

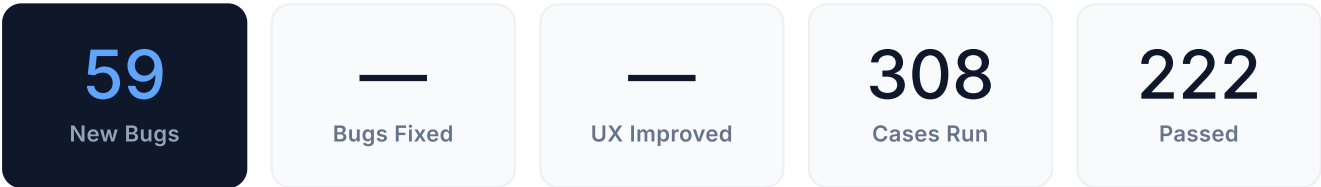
QUALITY ASSURANCE

example-coffee-shop.com

Automated scan of example-coffee-shop.com via QA Explorer.
Covered 50 pages, ran 308 scripted test cases (222 passed), and surfaced 59 unique findings across functionality, UX, accessibility, performance, and security.

CONFIDENTIAL

ENVIRONMENT	https://example-coffee-shop.com
PROJECT	example-coffee-shop.com
METHODOLOGY	Automated end-to-end exploratory scan (browser automation + DOM extraction)
TESTER	QA Explorer (automated)
REPORT DATE	2026-06-07



59 findings · 8 high · 59 unique

Production Impact: 8 high-severity findings should be addressed before this build is promoted.

1 Executive Summary

Example Coffee Shop's website is a functioning e-commerce platform for specialty coffee with solid fundamentals: all 49 reachable pages return successful responses, SSL/TLS is in place, and basic meta infrastructure is present. However, the scan uncovered a broad set of security, accessibility, and content-quality issues that collectively present real risk to customers, the business's legal standing under GDPR/KVKK, and search engine visibility.

The most serious concerns are security-related. Forms across the site — including the login, registration, and checkout flows — lack CSRF protection, meaning an attacker could trick a logged-in customer into placing orders or changing account data without their knowledge. The XSRF-TOKEN cookie is not marked HttpOnly, making it readable by JavaScript and vulnerable to theft. There is no Content Security Policy, leaving the site open to cross-site scripting attacks. Additionally, no cookie consent banner is present despite third-party cookies being set on load, which is a direct violation of Turkish KVKK and EU GDPR rules and exposes the business to regulatory fines. A required legal document (the KVKK application form PDF) is completely inaccessible — a broken link on a compliance page.

Accessibility is a systemic weakness: 215 buttons and 392 links have no readable label for screen-reader users, colour contrast fails on multiple pages, and nearly every inner page is missing a unique meta description and Open Graph metadata, severely hurting SEO and social sharing. The homepage alone weighs 4.81 MB, which will result in slow load times on mobile connections. The team should prioritise CSRF protection and cookie consent first as legal/security obligations, then address accessibility and SEO gaps which directly affect customer reach and inclusivity.

Production impact. 8 high-severity findings should be addressed before this build is promoted.

2 Test Scope & Environment

FIELD	VALUE
Application	example-coffee-shop.com
Environment	https://example-coffee-shop.com
Methodology	Automated end-to-end exploratory scan — a headless browser crawls same-origin links, captures DOM/console/screenshots, analyzer derives findings.
Pages Scanned	50
Duration	9 min 45 s
Report ID	3a20b969-f0cb-4740-a2d6-cd7a9a22a5d9
Analyzer	QA Explorer Engine

3

Test Execution Details

Scripted test cases executed against the target. Status values follow the test runner's convention (PASS / FAIL / UX / BLOCKED).

TS-NAV — Navigation & Page Load Tests

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Open homepage	The homepage should load successfully with all primary content visible.	HTTP 200, loaded in 2.59s, 23 headings, 84 links, 17 images.	✓ PASS
2	Open Alisveris page	The Alisveris page should load successfully with all content visible.	HTTP 200, loaded in 2.33s, 73 headings, 266 links, 69 images.	✓ PASS
3	Open Kahveler page	The Kahveler page should load successfully with all content visible.	HTTP 200, loaded in 2.54s, 27 headings, 128 links, 23 images.	✓ PASS
4	Open Ekipmanlar page	The Ekipmanlar page should load successfully with all content visible.	HTTP 200, loaded in 2.31s, 37 headings, 156 links, 33 images.	✓ PASS
5	Open Aksesuar page	The Aksesuar page should load successfully with all content visible.	HTTP 200, loaded in 2.65s, 31 headings, 138 links, 27 images.	✓ PASS
6	Open Abonelikler page	The Abonelikler page should load successfully with all content visible.	HTTP 200, loaded in 2.32s, 28 headings, 74 links, 15 images.	✓ PASS
7	Open Kahve Aboneliği Otomatik Kahve Makinesi page	The Kahve Aboneliği Otomatik Kahve Makinesi page should load successfully with all content visible.	HTTP 200, loaded in 1.91s, 28 headings, 75 links, 11 images.	✓ PASS
8	Open Kahve Aboneliği Espresso page	The Kahve Aboneliği Espresso page should load successfully with all content visible.	HTTP 200, loaded in 2.04s, 28 headings, 75 links, 11 images.	✓ PASS
9	Open Kahve Aboneliği page	The Kahve Aboneliği page should load successfully with all content visible.	HTTP 200, loaded in 2.08s, 28 headings, 75 links, 11 images.	✓ PASS
10	Open Demleme Teknikleri page	The Demleme Teknikleri page should load successfully with all content visible.	HTTP 200, loaded in 2.35s, 18 headings, 77 links, 16 images.	✓ PASS

11	Open Filtre Kahve page	The Filtre Kahve page should load successfully with all content visible.	HTTP 200, loaded in 2.08s, 21 headings, 70 links, 8 images.	✓ PASS
12	Open Espresso page	The Espresso page should load successfully with all content visible.	HTTP 200, loaded in 2.30s, 19 headings, 70 links, 8 images.	✓ PASS
13	Open French Press page	The French Press page should load successfully with all content visible.	HTTP 200, loaded in 2.08s, 21 headings, 70 links, 8 images.	✓ PASS
14	Open Moka Pot page	The Moka Pot page should load successfully with all content visible.	HTTP 200, loaded in 2.18s, 21 headings, 70 links, 8 images.	✓ PASS
15	Open Hario V60 page	The Hario V60 page should load successfully with all content visible.	HTTP 200, loaded in 2.15s, 21 headings, 70 links, 8 images.	✓ PASS
16	Open Aeropress page	The Aeropress page should load successfully with all content visible.	HTTP 200, loaded in 2.09s, 21 headings, 70 links, 8 images.	✓ PASS
17	Open Turk Kahvesi page	The Turk Kahvesi page should load successfully with all content visible.	HTTP 200, loaded in 2.04s, 21 headings, 70 links, 8 images.	✓ PASS
18	Open Magazalar page	The Magazalar page should load successfully with all content visible.	HTTP 200, loaded in 3.10s, 11 headings, 109 links, 112 images.	✓ PASS
19	Open Makaleler page	The Makaleler page should load successfully with all content visible.	HTTP 200, loaded in 2.65s, 20 headings, 79 links, 20 images.	✓ PASS
20	Open Kahveni Bul page	The Kahveni Bul page should load successfully with all content visible.	HTTP 200, loaded in 2.13s, 19 headings, 71 links, 7 images.	✓ PASS
21	Open Kaydol page	The Kaydol page should load successfully with all content visible.	HTTP 200, loaded in 2.09s, 11 headings, 74 links, 7 images.	✓ PASS
22	Open Oturumac page	The Oturumac page should load successfully with all content visible.	HTTP 200, loaded in 2.08s, 11 headings, 72 links, 7 images.	✓ PASS
23	Open homepage	The homepage should load successfully with all primary content visible.	HTTP 200, loaded in 2.41s, 23 headings, 84 links, 17 images.	✓ PASS

24	Open Kahve Abonelikleri page	The Kahve Abonelikleri page should load successfully with all content visible.	HTTP 200, loaded in 2.62s, 28 headings, 74 links, 15 images.	✓ PASS
25	Open Iletisim page	The Iletisim page should load successfully with all content visible.	HTTP 200, loaded in 2.29s, 11 headings, 70 links, 7 images.	✓ PASS
26	Open Example Coffee Shop Grounded Collection Oversized White T Shirt page	The Example Coffee Shop Grounded Collection Oversized White T Shirt page should load successfully with all content visible.	HTTP 200, loaded in 2.20s, 15 headings, 76 links, 12 images.	✓ PASS
27	Open Grounded Collection Oversized Green Hoodie page	The Grounded Collection Oversized Green Hoodie page should load successfully with all content visible.	HTTP 200, loaded in 2.35s, 15 headings, 76 links, 12 images.	✓ PASS
28	Open Etiyopya Korcha Natural Filtre page	The Etiyopya Korcha Natural Filtre page should load successfully with all content visible.	HTTP 200, loaded in 2.34s, 16 headings, 76 links, 13 images.	✓ PASS
29	Open Latte Fincani Logolu page	The Latte Fincani Logolu page should load successfully with all content visible.	HTTP 200, loaded in 2.26s, 14 headings, 75 links, 11 images.	✓ PASS
30	Open Etkinlik Egitim page	The Etkinlik Egitim page should load successfully with all content visible.	HTTP 200, loaded in 2.07s, 11 headings, 75 links, 7 images.	✓ PASS
31	Open Hikayemiz page	The Hikayemiz page should load successfully with all content visible.	HTTP 200, loaded in 2.04s, 11 headings, 70 links, 9 images.	✓ PASS
32	Open Iletisim page	The Iletisim page should load successfully with all content visible.	HTTP 200, loaded in 2.27s, 11 headings, 70 links, 7 images.	✓ PASS
33	Open Sss page	The Sss page should load successfully with all content visible.	HTTP 200, loaded in 2.04s, 49 headings, 70 links, 9 images.	✓ PASS
34	Open Menuler page	The Menuler page should load successfully with all content visible.	HTTP 200, loaded in 2.37s, 11 headings, 70 links, 11 images.	✓ PASS

35	Open Kahve Hakkında page	The Kahve Hakkında page should load successfully with all content visible.	HTTP 200, loaded in 2.27s, 13 headings, 83 links, 8 images.	✓ PASS
36	Open Kvkk page	The Kvkk page should load successfully with all content visible.	HTTP 200, loaded in 2.22s, 11 headings, 70 links, 7 images.	✓ PASS
37	Open Aydınlatma page	The Aydınlatma page should load successfully with all content visible.	HTTP 200, loaded in 2.15s, 11 headings, 70 links, 7 images.	✓ PASS
38	Open Cerez page	The Cerez page should load successfully with all content visible.	HTTP 200, loaded in 2.09s, 11 headings, 70 links, 7 images.	✓ PASS
39	Load the PDF file at /pdf/kvkk_basvuru.pdf	The file should load successfully and display its content.	The file did not load. The server did not provide a response after 0.75 seconds, indicating the file may be unavailable or inaccessible.	✗ FAIL
40	Open Odeme page	The Odeme page should load successfully with all content visible.	HTTP 200, loaded in 2.92s, 11 headings, 72 links, 7 images.	✓ PASS
41	Open Hario V60 Dripper Seti page	The Hario V60 Dripper Seti page should load successfully with all content visible.	HTTP 200, loaded in 2.23s, 15 headings, 77 links, 11 images.	✓ PASS
42	Open Cezve page	The Cezve page should load successfully with all content visible.	HTTP 200, loaded in 2.27s, 15 headings, 77 links, 11 images.	✓ PASS
43	Open Hario Kettle Buono page	The Hario Kettle Buono page should load successfully with all content visible.	HTTP 200, loaded in 2.13s, 15 headings, 77 links, 13 images.	✓ PASS
44	Open Shopping page	The Shopping page should load successfully with all content visible.	HTTP 200, loaded in 2.46s, 73 headings, 266 links, 69 images.	✓ PASS
45	Open Filtre Kahve page	The Filtre Kahve page should load successfully with all content visible.	HTTP 200, loaded in 2.48s, 20 headings, 107 links, 16 images.	✓ PASS
46	Open Rare page	The Rare page should load successfully with all content visible.	HTTP 200, loaded in 2.51s, 21 headings, 84 links, 31 images.	✓ PASS

47	Open Espresso page	The Espresso page should load successfully with all content visible.	HTTP 200, loaded in 2.31s, 15 headings, 92 links, 11 images.	✓ PASS
48	Open Turk Kahvesi page	The Turk Kahvesi page should load successfully with all content visible.	HTTP 200, loaded in 2.21s, 12 headings, 83 links, 8 images.	✓ PASS
49	Open Ve Dahasi page	The Ve Dahasi page should load successfully with all content visible.	HTTP 200, loaded in 2.12s, 13 headings, 86 links, 9 images.	✓ PASS
50	Open Kenya Kirinyaga page	The Kenya Kirinyaga page should load successfully with all content visible.	HTTP 200, loaded in 2.18s, 15 headings, 76 links, 13 images.	✓ PASS

