lemonade
Beyond Clicks

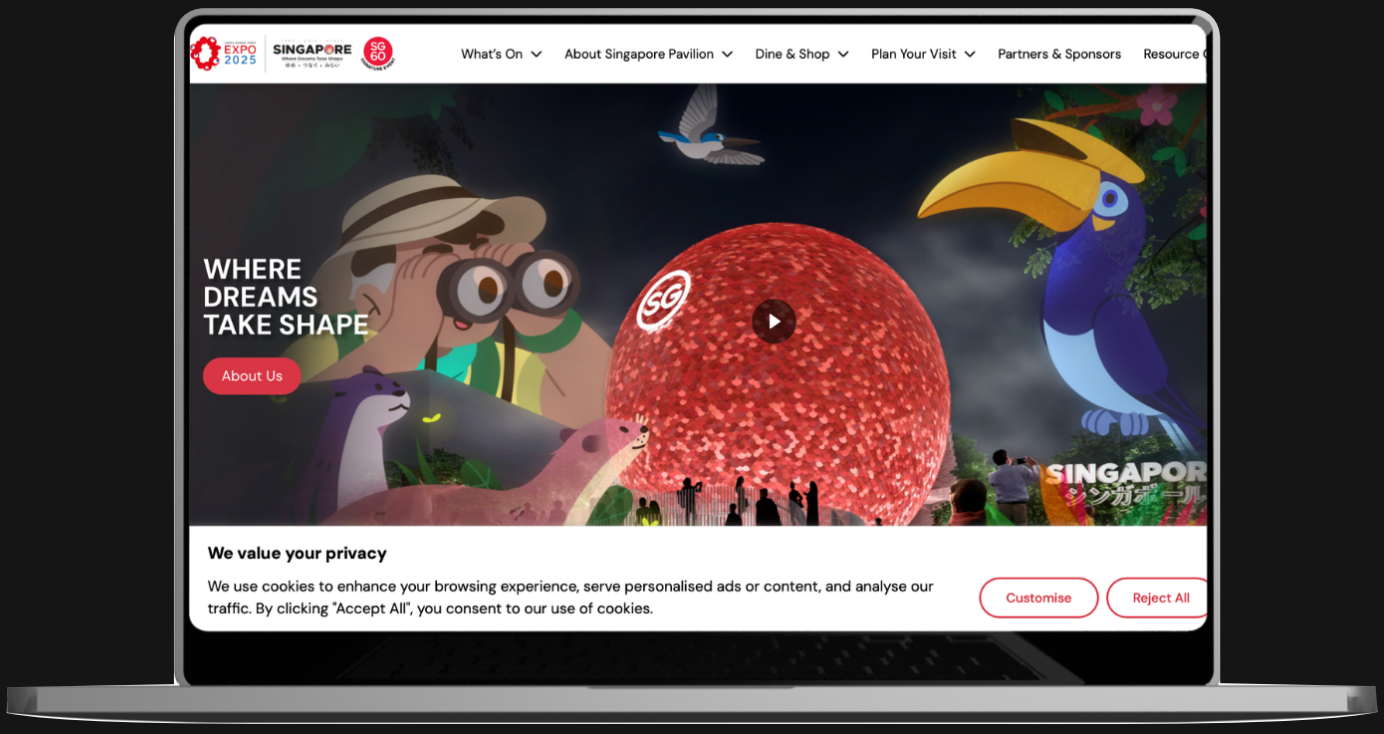
EXPO 2025 SINGAPORE PAVILION

Singapore Pavilion at World Expo 2025

Agency partnership case study
Website development, security coordination and ongoing support.

THE PARTNERSHIP

Kingsmen led the project and client relationship. Lemonade worked with its creative director and team to develop the website, refine its mobile experience, manage hosting and support security reviews and live operations.



01 / OUR ROLE

A website partner within the agency team.

A clear division of responsibility, built on an existing working relationship.

AN EXISTING WORKING RELATIONSHIP

Kingsmen approached Lemonade after working with us on website needs and internal microsites. We joined the Singapore Pavilion website project as the technical delivery partner, working alongside the creative director and team.

