



# Audit your website. Build your expertise.

Four complementary audits. Practical cybersecurity training. Clear next steps.



## Security evidence for your website. Cyber reflexes for your team.

KrakenShield brings Surface, Privacy, Code Analysis and authorised Penetration Testing together with the Academy and its learning credentials.



## Know where to look.

Choose an audit for the question you need to answer.

### 01 / Surface

What is visible from outside?  
SSL/TLS configuration, public records and homepage security headers.

### 02 / Privacy

What does the browser load?  
Compare the homepage before a choice, after refusal and after acceptance, where testable.

### 03 / Code Analysis

What needs a closer look in the project?  
Dependencies, possible secrets and static code patterns, with a component inventory.

### 04 / Penetration Test

What does an authorised test reveal?  
Scope-based checks for injection, misconfiguration and exposed services.

## Built for the people who own the next fix.

Website owners get an understandable starting point. Developers receive a focused review backlog. Cybersecurity professionals can examine the evidence, scope and limitations.

### 01 AUDIT

Collect evidence



### 02 REVIEW

Validate priorities



### 03 IMPROVE

Fix and rescan



## Surface audit

Your external starting point.

### SSL/TLS

Inspect HTTPS configuration and the certificate.

### Public footprint

Review DNS, email records and public domain information.

### Web signals

Review security headers on the final homepage response.

**KrakenShield**  
SSL/TLS SECURITY REPORT  
**example.com**  
96 / 100

**A-**  
REPORT GRADE

**SSL/TLS configuration score**

Critical findings: none listed in the report

**PRIORITY FINDINGS**

ANONYMISED REPORT EXCERPT / example.com

The supplied report scores A- / 96. Its priority action plan still flags TLS 1.3, HSTS and clickjacking protection.

#### 01 Domain

Website address



#### 02 External checks

TLS and public signals



#### 03 Report

Grades and evidence



#### 04 Rescan

Validate changes

The TLS grade covers the tested configuration, not the whole application.



# Privacy audit

Observe behaviour. Compare choices.

## Before a choice

Observe cookies, storage and third-party requests.

## After refusal

Check what changes if the refusal action is testable.

## After acceptance

Compare another clean browser session.

**KrakenShield**

PRIVACY AUDIT REPORT

**example.com**

70 / 100

**C**

REPORT GRADE

Observation score. Partial result.

0 high signals   3 checks   1/3 scenarios usable

PRIORITY FINDINGS

**TO CHECK**   Privacy policy link not detected

**TO CHECK**   Legal notice link not detected

**TO CHECK**   Referrer policy missing

Critical category not used. Refusal and acceptance unverified.  
Technical observation. Supplied report, 5 Oct 2026, pp. 1-3.

ANONYMISED REPORT EXCERPT / example.com

C / 70 is a partial result: only 1 of 3 scenarios was usable. Privacy and legal notice links were not detected; referrer policy needs review.

### 01 Homepage

Open in browser



### 02 Clean sessions

Before / refuse / accept



### 03 Compare

Storage and requests



### 04 Review

Findings and limits

Technical homepage observation, not legal certification. Refusal and acceptance remain unverified in this example.



## Code analysis

Turn scan data into a review backlog.

### SCA

Match detected dependency versions against vulnerability advisories.

### Secrets

Flag possible embedded credentials for review.

### SAST + SBOM

Review static patterns and a CycloneDX component inventory.

**KrakenShield**  
CODE SECURITY REPORT  
**example.com**  
812 findings

REPORT GRADE

42 third-party components scanned

0 critical 5 high 371 medium 436 low

PRIORITY FINDINGS

HIGH TinyMCE 6.8.6: XSS advisories

28 FLAGS Potential secrets to review

717 FLAGS Static code analysis findings

Validate exploitability and flagged patterns before fixing.  
Demo domain. Supplied report, 7 Oct 2026, pp. 1, 4.

ANONYMISED REPORT EXCERPT / example.com

Grade D: 812 findings across 42 components. 0 critical, 5 high, 371 medium and 436 low. Examples include TinyMCE XSS advisories, 28 potential secrets and 717 SAST flags.

