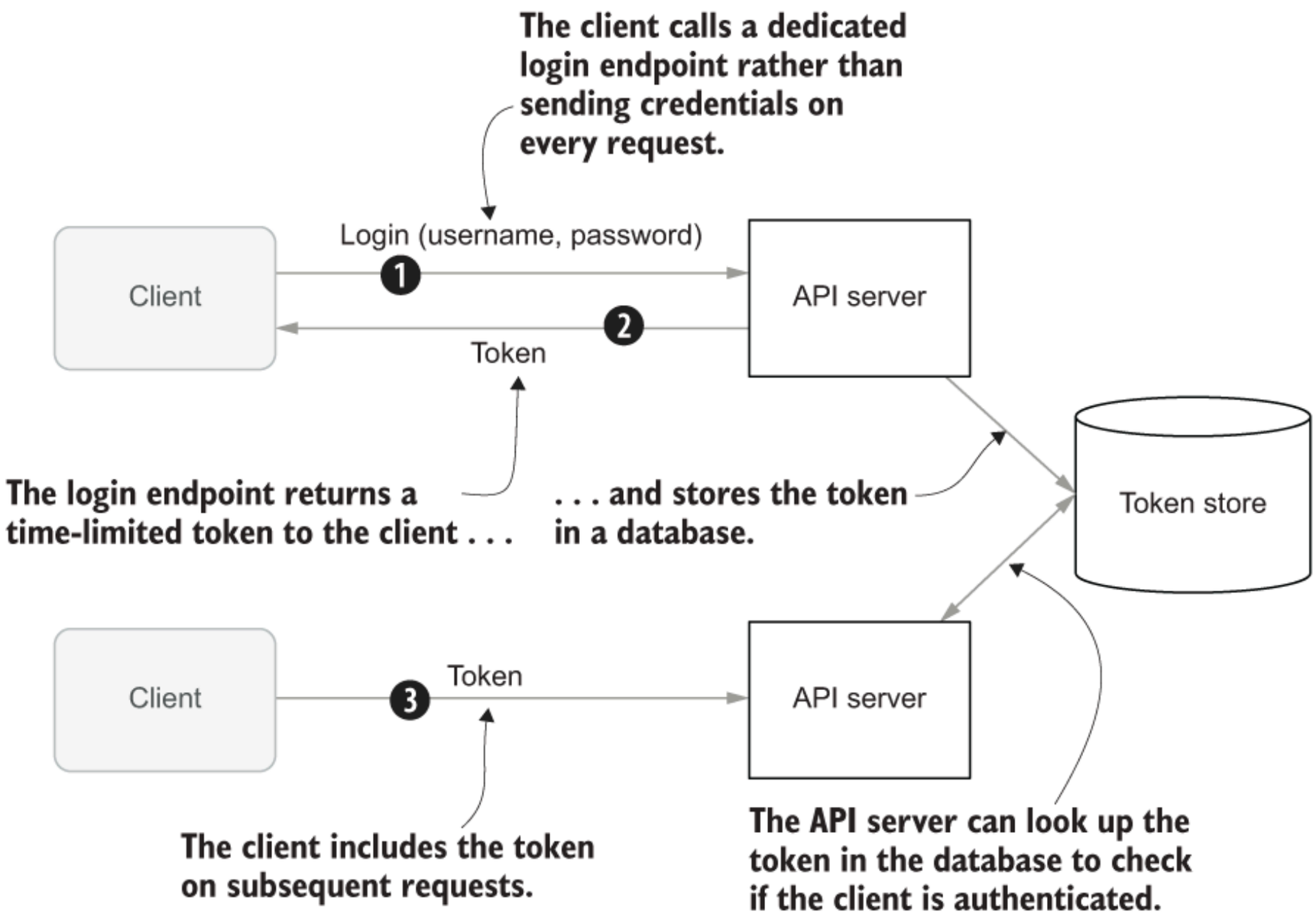
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Authorization or Access control