A PRACTICAL DIVISION OF RESPONSIBILITY

Kingsmen led the overall project and client relationship. Lemonade contributed development, mobile design input, hosting, security coordination and website support. The diagram below shows how the teams worked together.

RESPONDING TO URGENT CHANGES

As requests changed, we used focused development sprints and met directly with designers and compliance stakeholders. During hypercare, we also handled last-minute content changes.

KINGSMEN

- Project leadership
- Client relationship
- Creative director and team

LEMONADE

- Website development
- Hosting and maintenance
- Security coordination and support

WORKING TOGETHER

Design decisions | Security requirements | Urgent website changes

Agency leadership supported by a specialist website delivery team.

Kingsmen led the project and client relationship; Lemonade supported the website's technical delivery.

02 / TECHNICAL DELIVERY

Technical delivery beyond the interface.

The project portfolio describes three connected implementation workstreams.

CLOUD INFRASTRUCTURE & RESILIENCE

The portfolio describes a cloud cluster with automated load balancing and a CDN for traffic distribution, a mirrored backup server for automated failover, and Docker and Kubernetes hosting for the official event mobile application. These components were intended to support traffic handling and service continuity.

JAPANESE LOCALISATION & PERFORMANCE

The portfolio also records a Japanese-language version, server-side page caching, script minification and image optimisation. The intended benefit was to make the content accessible to Japanese readers and improve delivery across borders.

SECURITY & LIVE OPERATIONS

The portfolio describes a web application firewall and SSL/TLS protection alongside security review and event support. The supplied reports document an external black-box web application assessment and a separate vulnerability scan. Lemonade's delivery account covers security coordination, changes to site components and urgent content support.

Implementation scope: Lemonade project portfolio. Assessment method and results: supplied testing reports.

03 / DESIGN & DEVELOPMENT

Help the design work across screen sizes.

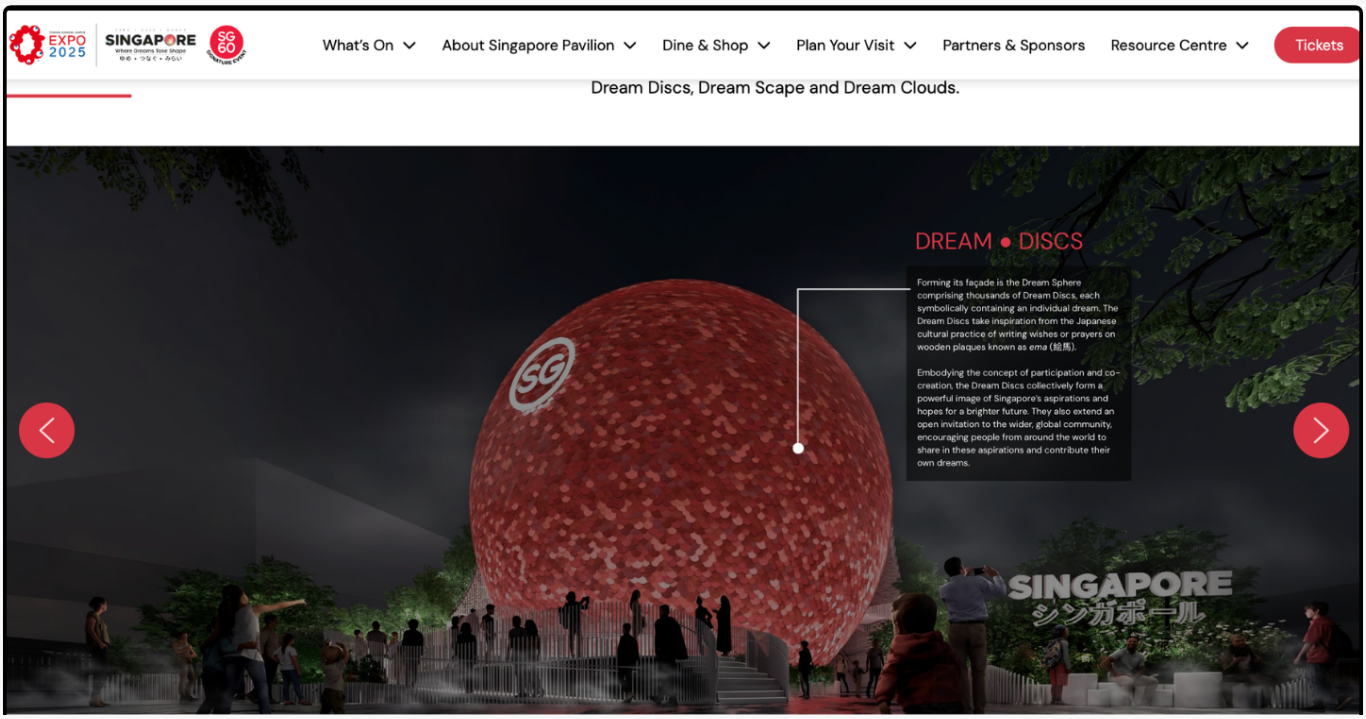
We contributed to design decisions as well as website development.