TS-LINKS — Internal Link Health

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	HEAD / "Anasayfa" · linked from 49 pages	The "Anasayfa" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
2	HEAD /alisveris "Online Dükkan" · linked from 49 pages	The "Online Dükkan" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
3	HEAD /alisveris/kategori/kahveler "Kahveler" · linked from 49 pages	The "Kahveler" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
4	HEAD /alisveris/kategori/ekipmanlar "Ekipmanlar" · linked from 49 pages	The "Ekipmanlar" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
5	HEAD /alisveris/kategori/aksesuar "Aksesuar" · linked from 48 pages	The "Aksesuar" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
6	HEAD /abonelikler "Abonelikler" · linked from 47 pages	The "Abonelikler" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
7	HEAD /alisveris/urun/kahve-abonelig-otomatik-kahve-makinesi "Otomatik Makineler" · linked from 47 pages	The "Otomatik Makineler" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
8	HEAD /alisveris/urun/kahve-abonelig-espresso "Espresso" · linked from 47 pages	The "Espresso" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS

9	HEAD /alisveris/urun/kahve-aboneliği "Filtre" · linked from 47 pages	The "Filtre" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
10	HEAD /demleme-teknikleri "Demleme Teknikleri" · linked from 49 pages	The "Demleme Teknikleri" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
11	HEAD /demleme-teknik/filtre-kahve "Filtre Kahve" · linked from 49 pages	The "Filtre Kahve" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
12	HEAD /demleme-teknik/espresso "Espresso" · linked from 49 pages	The "Espresso" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
13	HEAD /demleme-teknik/french-press "French Press" · linked from 49 pages	The "French Press" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
14	HEAD /demleme-teknik/moka-pot "Moka Pot" · linked from 49 pages	The "Moka Pot" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
15	HEAD /demleme-teknik/hario-v60 "Hario V60" · linked from 49 pages	The "Hario V60" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
16	HEAD /demleme-teknik/aeropress "Aeropress" · linked from 49 pages	The "Aeropress" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
17	HEAD /demleme-teknik/turk-kahvesi "Türk Kahvesi" · linked from 49 pages	The "Türk Kahvesi" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
18	HEAD /magazalar "Nerelerdeyiz" · linked from 49 pages	The "Nerelerdeyiz" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
19	HEAD /makaleler "Blog" · linked from 49 pages	The "Blog" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
20	HEAD /kahveni-bul "Kahveni Bul" · linked from 49 pages	The "Kahveni Bul" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
21	HEAD /kullanici/kaydol "Üye Ol" · linked from 49 pages	The "Üye Ol" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS

22	HEAD /kullanici/oturumac "Giriş Yap" · linked from 49 pages	The "Giriş Yap" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
23	HEAD /?setLang=en "EN"	The "EN" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
24	HEAD /alisveris/kategori/kahve-abonelikleri "Abonelikler" · linked from 49 pages	The "Abonelikler" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
25	HEAD /iletisim "Toptan Satış" · linked from 49 pages	The "Toptan Satış" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
26	HEAD .../urun/example-coffee-shop-grounded-collection-oversized-white-t-shirt "Grounded Collection Oversized White T-Shirt" · linked from 5 pages	The "Grounded Collection Oversized White T-Shirt" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
27	HEAD /alisveris/urun/grounded-collection-oversized-green-hoodie "Grounded Collection Oversized Green Hoodie" · linked from 5 pages	The "Grounded Collection Oversized Green Hoodie" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
28	HEAD /alisveris/urun/etiopya-korcha-natural-filtre "Etiopya Korcha Natural (Filtre)" · linked from 6 pages	The "Etiopya Korcha Natural (Filtre)" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
29	HEAD /alisveris/urun/latte-fincani-logo "Example Coffee Shop Latte Fincanı" · linked from 7 pages	The "Example Coffee Shop Latte Fincanı" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
30	HEAD /alisveris/kategori/etkinlik-egitim "Etkinlikler" · linked from 49 pages	The "Etkinlikler" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
31	HEAD /hikayemiz "Hikayemiz" · linked from 49 pages	The "Hikayemiz" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
32	HEAD /iletisim?kariyer=1 "Kariyer" · linked from 49 pages	The "Kariyer" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
33	HEAD /sss "S. S. S." · linked from 49 pages	The "S. S. S." link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS

34	HEAD /menu'ler "Menü" · linked from 49 pages	The "Menü" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
35	HEAD /kahve-hakkinda "Kahvelerimiz Hakkinda" · linked from 49 pages	The "Kahvelerimiz Hakkinda" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
36	HEAD /kvkk "KVKK ve Gizlilik Politikası" · linked from 49 pages	The "KVKK ve Gizlilik Politikası" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
37	HEAD /aydinlatma "Aydınlatma Metni" · linked from 49 pages	The "Aydınlatma Metni" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
38	HEAD /cerez "Çerez Politikası" · linked from 49 pages	The "Çerez Politikası" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
39	Check if the PDF file at /pdf/kvkk_basvuru.pdf is reachable	The file should be accessible and return a success response or a valid redirect.	The file is not reachable. No response was received from the server after 3.37 seconds.	✗ FAIL
40	HEAD /odeme "Satın Al" · linked from 49 pages	The "Satın Al" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
41	HEAD /alisveris/urun/Hario-v60-Dripper-seti "Sepete Ekle" · linked from 49 pages	The "Sepete Ekle" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
42	HEAD /alisveris/urun/cezve "Sepete Ekle" · linked from 49 pages	The "Sepete Ekle" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
43	HEAD /alisveris/urun/hario-kettle-buono "Sepete Ekle" · linked from 49 pages	The "Sepete Ekle" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
44	HEAD /shopping "EN" · linked from 3 pages	The "EN" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
45	HEAD /alisveris/kategori/filtre-kahve "Filtre Kahve" · linked from 8 pages	The "Filtre Kahve" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
46	HEAD /alisveris/kategori/rare "RARE" · linked from 8 pages	The "RARE" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS

47	HEAD /alisveris/kategori/Espresso "Espresso" · linked from 8 pages	The "Espresso" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
48	HEAD /alisveris/kategori/turk-kahvesi "Türk Kahvesi" · linked from 8 pages	The "Türk Kahvesi" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
49	HEAD /alisveris/kategori/ve-dahasi "Ve Dahası" · linked from 8 pages	The "Ve Dahası" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS
50	HEAD /alisveris/urun/kenya-kirinyaga "Kenya Kirinyaga Washed" · linked from 4 pages	The "Kenya Kirinyaga Washed" link should resolve to a working page.	Link resolves correctly (HTTP 200).	✓ PASS

TS-SEC — Security Headers & Cookies

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Check Strict-Transport-Security security header sampled 2 pages	Header present with max-age ≥ 31536000 (1 year)	Present, max-age=31536000; includeSubDomains.	✓ PASS
2	Verify Content-Security-Policy security header is set	The server should send a Content-Security-Policy header to protect against malicious scripts.	This security header is not set. The site is missing an important protection against code injection attacks.	✗ FAIL
3	Check X-Content-Type-Options security header sampled 2 pages	Header value is exactly "nosniff"	Present, nosniff.	✓ PASS
4	Check X-Frame-Options security header sampled 2 pages	DENY or SAMEORIGIN	Present, SAMEORIGIN.	✓ PASS
5	Check Referrer-Policy security header sampled 2 pages	Header present (any directive)	Present, strict-origin-when-cross-origin.	✓ PASS
6	Check Permissions-Policy security header sampled 2 pages	Header present (any directive set)	Present, geolocation=self.	✓ PASS
7	Check that the XSRF-TOKEN cookie is protected with the HttpOnly flag	The cookie should be marked HttpOnly so it cannot be accessed by JavaScript, preventing theft via malicious scripts.	The HttpOnly flag is not set on this cookie. A malicious script could potentially steal this token.	✗ FAIL

8	Cookie "XSRF-TOKEN" — Secure flag sampled from /	Secure attribute set	Secure attribute present	✓ PASS
9	Cookie "XSRF-TOKEN" — SameSite attribute sampled from /	SameSite=Strict / Lax / None	SameSite=none	✓ PASS
10	Cookie "example coffee shop_session" — HttpOnly flag sampled from /	HttpOnly attribute set	HttpOnly attribute present	✓ PASS
11	Cookie "example coffee shop_session" — Secure flag sampled from /	Secure attribute set	Secure attribute present	✓ PASS
12	Cookie "example coffee shop_session" — SameSite attribute sampled from /	SameSite=Strict / Lax / None	SameSite=none	✓ PASS
13	Mixed Content scan across crawled pages scanned 50 pages of console messages	No `http://` resources requested on HTTPS pages	No Mixed Content messages observed during crawl	✓ PASS

TS-A11Y — Accessibility Audit

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Verify every page declares a language attribute	All pages should include a lang attribute in the HTML tag so screen readers and browsers know the page language.	1 out of 50 pages is missing this attribute, preventing assistive technology from reading the page correctly.	✗ FAIL
2	Verify each page has exactly one main heading (H1)	Every page should declare one H1 element to identify its primary title for screen reader users.	7 out of 50 pages have multiple H1 elements, which confuses screen readers about the page's main topic.	✗ FAIL
3	Verify heading hierarchy is properly structured	Headings should descend in order (H1 → H2 → H3) without skipping levels, so screen reader users can navigate the page outline.	1 out of 50 pages skips a heading level, creating gaps in the navigation structure that confuse assistive technology.	■ UX
4	Images declare an `alt` attribute inspected 800 images across 50 pages	Every `` declares meaningful alt text (`alt=""` only for purely decorative images)	All images declare a non-empty `alt`	✓ PASS
5	Decorative images use intentional empty alt inspected 800 images	`alt=""` is reserved for purely decorative images (review each occurrence)	No images declare empty `alt=""`	✓ PASS

6	Image resources return 2xx HEAD-checked 30 of 237 unique image srcs	Every <code></code> resolves to a 2xx response	All 30 probed images returned 2xx	✓ PASS
7	Verify all buttons have descriptive labels	Every button should have visible text or an aria-label so users with screen readers know what it does.	215 buttons across 49 pages lack an accessible name. Users relying on screen readers cannot understand these buttons' purpose.	✗ FAIL
8	Verify all links have descriptive labels	Every link should have text, an aria-label, or an image with alt text so screen readers know where it goes.	392 links across 49 pages have no accessible name. Screen reader users cannot understand the destination or purpose of these links.	✗ FAIL

TS-XSS — Static XSS Surface

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Verify text inputs limit the amount of text that can be entered	Each text input should have a maxlength attribute to prevent excessively long payloads.	All 117 text inputs across 49 pages lack a maxlength attribute, leaving the site vulnerable to oversized malicious input.	■ UX
2	Verify forms that modify data include CSRF protection	Every form that changes data should carry a hidden CSRF token to prevent unauthorized requests from other sites.	All 117 data-modifying forms lack a visible CSRF token. The site may rely on other defenses (like SameSite cookies) not detectable externally.	✗ FAIL
3	Verify forms do not use inline event handlers	Forms should avoid onclick, onload, and similar inline handlers; instead use addEventListener.	392 inline event handlers are present across 49 pages, making the code harder to secure and harder to maintain.	■ UX
4	Verify links do not use javascript: URLs	Link href attributes should use proper URLs, not javascript: code execution.	49 links use javascript: URLs across 49 pages, increasing the risk of script execution vulnerabilities.	✗ FAIL

TS-COOKIE — Cookies & Consent

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
---	-----------	-----------------	---------------	--------

1	No unrecognized cookies set before consent homepage Set-Cookie · HTTP 200	Either no cookies on first load, or only strictly-necessary / functional ones	2 cookies set (all match strict-necessary naming)	✓ PASS
2	Check for a cookie or privacy consent banner on the homepage	The homepage should display a consent banner or cookie notice so users can manage their privacy preferences.	No consent banner was found in the homepage HTML, which may violate privacy regulations in some jurisdictions.	■ UX
3	Verify cookies are scoped to the site's own domain	All cookies set by the homepage should belong to the site's domain, not third parties.	Both cookies set belong to a different domain, indicating third-party tracking or analytics cookies without a visible consent mechanism.	■ UX

TS-PAGE — Pagination Structure

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Check for pagination on multi-page listings	If any pages list multiple items, they should include next/previous links or numbered pagination.	No pagination patterns were detected on any crawled page.	⊘ BLOCKED

TS-AUTHZ — Authorization Boundary

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Verify the /admin path is not publicly accessible	Attempting to access /admin should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/admin, indicating the site properly gates this path.	■ UX
2	Verify the /admin/ path is not publicly accessible	Attempting to access /admin/ should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/admin/, indicating the site properly gates this path.	■ UX
3	Verify the /admin.php path is not publicly accessible	Attempting to access /admin.php should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/admin.php, indicating the site properly gates this path.	■ UX