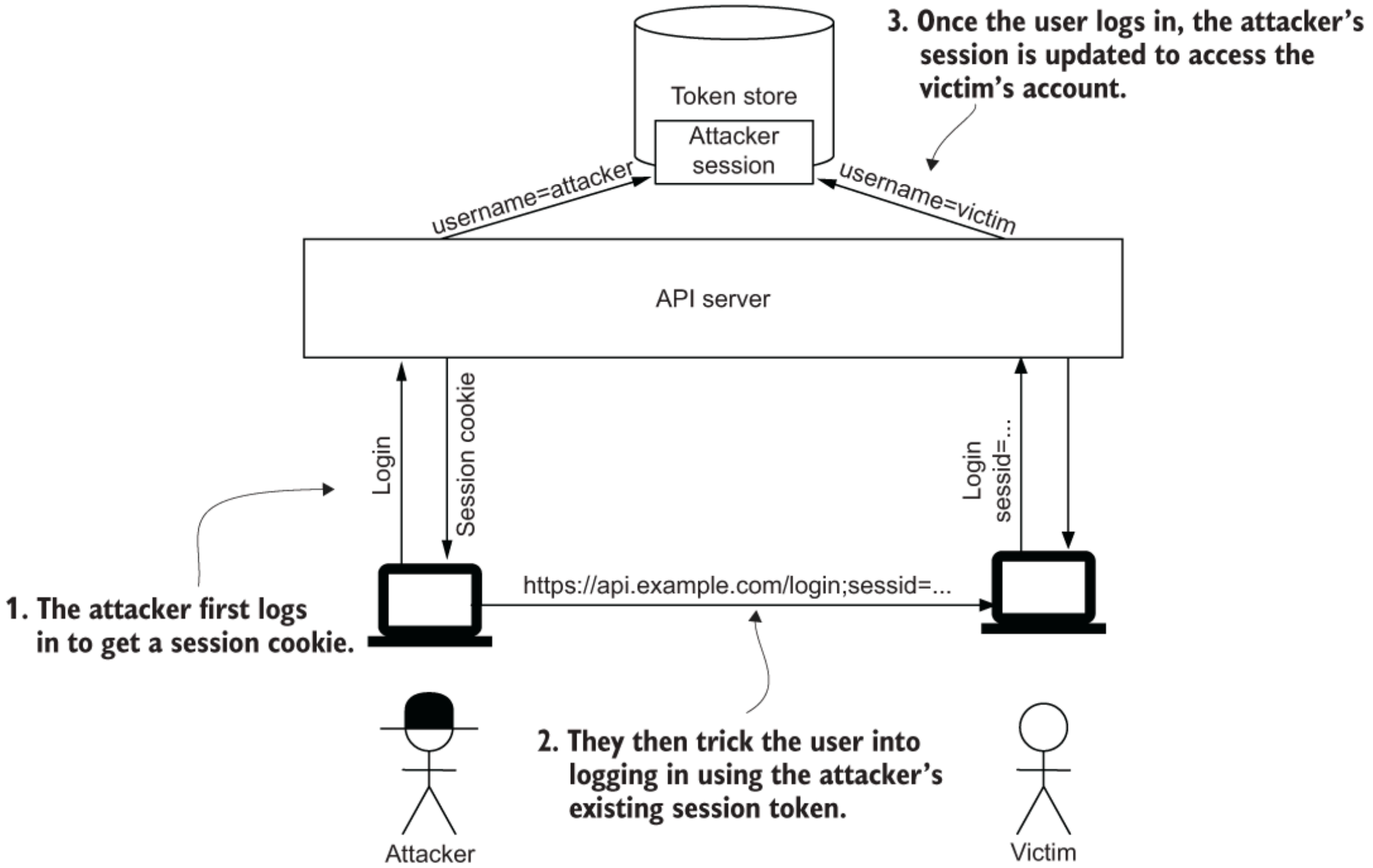
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Basic of Token-based



