HACK MY WEBSITE

Security Assessment Report

CRITICAL

A founder-ready assessment of launch risk, business impact, and the fixes your team should prioritize first.

ASSESSMENT TARGET
https://launch-ready-demo.ai

SCAN COMPLETED
08 Jul 2026 14:20 India Standard Time

GENERATED
08 Jul 2026 19:50 India Standard Time

METHOD
OWASP ZAP + Semgrep + Nuclei + AI narrative synthesis

RISK SCORE	TOTAL FINDINGS	HIGHEST SEVERITY
68	**6**	**CRITICAL**
Out of 100	Structured issues in final report	Top-priority issue class

Executive perspective

This sample report shows the kind of issues we regularly expect on fast-built AI websites: weak headers, exposed assets, unsafe admin surfaces, and overly trusting browser or API behavior. None of these are theoretical. A motivated attacker could use them to map the application, steal session context, or move toward sensitive customer workflows.

Top findings surfaced

- Public admin route discoverable
- Production source map exposed
- Missing Content-Security-Policy

EXECUTIVE SUMMARY

A cleaner founder view of what the scan actually means

This sample report shows the kind of issues we regularly expect on fast-built AI websites: weak headers, exposed assets, unsafe admin surfaces, and overly trusting browser or API behavior. None of these are theoretical. A motivated attacker could use them to map the application, steal session context, or move toward sensitive customer workflows.

TOTAL FINDINGS	CRITICAL + HIGH	RISK SCORE
6	3	68
Items included in this report	Issues most likely to block launch	Overall weighted exposure

Severity	Count	Interpretation
Critical	1	Immediate business risk or exploit path
High	2	Strong candidate for first remediation cycle
Medium	3	Should be fixed before broader growth
Low	2	Hardening issue that still improves resilience

WHAT MATTERS MOST

- Public admin route discoverable affects https://launch-ready-demo.ai/admin and should be reviewed as a critical-priority issue.
- Production source map exposed affects https://launch-ready-demo.ai/_next/static/chunks/app.js.map and should be reviewed as a high-priority issue.
- Missing Content-Security-Policy affects https://launch-ready-demo.ai/ and should be reviewed as a high-priority issue.

WHAT TO FIX FIRST

- Public admin route discoverable: if not request.user.is_admin:\n raise HTTPException(status_code=403, detail='Admin access required')
- Production source map exposed: productionBrowserSourceMaps: false
- Missing Content-Security-Policy: Content-Security-Policy: default-src 'self'; script-src 'self'; object-src 'none'; base-uri 'self'; frame-ancestors 'none';

QUICK WINS

- Cookie missing strict SameSite protection: harden session cookie attributes and confirm they are emitted consistently.
- Overly broad CORS policy on API route: close this hardening gap during the next deployment cycle and re-run the scan.
- Google API key exposed in frontend bundle context: close this hardening gap during the next deployment cycle and re-run the scan.

SINCE LAST SCAN

This is the first completed scan for this domain. Your next scan will show score movement, fixed issues, and newly introduced findings.

RETEST SUMMARY

No retest activity has been saved for the findings in this scan yet. Retesting becomes useful after fixes are deployed.

SCAN SCOPE AND LIMITATIONS

- Scan mode used: Public.
- Authentication method: None.
- Pages crawled: 6.
- Authenticated routes reached: 0.
- APIs observed: 1.
- JavaScript assets analyzed: 1.
- Seeded routes requested: None.
- Seeded routes reached: None.
- Browser login result: Not used.
- Authenticated findings tied to seeded routes: 0.
- Role comparison was not run for this scan.

FINDING 01 OF 06

Public admin route discoverable

SEVERITY	OWASP	TOOL SOURCE	CONFIDENCE	AFFECTED TARGET
CRITICAL	A01:2021 - Broken Access Control	Nuclei + custom route exposure check	High	https://launch-ready-demo.ai/admin

WHAT THIS MEANS

A sensitive admin-style route was publicly reachable and exposed enough structure to confirm that the application has privileged management surfaces on the public internet.

BUSINESS IMPACT

If authentication or authorization controls around this path are weak anywhere else in the stack, this becomes a direct path to user records, configuration, or internal actions.

ATTACK SCENARIO

A sensitive admin-style route was publicly reachable and exposed enough structure to confirm that the application has privileged management surfaces on the public internet.

TECHNICAL DETAILS

Tool source: Nuclei + custom route exposure check. Reference: The scanner identified a live /admin route with a recognizable login shell and response signature that confirms an admin surface exists publicly..

EVIDENCE FOUND

- Scanner source: NUCLEI + CUSTOM ROUTE EXPOSURE CHECK.
- A sensitive admin-style route was publicly reachable and exposed enough structure to confirm that the application has privileged management surfaces on the public intern…
- Scanner confidence: High
- Reference: The scanner identified a live /admin route with a recognizable login shell and response signature that confirms an admin surface exists publicly.