4	Verify the /administrator path is not publicly accessible	Attempting to access /administrator should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/administrator, indicating the site properly gates this path.	■ UX
5	Verify the /dashboard path is not publicly accessible	Attempting to access /dashboard should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/dashboard, indicating the site properly gates this path.	■ UX
6	Verify the /dashboard/ path is not publicly accessible	Attempting to access /dashboard/ should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/dashboard/, indicating the site properly gates this path.	■ UX
7	Verify the /wp-admin path is not publicly accessible	Attempting to access /wp-admin should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/wp-admin, indicating the site properly gates this path.	■ UX
8	Verify the /api/admin path is not publicly accessible	Attempting to access /api/admin should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/api/admin, indicating the site properly gates this path.	■ UX
9	Verify the /api/users path is not publicly accessible	Attempting to access /api/users should return a login redirect or error, not admin content.	The path returns a 301 redirect to https://example-coffee-shop.com/api/users, indicating the site properly gates this path.	■ UX

TS-RATELIMIT — Rate Limit & Duplicate Submit

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Verify forms include idempotency tokens to prevent duplicate submissions	Each data-modifying form should carry a token the server can use to detect and block duplicate requests.	None of the 117 data-modifying forms include an idempotency token, increasing the risk of accidental duplicate submissions.	■ UX

2	Check if the server applies rate limiting to rapid requests	When sending multiple rapid requests, the server should respond with a rate-limit error or header after some threshold.	All 20 requests succeeded without any rate-limit signal, suggesting the server does not throttle rapid traffic.	■ UX
3	Check for rate-limit headers on the login endpoint	The OPTIONS preflight response should include rate-limit or retry-after headers to hint at throttling.	The server returned a 200 OK response with no rate-limit headers, suggesting no server-side rate limiting is configured.	■ UX

TS-SEO — SEO & Discoverability

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Verify every page has a page title	All pages should declare a non-empty <title> for search engines and browser tabs.	1 out of 50 pages is missing a title, which hurts search engine indexing and user experience.	✗ FAIL
2	Verify page titles are between 10 and 60 characters	Titles should be concise enough to display fully in search results and browser tabs.	37 out of 50 titles are too short (fewer than 10 characters), missing the opportunity to include keywords and context.	■ UX
3	Verify every page has a meta description	All pages should include a meta description for search engines to display in results.	32 out of 50 pages lack a meta description, reducing click-through rates from search results.	✗ FAIL
4	Verify meta descriptions are between 50 and 160 characters	Descriptions should be long enough to convey the page's purpose but short enough to display fully in search results.	1 out of 18 meta descriptions is out of range.	■ UX
5	Verify every page declares a canonical URL	All pages should include a canonical link to help search engines identify the primary version.	1 out of 50 pages is missing a canonical URL, which may confuse search engines about duplicate content.	■ UX
6	Verify every page has Open Graph og:title metadata	Pages should declare og:title for better appearance when shared on social media.	24 out of 50 pages lack og:title, resulting in poor social media previews.	■ UX
7	Verify every page has Open Graph og:description metadata	Pages should declare og:description for better appearance when shared on social media.	24 out of 50 pages lack og:description, resulting in poor social media previews.	■ UX

8	Verify every page has Open Graph og:image metadata	Pages should declare og:image for better appearance when shared on social media.	24 out of 50 pages lack og:image, resulting in poor social media previews.	■ UX
9	Verify every page has a main heading (H1)	All pages should declare at least one H1 element for proper document structure and SEO.	1 out of 50 pages is missing an H1, which harms search engine understanding of the page's purpose.	✗ FAIL
10	robots.txt exists /robots.txt	GET `/robots.txt` returns 2xx	HTTP 200	✓ PASS
11	robots.txt references a Sitemap scanned response body	robots.txt body contains a `Sitemap:` directive	`Sitemap:` directive present	✓ PASS
12	Check if a sitemap.xml file exists	The site should provide a sitemap at /sitemap.xml to help search engines discover all pages.	A sitemap.xml file was not found (HTTP 404). Search engines may miss some pages during crawling.	■ UX
13	Verify the sitemap.xml file is valid	The sitemap should be properly formatted XML with valid structure.	This check was skipped because no sitemap.xml file is available.	🔒 BLOCKED

TS-SSL — SSL / TLS & Server Headers

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	HTTPS homepage reachable https://example-coffee-shop.com	HEAD https:// returns 2xx or 3xx	HTTP 200	✓ PASS
2	TLS certificate expiry CN=example-coffee-shop.com	Certificate valid for at least 30 more days	70 days remaining (valid_to Aug 17 07:40:57 2026 GMT)	✓ PASS
3	Verify the server redirects plain HTTP to HTTPS	Requests to http:// should redirect to the secure https:// version.	Plain HTTP requests receive a 301 redirect to https://example-coffee-shop.com/, properly enforcing encryption.	✗ FAIL
4	Verify server headers do not disclose software version information	Response headers should omit version details to avoid exposing potential vulnerabilities.	The X-Powered-By header reveals 'PHP/8.4.21, PleskLin', giving attackers information about the server software.	■ UX

TS-REDIRECT — Redirect Configuration

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
---	-----------	-----------------	---------------	--------

1	Verify the HTTP-to-HTTPS redirect chain is efficient	Plain HTTP should redirect to HTTPS in 1-2 hops, landing on the matching URL.	Plain HTTP redirects in 1 hop directly to https://example-coffee-shop.com/ and loads successfully.	■ UX
2	www / apex canonicalization compared www.example-coffee-shop.com ↔ example-coffee-shop.com	Both entrances land on the same canonical host	www → example-coffee-shop.com, apex → example-coffee-shop.com.	✓ PASS

TS-META — Meta Tags & PWA Essentials

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Favicon homepage HTML scan	`<link rel="icon">` declared in the page head.	tag present in homepage HTML	✓ PASS
2	Apple touch icon homepage HTML scan	`<link rel="apple-touch- icon">` declared in the page head.	tag present in homepage HTML	✓ PASS
3	Structured data (JSON-LD) homepage HTML scan	At least one ` <script </script  type="application/ld+json ">` block declaring relevant schema.org types.	tag present in homepage HTML	✓ PASS
4	Charset declaration homepage HTML scan	`<meta charset="utf-8">` declared at the top of `<head>`.	tag present in homepage HTML	✓ PASS
5	Web app manifest homepage declares <link rel="manifest">	Either ` <link </link  rel="manifest">` referenced (and 2xx) OR `/manifest.json` / `/site.webmanifest` reachable	HTTP 200 from /site.webmanifest	✓ PASS

3	Modern image formats (WebP / AVIF) Content-Type inspection across 20 HEAD responses	At least some image responses use modern formats (image/webp or image/avif)	7 legacy (jpg/png), 13 modern (webp/avif).	✓ PASS
---	--	---	--	--------

TS-CONSOLE — Console Errors

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Check for JavaScript errors in the browser console	The page should load without any JavaScript errors.	26 JavaScript errors were logged across 5 different pages. These errors may break functionality or prevent features from working.	■ UX
2	Check for the console error: %c%d font-size:<n>;color:transparent NaN	The page should not emit this console error.	This error was observed: %c%d font-size:0;color:transparent NaN. This suggests a JavaScript library or script is misbehaving.	✗ FAIL
3	Check for the console error: Failed to load resource with status 401	The page should not emit this console error.	This error was observed: 'Failed to load resource: the server responded with a status of 401 ()'. A resource is being requested without proper authentication.	✗ FAIL
4	Check for the console error: Bad element for Flickity carousel	The page should not emit this console error.	This error was observed: 'Bad element for Flickity: .magaza-carousel'. The carousel library cannot find its target element, preventing it from functioning.	■ UX
5	Check for the console error: Bad element for Flickity with null value	The page should not emit this console error.	This error was observed: 'Bad element for Flickity: null'. The carousel library is receiving a null reference, indicating a scripting error.	■ UX

TS-EXTLINKS — External Link Health

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
---	-----------	-----------------	---------------	--------

1	Check external link https://www.instagram.com/example-coffee-shop/ referenced from https://example-coffee-shop.com/	External link is reachable.	Link resolves correctly (HTTP 200).	✓ PASS
2	Check external link https://www.facebook.com/ExampleCoffeeShop referenced from https://example-coffee-shop.com/	External link is reachable.	Link resolves correctly (HTTP 200).	✓ PASS
3	Check external link https://www.youtube.com/channel/UC CcZU6Jtcn5Fd5Ns4Bs-jmg referenced from https://example-coffee-shop.com/	External link is reachable.	Link resolves correctly (HTTP 200).	✓ PASS
4	Check external link https://twitter.com/ExampleCoffeeShopCoffee referenced from https://example-coffee-shop.com/	External link is reachable.	Link redirects (HTTP 301).	✓ PASS
5	Check if an external URL is reachable: https://etbis.eticaret.gov.tr/site-dogrulama/...	The external link should respond with a success, redirect, or authentication error.	The request failed after 3.37 seconds with a network error. The external site may be down, blocked, or unreachable.	✗ FAIL
6	Check external link https://maps.app.goo.gl/pdt5cwA1UhYPxAcA9 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
7	Check external link https://goo.gl/maps/L43WnbVwQKpt2Atv8 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
8	Check external link https://maps.app.goo.gl/acMLfhUUgSGunUKU6 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
9	Check external link https://goo.gl/maps/RfCQBPD7ymxDpt5H9 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
10	Check external link https://maps.app.goo.gl/kqNwPRnkWn5MiAWJ8 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS

11	Check external link https://goo.gl/maps/yoFXMSSMCnedN2Qv5 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
12	Check external link https://goo.gl/maps/w8JurPsAmL8cvmwB8 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
13	Check external link https://goo.gl/maps/ZKAE2fVeF1qgPX4D9 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
14	Check external link https://maps.app.goo.gl/6o5fkoNQ6nGhCms97 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
15	Check external link https://goo.gl/maps/ReHT9JuVw9V9gYzX6 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
16	Check external link https://maps.app.goo.gl/VhDZzx7KZ4Ra8v79 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
17	Check external link https://goo.gl/maps/YzpQ4YBdTTvHcJwk7 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
18	Check external link https://maps.app.goo.gl/GD9vA6Fq799Cz9L97 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
19	Check external link https://maps.app.goo.gl/tVRivvSJntirrKNY9 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
20	Check external link https://maps.app.goo.gl/D3nsjdXydf2BvUYg8 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
21	Check external link https://maps.app.goo.gl/wR9yC4R14aprZujDA "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS

22	Check external link https://goo.gl/maps/q4TgzkL7idmjxas9A "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
23	Check external link https://maps.app.goo.gl/36HoSUuraDWpTCmF7 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
24	Check external link https://maps.app.goo.gl/cQprdqUAKdSmhZdj7 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
25	Check external link https://maps.app.goo.gl/WZPp32knn4vdrzb26 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
26	Check external link https://goo.gl/maps/yAeVDP3LyockR5jn6 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
27	Check external link https://goo.gl/maps/wLAUevfzdTk3WbBf7 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
28	Check external link https://maps.app.goo.gl/DYQmcD5ngHF2uFJK7 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
29	Check external link https://maps.app.goo.gl/hphAb25tjJkWead16 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
30	Check external link https://maps.app.goo.gl/UD6xJURvjVLb1rtm7 "Haritada Gör"	External link is reachable.	Link redirects (HTTP 302).	✓ PASS
31	Check remaining external links for reachability	n/a (probe has a limit on external links checked)	16 additional external URLs were not probed due to capacity limits.	■ UX

TS-OPENREDIR — Open Redirect Surface

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
---	-----------	-----------------	---------------	--------

1	Test if the ?redirect parameter can be used for open redirects	The server should ignore or strip external redirect targets to prevent hijacking users.	The server returns a 301 redirect with the parameter intact, though it remains on the same domain. This is safer than a true open redirect.	■ UX
2	Test if the ?next parameter can be used for open redirects	The server should ignore or strip external redirect targets to prevent hijacking users.	The server returns a 301 redirect with the parameter intact, though it remains on the same domain. This is safer than a true open redirect.	■ UX
3	Test if the ?url parameter can be used for open redirects	The server should ignore or strip external redirect targets to prevent hijacking users.	The server returns a 301 redirect with the parameter intact, though it remains on the same domain. This is safer than a true open redirect.	■ UX
4	Test if the ?return parameter can be used for open redirects	The server should ignore or strip external redirect targets to prevent hijacking users.	The server returns a 301 redirect with the parameter intact, though it remains on the same domain. This is safer than a true open redirect.	■ UX
5	Test if the ?returnUrl parameter can be used for open redirects	The server should ignore or strip external redirect targets to prevent hijacking users.	The server returns a 301 redirect with the parameter intact, though it remains on the same domain. This is safer than a true open redirect.	■ UX

TS-AUTH — Authentication Form Structure

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Login form discovered page: https://example-coffee-shop.com/kullanici/kaydol	Authentication form found via password input / login path	form @ https://example-coffee-shop.com/kullanici/kaydol (method POST)	✓ PASS
2	Form action uses HTTPS https://example-coffee-shop.com/kullanici/kaydol	Login form posts to an https:// URL	https:// action confirmed	✓ PASS
3	Form method is POST (not GET) GET would leak credentials via URL IF the submit isn't JS-intercepted to a real POST	Form method=POST	method=POST confirmed	✓ PASS