THE WORK

Our input covered usability and navigation, mobile responsiveness, technical feasibility, performance considerations and accessibility. One specific intervention was working with the agency team to revise the slider design for a more mobile-friendly experience.

THE REASON

A visual interaction needs to work within the space available on a phone. We collaborated with the designers on that adaptation as part of developing the site.



The pavilion feature combines imagery, explanatory content and slider controls.

Website screenshot: pavilion section. Mobile design collaboration is described in the project-owner account.

04 / SECURITY COORDINATION

Security testing, with practical follow-through.

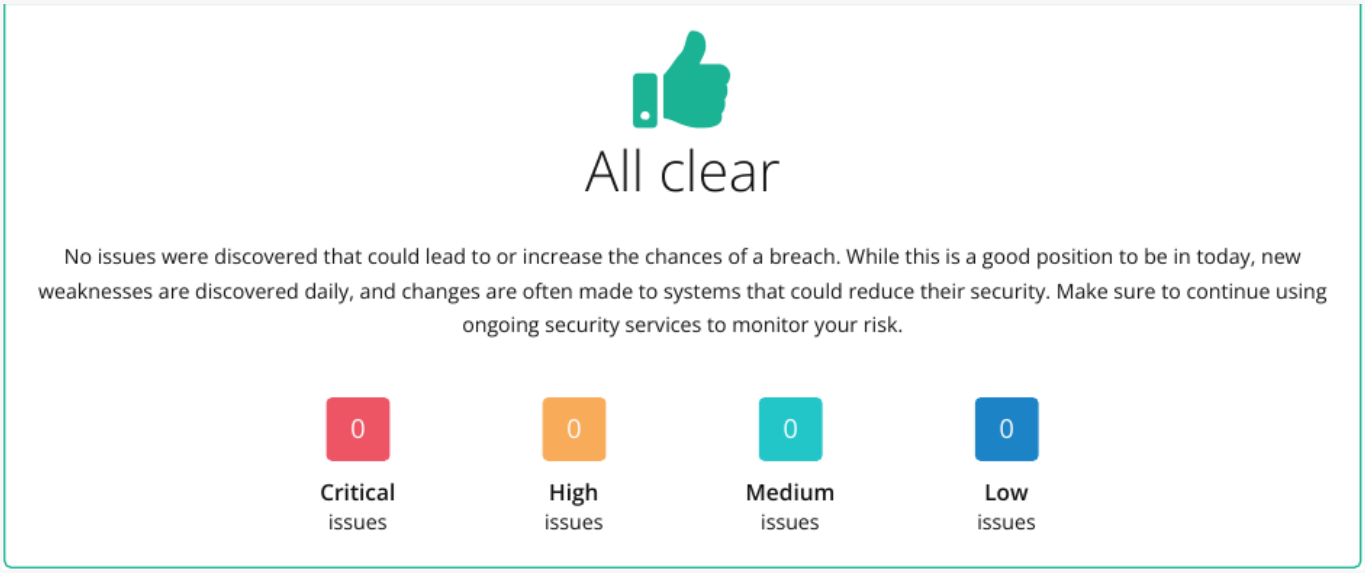
External black-box web application penetration testing and vulnerability scanning.