RECOMMENDED REMEDIATION

- Restrict the route behind IP allowlists, private networking, or zero-trust access.
- Require strong server-side authorization for every admin action.
- Rate-limit and monitor all admin authentication attempts.

CURSOR / CLAUDE CODE FIX PROMPT

Copy and paste this into your AI editor to fix this issue automatically:

```
Review the component/file at "https://launch-ready-demo.ai/admin" and resolve the "Public admin route discoverable" vulnerability by applying these fixes: Restrict the route behind IP allowlists, private networking, or zero-trust access.; Require strong server-side authorization for every admin action.; Rate-limit and monitor all admin authentication attempts..
```

Launch note: Treat this as a launch blocker until the issue is remediated and re-tested.

FINDING 02 OF 06

Production source map exposed

SEVERITY	OWASP	TOOL SOURCE	CONFIDENCE	AFFECTED TARGET
HIGH	A05:2021 - Security Miscon figuration	Custom AI-built website check	High	https://launch-ready-demo.ai/_next/static/chunks/app.js.map

WHAT THIS MEANS

A production JavaScript source map was publicly accessible, making the application easier to reverse-engineer.

BUSINESS IMPACT

Source maps can reveal internal file structure, component names, API paths, and implementation details that reduce the effort required for targeted attacks.

ATTACK SCENARIO

A production JavaScript source map was publicly accessible, making the application easier to reverse-engineer.

TECHNICAL DETAILS

Tool source: Custom AI-built website check. Reference: A .map asset returned a successful response and exposed original source references from the production bundle..

EVIDENCE FOUND

- Scanner source: CUSTOM AI-BUILT WEBSITE CHECK.
- A production JavaScript source map was publicly accessible, making the application easier to reverse-engineer.
- Scanner confidence: High
- Reference: A .map asset returned a successful response and exposed original source references from the production bundle.

RECOMMENDED REMEDIATION

- Disable production source maps in your frontend build.
- Invalidate any already-cached source map URLs from the CDN.
- Re-scan after deployment to confirm the files are no longer reachable.

CURSOR / CLAUDE CODE FIX PROMPT

Copy and paste this into your AI editor to fix this issue automatically:

```
Review the component/file at
"https://launch-ready-demo.ai/_next/static/chunks/app.js.map" and resolve the
"Production source map exposed" vulnerability by applying these fixes: Disable
production source maps in your frontend build.; Invalidate any already-cached source
map URLs from the CDN.; Re-scan after deployment to confirm the files are no longer
reachable..
```

Launch note: This should be part of the first remediation sprint before driving more traffic to the site.

FINDING 03 OF 06

Missing Content-Security-Policy

SEVERITY	OWASP	TOOL SOURCE	CONFIDENCE	AFFECTED TARGET
HIGH	A05:2021 - Security Miscon figuration	OWASP ZAP + header hardening check	High	https://launch-ready-demo.ai/

WHAT THIS MEANS

The main application response did not set a Content-Security-Policy header.

BUSINESS IMPACT

Without CSP, any client-side injection issue becomes much easier to weaponize because the browser has fewer limits on script execution sources.

ATTACK SCENARIO

The main application response did not set a Content-Security-Policy header.

TECHNICAL DETAILS

Tool source: OWASP ZAP + header hardening check. Reference: The scanner captured the main page response headers and confirmed that CSP was missing from the production response..

EVIDENCE FOUND

- Scanner source: OWASP ZAP + HEADER HARDENING CHECK.
- The main application response did not set a Content-Security-Policy header.
- Scanner confidence: High
- Reference: The scanner captured the main page response headers and confirmed that CSP was missing from the production response.

RECOMMENDED REMEDIATION

- Define a strict Content-Security-Policy for scripts, styles, images, and connections.
- Start with report-only mode if needed, then move to enforcement.

CURSOR / CLAUDE CODE FIX PROMPT

Copy and paste this into your AI editor to fix this issue automatically:

```
Review the component/file at "https://launch-ready-demo.ai/" and resolve the
"Missing Content-Security-Policy" vulnerability by applying these fixes: Define a
strict Content-Security-Policy for scripts, styles, images, and connections.; Start
with report-only mode if needed, then move to enforcement..
```

Launch note: This should be part of the first remediation sprint before driving more traffic to the site.

FINDING 04 OF 06

Cookie missing strict SameSite protection

SEVERITY	OWASP	TOOL SOURCE	CONFIDENCE	AFFECTED TARGET
MEDIUM	A07:2021 - Identification and Authentication Failures	Header and cookie check	Medium	https://launch-ready-demo.ai/login

WHAT THIS MEANS

The session cookie did not use the strongest cross-site restriction available for this flow.

BUSINESS IMPACT

Weak cookie attributes can increase exposure to cross-site request scenarios and session abuse, especially in mixed-origin deployments.

ATTACK SCENARIO

The session cookie did not use the strongest cross-site restriction available for this flow.