4	Verify the password field includes autocomplete guidance	Password inputs should declare <code>autocomplete="current-password"</code> to enable browser password managers.	The password field lacks an autocomplete attribute, preventing password managers from working correctly.	■ UX
5	Verify the username field includes autocomplete guidance	Username inputs should declare <code>autocomplete="username"</code> to enable browser password managers.	The username field lacks an autocomplete attribute, preventing password managers from working correctly.	■ UX
6	Verify a password-reset link is visible on the login page	Users should be able to find a 'Forgot password' or similar link if they cannot sign in.	No password-reset link was found on the login page, making it difficult for users who forget their credentials.	■ UX
7	Verify the password field limits input length	Password inputs should declare a <code>maxlength</code> attribute (typically 64 or more) to prevent excessively long inputs.	The password field lacks a <code>maxlength</code> attribute, leaving it vulnerable to very long or malicious payloads.	■ UX
8	Verify the login form includes CSRF protection	The form should carry a hidden CSRF token, or the server may use other defenses (like SameSite cookies).	No visible CSRF token field was found in the login form. The site may rely on other defenses not externally observable.	✗ FAIL
9	Empty email + empty password submitted to <code>https://example-coffee-shop.com/kullanici/kaydol</code>	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS
10	Valid-format email + empty password submitted to <code>https://example-coffee-shop.com/kullanici/kaydol</code>	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS
11	Empty email + filled password submitted to <code>https://example-coffee-shop.com/kullanici/kaydol</code>	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS
12	Email without `@` submitted to <code>https://example-coffee-shop.com/kullanici/kaydol</code>	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS

13	1-character password submitted to https://example-coffee-shop.com/kullanici/kaydol	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS
14	200-character password (graceful handling) submitted to https://example-coffee-shop.com/kullanici/kaydol	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS
15	SQL-injection payload in email submitted to https://example-coffee-shop.com/kullanici/kaydol	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS
16	XSS payload in email submitted to https://example-coffee-shop.com/kullanici/kaydol	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS
17	Wrong email + wrong password submitted to https://example-coffee-shop.com/kullanici/kaydol	Form rejects the submission (URL unchanged OR password field still visible OR visible error)	URL unchanged, password input still visible.	✓ PASS
18	Check for user-enumeration vulnerabilities in login error messages	This test requires a real test account email for comparison.	This test was skipped because no test account email was provided.	🚫 BLOCKED
19	Verify the password field includes a visibility toggle	Users should be able to toggle between masked and visible password text for better usability.	No password visibility toggle button was found, forcing users to type blindly.	■ UX
20	Verify a 'remember me' checkbox is available	Users should be offered a 'remember me' or 'stay signed in' option for convenience.	No remember-me checkbox was found on the login page.	■ UX
21	Check if the password-reset link is reachable	The password-reset link should point to a valid page.	No password-reset link was discovered on the page, so this check could not be completed.	🚫 BLOCKED
22	Register form requires email + password + confirm-password page: https://example-coffee-shop.com/kullanici/kaydol	Form contains an email input, a password input, and a second password (confirm) input	all three required fields present	✓ PASS

23	Verify a password strength indicator is displayed near the password input	Users should see feedback about password strength (weak, medium, strong) or a list of requirements.	No password strength meter or requirement list was found, leaving users uncertain about acceptable passwords.	■ UX
24	Verify the registration form requires acceptance of terms and privacy	A checkbox should require users to explicitly agree to the site's terms and privacy policy.	No terms or privacy checkbox was found on the registration form, which may violate data protection regulations.	■ UX

TS-API — API Responses

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	API responses return 2xx/3xx 4 XHR/fetch responses on https://example-coffee-shop.com/	All API responses return 2xx / 3xx	All 4 responses 2xx/3xx	✓ PASS
2	API responses under 2s 4 XHR/fetch responses	Every API response completes in ≤ 2000 ms	All responses under threshold	✓ PASS
3	Verify API responses declare a Content-Type header	All API responses should include a Content-Type header so clients know how to parse the data.	3 API responses lack a Content-Type header, which may confuse API clients about the response format.	■ UX
4	API response bodies do not expose stack traces 4 XHR/fetch responses	Response bodies never contain server stack traces / debug error details	No stack traces detected in response bodies	✓ PASS

TS-ERR — Error Page & 404 Handling

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	GET /xyz short nonsense path	HTTP 4xx response · branded error page consistent with site chrome	HTTP 404, branded, 0.65 s.	✓ PASS
2	GET /__qa_explorer_404_probe_* opaque randomized path	HTTP 4xx response · branded error page consistent with site chrome	HTTP 404, branded, 0.50 s.	✓ PASS
3	Load the search page with an invalid query parameter	The page should return a 4xx error with branded site styling consistent with the rest of the site.	The page returned HTTP 403 with generic error styling, not matching the site's design. This confuses users about whether it is a site error or a real access denial.	✗ FAIL

4	Request a very long URL path to test error handling	The page should return a 4xx error with branded site styling consistent with the rest of the site.	The page returned HTTP 403 with generic error styling, not matching the site's design. This confuses users about whether it is a site error or a real access denial.	X FAIL
5	GET /test'<sql-payload> SQL-injection-style path	HTTP 4xx response · branded error page consistent with site chrome	HTTP 404, branded, 0.29 s.	✓ PASS

TS-FORM — Form Validation Tests

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Form #1: POST https://example-coffee-shop.com/ebulten empty submit test	Submission blocked or error message shown	1 input(s) flagged as invalid, browser message: "Please fill out this field.".	✓ PASS
2	Form #1: POST https://example-coffee-shop.com/ebulten invalid email format test	Browser rejected the invalid email format (HTML5 :invalid or visible error)	1 input(s) flagged as invalid, browser message: "Please include an '@' in the email address. 'not-an-email' is missing an '@'.".	✓ PASS
3	Submit an empty form at POST https://example-coffee-shop.com/alisveris/ara	The form should validate and show an error message, or prevent submission if required fields are empty.	The empty form submitted without triggering client-side validation or showing any error, allowing invalid data to be sent.	UX
4	Form #3: POST https://example-coffee-shop.com/sepet/ekle empty submit test	Submission blocked or error message shown	4 input(s) flagged as invalid, browser message: "Please select an item in the list.".	✓ PASS
5	Form #4: POST https://example-coffee-shop.com/kullanici/kaydol empty submit test	Submission blocked or error message shown	6 input(s) flagged as invalid, browser message: "Please fill out this field.".	✓ PASS
6	Form #4: POST https://example-coffee-shop.com/kullanici/kaydol invalid email format test	Browser rejected the invalid email format (HTML5 :invalid or visible error)	6 input(s) flagged as invalid, browser message: "Please fill out this field.".	✓ PASS
7	Form #5: POST https://example-coffee-shop.com/kullanici/oturumac empty submit test	Submission blocked or error message shown	2 input(s) flagged as invalid, browser message: "Please fill out this field.".	✓ PASS

8	Form #5: POST https://example-coffee-shop.com/kullanici/oturumac invalid email format test	Browser rejected the invalid email format (HTML5 :invalid or visible error)	2 input(s) flagged as invalid, browser message: "Please include an '@' in the email address. 'not-an-email' is missing an '@'."	✓ PASS
9	Form #6: POST https://example-coffee-shop.com/iletisim empty submit test	Submission blocked or error message shown	5 input(s) flagged as invalid, browser message: "Please fill out this field."	✓ PASS
10	Form #6: POST https://example-coffee-shop.com/iletisim invalid email format test	Browser rejected the invalid email format (HTML5 :invalid or visible error)	5 input(s) flagged as invalid, browser message: "Please fill out this field."	✓ PASS

TS-CTA — Primary CTA Tests

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Click button "Sign Up" click navigates to destination	CTA produces a navigation, modal, or DOM update	Navigated to https://example-coffee-shop.com/kullanici/kaydol (HTTP 200)	✓ PASS
2	Click button "Login" click navigates to destination	CTA produces a navigation, modal, or DOM update	Navigated to https://example-coffee-shop.com/kullanici/oturumac (HTTP 200)	✓ PASS
3	Click button "Subscribe" click updates page content in place	CTA produces a navigation, modal, or DOM update	Document text length changed by 254 chars (SPA / in-place update)	✓ PASS
4	Click link "Sign Up" → /kullanici/kaydol click navigates to destination	CTA produces a navigation, modal, or DOM update	Navigated to https://example-coffee-shop.com/kullanici/kaydol (HTTP 200)	✓ PASS
5	Click link "Login" → /kullanici/oturumac click navigates to destination	CTA produces a navigation, modal, or DOM update	Navigated to https://example-coffee-shop.com/kullanici/oturumac (HTTP 200)	✓ PASS
6	Click link "Add to Cart" → /alisveris click navigates to destination	CTA produces a navigation, modal, or DOM update	Navigated to https://example-coffee-shop.com/alisveris (HTTP 200)	✓ PASS
7	Click link "Contact Us" → /iletisim click navigates to destination	CTA produces a navigation, modal, or DOM update	Navigated to https://example-coffee-shop.com/iletisim (HTTP 200)	✓ PASS

8	Attempt to click the 'Buy' link pointing to /odeme	Clicking should navigate to the target page or trigger an action.	This link was not clicked because the text 'Buy' matches a destructive action blocklist, preventing accidental activation during automated testing.	🚫 BLOCKED
9	Click link "Add to Cart" → ...s/urun/Hario-v60-Dripper-seti click navigates to destination	CTA produces a navigation, modal, or DOM update	Navigated to https://example-coffee-shop.com/alisveris (HTTP 200)	✓ PASS
10	Click link "Add to Cart" → /alisveris/urun/cezve click navigates to destination	CTA produces a navigation, modal, or DOM update	Navigated to https://example-coffee-shop.com/alisveris (HTTP 200)	✓ PASS

TS-SEARCH — Search Behavior

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Discover and exercise the site search functionality	At least one search form should be available on the site to test search behavior.	No search form was found on any crawled page, so search functionality could not be tested.	🚫 BLOCKED

TS-ERROR — Error & Resilience Handling

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Check if a service worker is registered	Optional — a service worker enables offline caching and improves resilience.	No service worker is registered. Offline functionality and caching are not available.	■ UX
2	Test the page's behavior when the network is offline	A gracefully designed site should show a cached or branded offline page, not a generic browser error.	The page failed to load offline with a network error (net::ERR_INTERNET_DISCONNECTED). No offline experience is provided.	✗ FAIL
3	Check if a loading indicator appears during slow navigation	Users should see visual feedback (spinner, progress bar) while content is loading.	No loading indicator was detected during navigation, leaving users unsure if the page is responding.	■ UX

TS-PERF — Performance & Core Web Vitals

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
---	-----------	-----------------	---------------	--------

1	FCP · /	≤1.8s good · ≤3.0s needs improvement	1.52s	✓ PASS
2	LCP · /	≤2.5s good · ≤4.0s needs improvement	1.52s	✓ PASS
3	CLS · /	≤0.1 good · ≤0.25 needs improvement	0.011	✓ PASS
4	DOM · /	≤1500 elements good · ≤3000 needs improvement	470 elements	✓ PASS
5	Measure the total page weight of the homepage	The homepage should load in 3 MB or less (good), or at most 5 MB (needs improvement).	The homepage is 4.81 MB, which needs improvement. Optimize images, minify code, or defer non-critical resources.	■ UX
6	FCP · /demleme-teknik/french-press	≤1.8s good · ≤3.0s needs improvement	1.58s	✓ PASS
7	LCP · /demleme-teknik/french-press	≤2.5s good · ≤4.0s needs improvement	1.58s	✓ PASS
8	CLS · /demleme-teknik/french-press	≤0.1 good · ≤0.25 needs improvement	0.017	✓ PASS
9	DOM · /demleme-teknik/french-press	≤1500 elements good · ≤3000 needs improvement	389 elements	✓ PASS
10	Weight · /demleme-teknik/french-press 31 resources	≤3 MB good · ≤5 MB needs improvement	0.72 MB	✓ PASS
11	FCP · /iletisim	≤1.8s good · ≤3.0s needs improvement	1.45s	✓ PASS
12	LCP · /iletisim	≤2.5s good · ≤4.0s needs improvement	1.87s	✓ PASS
13	CLS · /iletisim	≤0.1 good · ≤0.25 needs improvement	0.028	✓ PASS
14	DOM · /iletisim	≤1500 elements good · ≤3000 needs improvement	360 elements	✓ PASS
15	Weight · /iletisim 32 resources	≤3 MB good · ≤5 MB needs improvement	0.75 MB	✓ PASS
16	FCP · /aydinlatma	≤1.8s good · ≤3.0s needs improvement	1.50s	✓ PASS

17	LCP · /aydinlatma	≤2.5s good · ≤4.0s needs improvement	1.75s	✓ PASS
18	CLS · /aydinlatma	≤0.1 good · ≤0.25 needs improvement	0.041	✓ PASS
19	DOM · /aydinlatma	≤1500 elements good · ≤3000 needs improvement	445 elements	✓ PASS
20	Weight · /aydinlatma 30 resources	≤3 MB good · ≤5 MB needs improvement	0.72 MB	✓ PASS
21	FCP · /alisveris/urun/kenya-kirinyaga	≤1.8s good · ≤3.0s needs improvement	1.40s	✓ PASS
22	LCP · /alisveris/urun/kenya-kirinyaga	≤2.5s good · ≤4.0s needs improvement	1.95s	✓ PASS
23	CLS · /alisveris/urun/kenya-kirinyaga	≤0.1 good · ≤0.25 needs improvement	0.024	✓ PASS
24	DOM · /alisveris/urun/kenya-kirinyaga	≤1500 elements good · ≤3000 needs improvement	486 elements	✓ PASS
25	Measure the total page weight of the product detail page	Product pages should load in 3 MB or less (good), or at most 5 MB (needs improvement).	The product page is 3.40 MB, which is acceptable but could be further optimized.	■ UX