#### 01 Local project

Read source locally



#### 02 Scan data

Selected findings



#### 03 Prioritise

Review and assign



#### 04 Fix + rescan

Test corrections

Validate exploitability and patterns. Source files are read locally; selected findings and component data feed the report.



# Penetration test

A defined target. A controlled test.

## Authorise

Prove domain control and activate the testing mandate.

## Scope

Define permitted targets and the testing window.

## Control

Use an enrolled runner, follow progress and stop the test.

**KrakenShield**  
**PENETRATION TEST REPORT**  
**example.com**  
**22 findings**

**B**  
REPORT GRADE

**External test behind a WAF**

0 critical 0 high 2 medium 7 low 13 info

**PRIORITY FINDINGS**

**MEDIUM** Login CSP allows broad script sources

**LOW** Development files publicly served

**LOW** Cookies lack protection attributes

The WAF affected testing and may hide application issues.  
Demo domain. Supplied report, 4 Oct 2026, pp. 1, 5-6.

ANONYMISED REPORT EXCERPT / example.com

Grade B: 22 findings, including 0 critical, 0 high, 2 medium, 7 low and 13 informational. Review login CSP, exposed development files and cookie protections.

### 01 Authorise

Control and mandate



### 02 Scope

Targets and window



### 03 Run tests

Configured checks



### 04 Review

Evidence and limits

The WAF affected the test and may hide application issues. Coverage depends on scope and scanner templates.



# Evidence first. Action next.

A scan is the start of a review, not the end of security work.

## 01 / Validate in context

Confirm affected versions, reachable functionality and compensating controls. A component match or pattern requires application-specific review.

## 02 / Assign the next change

Give each confirmed issue an owner. Prioritise by severity, exposure and business impact. Test the correction before deployment.

## 03 / Rescan and compare

Check the finding again after the change. Keep evidence of the result and review issues outside the tested scope.

## OWASP-related checks, with a defined scope.

The pentest can include SQL injection detection, template-dependent XSS checks, security misconfiguration, exposed files and services. This does not imply a full OWASP Top 10 assessment.



# Train yourself. Train your team.

Belinda and Nestor make everyday cybersecurity habits concrete.



## Your expert learning companions

The Cyber reflexes course combines 12 short modules with a final assessment. Learn individually or through your organisation, with progress tracking and verifiable completion evidence.

### Everyday situations

- QR codes and suspicious links.
- Travel and screen privacy.
- Backups and recovery checks.
- Visitor access and badges.
- Safe sharing and location clues.

### A practical learning path

- Follow the modules.
- Review scenarios and key habits.
- Complete the final assessment.
- Earn your Awareness credential.
- Keep practising with your team.



## Make progress visible.

KrakenShield credentials connect learning with practical use of the platform.



### Awareness

Complete the 12-module Cyber reflexes course and pass its final assessment. A milestone for everyday security habits.



### Associate

Build and assess your cybersecurity foundations through the KrakenShield Associate examination. Explore the preparation and assessment in your account.



### Cybersecurity Master

Hold the KrakenShield Associate badge and run all four audits: Surface, Privacy, Code Analysis and Penetration Test. Available now.

[Explore the credentials and their requirements](#)



KrakenShield

START WITH KRAKENSHIELD

# Your next step starts here.

Audit your website. Build your expertise. Train your team.



## Explore KrakenShield

Create your account, choose the audit that answers your first question, then turn the findings into a practical action plan. Continue learning with KrakenShield Academy.

**krakenshield.eu**

### REPORT SOURCES & READING NOTES

Supplied reports: Surface, 6 Oct 2026 (pp. 1-2); Privacy, 5 Oct 2026 (pp. 1-3); Code rescan, 7 Oct 2026 (pp. 1, 4); Pentest, 4 Oct 2026 (pp. 1, 5-6). Grades use different scopes and are not directly comparable. example.com is an anonymisation alias, not a new scan. Brand scenes are illustrative.