Sample Security Review Report

Prepared by Alekh Verma - Ethical Hacker & Cybersecurity Builder

Report Type	Website / Web App Security Review Sample
Client	Demo Client - Example Only
Scope	Public website and approved configuration review only
Status	Sample document for format preview
Website	https://alekhverma.vercel.app/services

Important: This is a sample report used to show structure, tone, and deliverable quality. It does not describe a real client, real target, or live vulnerability. All cybersecurity services require clear permission and approved scope.

Breaking limits, not laws. Security is discipline, not decoration.

1. Executive Summary

This sample report demonstrates how a security review can be presented to a founder, website owner, developer, or small business. The goal is simple: identify practical risks, explain them clearly, and provide fix-first guidance without harmful exploitation steps.

Overall risk level	**Medium** - based on sample observations
Primary concern	Misconfiguration and missing protective controls
Recommended action	Fix high-priority configuration gaps first, then perform a retest
Delivery style	Business-readable report with clear technical guidance

2. Approved Scope

- Review only the website/app, domain, repository, or cloud rules explicitly approved by the owner.
- No testing of third-party systems, personal accounts, or services outside the written scope.
- No data theft, phishing, malware, account takeover, bypassing, or illegal access.
- Findings are written for defense, remediation, and risk reduction.

3. Sample Finding Summary

#	Finding	Severity	Status
1	Missing or weak browser security headers	Medium	Fix recommended
2	Public diagnostic or metadata exposure risk	Low	Review recommended
3	Repository and deployment secret hygiene needs improvement	Medium	Fix recommended

Missing or weak browser security headers

Finding title	Missing or weak browser security headers
Severity	**Medium**
Affected area	Public website response headers
Impact	May reduce browser-side protection and weaken visitor safety posture.
Evidence	Observed header posture does not show every recommended protective control. Evidence would be provided as a safe screenshot or header summary in a real report.
Recommended fix	Add and verify a clear security header policy appropriate to the application, then retest in production.
Priority	Fix in the next update cycle.

Public diagnostic or metadata exposure risk

Finding title	Public diagnostic or metadata exposure risk
Severity	**Low**
Affected area	Public files, metadata paths, build artifacts, or diagnostic endpoints
Impact	Unnecessary public information can help attackers understand the technology stack or deployment habits.
Evidence	Sample-only observation. In a real review, only safe non-sensitive evidence would be shown.
Recommended fix	Remove unnecessary public debug files, restrict diagnostic endpoints, and keep only intended public assets.
Priority	Review during the next cleanup and deployment pass.

Repository and deployment secret hygiene needs improvement

Finding title	Repository and deployment secret hygiene needs improvement
Severity	**Medium**
Affected area	GitHub, deployment environment, environment variables, and public repo configuration
Impact	Exposed secrets or unsafe deployment settings can lead to account compromise, data exposure, or service abuse.
Evidence	The real report would list safe file/path references without revealing secret values.
Recommended fix	Rotate any exposed credentials, audit environment variables, protect production branches, and verify deployment settings.
Priority	Fix immediately if any live secret is confirmed.

4. Fix Priority Checklist

- **Priority 1:** Confirm ownership and approved scope before any active testing.
- **Priority 2:** Resolve exposed secrets, unsafe permissions, or public data exposure first.
- **Priority 3:** Improve headers, deployment hygiene, account security, and backup readiness.
- **Priority 4:** Retest fixes and document what changed.

5. Report Delivery Format

A real paid engagement can include a PDF report, summary message, remediation checklist, screenshots where useful, and optional follow-up retest guidance. The final format depends on the service scope and client needs.

Deliverables	Executive summary, findings, evidence, fix steps, priority checklist, scope notes
Payment flow	Manual UPI/bank payment after scope approval
Work starts	After payment confirmation and written scope approval
Report goal	Help the client fix risk, not provide harmful abuse instructions

6. Authorization Statement

All cybersecurity work must be authorized by the owner or responsible party. Requests involving illegal access, account hacking, data theft, bypassing systems, phishing, malware, or testing without permission are not accepted.

Contact: https://alekhverma.vercel.app/services
Official profile: https://alekhverma.vercel.app/alekh-verma