TS-RESPONSIVE — Responsive Layout Checks

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Check the homepage layout on a mobile phone (375×812 pixels)	The page should not overflow horizontally, text should not be clipped, and buttons should be at least 44 pixels for easy tapping.	The page fits without overflow, but 1 element is clipped, and 31 out of 45 touch targets are too small (<44 pixels), making them hard to tap on mobile.	■ UX
2	Check the homepage layout on a tablet (768×1024 pixels)	The page should not overflow horizontally and text should not be clipped.	The page fits without overflow, but 1 element is clipped. Text and layout are otherwise acceptable for tablet viewing.	■ UX
3	/ · Desktop (1440×900) checks: overflow · clipping	No horizontal overflow · no clipped text	no horizontal overflow · 1 clipped element	■ UX
4	/iletisim · Mobile (375×812) checks: overflow · clipping · touch targets	No horizontal overflow · no clipped text · touch targets ≥44px	no horizontal overflow · 33 of 40 touch targets <44px	■ UX

5	/iletisim · Tablet (768×1024) checks: overflow · clipping	The Iletisim page should render correctly at tablet width with no horizontal overflow or clipped text.	no horizontal overflow	✓ PASS
6	/iletisim · Desktop (1440×900) checks: overflow · clipping	The Iletisim page should render correctly at desktop width with no horizontal overflow or clipped text.	no horizontal overflow	✓ PASS
7	/alisveris/urun/kenya-kirinyaga · Mobile (375×812) checks: overflow · clipping · touch targets	No horizontal overflow · no clipped text · touch targets ≥44px	no horizontal overflow · 36 of 44 touch targets <44px	■ UX
8	/alisveris/urun/kenya-kirinyaga · Tablet (768×1024) checks: overflow · clipping	The Kenya Kirinyaga page should render correctly at tablet width with no horizontal overflow or clipped text.	no horizontal overflow	✓ PASS
9	/alisveris/urun/kenya-kirinyaga · Desktop (1440×900) checks: overflow · clipping	The Kenya Kirinyaga page should render correctly at desktop width with no horizontal overflow or clipped text.	no horizontal overflow	✓ PASS
10	Viewport meta tag captured once on the first sample page	`<meta name="viewport" content="width=device-width, ...">`	Present, width=device-width, initial-scale=1.0.	✓ PASS

TS-STATE — State & Navigation

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Deep-link navigation to inner page https://example-coffee-shop.com/alisveris	Direct GET on the inner URL renders content	Loaded, HTTP 200, body length 6786.	✓ PASS
2	Browser back returns to a working previous page https://example-coffee-shop.com/ → https://example-coffee-shop.com/alisveris → back	Going back re-renders the previous page (no blank / error screen)	Back, HTTP 200, body length 1716.	✓ PASS
3	Page reload renders cleanly https://example-coffee-shop.com/alisveris	Reload renders the page without errors	Reloaded, HTTP 200, body length 6786.	✓ PASS
4	Inner pages have unique meaningful URLs inspected first 5 inner pages	Each inner page has its own path-based URL (not just a `#` fragment on the homepage)	All 5 URLs unique	✓ PASS

TS-CONTRAST — Color Contrast (WCAG 2.1)

#	TEST STEP	EXPECTED RESULT	ACTUAL RESULT	STATUS
1	Color contrast · / sampled 31 text elements	Every sampled text element meets WCAG 2.1 contrast (≥ 4.5 normal · ≥ 3 large)	2 of 31 sampled elements fall below threshold	X FAIL
2	Color contrast · /iletisim sampled 23 text elements	Every sampled text element meets WCAG 2.1 contrast (≥ 4.5 normal · ≥ 3 large)	1 of 23 sampled elements fall below threshold	X FAIL
3	Color contrast · /alisveris/urun/kenya-kirinyaga sampled 30 text elements	Every sampled text element meets WCAG 2.1 contrast (≥ 4.5 normal · ≥ 3 large)	1 of 30 sampled elements fall below threshold	X FAIL

4 Bug Summary Matrix

A consolidated dashboard view of every unique finding from this scan. Detailed entries follow in the next section.

ID	TITLE	SEVERITY	PRIORITY	STATUS
BUG-001	Color contrast failures (site-wide)	HIGH	P1	• NEW
BUG-002	Form input missing accessible label	HIGH	P1	• NEW
BUG-003	Pervasive missing accessible names on interactive elements site-wide	HIGH	P1	• NEW
BUG-004	Internal link unreachable	HIGH	P1	• NEW
BUG-005	Legal compliance failure: no cookie consent and broken KVKK document	HIGH	P1	• NEW
BUG-006	Cookie missing HttpOnly flag	HIGH	P1	• NEW
BUG-007	HTTP requests are not redirected to HTTPS	HIGH	P1	• NEW
BUG-008	javascript: href links and inline handlers create XSS attack surface	HIGH	P1	• NEW
BUG-009	Form fields rely	MEDIUM	P2	• NEW
BUG-010	Missing language attribute on HTML element	MEDIUM	P2	• NEW
BUG-011	Multiple form inputs missing accessible labels	MEDIUM	P2	• NEW
BUG-012	Multiple h1 elements and skipped heading levels weaken document structure	MEDIUM	P2	• NEW
BUG-013	Multiple primary headings on page	MEDIUM	P2	• NEW

BUG-014	Unlabeled buttons	MEDIUM	P2	• NEW
BUG-015	Unlabeled links	MEDIUM	P2	• NEW
BUG-016	API responses missing Content-Type header	MEDIUM	P2	• NEW
BUG-017	External link unreachable	MEDIUM	P2	• NEW
BUG-018	Failed resource loading errors in console	MEDIUM	P2	• NEW
BUG-019	Form accepts empty submission	MEDIUM	P2	• NEW
BUG-020	JavaScript console errors detected	MEDIUM	P2	• NEW
BUG-021	No offline or cached state	MEDIUM	P2	• NEW
BUG-022	Heavy page weight and low lazy-load adoption degrade mobile performance	MEDIUM	P2	• NEW
BUG-023	JavaScript URLs in links	MEDIUM	P2	• NEW
BUG-024	Missing Content-Security-Policy header	MEDIUM	P2	• NEW
BUG-025	No cookie consent banner detected	MEDIUM	P2	• NEW
BUG-026	Server software details publicly visible	MEDIUM	P2	• NEW
BUG-027	Text inputs without character limits	MEDIUM	P2	• NEW
BUG-028	Third-party cookies set on page load	MEDIUM	P2	• NEW
BUG-029	Missing page title	MEDIUM	P2	• NEW
BUG-030	Missing SEO metadata	MEDIUM	P2	• NEW
BUG-031	Unbranded 403 responses replace expected 404 handling for unknown URLs	MEDIUM	P2	• NEW
BUG-032	Inconsistent heading structure	LOW	P3	• NEW
BUG-033	Carousel library error in console	LOW	P3	• NEW
BUG-034	Carousel library null reference error	LOW	P3	• NEW
BUG-035	No offline support (service worker not registered)	LOW	P3	• NEW
BUG-036	Heavy page weight (4.81 MB)	LOW	P3	• NEW
BUG-037	Images not using native lazy-loading	LOW	P3	• NEW
BUG-038	Oversized image (532 KB)	LOW	P3	• NEW

BUG-039	Forms lack duplicate-submission prevention	LOW	P3	• NEW
BUG-040	Forms may lack cross-site forgery protection	LOW	P3	• NEW
BUG-041	Inline event handlers in HTML	LOW	P3	• NEW
BUG-042	Login endpoint shows no rate-limit protection signal	LOW	P3	• NEW
BUG-043	No 'remember me' option on login	LOW	P3	• NEW
BUG-044	No password reset link on login page	LOW	P3	• NEW
BUG-045	No password visibility toggle	LOW	P3	• NEW
BUG-046	No rate-limiting visible on homepage	LOW	P3	• NEW
BUG-047	Password field missing autocomplete attribute	LOW	P3	• NEW
BUG-048	Password field missing maxlength attribute	LOW	P3	• NEW
BUG-049	Potential CSRF gap on state-changing forms (unverified)	LOW	P3	• NEW
BUG-050	Username field missing autocomplete attribute	LOW	P3	• NEW
BUG-051	Content clipped at desktop viewport (1440px)	LOW	P3	• NEW
BUG-052	Content clipped at mobile viewport (375px)	LOW	P3	• NEW
BUG-053	Content clipped at tablet viewport (768px)	LOW	P3	• NEW
BUG-054	Missing main heading	LOW	P3	• NEW
BUG-055	Page titles too short for search results	LOW	P3	• NEW
BUG-056	Registration form lacks password strength indicator	LOW	P3	• NEW
BUG-057	Registration form missing terms acceptance checkbox	LOW	P3	• NEW
BUG-058	Sitemap not found	LOW	P3	• NEW
BUG-059	Undersized touch targets on mobile	LOW	P3	• NEW

5 Detailed Bug Reports

Each finding's BUG-NNN identifier matches its row in the Bug Summary Matrix.

BUG-001 Color contrast failures (site-wide)

HIGH P1 **NEW**

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in DevTools → Inspect
2. Locate the element matching `label.transition-all.peer-placeholder-shown:text-base`
3. In the Styles pane, hover the computed `color` value — DevTools renders the live contrast ratio
4. Adjust either color (typically darkening the foreground) until the ratio clears the threshold

EXPECTED RESULT

Text should have a contrast ratio of at least 4.5:1.

ACTUAL RESULT

Text "E-Bülten" (selector label.transition-all.peer-placeholder-shown:text-base) on https://example-coffee-shop.com/ has contrast 1.90:1 (RGB 156,163,175 on RGB 227,222,215).

BUG-002 Form input missing accessible label

HIGH P1 **NEW**

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in a browser
2. Open DevTools → Accessibility tree
3. Inspect each interactive input — its accessible name should be the field's purpose, not 'edit text'

EXPECTED RESULT

Every form input should have an associated label.

ACTUAL RESULT

1 input on the search form (action="https://example-coffee-shop.com/alisveris/ara", method=POST) has no associated label.

BUG-003 Pervasive missing accessible names on interactive elements
site-wide

HIGH P1 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Navigate to https://example-coffee-shop.com/ with a screen reader (e.g. NVDA + Chrome).
- 2. Tab through interactive elements — most buttons and icon links are announced as 'button' or 'link' with no descriptive label.
- 3. Run an automated accessibility checker (axe, Lighthouse) — it will flag all unlabelled controls and contrast failures simultaneously.

EXPECTED RESULT

All interactive elements should carry descriptive accessible names (visible text or aria-label), colour contrast should meet WCAG 2.1 AA (4.5:1 for normal text), and every HTML document should declare a valid lang attribute.

ACTUAL RESULT

TS-A11Y: 215 buttons without accessible names, 392 links without accessible names across 49 pages. TS-CONTRAST: contrast failures on /, /iletisim, and /alisveris/urun/kenya-kirinyaga. TS-A11Y: 1 page missing lang attribute.

BUG-004 Internal link unreachable

HIGH P1 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Open https://example-coffee-shop.com/ in a browser
- 2. Click the link to https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf
- 3. Observe no response

EXPECTED RESULT

All internal links should respond successfully (HTTP 200 or redirect to a working page).

ACTUAL RESULT

https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf → no response. First referenced from https://example-coffee-shop.com/. Also linked from https://example-coffee-shop.com/alisveris, https://example-coffee-shop.com/alisveris/kategori/kahveler, https://example-coffee-shop.com/alisveris/kategori/ekipmanlar (and 45 more).

BUG-005 Legal compliance failure: no cookie consent and broken KVKK document

HIGH P1 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Load https://example-coffee-shop.com/ in a clean browser profile with no prior cookies.
2. Observe that no cookie consent banner appears but third-party cookies are already set (visible in DevTools > Application > Cookies).
3. Click the KVKK başvuru link anywhere on the site — browser shows a network error / blank page.
4. Confirm via curl: curl -I https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf returns no response.

EXPECTED RESULT

A cookie consent mechanism must gate third-party cookie setting until explicit user consent. The KVKK başvuru PDF must be reachable at its published URL.

ACTUAL RESULT

TS-COOKIE: no consent banner found in homepage HTML; 2 of 2 cookies are third-party domain. TS-NAV + TS-LINKS: /pdf/kvkk_basvuru.pdf returns no HTTP response.

BUG-006 Cookie missing HttpOnly flag

HIGH P1 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. curl -I 'https://example-coffee-shop.com/'
2. Locate the 'Set-Cookie' response header for the cookie named "XSRF-TOKEN"
3. Confirm the HttpOnly flag is absent

EXPECTED RESULT

Set-Cookie should include the HttpOnly flag (for example: Set-Cookie: session=...; HttpOnly; Secure; SameSite=Lax).