HOW THE WEBSITE WAS TESTED

The penetration test combined manual investigation and validation with automated tools. Its test criteria referenced OWASP Top 10 and SANS guidance. Our role included security coordination, changes to site components and discussions with designers and compliance stakeholders.

THE CHECKS COVERED

Recorded checks included injection; authentication and sessions; access control and password reset; sensitive data exposure; security configuration, TLS and security headers; cross-site scripting and clickjacking; vulnerable components; and logging and monitoring. The separate Intruder scan reported no issues within its scope.



Vulnerability scan result: no issues reported within the scan scope.

Sources: supplied penetration-test and vulnerability-scan reports. Test findings and scan results have distinct scopes.

05 / INSIDE THE PENETRATION TEST

See the checks behind the assessment.

Selected excerpts from the original test-criteria tables show what the assessment examined.

INJECTION CHECKS

WEBAPP PENETRATION TEST VALIDATION		
OWASP Test Criteria	**Performed**	**Vulnerable**
1. Injection		
Test for SQL Injection	YES	NO
Injection Attack: Bypassing Authentication	YES	NO
Test for LDAP Injection	YES	NO
Test for ORM Injection	YES	NO
Test for SSI Injection	YES	NO
Test for XPath Injection	YES	NO

Selected injection checks: SQL, authentication bypass, LDAP, ORM, SSI and XPath.

ACCESS CONTROL CHECKS

5. Broken Access Control		
Test for Missing Function Level Access Control	YES	NO
Test for Insecure Direct Object Reference	YES	NO
Test for Bypassing Authorization	YES	NO
Test for Access Control Issues	YES	YES
Test for Privilege Escalation	YES	NO
Test for Directory Traversal/File Include	YES	NO
Test for Weak Password Change or Reset Functionalities	YES	NO
Test for Vulnerable Remember Password	YES	NO
Test User Registration Process	YES	NO

Source: penetration-testing report, PDF pages 22-23. Table results describe the assessment, not a remediation retest.

06 / AUTHENTICATION & CONFIGURATION

Examine access. Check the configuration.

The assessment examined login protections, session behaviour and server security settings.

AUTHENTICATION & SESSION CHECKS

2. Broken Authentication and Session Management		
Brute Force Authentication	YES	NO
Test for Weak Lockout Mechanism	YES	NO
Bypassing Authentication	YES	NO
Hack Cookies and Manipulate Sessions	YES	NO
Test Token Generation	YES	NO

Checks included brute-force attempts, lockout behaviour, login bypass, cookies and token generation.

SECURITY CONFIGURATION & TLS

6. Security Misconfiguration		
Test for Security Misconfiguration Issues	YES	YES
Application Fingerprinting and Service Enumeration	YES	NO
Test HTTP Methods	YES	NO
Test Cross Origin Resource Sharing (CORS)	YES	NO
Test HTTP Strict Transport Security	YES	YES
Test SSL/TLS	YES	NO
Test File Extensions Handling for Sensitive Information	YES	NO
Enumerate Infrastructure and Application Admin Interfaces	YES	NO
Test for Error Code	YES	NO

Penetration-test excerpts, PDF pages 22-23. Columns: test criterion, performed, vulnerable. Original assessment results.

07 / BROWSER & AUTOMATED CHECKS

Review browser risks. Scan for known weaknesses.

Manual assessment was supported by a separate automated vulnerability scan.

CROSS-SITE SCRIPTING CHECKS

7. Cross-Site Scripting (XSS)		
Test for Reflected XSS	YES	NO
Test for Persistent XSS	YES	NO

Selected browser-side checks from the penetration-test table: reflected and persistent XSS.

AUTOMATED VULNERABILITY SCAN

Total checks	Targets	Issues discovered
19,105	1	0

The scanner recorded 19,105 automated checks on one target, with no issues returned by that scan. This count describes scanner checks, not manual penetration tests.

