WEBSITE SECURITY / ACTION REPORT

Understand the risk. Know what to fix.

https://invoice-lab.example

A readable assessment for business owners and the people who maintain their website.

RECORDED FINDINGS	SCAN STATUS	REVIEW STATUS
1	Completed	Human review needed

What this report gives you

A prioritized finding list, plain-language impact, supporting evidence, remediation guidance and a checklist for confirming fixes.

Read the summary first. Share the finding details with your developer or security team. After changes, arrange a scoped retest.

Report reference: SAMPLE / FICTIONAL DATA

Prepared: 2026-09-22

This is an illustrative report using fictional lab data. It is not evidence about your website.

Executive summary

The assessment recorded 1 finding(s). Review the evidence before making changes and confirm fixes with a retest.

PRIORITY	COUNT	HOW TO USE IT
CRITICAL	0	Urgent review and containment with your technical team.
HIGH	0	Prioritize remediation after confirming the evidence.
MEDIUM	1	Schedule a fix and check related configuration.
LOW	0	Address through normal hardening work.
INFO	0	Context for your team; not a confirmed exploit.

Your immediate next step

Assign a technical owner to each recorded finding. Check whether the affected endpoint or setting exists in your environment, reproduce only within authorized scope, apply the fix, and save retest evidence.

Recorded coverage

The engine logged 8 reviewed surfaces and 1 coverage gap(s). These are engine records, not independent assurance that every route or vulnerability class was tested.

Scope and limitations

Target: https://invoice-lab.example
Scope: the approved HTTPS hostname on port 443. No subdomains or third-party services are implied. This run does not establish full authenticated-user, source-code, infrastructure, load-test or regulatory coverage.

How results are counted

Counts and finding details in this PDF come from the structured findings file. Narrative-only observations are not promoted into confirmed findings. Automated severity and evidence still require human review. Where no evidence was recorded, this report says so.

FINDING 01 / MEDIUM

A sensitive endpoint is listed in robots.txt

What was observed

The fictional Invoice Lab lists /debug/config in its public robots.txt file. Anyone can read this file and learn that the endpoint exists. A Disallow entry is a crawler instruction, not an access-control rule.

Why it matters

This can make sensitive endpoints easier to discover. The risk depends on whether the endpoint is accessible and what it exposes; the path listing alone does not prove customer data was stolen.

Affected area

/robots.txt

Supporting evidence

Illustrative request: GET /robots.txt
Illustrative response: 200 OK
User-agent: *
Disallow: /debug/config

Recommended remediation

1. Remove sensitive path names from public crawler instructions where appropriate.
2. Remove the debug endpoint from production, or enforce server-side authentication and authorization.
3. Confirm that unauthenticated requests to the endpoint are rejected. Removing a robots.txt line alone does not secure it.

Technical explanation

robots.txt is intended for cooperative crawlers. It neither authenticates users nor prevents direct requests to listed paths. This example uses fictional data and demonstrates the report format.

Engine-reported CVSS: 5.3. This technical score is not a measure of your business loss.

Confirm the fix

Repeat the authorized check after remediation. Confirm the original behavior is no longer reproducible and that legitimate user activity still works. Record who tested it, when, and what evidence supports closure.

Turn findings into action

1. Review and assign

Share this report with the person responsible for your website. Confirm each finding and assign an owner. Avoid making production changes solely from an automated severity label.

2. Fix in a controlled environment

Back up relevant configuration, test the proposed change in staging and check normal user journeys. Schedule production changes through your usual process.

3. Retest and record

Recheck the affected behavior within the agreed scope. Save evidence of the fix and any remaining limitations. A later scan is a new assessment, not a guarantee of ongoing security.

4. Keep the report private

Findings can help someone target your website. Share only with authorized colleagues. Protego report objects expire after 30 days; downloaded or emailed copies remain under the recipient's control.

How this service is built

Strix is an open-source AI penetration-testing tool from usestrix. Protego wraps that engine with an online workflow, scoped AWS execution, Claude via Amazon Bedrock, payment integration and customer reporting. Protego did not create Strix and is not presented as endorsed by its maintainers.

Technology and support

Strix is licensed under Apache License 2.0. Project: github.com/usestrix/strix. Protego prepares this report independently. Questions about delivery or a finding: contact@protego.me. Include your report reference, and do not send passwords or sensitive evidence in an initial email.