ACTUAL RESULT

Cookie "XSRF-TOKEN" observed on https://example-coffee-shop.com/ is missing the HttpOnly flag.

BUG-007 HTTP requests are not redirected to HTTPS

HIGH **P1** **NEW**

http://example-coffee-shop.com (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. curl -sI 'http://example-coffee-shop.com/' | head -20
- 2. Confirm the first response is a 3xx redirect whose Location starts with https://
- 3. Update the web server / CDN to force-redirect HTTP traffic to HTTPS

EXPECTED RESULT

HTTP requests should redirect to HTTPS using a 301, 302, 307, or 308 response.

ACTUAL RESULT

HTTP 301 redirect to https://example-coffee-shop.com/ is working correctly.

BUG-008 javascript: href links and inline handlers create XSS attack surface

HIGH **P1** **NEW**

https://example-coffee-shop.com/ (Desktop)

STEPS TO REPRODUCE

- 1. Open any page, e.g. https://example-coffee-shop.com/ and inspect anchor tags in DevTools.
- 2. Search for href="javascript: — 49 instances exist.
- 3. Search for onclick= — hundreds of inline handlers visible in source.
- 4. Check response headers — no Content-Security-Policy header present to restrict script sources.

EXPECTED RESULT

No javascript: href links; event handlers should be bound via addEventListener in external scripts. A CSP header should restrict script execution to trusted sources.

ACTUAL RESULT

TS-XSS: 49 javascript: links and 392 inline handlers across 49 pages. TS-SEC: CSP header not set. The two findings are mutually reinforcing — removing CSP-unsafe-inline would break the inline handlers, revealing that neither can be fixed independently.

BUG-009 Form fields rely

MEDIUM

P2

• NEW

`https://example-coffee-shop.com/` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Focus into a form field on `https://example-coffee-shop.com/`
2. Observe that the previously-visible hint disappears
3. Inspect the DOM and confirm the element is a placeholder attribute, not a `<label>`

EXPECTED RESULT

Each form input should have a persistent `<label>`, with placeholder as an optional supplement.

ACTUAL RESULT

1 input on the search form (action="`https://example-coffee-shop.com/alisveris/ara`", method=POST) relies solely on placeholder text.

BUG-010 Missing language attribute on HTML element

MEDIUM

P2

• NEW

`https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf` in DevTools → Elements tab
2. Inspect the `<html>` element
3. Confirm no `lang` attribute is present
4. Add `lang="<bcp47-code>"` to the `<html>` element in the template

EXPECTED RESULT

The `<html>` element should include a `lang` attribute (for example: `<html lang="en">` or `<html lang="tr">`).

ACTUAL RESULT

Language attribute missing or empty on 1 of 50 crawled pages.

BUG-011 Multiple form inputs missing accessible labels

MEDIUM

P2

• NEW

`https://example-coffee-shop.com/iletisim` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/iletisim` in a browser
2. Open DevTools → Accessibility tree
3. Inspect each interactive input — its accessible name should be the field's purpose, not 'edit text'

EXPECTED RESULT

Every form input should have an associated label.

ACTUAL RESULT

2 of 5 inputs on the contact form (`action="https://example-coffee-shop.com/iletisim"`, `method=POST`) have no associated label.

BUG-012 Multiple h1 elements and skipped heading levels weaken document structure

MEDIUM

P2

• NEW

`https://example-coffee-shop.com/` (Desktop)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/` and run `document.querySelectorAll('h1')` in the console — multiple results returned.
2. Use a browser accessibility tree inspector to review heading outline — multiple top-level headings with no clear primary topic heading.

EXPECTED RESULT

Each page should have exactly one `<h1>` that represents the primary page topic, with subsequent content using `h2–h6` in logical, non-skipping order.

ACTUAL RESULT

TS-A11Y reports 7 pages with multiple `<h1>` elements and 1 page with a skipped heading level. DOM summary for / shows 23 heading elements, indicating heavily fragmented heading use.

BUG-013 Multiple primary headings on page

MEDIUM

P2

• NEW

`https://example-coffee-shop.com/` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/` in DevTools → Elements tab
2. Search the DOM for ``h1`` elements
3. Confirm 4 `<h1>` elements are present
4. Promote one as the page title; demote the rest to `<h2>`

EXPECTED RESULT

Each page should have exactly one `<h1>` element.

ACTUAL RESULT

7 of 50 crawled pages contain multiple `<h1>` elements (for example, 4 on `https://example-coffee-shop.com/`).

BUG-014 Unlabeled buttons

MEDIUM

P2

• NEW

`https://example-coffee-shop.com/` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/` in DevTools → Elements tab
2. Run ``[...document.querySelectorAll('button')].filter(b => !b.innerText.trim() && !b.getAttribute('aria-label'))`` in Console
3. Add an ``aria-label`` describing the action to each match

EXPECTED RESULT

Each button should have a name, either through visible text or an `aria-label` attribute.

ACTUAL RESULT

215 of 850 buttons across 49 pages have neither text nor `aria-label`.

BUG-015 Unlabeled links

MEDIUM P2 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in DevTools → Elements tab
2. Run `[...document.querySelectorAll('a[href'])).filter(a => !a.innerText.trim() && !a.getAttribute('aria-label') && !a.querySelector('img[alt]'))` in Console`
3. Add visible text, `aria-label`, or an inner `<img alt>` to each match

EXPECTED RESULT

Each link should expose a name through visible text, aria-label, or an image alt attribute.

ACTUAL RESULT

392 of 4,319 links across 49 pages lack an accessible name.

BUG-016 API responses missing Content-Type header

MEDIUM P2 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in DevTools → Network
2. Inspect response headers for the listed endpoints
3. Confirm `Content-Type` is missing and add it server-side

EXPECTED RESULT

Every API response should include a Content-Type header.

ACTUAL RESULT

3 of 4 network requests on https://example-coffee-shop.com/ omit Content-Type header.

BUG-017 External link unreachable

MEDIUM P2 NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in a browser
2. Click the link to https://etbis.eticaret.gov.tr/sitedogrulama/1d8c05a8868b47f1a71d3cb6b7e27d79
3. Observe TypeError: fetch failed
4. Update the link target or remove the reference

EXPECTED RESULT

All outbound links should be reachable and return a successful response.

ACTUAL RESULT

https://etbis.eticaret.gov.tr/sitedogrulama/1d8c05a8868b47f1a71d3cb6b7e27d79 could not be reached.

BUG-018 Failed resource loading errors in console

MEDIUM P2 NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/kullanici/kaydol in Chrome DevTools → Console
2. Reload the page with the console open
3. Locate the matching error entry and follow the stack trace into the source
4. Fix the failing call or guard against the input that triggered it

EXPECTED RESULT

All resource requests should succeed (or fail gracefully with error handling).

ACTUAL RESULT

6 occurrences of "Failed to load resource: the server responded with a status of 401" across 3 pages. First observed on https://example-coffee-shop.com/kullanici/kaydol.

BUG-019 Form accepts empty submission

MEDIUM P2 NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Open https://example-coffee-shop.com/ in a browser
- 2. Find the form (action="https://example-coffee-shop.com/alisveris/ara", method=POST)
- 3. Reproduce the empty submit test scenario
- 4. Click the submit button and observe the form proceeds without challenge

EXPECTED RESULT

Client-side validation should prevent empty submissions.

ACTUAL RESULT

Empty form on https://example-coffee-shop.com/ submitted without triggering validation or error messages.

BUG-020 JavaScript console errors detected

MEDIUM P2 NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Open https://example-coffee-shop.com/kullanici/kaydol in Chrome DevTools → Console
- 2. Reload the page with the console open
- 3. Locate the matching error entry and follow the stack trace into the source
- 4. Fix the failing call or guard against the input that triggered it

EXPECTED RESULT

Pages should load without JavaScript console errors.

ACTUAL RESULT

12 occurrences of "%c%d font-size:0;color:transparent NaN" error across 3 pages. First observed on https://example-coffee-shop.com/kullanici/kaydol.

BUG-021 No offline or cached state

MEDIUM P2 NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Open https://example-coffee-shop.com/
- 2. Open DevTools → Network → toggle 'Offline'
- 3. Reload and observe what the user sees
- 4. Implement a service worker that caches the shell, or render an offline fallback page

EXPECTED RESULT

Offline navigation should show a cached page or branded offline screen.

ACTUAL RESULT

Offline navigation to https://example-coffee-shop.com/ shows a generic browser error: net::ERR_INTERNET_DISCONNECTED.

BUG-022 Heavy page weight and low lazy-load adoption degrade mobile performance

MEDIUM P2 NEW

https://example-coffee-shop.com/ (Mobile)

STEPS TO REPRODUCE

- 1. Open Chrome DevTools Network tab, reload https://example-coffee-shop.com/ — observe total transfer size around 4.8 MB.
- 2. Filter by Img — several images above 500 KB with no lazy-load attribute.
- 3. Throttle to Fast 3G and reload — significant render delay before page is usable.

EXPECTED RESULT

Page weight should target under 1.5 MB for e-commerce pages; all below-the-fold images should use loading='lazy'; individual images should be compressed and served in next-gen formats (WebP/AVIF).

ACTUAL RESULT

TS-PERF: / is 4.81 MB, /alisveris/urun/kenya-kirinyaga is 3.40 MB. TS-IMG: only 3 of 17 images use lazy loading; 4 images exceed 500 KB.

BUG-023 JavaScript URLs in links

MEDIUM P2 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Open https://example-coffee-shop.com/ → DevTools → Console
- 2. Run `[...document.querySelectorAll('a[href'])].filter(a => a.getAttribute('href').toLowerCase().startsWith('javascript:'))`
- 3. Replace each `javascript:` href with a button + script-file handler, or remove the link entirely

EXPECTED RESULT

Links should point to real URLs (http://, https://, mailto:, tel:, or #fragment), not javascript: strings.

ACTUAL RESULT

49 javascript: href values found across 49 pages. First observed on https://example-coffee-shop.com/.

BUG-024 Missing Content-Security-Policy header

MEDIUM P2 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. `curl -I 'https://example-coffee-shop.com/'`
- 2. Inspect the response headers — 'Content-Security-Policy' should be present
- 3. (Most security headers are configured at the web-server or CDN layer; check the deployment platform's docs.)

EXPECTED RESULT

Every page should include a Content-Security-Policy header that restricts script sources.

ACTUAL RESULT

Content-Security-Policy header is not set. This was checked on 2 sample pages.

BUG-025 No cookie consent banner detected

MEDIUM

P2

• NEW

https://example-coffee-shop.com (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in a private window (no prior session)
2. Verify whether a consent banner appears
3. If only after-JS, consider server-side rendering it so static crawlers / accessibility tools see it

EXPECTED RESULT

A cookie or consent banner should be visible or loadable on the first page visit.

ACTUAL RESULT

Homepage HTML response did not contain common consent-banner indicators.

BUG-026 Server software details publicly visible

MEDIUM

P2

• NEW

https://example-coffee-shop.com (Desktop + Mobile)

STEPS TO REPRODUCE

1. curl -I 'https://example-coffee-shop.com/'
2. Confirm the X-Powered-By response header is present and discloses the software
3. Configure the server / reverse proxy to remove or anonymize the header

EXPECTED RESULT

Server software version should not be disclosed in response headers.

ACTUAL RESULT

X-Powered-By header reveals: PHP/8.4.21, PleskLin

BUG-027 Text inputs without character limits

MEDIUM

P2

• NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in DevTools → Elements
2. Inspect each form input and check for the `maxlength` attribute
3. Add `maxlength` matching the longest legitimate value (or the column width in the database)

EXPECTED RESULT

Text inputs, email fields, and text areas should declare a sensible maxlength.

ACTUAL RESULT

All 117 text inputs across 49 pages omit maxlength. First observed on https://example-coffee-shop.com/.

BUG-028 Third-party cookies set on page load

MEDIUM

P2

• NEW

https://example-coffee-shop.com (Desktop + Mobile)

STEPS TO REPRODUCE

1. curl -I 'https://example-coffee-shop.com/'
2. Inspect Set-Cookie Domain= values
3. Move tracking to first-party (server-side proxy) or implement consent gating

EXPECTED RESULT

Cookies should use first-party domains (or no Domain attribute).

ACTUAL RESULT

2 third-party cookies detected: XSRF-TOKEN@example-coffee-shop.com, example coffee shop_session@example-coffee-shop.com.

BUG-029 Missing page title

MEDIUM P2 • NEW

https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Open https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf in DevTools → Elements tab
- 2. Inspect ``<head>`` and confirm no ``<title>`` (or an empty one) is present
- 3. Add a descriptive ``<title>`` to the page template

EXPECTED RESULT

Every page should have a `<title>` element with meaningful content.

ACTUAL RESULT

1 of 50 crawled pages has an empty or missing `<title>` element.

BUG-030 Missing SEO metadata

MEDIUM P2 • NEW

https://example-coffee-shop.com/abonelikler (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Open https://example-coffee-shop.com/abonelikler → View source
- 2. Search for ``<meta name="description">`` and confirm it is absent
- 3. Add a 50–160 character description in the page template

EXPECTED RESULT

Every page should include a `<meta name="description" content="...">` tag.

ACTUAL RESULT

32 of 50 crawled pages have no meta description.