ENCRYPTION & MISCONFIGURATION COVERAGE

Encryption weaknesses

Weaknesses in SSL/TLS implementations, such as:

- 'Heartbleed', 'CRIME', 'BEAST' and 'ROBOT'
- Weak encryption ciphers & protocols
- SSL certificate misconfigurations
- Unencrypted services such as FTP

Common mistakes & misconfigurations

- VPN configuration weaknesses
- Exposed SVN/git repositories
- Unsupported operating systems
- Open mail relays
- DNS servers allowing zone transfer

The scanner report lists these examples of its check coverage.

Sources: penetration-testing report, PDF page 23; vulnerability-scan report, page 2. Results apply to their assessment scopes.

08 / HOSTING & LIVE SUPPORT

Keep a technical team behind the live website.

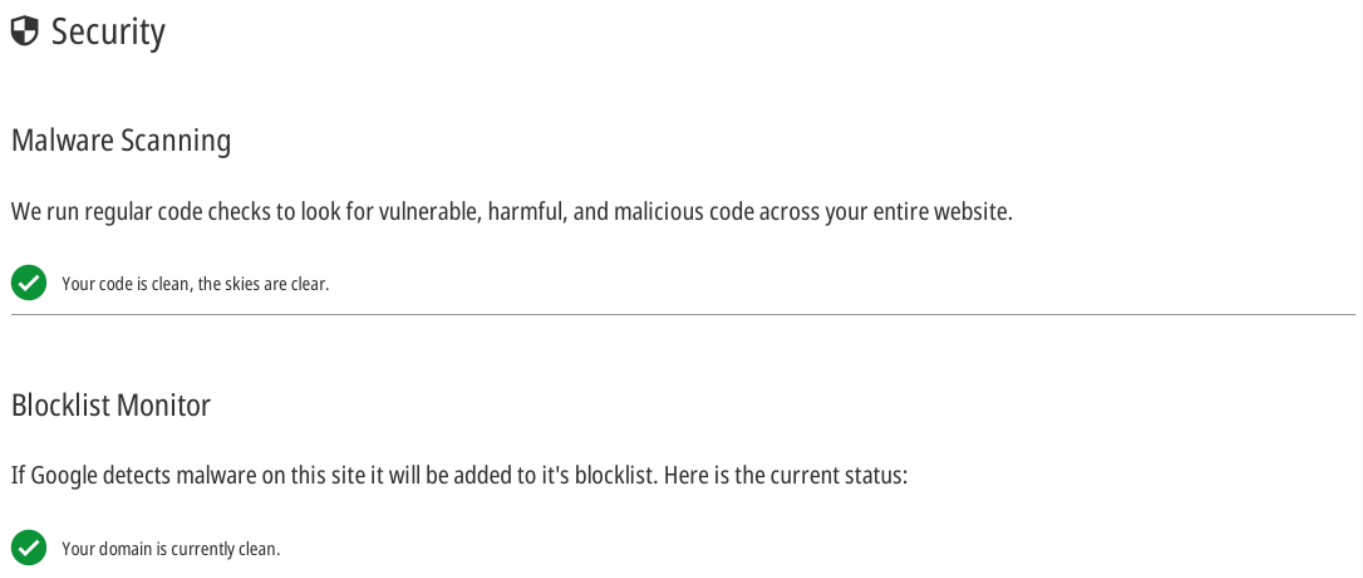
Our responsibilities extended beyond the initial build.

HOSTING, MONITORING AND SUPPORT

We managed hosting on a cloud server with a CDN and firewall. Our support responsibilities included uptime and traffic monitoring, security updates, server management, backups and recovery, and urgent technical support during hypercare.

ACTIVE WEBSITE CARE

Maintenance records show software version updates and clean malware and blocklist checks. This work formed part of our ongoing care for the website, alongside monitoring and technical support.



Malware and blocklist checks recorded as clean in the maintenance report.

MAINTENANCE IN ACTION

Recorded updates to the site theme and security, backup and optimisation tools.

Supporting evidence: security-check results and maintenance activity log.

09 / DOCUMENTED WEBSITE CARE

Website care. Visible results.