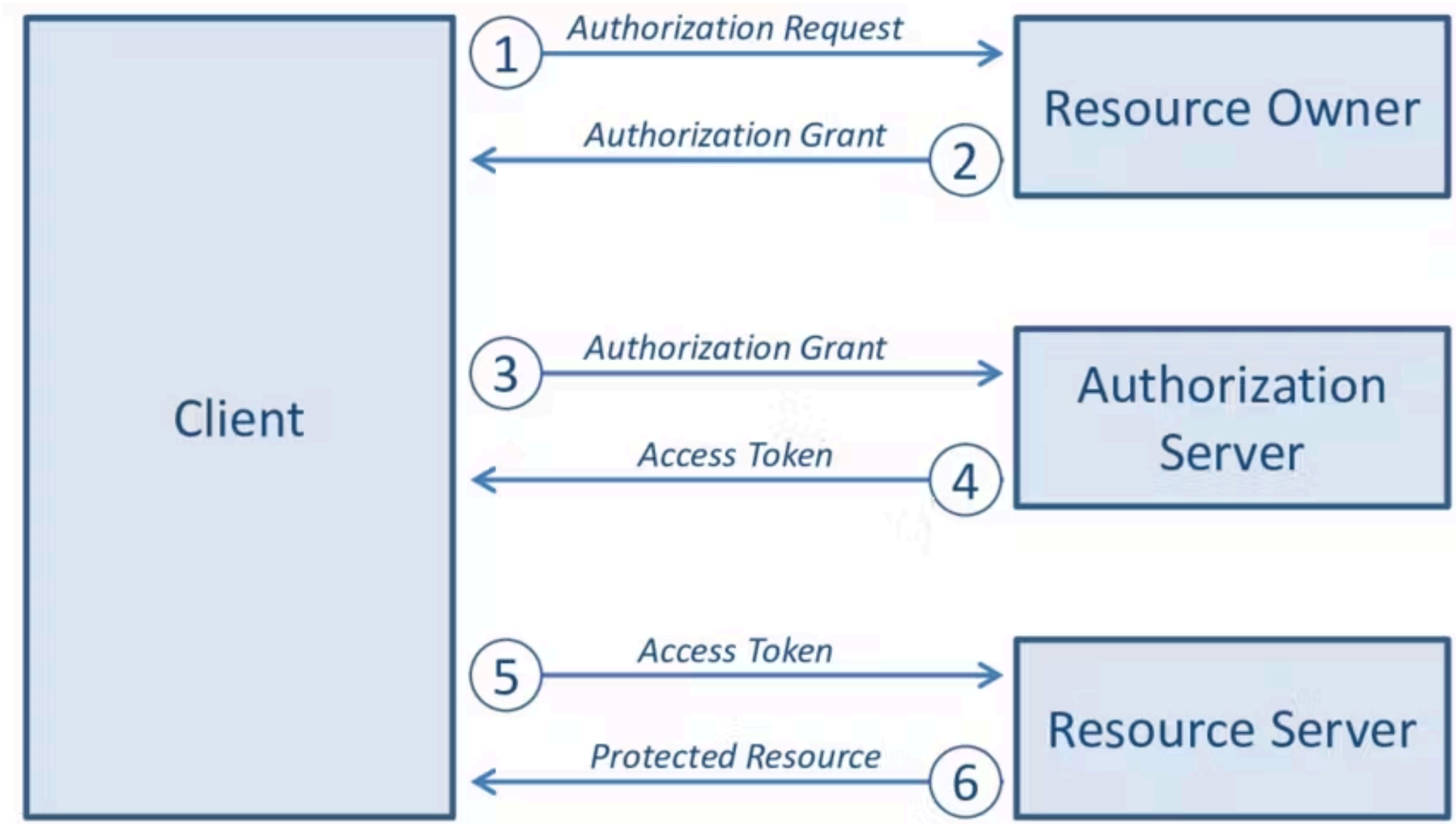
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Attack !!