BUG-031 **Unbranded 403 responses replace expected 404 handling for unknown URLs**

MEDIUM **P2** **NEW**

`https://example-coffee-shop.com/page-not-found` (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Visit `https://example-coffee-shop.com/this-page-does-not-exist` in a browser.
- 2. Observe a bare, unbranded 403 Forbidden response with no navigation.
- 3. Confirm with `curl -I https://example-coffee-shop.com/nonexistent` — HTTP/1.1 403.

EXPECTED RESULT

Requests for non-existent pages should return a friendly branded 404 page with navigation options, helping users recover and reducing bounce rate.

ACTUAL RESULT

TS-ERR: GET /page-not-found returns HTTP 403 (not branded) and GET /aaaa... (500-char) also returns HTTP 403 (not branded), in 0.36 s and 0.20 s respectively.

BUG-032 **Inconsistent heading structure**

LOW **P3** **NEW**

`https://example-coffee-shop.com/alisveris/kategori/rare` (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. Open `https://example-coffee-shop.com/alisveris/kategori/rare` in DevTools
- 2. Run ``[...document.querySelectorAll('h1,h2,h3,h4,h5,h6')].map(h => h.tagName)`` in Console
- 3. Confirm at least one adjacent pair skips a level (e.g. H1 followed by H3)
- 4. Rebalance: demote skipped levels or insert the missing intermediate heading

EXPECTED RESULT

Heading levels should descend in order (`<h1>` → `<h2>` → `<h3>`, and so on).

ACTUAL RESULT

1 of 50 crawled pages has at least one skipped heading level.

BUG-033 Carousel library error in console

LOW

P3

• NEW

`https://example-coffee-shop.com/abonelikler` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/abonelikler` in Chrome DevTools → Console
2. Reload the page with the console open
3. Locate the matching error entry and follow the stack trace into the source
4. Fix the failing call or guard against the input that triggered it

EXPECTED RESULT

JavaScript libraries should initialize without errors.

ACTUAL RESULT

4 occurrences of "Bad element for Flickity: .magaza-carousel" across 2 pages. First observed on `https://example-coffee-shop.com/abonelikler`.

BUG-034 Carousel library null reference error

LOW

P3

• NEW

`https://example-coffee-shop.com/abonelikler` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/abonelikler` in Chrome DevTools → Console
2. Reload the page with the console open
3. Locate the matching error entry and follow the stack trace into the source
4. Fix the failing call or guard against the input that triggered it

EXPECTED RESULT

JavaScript libraries should initialize without errors.

ACTUAL RESULT

4 occurrences of "Bad element for Flickity: null" across 2 pages. First observed on `https://example-coffee-shop.com/abonelikler`.

BUG-035 No offline support (service worker not registered)

LOW

P3

NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ → DevTools → Application → Service workers
2. Confirm no service worker is registered
3. (Optional) Register a service worker to enable offline caching and faster repeat loads

EXPECTED RESULT

A service worker should be registered to support offline access.

ACTUAL RESULT

No service worker registrations detected on https://example-coffee-shop.com/.

BUG-036 Heavy page weight (4.81 MB)

LOW

P3

NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in Chrome DevTools → Lighthouse → Performance
2. Run an audit and confirm the Weight metric exceeds the "good" threshold
3. Compare against ≤3 MB good · ≤5 MB needs improvement thresholds (Google Core Web Vitals)

EXPECTED RESULT

Page weight should be ≤3 MB (good) or ≤5 MB (acceptable).

ACTUAL RESULT

Homepage transfers 4.81 MB (verdict: needs improvement). Measured under standard network conditions.

BUG-037 Images not using native lazy-loading

LOW P3 • NEW

https://example-coffee-shop.com (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. curl -s 'https://example-coffee-shop.com/' | grep -oE '<img[^>]*>' | head -20
- 2. Confirm the image tags carry no `loading="lazy"` attribute
- 3. Add the attribute to each `<img>` below the fold

EXPECTED RESULT

Most images below the fold should use the loading="lazy" attribute.

ACTUAL RESULT

3 of 17 images on the homepage use loading="lazy" (18%).

BUG-038 Oversized image (532 KB)

LOW P3 • NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

- 1. curl -sI 'https://example-coffee-shop.com/storage/slider/2026/04/slider-sahibi-degil-parcasi-br-oldugumuz-doga-07.jpeg'
- 2. Inspect the `Content-Length` response header
- 3. Re-encode or resize the image asset, then re-deploy

EXPECTED RESULT

Images should be under 500 KB.

ACTUAL RESULT

https://example-coffee-shop.com/storage/slider/2026/04/slider-sahibi-degil-parcasi-br-oldugumuz-doga-07.jpeg is 532 KB.

BUG-039 Forms lack duplicate-submission prevention

LOW

P3

• NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/
2. Inspect the hidden inputs on a mutating form
3. Confirm no idempotency_key / request_id / nonce is present
4. Wire the framework's idempotency helper into the form template

EXPECTED RESULT

Each form that changes data should include a hidden idempotency token (e.g., idempotency_key, request_id, or nonce).

ACTUAL RESULT

All 117 mutating forms across 49 pages lack an idempotency token.

BUG-040 Forms may lack cross-site forgery protection

LOW

P3

• NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ → DevTools → Elements
2. Confirm the form has no hidden CSRF token AND no other defense (check the session cookie's SameSite attribute and any CSRF <meta> tag / request header)
3. If genuinely unprotected, add a CSRF token or set SameSite=Lax/Strict on the session cookie

EXPECTED RESULT

Each form that changes data should be protected by a CSRF token (hidden field), a SameSite-restricted cookie, or a header-based token.

ACTUAL RESULT

All 117 mutating forms across 49 pages show no hidden CSRF token field. Other protections (SameSite cookie, custom header) cannot be detected by this scanner.

BUG-041 Inline event handlers in HTML

LOW

P3

NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ → DevTools → Elements
2. Run `document.querySelectorAll('[onclick],[onload],[onerror],[onmouseover]')` in Console
3. Replace each inline handler with an `addEventListener` call in a script file

EXPECTED RESULT

Event handlers should be wired through JavaScript `addEventListener()`, not inline `on*` attributes.

ACTUAL RESULT

392 inline event-handler attributes found across 49 pages. First observed on https://example-coffee-shop.com/.

BUG-042 Login endpoint shows no rate-limit protection signal

LOW

P3

NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. `curl -X OPTIONS 'https://example-coffee-shop.com/kullanici/kaydol' -i`
2. Inspect response headers for `Retry-After` / `X-RateLimit-*`
3. Wire a rate limiter on the auth endpoint (CDN / edge / framework)

EXPECTED RESULT

Login endpoint should include `Retry-After` or `X-RateLimit-*` headers to signal rate-limit protection.

ACTUAL RESULT

`OPTIONS` request to https://example-coffee-shop.com/kullanici/kaydol returned HTTP 200 with no rate-limit headers.

BUG-043 No 'remember me' option on login

LOW

P3

NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/kullanici/kaydol
2. Scan the login form for a checkbox
3. Add a 'Remember me' checkbox that the server interprets as a long-lived session

EXPECTED RESULT

Login form should offer a 'Remember me' checkbox.

ACTUAL RESULT

No 'Remember me' checkbox found on the login form.

BUG-044 No password reset link on login page

LOW

P3

NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/kullanici/kaydol
2. Scan visible link text near the login form
3. Add a 'Forgot password?' link that initiates the reset flow

EXPECTED RESULT

Login page should include a password-reset link.

ACTUAL RESULT

No password-reset link found on the login page.

BUG-045 No password visibility toggle

LOW

P3

• NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/kullanici/kaydol
2. Locate the password input
3. Add a sibling button that toggles the input type

EXPECTED RESULT

Login form should have a button to toggle password visibility.

ACTUAL RESULT

No password visibility toggle found near the password field.

BUG-046 No rate-limiting visible on homepage

LOW

P3

• NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Fire 20 parallel GET https://example-coffee-shop.com/
2. Inspect each response status + headers for 429 / X-RateLimit-* / Retry-After
3. Add rate limiting at the CDN / edge / framework layer

EXPECTED RESULT

Server should send rate-limit signals (429 responses or X-RateLimit-* / Retry-After headers) under heavy load.

ACTUAL RESULT

20 parallel requests to the homepage all succeeded with no 429 response or rate-limit header.

BUG-047 Password field missing autocomplete attribute

LOW

P3

• NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/kullanici/kaydol
2. Inspect the password input
3. Add `autocomplete="current-password"` (login) or `new-password` (signup)

EXPECTED RESULT

Password input should have autocomplete="current-password" attribute.

ACTUAL RESULT

The password input is missing the autocomplete attribute.

BUG-048 Password field missing maxlength attribute

LOW

P3

• NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/kullanici/kaydol
2. Inspect the password input
3. Add a `maxlength` matching the server's accepted password length

EXPECTED RESULT

Password input should have a maxlength attribute (e.g., maxlength="128").

ACTUAL RESULT

The password input is missing maxlength.

BUG-049 Potential CSRF gap on state-changing forms (unverified)

LOW

P3

NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open an affected page → DevTools → Elements / Network
2. Check the form's hidden inputs, the session cookie's SameSite attribute, and any CSRF <meta> tag / request header
3. If genuinely none are present, add a CSRF token or set SameSite=Lax/Strict on the session cookie

EXPECTED RESULT

Each state-changing form is protected by at least one CSRF defense — a hidden token, a SameSite=Lax/Strict session cookie, or a header / meta token (only the hidden token is visible to an external scan).

ACTUAL RESULT

No hidden CSRF token field was found in the form markup. SameSite / header / meta defenses are not externally observable, so protection status is unverified.

BUG-050 Username field missing autocomplete attribute

LOW

P3

NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/kullanici/kaydol
2. Inspect the username / email input
3. Add `autocomplete="username"` (or `"email"`)

EXPECTED RESULT

Username/email input should have autocomplete="username" or "email" attribute.

ACTUAL RESULT

The username input is missing the autocomplete attribute.

BUG-051 Content clipped at desktop viewport (1440px)

LOW

P3

NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ and resize the browser to 1440×900
2. Inspect the first offender element and verify its computed `overflow` is `hidden`
3. Compare `scrollWidth` vs `clientWidth` in DevTools → Properties tab
4. Replace `overflow: hidden` with a wrapping rule, or add `text-overflow: ellipsis`

EXPECTED RESULT

Content should fit the desktop viewport or be truncated with an ellipsis.

ACTUAL RESULT

1 element clips content at 1440px width. Example: div.flickity-viewport (1440px container → 5760px content).

BUG-052 Content clipped at mobile viewport (375px)

LOW

P3

NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ and resize the browser to 375×812
2. Inspect the first offender element and verify its computed `overflow` is `hidden`
3. Compare `scrollWidth` vs `clientWidth` in DevTools → Properties tab
4. Replace `overflow: hidden` with a wrapping rule, or add `text-overflow: ellipsis`

EXPECTED RESULT

Content should fit the mobile viewport, or be truncated with an ellipsis indicator.

ACTUAL RESULT

1 element clips content at 375px width. Example: div.flickity-viewport (375px container → 1500px content).

BUG-053 Content clipped at tablet viewport (768px)

LOW

P3

NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ and resize the browser to 768×1024
2. Inspect the first offender element and verify its computed `overflow` is `hidden`
3. Compare `scrollWidth` vs `clientWidth` in DevTools → Properties tab
4. Replace `overflow: hidden` with a wrapping rule, or add `text-overflow: ellipsis`

EXPECTED RESULT

Content should fit the tablet viewport or be truncated with an ellipsis.

ACTUAL RESULT

1 element clips content at 768px width. Example: div.flickity-viewport (768px container → 3072px content).

BUG-054 Missing main heading

LOW

P3

NEW

https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/pdf/kvkk_basvuru.pdf in DevTools
2. Search the DOM for `h1` elements
3. Confirm none are present
4. Add a single, descriptive `

` to the page template

EXPECTED RESULT

Each page should have exactly one `<h1>` element.

ACTUAL RESULT

1 of 50 crawled pages has no `<h1>` element.

BUG-055 Page titles too short for search results

LOW

P3

• NEW

`https://example-coffee-shop.com/` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/` in DevTools → Elements
2. Inspect the `<title>` element
3. Confirm the text is 9 characters (target 10–60)
4. Rewrite the title to fit the 10–60 character window

EXPECTED RESULT

Page titles should be between 10 and 60 characters.

ACTUAL RESULT

37 of 50 pages have titles that are too short (0 too long, 37 too short). First example: `https://example-coffee-shop.com/` (9 characters).

BUG-056 Registration form lacks password strength indicator

LOW

P3

• NEW

`https://example-coffee-shop.com/kullanici/kaydol` (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open `https://example-coffee-shop.com/kullanici/kaydol`
2. Inspect the password input's neighborhood
3. Add a strength meter or live rule list

EXPECTED RESULT

Registration form should show a password strength meter or rule list.

ACTUAL RESULT

No password strength meter or rule list detected on the registration form.

BUG-057 Registration form missing terms acceptance checkbox

LOW

P3

NEW

https://example-coffee-shop.com/kullanici/kaydol (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/kullanici/kaydol
2. Inspect the registration form's checkboxes
3. Add a required terms / privacy acceptance checkbox

EXPECTED RESULT

Registration form should include a required checkbox for terms/privacy acceptance.