TECHNICAL DETAILS

Tool source: Header and cookie check. Reference: The Set-Cookie header was observed without the expected strict SameSite setting for a login or session cookie..

EVIDENCE FOUND

- Scanner source: HEADER AND COOKIE CHECK.
- The session cookie did not use the strongest cross-site restriction available for this flow.
- Scanner confidence: Medium
- Reference: The Set-Cookie header was observed without the expected strict SameSite setting for a login or session cookie.

RECOMMENDED REMEDIATION

- Use Secure, HttpOnly, and the strongest valid SameSite policy for your product flow.
- Review whether any third-party redirect flow truly requires a weaker cookie policy.

CURSOR / CLAUDE CODE FIX PROMPT

Copy and paste this into your AI editor to fix this issue automatically:

```
Review the component/file at "https://launch-ready-demo.ai/login" and resolve the "Cookie missing strict SameSite protection" vulnerability by applying these fixes: Use Secure, HttpOnly, and the strongest valid SameSite policy for your product flow.; Review whether any third-party redirect flow truly requires a weaker cookie policy..
```

Launch note: This should be scheduled before broader scale-up so small weaknesses do not stack into larger risk.

FINDING 05 OF 06

Overly broad CORS policy on API route

SEVERITY	OWASP	TOOL SOURCE	CONFIDENCE	AFFECTED TARGET
MEDIUM	A05:2021 - Security Miscon figuration	Custom API behavior check	Medium	https://launch-ready-demo.ai/api/profile

WHAT THIS MEANS

An API response accepted a broader origin pattern than expected for a user-data endpoint.

BUSINESS IMPACT

Loose CORS policies increase the chance that sensitive API responses can be requested from unintended browser origins if other auth controls are weak.

ATTACK SCENARIO

An API response accepted a broader origin pattern than expected for a user-data endpoint.

TECHNICAL DETAILS

Tool source: Custom API behavior check. Reference: The endpoint responded with an Access-Control-Allow-Origin value that was broader than the expected production frontend origin..

EVIDENCE FOUND

- Scanner source: CUSTOM API BEHAVIOR CHECK.
- An API response accepted a broader origin pattern than expected for a user-data endpoint.
- Scanner confidence: Medium
- Reference: The endpoint responded with an Access-Control-Allow-Origin value that was broader than the expected production frontend origin.

RECOMMENDED REMEDIATION

- Allow only the exact production frontend origin.
- Avoid wildcard or environment-wide defaults for authenticated endpoints.

CURSOR / CLAUDE CODE FIX PROMPT

Copy and paste this into your AI editor to fix this issue automatically:

```
Review the component/file at "https://launch-ready-demo.ai/api/profile" and resolve the "Overly broad CORS policy on API route" vulnerability by applying these fixes: Allow only the exact production frontend origin.; Avoid wildcard or environment-wide defaults for authenticated endpoints..
```

Launch note: This should be scheduled before broader scale-up so small weaknesses do not stack into larger risk.

FINDING 06 OF 06

Google API key exposed in frontend bundle context

SEVERITY	OWASP	TOOL SOURCE	CONFIDENCE	AFFECTED TARGET
LOW	A02:2021 - Cryptographic Failures	Custom secret pattern check	High	https://launch-ready-demo.ai/_next/static/chunks/main.js

WHAT THIS MEANS

A public-facing JavaScript bundle contained a Google API key pattern that should be reviewed for scope and restrictions.

BUSINESS IMPACT

Some frontend keys are expected to be public, but they still need strict domain restrictions and service scoping to avoid abuse and billing exposure.

ATTACK SCENARIO

A public-facing JavaScript bundle contained a Google API key pattern that should be reviewed for scope and restrictions.

TECHNICAL DETAILS

Tool source: Custom secret pattern check. Reference: The scanner matched a Google API key pattern in a production JavaScript asset and flagged it for scope review..

EVIDENCE FOUND

- Scanner source: CUSTOM SECRET PATTERN CHECK.
- A public-facing JavaScript bundle contained a Google API key pattern that should be reviewed for scope and restrictions.
- Scanner confidence: High
- Reference: The scanner matched a Google API key pattern in a production JavaScript asset and flagged it for scope review.

RECOMMENDED REMEDIATION

- Restrict the key to the exact production domains.
- Disable unused Google APIs tied to the key.
- Rotate the key if its scope is broader than intended.

CURSOR / CLAUDE CODE FIX PROMPT

Copy and paste this into your AI editor to fix this issue automatically:

```
Review the component/file at
"https://launch-ready-demo.ai/_next/static/chunks/main.js" and resolve the "Google
API key exposed in frontend bundle context" vulnerability by applying these fixes:
Restrict the key to the exact production domains.; Disable unused Google APIs tied to
the key.; Rotate the key if its scope is broader than intended..
```

Launch note: This is a hardening item that still improves trust and resilience when cleaned up.