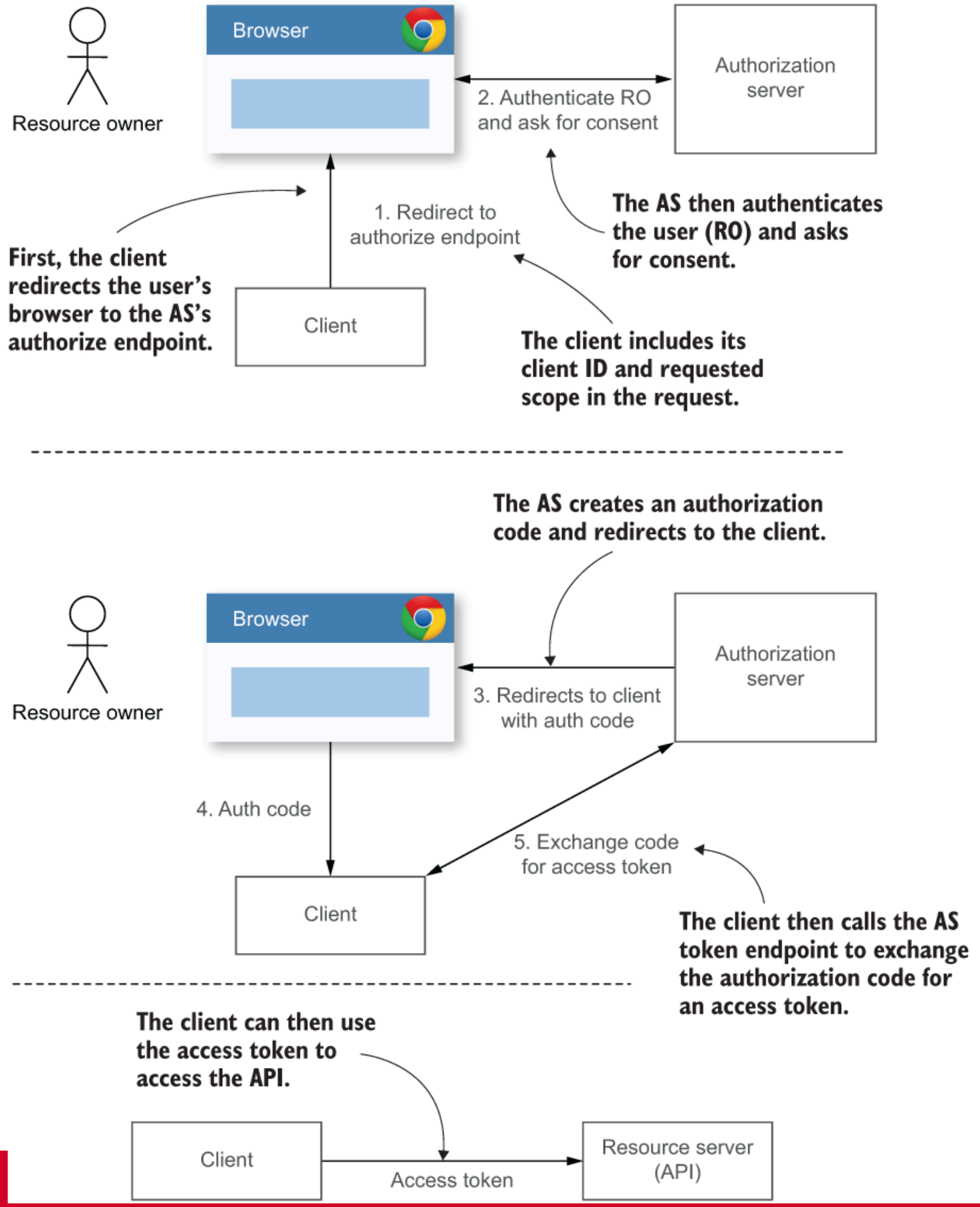
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

OAuth 2.0



https://oauth.net/2/

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.



© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

Q/A

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.