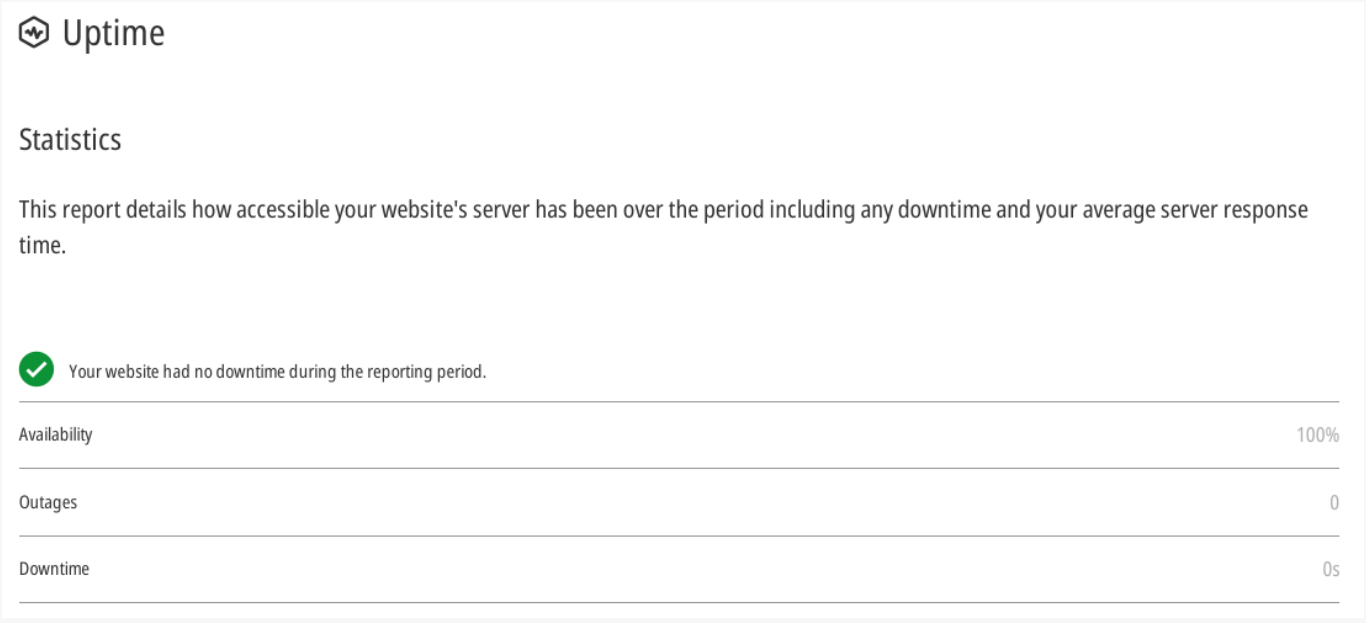
Monitoring and maintenance supported the website beyond development.

RECORDED AVAILABILITY

The maintenance report records 100% availability, zero outages and zero downtime during the monitored reporting period.

ONGOING TECHNICAL ATTENTION

The maintenance records show updates to the site theme and security, backup and optimisation tools. Together with malware and blocklist checks, these records demonstrate active care for the website.



Supporting evidence: maintenance report. Availability applies to the monitored reporting period.

lemonade
Beyond Clicks

10 / PARTNER EXPERIENCE

Confidence in the team behind the website.

The partner experience matters alongside the technical delivery.

WHAT THE PARTNERSHIP MEANT

Our role brought website development, security coordination, hosting and live support into the agency’s delivery team. The feedback shared in the project-owner interview highlights the reassurance, efficiency and responsiveness the team valued.

PARTNER FEEDBACK

> The team felt reassured working with Lemonade and valued our efficiency, responsiveness, and expertise in website development and enterprise website security.

Kingsmen team feedback, as recalled by Lemonade’s project owner. Paraphrased from the project interview.

PLAN YOUR NEXT EVENT WEBSITE WITH LEMONADE

Share your creative brief, launch milestone, security requirements and support window. We can discuss how to work alongside your agency.

lemonade-it.com

Partner feedback paraphrased from Lemonade’s project-owner interview.