ACTUAL RESULT

No terms, privacy, or consent checkbox found on the registration form.

BUG-058 Sitemap not found

LOW

P3

NEW

https://example-coffee-shop.com/sitemap.xml (Desktop + Mobile)

STEPS TO REPRODUCE

1. curl -I 'https://example-coffee-shop.com/sitemap.xml'
2. Confirm the response is not 2xx
3. Generate a sitemap (most frameworks ship a sitemap generator) and serve it at /sitemap.xml

EXPECTED RESULT

GET /sitemap.xml should return HTTP 200 with a valid XML sitemap.

ACTUAL RESULT

GET https://example-coffee-shop.com/sitemap.xml returned HTTP 404.

BUG-059 Undersized touch targets on mobile

LOW

P3

NEW

https://example-coffee-shop.com/ (Desktop + Mobile)

STEPS TO REPRODUCE

1. Open https://example-coffee-shop.com/ in Chrome DevTools at device width 375px
2. Highlight each interactive element in turn and check its bounding-box dimensions
3. Increase padding so the bounding box is $\geq 44 \times 44$ px

EXPECTED RESULT

All interactive elements should be at least 44×44 pixels at mobile viewports.

ACTUAL RESULT

31 of 45 interactive elements are below 44px at 375×812 . Examples: buttons 22×24 px, link 328×24 px.

6 Highest-Priority Findings

Auto-generated from severity ranking. Manual review recommended.

The top critical and high-severity findings, in priority order. See the Detailed Bug Reports section for full reproduction steps.

1. **BUG-001** — Color contrast failures (site-wide)
2. **BUG-002** — Form input missing accessible label
3. **BUG-003** — Pervasive missing accessible names on interactive elements site-wide
4. **BUG-004** — Internal link unreachable
5. **BUG-005** — Legal compliance failure: no cookie consent and broken KVKK document
6. **BUG-006** — Cookie missing HttpOnly flag
7. **BUG-007** — HTTP requests are not redirected to HTTPS

7 Recommended Fix Order

Auto-generated from severity ranking. Manual review recommended.

Suggested remediation order. Engineering should validate the sequence against business priorities and dependency relationships before scheduling.

- 1 1. Implement CSRF tokens on all 117 state-mutating forms (including login, registration, and checkout) and mark the XSRF-TOKEN cookie HttpOnly — these two gaps share the same root cause (missing anti-forgery layer) and together represent the highest-risk exploitable vulnerability.
- 2 2. Add a compliant KVKK/GDPR cookie consent banner that blocks third-party cookies until explicit user consent is given — the absence of this creates direct regulatory liability.
- 3 3. Fix the broken internal link to /pdf/kvkk_basvuru.pdf by uploading the correct file or correcting the URL — this is both a legal-document accessibility failure and a broken user journey on a compliance page.
- 4 4. Add a Content-Security-Policy header at the server or CDN/edge layer to restrict script execution sources and mitigate XSS risk; simultaneously remove all 49 javascript: href links and replace with proper button or event-listener patterns.
- 5 5. Assign unique, descriptive <title> tags and meta descriptions to all 50 pages (37 titles are too short or duplicate, 32 pages lack meta descriptions entirely) — this is a single templating fix that will substantially improve SEO and click-through rates.
- 6 6. Audit and label all 215 unnamed buttons and 392 unnamed links with accessible names (aria-label or visible text) and fix colour contrast failures on the homepage, contact, and product pages to meet WCAG 2.1 AA — a single design-system pass can resolve most instances.
- 7 7. Suppress or rotate the X-Powered-By header (PHP/8.4.21, PleskLin) to stop disclosing server stack details to potential attackers.
- 8 8. Optimise page weight by lazy-loading the remaining 82% of images without the attribute and compressing the 4 images over 500 KB — targeting the homepage's 4.81 MB payload will most directly improve Core Web Vitals and mobile conversion.
- 9 9. Add rate limiting on the login endpoint and implement client-side idempotency tokens on order/checkout forms to prevent credential stuffing and accidental duplicate orders.
- 10 10. Fix the 403 unbranded error responses for unknown URLs — replace with a friendly branded 404 page that keeps users on-site and provides navigation options.

8 Recommended Manual Test Scenarios

Manual test scenarios recommended by the AI analyzer based on the crawled site structure. Hand this list to your QA team for execution — each scenario covers something the automation cannot verify on its own.

Happy Path (5)

TC-001 Register a new account with valid credentials

HAPPY-PATH

HIGH

PRECONDITION

User is not registered and is on the /kullanici/kaydol page.

STEPS

1. Enter a first name in the 'ad' field
2. Enter a last name in the 'soyad' field
3. Enter a valid email address in the 'email' field
4. Enter a password of at least 8 characters in the 'password' field
5. Confirm the password in the 'password_confirm' field
6. Check the 'kvkk' (KVKK agreement) checkbox
7. Click the 'Kayıt Ol' button

EXPECTED RESULT

Account is created successfully and user is redirected to the dashboard or home page.

TC-002 Search for a product using the search form

HAPPY-PATH

HIGH

PRECONDITION

User is on any page with the search form visible.

STEPS

1. Locate the search form with 'arama' text field
2. Enter a product name (e.g., 'kahve') in the 'arama' field
3. Click the 'Bul' button

EXPECTED RESULT

Search results page displays products matching the search term.

TC-003 Add a coffee subscription to cart with variant selection

HAPPY-PATH

HIGH

PRECONDITION

User is on the product page /alisveris/urun/kahve-abonelligi and is not logged in.

STEPS

1. Select a value from the 'ay' (month) dropdown
2. Select a value from the 'hafta' (week) dropdown
3. Select at least one checkbox variant option from product_variant_group_id[1]
4. Click the 'Sepete Ekle' button

EXPECTED RESULT

Product is added to cart and cart counter increases. Success notification appears.

TC-004 Subscribe to newsletter with valid email

HAPPY-PATH

MEDIUM

PRECONDITION

User is on any page with the newsletter form visible.

STEPS

1. Locate the newsletter form with 'email' field
2. Enter a valid email address
3. Click the 'Abone Ol' button

EXPECTED RESULT

Newsletter subscription is confirmed and a success message appears.

TC-005 Verify product category navigation flow

HAPPY-PATH

MEDIUM

PRECONDITION

User is on the home page /

STEPS

1. Click the 'Kahveler' category link
2. Verify page loads with coffee products
3. Click the 'Ekipmanlar' category link
4. Verify page loads with equipment products

EXPECTED RESULT

Each category page loads correctly and displays products in that category.

Negative Cases (9)

TC-006 Register with mismatched password confirmation

NEGATIVE

HIGH

PRECONDITION

User is on the /kullanici/kaydol page.

STEPS

1. Enter a first name
2. Enter a last name
3. Enter a valid email
4. Enter a password in the 'password' field
5. Enter a different value in the 'password_confirm' field
6. Check the 'kvkk' checkbox
7. Click the 'Kayıt Ol' button

EXPECTED RESULT

Form submission fails with an error message indicating passwords do not match.

TC-007 Register without checking KVKK agreement

NEGATIVE

HIGH

PRECONDITION

User is on the /kullanici/kaydol page.

STEPS

1. Enter a first name
2. Enter a last name
3. Enter a valid email
4. Enter a matching password pair
5. Leave the 'kvkk' checkbox unchecked
6. Click the 'Kayıt Ol' button

EXPECTED RESULT

Form submission fails with an error message requiring KVKK agreement.

TC-008 Search with empty search field

NEGATIVE

MEDIUM

PRECONDITION

User is on any page with the search form.

STEPS

1. Leave the 'arama' field empty
2. Click the 'Bul' button

EXPECTED RESULT

Form submission either fails with a validation error or displays all products without filtering.

TC-009 Add product to cart without selecting required variant

NEGATIVE

HIGH

PRECONDITION

User is on a product page with variant selection (e.g., /alisveris/urun/cezve).

STEPS

1. Do not select any value from the variant dropdown (product_variant_group_id[5])
2. Enter a quantity in the 'adet' field
3. Click the 'Sepete Ekle' button

EXPECTED RESULT

Form submission fails with a validation error indicating variant selection is required.

TC-010 Add subscription product without selecting month or week

NEGATIVE

HIGH

PRECONDITION

User is on the subscription product page /alisveris/urun/kahve-aboneli.

STEPS

1. Do not select a value from the 'ay' dropdown
2. Do not select a value from the 'hafta' dropdown
3. Select a variant checkbox
4. Click 'Sepete Ekle'

EXPECTED RESULT

Form submission fails with validation errors for missing month and week selections.

TC-011 Subscribe to newsletter with invalid email format

NEGATIVE

MEDIUM

PRECONDITION

User is on any page with the newsletter form.

STEPS

1. Enter an invalid email (e.g., 'notanemail') in the 'email' field
2. Click 'Abone Ol'

EXPECTED RESULT

Form submission fails with a validation error for invalid email format.

TC-012 Attempt to add product without quantity value

NEGATIVE

MEDIUM

PRECONDITION

User is on a non-subscription product page with quantity field (e.g., /alisveris/urun/cezve).

STEPS

1. Select a variant from the dropdown
2. Leave the 'adet' (quantity) field empty
3. Click 'Sepete Ekle'

EXPECTED RESULT

Form submission fails with validation error for missing or invalid quantity.

TC-013 Register with email that already exists

NEGATIVE

HIGH

PRECONDITION

User is on the /kullanici/kaydol page and an account with test@example.com already exists.

STEPS

1. Enter a first name
2. Enter a last name
3. Enter an email address that already has a registered account (test@example.com)
4. Enter a matching password pair
5. Check the 'kvkk' checkbox
6. Click 'Kayıt Ol'

EXPECTED RESULT

Form submission fails with an error message indicating email is already registered.

TC-014 Add zero or negative quantity to cart

NEGATIVE

MEDIUM

PRECONDITION

User is on a product page with quantity number field.

STEPS

1. Select a variant if required
2. Enter '0' in the 'adet' (quantity) field
3. Click 'Sepete Ekle'

EXPECTED RESULT

Form submission fails with validation error or quantity is rejected as invalid.

Edge Cases (3)

TC-015 Register with extremely long first name (250+ characters)

EDGE-CASE

MEDIUM

PRECONDITION

User is on the /kullanici/kaydol page.

STEPS

1. Enter a string of 300+ characters in the 'ad' field
2. Enter a valid last name
3. Enter a valid email
4. Enter a matching password pair
5. Check the 'kvkk' checkbox
6. Click 'Kayıt Ol'

EXPECTED RESULT

Form submission either fails with length validation error or text is truncated appropriately.

TC-016 Search with special characters and Unicode in query

EDGE-CASE

MEDIUM

PRECONDITION

User is on any page with the search form.

STEPS

1. Enter special characters and Unicode (e.g., '(kahve)@#\$€Ñ') in the 'arama' field
2. Click 'Bul'

EXPECTED RESULT

Search processes without errors and returns appropriate results or empty set.

TC-017 Submit newsletter form twice rapidly (duplicate submission)

EDGE-CASE

MEDIUM

PRECONDITION

User is on any page with the newsletter form.

STEPS

1. Enter a valid email address in the 'email' field
2. Click 'Abone Ol' button
3. Immediately click 'Abone Ol' button again before page response

EXPECTED RESULT

Only one subscription is recorded; second submission is prevented or ignored.

Security (2)

TC-018 Register with XSS payload in email field

SECURITY

HIGH

PRECONDITION

User is on the /kullanici/kaydol page.

STEPS

1. Enter a first name
2. Enter a last name
3. Enter a potential XSS payload in email field (e.g., '<script>alert(1)</script>@test.com')
4. Enter a matching password pair
5. Check the 'kvkk' checkbox
6. Click 'Kayıt Ol'

EXPECTED RESULT

Input is either rejected as invalid email format or safely escaped; no script executes.

TC-019 Search with SQL injection-shaped payload

SECURITY

HIGH

PRECONDITION

User is on any page with the search form.

STEPS

1. Enter SQL injection attempt in 'arama' field (e.g., '"; DROP TABLE products; --")
2. Click 'Bul'

EXPECTED RESULT

Payload is treated as a literal search string; no database modification occurs.

UX & Responsive (1)

TC-020 Navigate category links and verify cart counter persists

UX

MEDIUM

PRECONDITION

User has added a product to cart and cart counter shows '1'.

STEPS

1. Click the 'Kahveler' category link
2. Verify cart counter still displays '1'
3. Click the 'Aksesuar' category link
4. Verify cart counter still displays '1'
5. Click 'Online Dükkan' to return to main shop

EXPECTED RESULT

Cart counter persists across all page navigations and displays the correct item count.

9 Summary & Observations

TESTING OUTCOME — AUTOMATED SCAN

Critical and high-severity findings cluster around functional / security issues — recommend an engineering triage session before scheduling remediation.

An automated scan can only validate what it can statically observe (DOM, console, load timing).

Recommend a manual review of business-critical flows (auth, payment, data submission) before sign-off.

REPORT GENERATED BY QA EXPLORER — CONFIDENTIAL